TREND MICRO

OfficeScan™ Client/Server Edition 8

for Enterprise and Medium Business

Administrator's Guide

Endpoint Security

Document Part No. OSEM83042/70123

Release Date: May 2007

Protected by U.S. Patent No. 5,623,600; 5,889,943; 5,951,698; 6.119,165

The user documentation for Trend Micro OfficeScan introduces the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

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

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

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

Contents

Chapter 7: Managing OfficeScan Using Control Manager

List of Tables

Chapter 1

Introducing OfficeScan

Topics in this chapter:

About OfficeScan

Trend Micro™ OfficeScan™ protects enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks. As an integrated solution, it guards desktops, laptops, and network servers, while the Web-based management console makes it easy to set coordinated security policy and deploy automatic updates on every client and server.

By integrating with Trend Micro Network VirusWall™ or any Network Admission Control (NAC) device, OfficeScan can enforce policy on non-compliant computers, and then remedy, redirect, restrict, deny, or permit network access.

The chapter provides an overview of OfficeScan features, functionality, and technology.

New in this Release

OfficeScan includes the following new features and enhancements:

Antivirus

IntelliTrap

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of virus/malware entering your network by blocking files with real-time compressed executable files.

To enable IntelliTrap, go to **Networked Computers > Client Management > Settings > {Scan Type} > Virus/Malware** tab **> Scan Settings**.

GeneriClean

GeneriClean, also known as referential cleaning, is a new technology for cleaning viruses/malware even without the availability of virus cleanup components. Using a detected file as basis, GeneriClean determines if the detected file has a corresponding process/service in memory and a registry entry, and then removes them altogether.

Firewall

Logging allowed traffic

In addition to allowing or denying traffic based on firewall policies, OfficeScan clients can now log allowed traffic and, if granted the privilege, send these logs to the server. You can then audit allowed traffic coming from client

computers and identify possible malicious activity without disrupting client users.

Client firewall logs

You can allow certain clients to automatically send firewall logs to the server (in **Networked Computers > Client Management > Settings > Privileges and Other Settings**) and configure a schedule for sending the logs (**Networked Computers > Global Client Settings**).

Web Threat Protection

Web Reputation

In addition to file-based scanning, OfficeScan now includes the capability to detect and block Web-based security risks, including phishing attacks. See *Web Reputation Configuration* on page 2-36 for more information.

Configure Web Reputation settings by going to **Networked Computers > Web Reputation**.

Anti-spyware

OfficeScan comes with a new spyware scanning and cleanup engine that can detect and clean more spyware/grayware than ever before, with fewer false positives.

The product includes the following new features:

Real-time detection

Real-time spyware/grayware scanning for file system prevents or stops spyware execution.

Spyware/Grayware restore

After taking action on a spyware/grayware, OfficeScan clients back up spyware/grayware data, which the OfficeScan server can restore anytime if the spyware/grayware is deemed safe. You can choose spyware/grayware data segments to restore.

To restore spyware/grayware, go to **Networked Computers > Client Management > Tasks > Spyware/Grayware Restore**.

Assessment mode

Assessment mode allows you to first evaluate whether spyware/grayware is legitimate and then take action based on your evaluation. For example, you can add the legitimate ones to the spyware/grayware approved list.

To configure assessment mode settings, go to **Networked Computers > Global Client Settings > Spyware/Grayware Settings**.

Rootkit detection

This version also includes a new component for detecting and removing rootkits. Currently on the rise, rootkits corrupt regular operating system functions that application programs assume are valid to gain a great deal of control on the user's computer. Rootkits are extremely hard to remove without rebuilding the computer.

Component Duplication

Downloading a full pattern each time OfficeScan updates its components consumes substantial bandwidth. This version of OfficeScan can perform smaller pattern downloads by limiting the download to only the new available patterns. See *Component Duplication* on page 2-7 for more information.

Plug-in Manager

Plug-in programs are developed outside of a product release and are not yet fully integrated into OfficeScan. With Plug-in Manager, you no longer need to wait for a product release to start using the plug-in programs.

Plug-in Manager displays the programs for both the OfficeScan server and client in the OfficeScan Web console as soon as they become available. You can then install and manage the programs from the Web console, including deploying the client plug-in programs to clients.

Download and install Plug-in Manager by clicking **Plug-in Manager** on the main menu of the Web console. After the installation, you can check for available plug-in programs.

Web Console Management

- Administrators and client users can now manage anti-spyware and antivirus features separately.
- Manage all client-related tasks using the menu items above the client tree.
- Manage notification messages and settings in the Web console by clicking Notifications in the main menu.

Platform Support

Microsoft certifies the OfficeScan client to support the Windows™ Vista™ platform (32-bit and 64-bit).

Note: The OfficeScan server does not support Windows Vista.

Computers running Windows Vista will have most OfficeScan programs and features, except for the following:

- Microsoft Outlook™ Mail Scan
- Check Point™ SecureClient™
- Cisco™ NAC 2
- Watchdog DLL injection function
- Image Setup utility (ImgSetup.exe)

  Note: Even if Image Setup is not supported, clients have the capability to automatically change the GUID when prompted by the server to do so.

- Infection source notification (The Alerter Service is removed)

Key Features and Benefits

OfficeScan provides the following features and benefits:

Security Risk Protection

OfficeScan protects your networked computers from viruses/malware, spyware/grayware and Web threats. The OfficeScan client provides security risk protection and reports events to, and gets updates from, the OfficeScan server. The OfficeScan server hosts the Web console, downloads updates from an update source (such as the Trend Micro ActiveUpdate server), and initiates clients to update components.

Enhanced Anti-spyware Capabilities

OfficeScan protects against a wide variety of spyware, including adware, dialers, joke programs, remote-access tools, and password cracking applications. Using an extensive, up-to-date spyware database and customized exclusion lists, it minimizes the risk of spyware-related slowdowns, crashes, and support calls. It also prevents key loggers from stealing confidential information, preserves bandwidth, and secures business productivity. These capabilities complement the anti-spyware functionality in Trend Micro InterScan™ Web Security Suite—together providing end-to-end spyware protection from the Web gateway to client/server networks.

Centralized Management

A Web-based management console gives administrators transparent access to all clients and servers on the network. The Web console coordinates automatic deployment of security policies, pattern files, and software updates on every client and server. And with Outbreak Prevention Services, it shuts down infection vectors and rapidly deploys attack-specific security policies to prevent or contain outbreaks before pattern files are available. OfficeScan also performs real-time monitoring, provides event notification, and delivers comprehensive reporting. Administrators can perform remote administration, set customized policy for individual desktops or groups, and lock client security settings.

Security and Policy Enforcement

OfficeScan provides seamless integration of the Cisco™ Trust Agent, enabling the most effective policy enforcement within a Cisco Self-Defending Network. OfficeScan also includes a Policy Server for automated communication with Cisco Access Control Servers. When integrated with Trend Micro Network VirusWall™ or any Network Admission Control (NAC) device, OfficeScan can check clients trying to enter the network and then remedy, redirect, restrict, deny, or permit access. If a computer is vulnerable or becomes infected, OfficeScan can automatically isolate it and its network segments until all PCs are updated or cleanup is complete.

OfficeScan Firewall

The OfficeScan firewall protects clients and servers on the network using stateful inspection, high performance network virus scanning, and elimination. Through the central management console, you can create rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.

Note: You can install, configure, and use the OfficeScan firewall on Windows XP computers that also have Windows Firewall enabled. However, you must manage you policies carefully to avoid creating conflicting firewall policies and producing unexpected results. For example, if you configure one firewall to allow traffic from a certain port but the other firewall blocks traffic from the same port, OfficeScan blocks the traffic. See your Microsoft documentation for details on Internet Connection Firewall.

Traffic filtering

The OfficeScan firewall filters all incoming and outgoing traffic, providing the ability to block certain types of traffic based on the following criteria:

- Direction (inbound/outbound)
- Protocol (TCP/UDP/ICMP)
- Destination ports
- Source and destination computers

Scanning for network viruses

The OfficeScan firewall also examines each packet for network viruses.

Customizable profiles and policies

The OfficeScan firewall gives you the ability to configure policies to block or allow specified types of network traffic. Assign a policy to one or more profiles, which you can then deploy to specified OfficeScan clients. This provides a highly customized method of organizing and configuring firewall settings for your clients.

Stateful inspection

The OfficeScan firewall is a stateful inspection firewall; it monitors all connections to the client and remembers all connection states. It can identify specific conditions in any connection, predict what actions should follow, and detect disruptions in normal connection. Filtering decisions, therefore, are based not only on profiles and policies, but also on the context established by analyzing connections and filtering packets that pass through the firewall.

Intrusion Detection System

The OfficeScan firewall also includes an Intrusion Detection System (IDS). When enabled, IDS can help identify patterns in network packets that may indicate an attack on the client. The OfficeScan firewall can help prevent the following well-known intrusions:

- **Too Big Fragment:** A Denial of Service attack where a hacker directs an oversized TCP/UDP packet at a target computer. This can cause the computer's buffer to overflow, which can freeze or reboot the computer.
- **Ping of Death:** A Denial of Service attack where a hacker directs an oversized ICMP packet at a target computer. This can cause the computer's buffer to overflow, which can freeze or reboot the computer.
- **Conflicted ARP:** A type of attack where a hacker sends an Address Resolution Protocol (ARP) request with the same source and destination IP address. The target computer continually sends an ARP response (its MAC address) to itself, causing it to freeze or crash.

- **SYN Flood:** A Denial of Service attack where a program sends multiple TCP synchronization (SYN) packets to a computer, causing the computer to continually send synchronization acknowledgment (SYN/ACK) responses. This can exhaust computer memory and eventually crash the computer.
- **Overlapping Fragment:** Similar to a Teardrop attack, this Denial of Service attack sends overlapping TCP fragments to a computer. This overwrites the header information in the first TCP fragment and may pass through a firewall. The firewall may then allow subsequent fragments with malicious code to pass through to the target computer.
- **Teardrop:** Similar to an overlapping fragment attack, this Denial of Service attack deals with IP fragments. A confusing offset value in the second or later IP fragment can cause the receiving computer operating system to crash when attempting to reassemble the fragments.
- **Tiny Fragment Attack:** A type of attack where a small TCP fragment size forces the first TCP packet header information into the next fragment. This can cause routers that filter traffic to ignore the subsequent fragments, which may contain malicious data.
- **Fragmented IGMP:** A Denial of Service attack that sends fragmented IGMP packets to a target computer, which cannot properly process the IGMP packets. This can freeze or slow down the computer.
- **LAND Attack:** A type of attack that sends IP synchronization (SYN) packets with the same source and destination address to a computer, causing the computer to send the synchronization acknowledgment (SYN/ACK) response to itself. This can freeze or slow down the computer.

Firewall violation outbreak monitor

The OfficeScan firewall sends a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack.

Client firewall privileges

You can grant client users the privilege to view their firewall settings on the OfficeScan client console. You can also grant users the privilege to enable or disable the firewall, the Intrusion Detection System, and the firewall violation notification message.

Damage Cleanup Services

Damage Cleanup Services™ cleans computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process. OfficeScan and Damage Cleanup Services are key components of Trend Micro Enterprise Protection Strategy (EPS)—designed to proactively manage the outbreak lifecycle—from vulnerability prevention to malicious code elimination.

For more information on Enterprise Protection Strategy, go to the following Web site:

http://us.trendmicro.com/us/home/enterprise

The Damage Cleanup Services solution

To address the threats and nuisances posed by Trojans, Damage Cleanup Services does the following:

- Detects and removes live Trojans
- Kills processes that Trojans create
- Repairs system files that Trojans modify
- Deletes files and applications that Trojans drop

Because DCS runs automatically in the background, you do not need to configure it. Users are not even aware when it runs. However, OfficeScan may sometimes notify the user to restart their computer to complete the process of removing a Trojan.

The OfficeScan Server

The OfficeScan HTTP-based server is the central repository for all client configurations, security risk logs, and client programs and updates.

The server performs two important functions:

- Installs, monitors, and manages networked computer clients
- Downloads components from the Trend Micro update server and distributes them to clients

The OfficeScan server is capable of providing real-time, bidirectional communication between the server and clients. You can manage the clients from a browser-based Web console, which you can access from virtually anywhere on the network. The server communicates with the client (and the client with the server) through HyperText Transfer Protocol (HTTP). The server can only install HTTP-based clients. You cannot install an HTTP-based client if the client computer does not support TCP/IP.

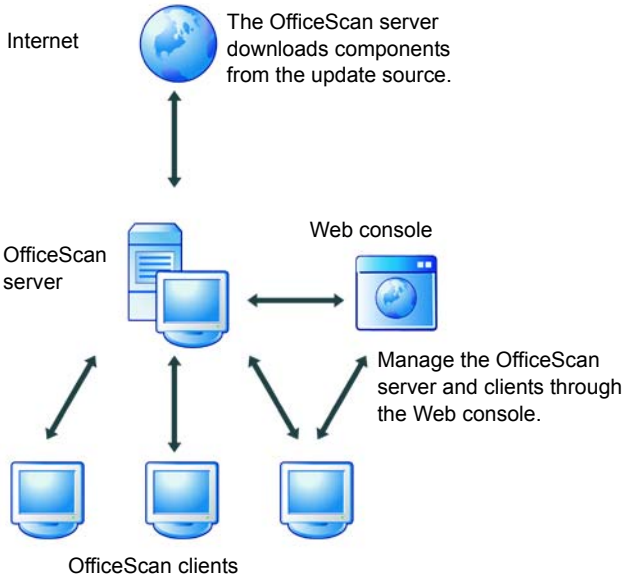


FIGURE 1-1 How the HTTP-based server works

The OfficeScan Client

Protect Windows computers from security risks by installing the OfficeScan client on each computer. The client provides three methods of scanning: Real-time Scan, Scheduled Scan, and Manual Scan.

The client reports to the parent server from which it was installed. You can have clients report to another server by using the Client Mover tool (see the online help for more information about this tool). The client sends events and status information to the server in real time to provide you with updated client information. Examples of events are virus/malware detection, client startup, client shutdown, start of a scan, and completion of an update.

Configure scan settings on clients from the client console (if you grant users this privilege) and the server Web console. To enforce uniform desktop protection across the network, choose not to grant the clients privileges to modify the scan settings or to remove the client program.

There are two types of OfficeScan clients:

- Normal clients
- Roaming clients

Normal clients

Normal clients maintain a continuous connection with the server. The OfficeScan system tray icon changes to reflect the status of the normal client.

Note: OfficeScan uses the Real-time Scan Service not only for Real-time Scan, but also for Manual Scan and Scheduled Scan. This means that if the Real-time Scan service stops, the client computer becomes unprotected. The icon's color changes to red if Real-time Scan stops running.

TABLE 1-1. Normal client icons

Icon	Status	Description	Real-time Scan
	Online	All components are up-to-date and services work properly.	Enabled

TABLE 1-1. Normal client icons

Icon	Status	Description	Real-time Scan
	Online	The pattern file has not been updated for a while.	Enabled
	Online	Scan Now, Manual Scan, or Scheduled Scan is running. This icon displays during virus/malware and spyware/grayware scanning.	Enabled
	Online	Real-time Scan has been disabled. **Note:** If you disable Real-time Scan for spyware/grayware but enable Real-time Scan for virus/malware, the Real-time Scan status on the client is "enabled" and the client icon is: 	Disabled
	Online	Real-time Scan has been disabled and the pattern file has not been updated for a while.	Disabled
	Online	Real-time Scan Service has been stopped.	Disabled
	Online	Real-time Scan Service has been stopped and the pattern file has not been updated for a while.	Disabled
	Offline	The client is disconnected from the server.	Enabled
	Offline	The client is disconnected from the server and the pattern file has not been updated for a while.	Enabled
	Offline	The client is disconnected and Real-time Scan has been disabled.	Disabled
	Offline	The client is disconnected from the server, Real-time Scan has been disabled, and the pattern file has not been updated for a while.	Disabled

TABLE 1-1. Normal client icons

Icon	Status	Description	Real-time Scan
	Offline	The client is disconnected from the server and Real-time Scan Service has been stopped.	Disabled
	Offline	The client is disconnected from the server, Real-time Scan Service has been stopped, and the pattern file has not been updated for a while.	Disabled

Roaming clients

Clients on roaming mode are isolated from, and therefore cannot 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. Although communication with the server is lost, roaming clients with Internet connection can still update components if configured to get updates from an Update Agent or the Trend Micro ActiveUpdate server.

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

Updates to roaming clients appear only on the following occasions:

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

For more information on how to update clients, see *Client Update* on page 2-13.

The OfficeScan system tray icon changes to reflect the status of the roaming client.

Note: OfficeScan uses the Real-time Scan Service not only for Real-time Scan, but also for Manual Scan and Scheduled Scan. This means that if the Real-time Scan service stops, the client computer becomes unprotected. The icon's color changes to red if Real-time Scan stops running.

TABLE 1-2. Roaming client icons

Icon	Description	Real-time Scan
	All components are up-to-date and services work properly.	Enabled
	Real-time Scan has been disabled.	Disabled
	The pattern file has not been updated for a while.	Enabled
	Real-time Scan has been disabled and the pattern file has not been updated for a while.	Disabled
	Real-time Scan Service has been stopped.	Disabled
	Real-time Scan Service has been stopped and the pattern file has not been updated for a while.	Disabled

Required user actions

Perform the necessary actions if the client icon indicates any of the following conditions.

TABLE 1-3. Client conditions that require user actions

Condition	Action
Pattern file not updated for a while	Client users need to update components. From the Web console, you can configure component update settings in **Updates > Networked Computers**, or grant users the privilege to update in **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab **> Component Update Privileges**.
Real-time Scan service stopped	Users can manually start the service (OfficeScanNT RealTime Scan) from the Windows Services screen.
Real-time Scan disabled	Enable Real-time Scan from the Web console (**Networked Computers > Client Management > Settings > Real-time Scan Settings**).
Real-time Scan disabled and client on roaming mode	Users need to disable roaming mode first. After disabling roaming mode, enable Real-time Scan from the Web console.
Client disconnected from the server	First 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: • If the connection status on both the server and client is offline, check the network connection. • 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. • If the connection status on the client is online but offline on the server, check your OfficeScan firewall settings. Firewall may block server-to-client communication, but allow client-to-server communication. • 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 did not update on the server (for example, when the client is reloaded). You can try to redeploy the client.

Client features for supported operating systems

The OfficeScan client supports Windows 2000, XP/Server 2003 (32-bit and 64-bit) and Vista operating systems.

TABLE 1-4. Client features

Feature	Windows 2000	Windows XP/Server 2003 (32-bit)	Windows XP/Server 2003 (64-bit)	Windows Vista
Manual Scan, Real-time Scan, and Scheduled Scan				
Component update (manual and scheduled update)				
Update Agent				
Web Reputation				
Microsoft Outlook mail scan				
OfficeScan firewall				
Damage Cleanup Services				
Support for Cisco NAC				
Plug-in Manager				
Roaming mode				

TABLE 1-4. Client features

Feature	Windows 2000	Windows XP/Server 2003 (32-bit)	Windows XP/Server 2003 (64-bit)	Windows Vista
SecureClient support	✓	✓		

OfficeScan Components and Programs

OfficeScan includes the following components and programs:

TABLE 1-5. OfficeScan components

Component	Description
Antivirus	
Virus Pattern	A file that helps OfficeScan identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus (see *The Virus Pattern* on page 1-20 for more information)
Virus Scan Engine	The engine that scans for and takes appropriate action on viruses/malware; supports 32-bit and 64-bit platforms
IntelliTrap Pattern	The file for detecting real-time compression files packed as executable files
IntelliTrap Exception Pattern	The file containing a list of "approved" compression files
Anti-spyware	
Spyware Pattern	The file that identifies spyware/grayware in files and programs, modules in memory, Windows registry and URL shortcuts
Spyware Scan Engine	The engine that scans for and takes appropriate action on spyware/grayware; supports 32-bit and 64-bit platforms

TABLE 1-5. OfficeScan components

Component	Description
Spyware Active-monitoring Pattern	File used for real-time spyware/grayware scanning **Note:** This component is only available if you activate both Antivirus and Web Threat Protection services.
Venus Spy Trap Engine	Allows applications to monitor new executable files and deletes spyware/grayware upon discovery; supports 32-bit and 64-bit platforms **Note:** This component is available if you activate the Web Threat Protection service only. If you activated both Antivirus and Web Threat Protection services, this component is not available.
Damage Cleanup Services	
Virus Cleanup Engine	The engine Damage Cleanup Services uses to scan for and remove Trojans and Trojan processes; supports 32-bit and 64-bit platforms
Virus Cleanup Template	Used by the Virus Cleanup Engine, this template helps identify Trojan files and processes so the engine can eliminate them
Firewall	
Common Firewall Driver	Used with the Common Firewall Pattern to scan client computers for network viruses; supports 32-bit and 64-bit platforms
Common Firewall Pattern	Like the Virus Pattern, this file helps OfficeScan identify virus signatures, unique patterns of bits and bytes that signal the presence of a network virus
Web Reputation	
URL Filtering Engine	The engine that facilitates communication between OfficeScan and the Trend Micro URL Filtering Service. The URL Filtering Service is a system that rates URLs and provides rating information to OfficeScan.
Common component	

TABLE 1-5. OfficeScan components

Component	Description
Anti-rootkit Driver	A kernel mode driver used by the Spyware Scan Engine that provides functionality to bypass any potential redirection by rootkits; supports 32-bit platforms

TABLE 1-6. OfficeScan programs

Program	Description
Client program	The OfficeScan client program, which provides the actual protection from security risks; supports 32-bit and 64-bit platforms
Cisco Trust Agent	The program used to enable communication between the client and routers that support Cisco NAC; will work only if you install Policy Server for Cisco NAC
Hot fixes and security patches	Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the OfficeScan server and/or client program

Note: In addition to these components, OfficeScan clients also receive updated configuration files from the OfficeScan server. Clients need the configuration files to apply new settings. Each time you modify OfficeScan settings through the Web console, the configuration files change.

The Virus Pattern

The Trend Micro Virus Scan Engine uses an external data file, called the Virus Pattern. It contains information that helps OfficeScan identify the latest virus/malware and mixed attacks. Trend Micro creates and releases new versions of the Virus Pattern several times a week, and any time after the discovery of a particularly damaging virus/malware.

All Trend Micro products using the ActiveUpdate function can detect the availability of a new version of the Virus Pattern on the Trend Micro server, and/or automatically poll the server to get the latest file.

Tip: Trend Micro recommends scheduling automatic updates at least weekly, which is the default setting for all shipped products.

You can download the Virus Pattern and other OfficeScan pattern files from the following Web site, where you can also find the current version, release date, and a list of all the new virus definitions included in the file:

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

The Trend Micro Scan Engine

At the heart of all Trend Micro products lies a scan engine. Originally developed in response to early file-based computer viruses, the scan engine today is exceptionally sophisticated and capable of detecting Internet worms, mass-mailers, Trojan horse threats, phish sites, spyware, and network exploits as well as viruses. The scan engine detects two types of threats:

- **in the wild:** Actively circulating
- **in the zoo:** Controlled viruses not in circulation but developed and used for research

Rather than scanning every byte of every file, the engine and pattern file work together to identify not only tell-tale characteristics of the virus code, but the precise location within a file that the virus would hide. OfficeScan removes virus/malware upon detection and restores the integrity of the file.

International computer security organizations, including ICSA (International Computer Security Association), certify the Trend Micro scan engine annually.

Updating the Scan Engine

By storing the most time-sensitive virus/malware information in the Virus Pattern, Trend Micro is able to minimize the number of scan engine updates while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. Trend Micro releases new engines under the following circumstances:

- Incorporation of new scanning and detection technologies into the software
- Discovery of a new, potentially harmful virus/malware that the scan engine cannot handle
- Enhancement of the scanning performance
- Addition of file formats, scripting languages, encoding, and/or compression formats

Hot Fixes, Patches, and Service Packs

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

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

- **Hot fix:** A workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes do not (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).
- **Security patch:** A hot fix focusing on security issues suitable for deployment to all customers. Windows security patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Patch:** A group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program, while non-Windows patches commonly have a setup script.

- **Service pack:** A consolidation of hot fixes, patches, and feature enhancements significant enough to be a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

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

http://www.trendmicro.com/download

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

Note: By default, the OfficeScan clients can install hot fixes. If you do not want clients to install hot fixes, change client update settings in the Web console by going to **Networked Computers > Client Management > Settings > Privileges and Other Settings > Other Settings** tab.

Security Risks

Security risk is the collective term for virus/malware, spyware/grayware, and Web threats. OfficeScan protects computers from the following security risks:

Viruses and Malware

Tens of thousands of virus/malware exist, with more being created each day. Although once most common in DOS or Windows, computer viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and Web sites.

TABLE 1-7. Virus and malware types

Type	Description
Joke program	A virus-like program that often manipulates the appearance of things on a computer monitor

TABLE 1-7. Virus and malware types

Type	Description
Trojan horse	An executable program that does not replicate but instead resides on systems to perform malicious acts, such as opening ports for hackers to enter. A Trojan program often uses ports to gain access to computers. An application that claims to rid your computer of viruses when it actually introduces viruses onto your computer is an example of a Trojan program. Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those already running on the system.
Virus	A program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes.
ActiveX malicious code	Code that resides on Web pages that execute ActiveX™ controls
Boot sector virus	A virus that infects the boot sector of a partition or a disk
COM and EXE file infector	An executable program with .com or .exe extension
Java malicious code	Operating system-independent virus code written or embedded in Java™
Macro virus	A virus encoded as an application macro and often included in a document
VBScript, JavaScript or HTML virus	A virus that resides on Web pages and downloaded through a browser
Worm	A self-contained program or set of programs able to spread functional copies of itself or its segments to other computer systems, often through email
Test virus	An inert file that acts like a real virus and is detectable by virus-scanning software. Use test viruses, such as the EICAR test script, to verify that your antivirus installation scans properly.

TABLE 1-7. Virus and malware types

Type	Description
Packer	A compressed and/or encrypted Windows or Linux™ executable program, often a Trojan horse program. Compressing executables makes packer more difficult for antivirus products to detect.

Network Viruses

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the virus/malware mentioned above, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of client computers, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.

The OfficeScan firewall works with the Common Firewall Pattern to identify and block network viruses.

Spyware and Grayware

Your computers are at risk from potential threats other than viruses/malware. Spyware/Grayware refers to applications or files not classified as viruses or Trojans, but can still negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization. Often spyware/grayware performs a variety of undesired and threatening actions such as irritating users with pop-up windows, logging user keystrokes, and exposing computer vulnerabilities to attack.

Types of spyware/grayware

OfficeScan detects the following spyware/grayware types:

TABLE 1-8. Spyware and grayware types

Type	Description
Spyware	Gathers data, such as account user names, passwords, credit card numbers, and other confidential information, and transmits it to third parties
Adware	Displays advertisements and gathers data, such as Web surfing preferences, used for targeting future advertising at the user
Dialer	Changes client Internet settings and can force a computer to dial pre-configured phone numbers through a modem. These are often pay-per-call or international numbers that can result in a significant expense for your organization.
Joke program	Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking tool	Helps hackers enter a computer
Remote access tool	Helps hackers remotely access and control a computer
Password cracking application	Helps decipher account user names and passwords
Others	Other types of potentially malicious programs

How spyware/grayware gets into your network

Spyware/Grayware often gets into a corporate network when users download legitimate software that have grayware applications included in the installation package. Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the application and its intended use to collect personal data; however, users often overlook this information or do not understand the legal jargon.

Potential risks and threats

The existence of spyware and other types of grayware on your network have the potential to introduce the following:

- **Reduced computer performance:** To perform their tasks, spyware/grayware applications often require significant CPU and system memory resources.
- **Increased Web browser-related crashes:** Certain types of grayware, such as adware, often display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a computer restart.
- **Reduced user efficiency:** By needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users become unnecessarily distracted from their main tasks.
- **Degradation of network bandwidth:** Spyware/Grayware applications often regularly transmit the data they collect to other applications running on your network or to locations outside of your network.
- **Loss of personal and corporate information:** Not all data spyware/grayware applications collect is as innocuous as a list of Web sites users visit. Spyware/Grayware can also collect the user names and passwords users type to access their personal accounts, such as a bank account, and corporate accounts that access resources on your network.
- **Higher risk of legal liability:** If computer resources on your network are hijacked, hackers may be able to utilize your client computers to launch attacks or install spyware/grayware on computers outside your network. The participation of your network resources in these types of activities could leave your organization legally liable to damages incurred by other parties.

Guarding against spyware/grayware

There are many steps you can take to prevent the installation of spyware/grayware onto your computer. Trend Micro suggests adhering to the following standard practices:

- Configure all types of scans (Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now) to scan for and remove spyware/grayware files and applications. See *Scan Types* on page 2-21 for more information.
- Educate your client users to do the following:
  - Read the End User License Agreement (EULA) and included documentation of applications they download and install on their computers.
  - Click No to any message asking for authorization to download and install software unless client users are certain both the creator of the software and the Web site they view are trustworthy.
  - Disregard unsolicited commercial email (spam), especially if the spam asks users to click a button or hyperlink.
- Configure Web browser settings that ensure a strict level of security. Trend Micro recommends requiring Web browsers to prompt users before installing ActiveX controls. To increase the security level for Internet Explorer™ (IE), go to **Tools > Internet Options > Security** and move the slider to a higher level. If this setting causes problems with Web sites you want to visit, click **Sites...**, and add the sites you want to visit to the trusted sites list.
- If using Microsoft Outlook, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages.
- Do not allow the use of peer-to-peer file-sharing services. Spyware and other grayware applications may be masked as other types of files your users may want to download, such as MP3 music files.
- Periodically examine the installed software on your client computers and look for applications that may be spyware or other grayware. If you find an application or file that OfficeScan cannot detect as grayware but you think is a type of grayware, send it to Trend Micro: http://subwiz.trendmicro.com/SubWiz. TrendLabs will analyze the files and applications you submit.
- Keep your Windows operating systems updated with the latest patches from Microsoft. See the Microsoft Web site for details.

Phish Attacks

Phish, or phishing, is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site.

In a typical scenario, unsuspecting users get an urgent sounding (and authentic looking) email telling them there is a problem with their account that they must immediately fix to avoid account termination. The email will include a URL to a Web site that looks exactly like the real thing (it is simple to copy a legitimate email and a legitimate Web site but then change the so-called backend—the recipient of the collected data.

The email tells the user to log on to the site and confirm some account information. A hacker receives data a user provides, such as logon name, password, credit card number, or social security number.

Phish fraud is fast, cheap, and easy to perpetuate. It is also potentially quite lucrative for those criminals who practice it. Phish is hard for even computer-savvy users to detect. And it is hard for law enforcement to track down. Worse, it is almost impossible to prosecute.

Please report to Trend Micro any Web site you suspect to be a phishing site. See *Sending Suspicious Files to Trend Micro* on page 9-4 for more information.

OfficeScan Documentation

The documentation set for OfficeScan includes the following:

- **Installation and Deployment Guide:** A PDF document containing requirements and procedures for installing the OfficeScan server and client
- **Administrator's Guide:** A PDF document containing OfficeScan overview, getting started information, security risk protection, and OfficeScan management
- **Online help:** HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. The Online help is accessible from the OfficeScan server and client consoles. Help files are also available for the Policy Server console, Vulnerability Scanner tool and 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 online or printed documentation.

You can download the latest version of the Installation and Deployment Guide and the Administrator's Guide at http://www.trendmicro.com/download.

Terminology

TABLE 1-9. Terminology used in OfficeScan documentation

Terminology	Description
Client	The OfficeScan client program
Client computer	A computer where you install the OfficeScan client
Client user (or user)	The person managing the OfficeScan client on the client computer
Server	The OfficeScan server program
Server computer	The computer where you install the OfficeScan server
Administrator (or OfficeScan administrator)	The person managing the OfficeScan server
Security risk	The collective term for virus/malware, spyware/grayware, and Web threats
Product service	Includes Antivirus, Damage Cleanup Services, and Web Threat Protection–all of which you can activate during OfficeScan installation
OfficeScan service	Services hosted by the 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 risk

Chapter 2

Getting Started with OfficeScan

Topics in this chapter:

The Web Console

The Web console is the central point for monitoring OfficeScan throughout your corporate network. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. The Web console uses standard Internet technologies, such as Java, CGI, HTML, and HTTP.

You can use the Web console to do the following:

- Manage clients installed on networked computers
- Group clients into logical domains for simultaneous configuration and management
- Set scan configurations and invoke manual scan on a single or multiple networked computers
- Receive notifications about security risks on your network and view logs sent by clients
- Declare outbreaks using email, pager, and SNMP Trap

Open the Web console from any computer on the network that has the required Web browser and communication protocols. On the Web browser, type one of the following in the address bar based on the type of OfficeScan server installation:

- Without SSL on a default site: http://{OfficeScan server}/OfficeScan
- Without SSL on a virtual site: http://{OfficeScan server}:{port number}/OfficeScan
- With SSL on a default site: https://{OfficeScan server}/OfficeScan
- With SSL on a virtual site: https://{OfficeScan server}:{port number}/OfficeScan

Note: If you upgraded from a previous version of OfficeScan, Web browser and proxy server cache files may prevent the OfficeScan Web console from loading properly. Clear the cache memory on your browser and on any proxy servers located between the OfficeScan server and the computer you use to access the Web console.

OfficeScan Domains

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

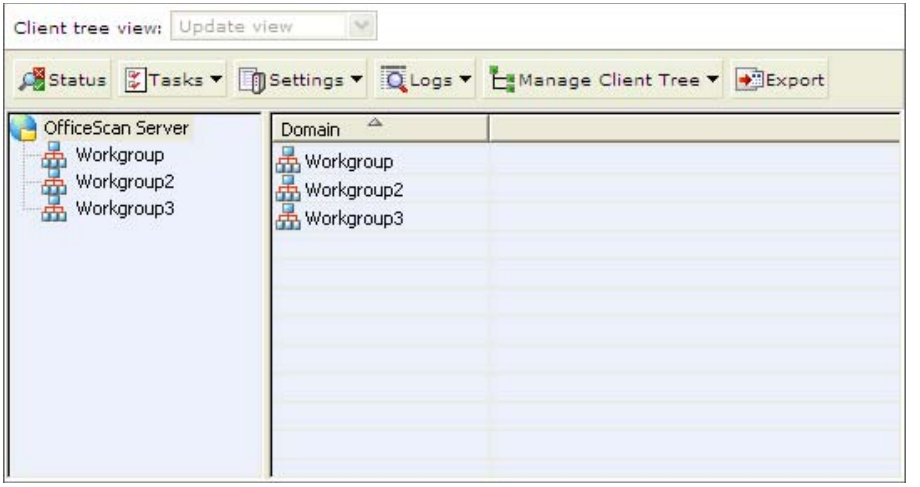


FIGURE 2-1 The OfficeScan client tree with a list of domains

For ease of management, group clients based on their departments or the functions they perform. Also group clients that are at a greater risk of infection to apply a more secure configuration to all of them.

An OfficeScan domain is different from a Microsoft Windows domain. There can be several OfficeScan domains in one Microsoft Windows domain.

By default, OfficeScan simulates your network domains. The domain and client names in the client tree have the same names as the domain and computer names in your network. OfficeScan also assigns clients based on the domain structure of your network. You can delete or rename the domains that OfficeScan created for you, create a new domain, or transfer clients from one domain to another.

Tip: You can also group your clients by existing NetBIOS, Windows Active Directory™, or DNS domains. To use this setting, in the Web console, go to **Networked Computers > Global Client Settings > Client Grouping**.

Proxy Settings

You can configure the OfficeScan server to use Internet proxy settings when connecting to the ActiveUpdate server to update components. Similarly, you can configure clients to use intranet proxy settings when communicating with the server and updating components. Other proxy settings clients can use when updating components include automatic proxy settings and user-configured proxy settings (if you grant client users the privilege to configure proxy settings).

Proxy for Server Component Update

To configure the server to use a proxy server to access the Internet and connect to the ActiveUpdate server, go to **Administration > Proxy Settings > Internet Proxy**. See *Server Update* on page 2-8 for details on server component update.

Proxy for Client Component Update

OfficeScan clients use proxy settings during automatic update or when performing "Update Now". See *Client update methods* on page 2-14 for more information on automatic update and Update Now.

TABLE 2-1. Proxy settings used during client component update

Update Method	Proxy Settings Used	Usage
Automatic update	• Automatic proxy settings configured in **Networked Computers > Global Client Settings**. • Intranet proxy settings configured in **Administration > Proxy Settings > Intranet Proxy** tab.	• OfficeScan clients will first use automatic proxy settings to update components. • If automatic proxy settings are not enabled, intranet proxy settings will be used. • If both are disabled, clients will not use any proxy settings.
Update Now	• Automatic proxy configuration settings configured in **Networked Computers > Global Client Settings**. • User-configured proxy settings. You can grant client users the privilege to configure proxy settings in **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab.	• OfficeScan clients will first use automatic proxy settings to update components. • If automatic proxy settings are not enabled, user-configured proxy settings will be used. • If both are disabled, or if automatic proxy settings are disabled and client users do not have the required privilege, clients will not use any proxy when updating components.

Component Updates

To help ensure that clients stay protected against the latest security risks, regularly update the OfficeScan components. See *OfficeScan Components and Programs* on page 1-18 for information about the different components.

To configure OfficeScan to update components, do the following:

1. Update the server. See *Server Update* on page 2-8.
2. Assign certain clients to act as Update Agents and configure settings (see *Update Agent* on page 2-11 for more information).
3. Update the clients. See *Client Update* on page 2-13.

Update Source

When choosing the update source, consider the bandwidth of the sections of your network that are between clients and the update source(s) (see the *Installation and Deployment Guide* for more information on how updates affect network traffic). The following table describes the different component update options and recommendations when to use them.

TABLE 2-2. Component update options

Update Option	Description	Recommendation
ActiveUpdate server >> OfficeScan server >> Clients	The OfficeScan server receives updated components from the ActiveUpdate server (or other update source) and initiates component update on clients.	Use this method if there are no 'low-bandwidth' sections of your network between the OfficeScan server and clients.
ActiveUpdate server >> OfficeScan server >> Update Agents >> Clients	The OfficeScan server receives updated components from the ActiveUpdate server (or other update source) and initiates component update on clients. Clients acting as Update Agents then notify clients to update components.	Use this method to balance the traffic load on your network if there are 'low-bandwidth' sections of your network between the OfficeScan server and clients.

TABLE 2-2. Component update options

Update Option	Description	Recommendation
ActiveUpdate server >> Update Agents >> Clients	Update Agents receive updated components directly from the ActiveUpdate server (or other update source) and notifies clients to update components.	Use this method only if you experience problems updating Update Agents from the OfficeScan server or from other Update Agents. Under most circumstances, Update Agents receive updates faster from the OfficeScan server or from other Update Agents than from an external update source.
ActiveUpdate server >> clients	OfficeScan clients receive updated components directly from the ActiveUpdate server (or other update source).	Use this method only if you experience problems updating clients from the OfficeScan server or from Update Agents. Under most circumstances, your clients receive updates faster from the OfficeScan server or from Update Agents than from an external update source.

Component Duplication

When the latest version of a full pattern file is available for download from the Trend Micro ActiveUpdate server, 14 "incremental patterns" also become available. Incremental patterns are smaller versions of the full pattern file that account for the difference between the latest and previous full pattern file versions. For example, if the latest version is 175, incremental pattern v_173.175 contains signatures in version 175 not found in version 173 (version 173 is the previous full pattern version since pattern numbers are released in increments of 2. Incremental pattern v_171.175 contains signatures in version 175 not found in version 171.

To reduce network traffic generated when downloading the latest pattern, OfficeScan performs component duplication, a component update method where the OfficeScan server or Update Agent downloads only incremental patterns.

Component duplication applies to the following components:

- Virus Pattern
- Spyware Pattern
- Spyware Active-monitoring pattern
- Virus Cleanup Template
- IntelliTrap Exception Pattern

For information on how component duplication works for both the OfficeScan server and Update Agent, see the following sections:

- *Component duplication process for the OfficeScan server* on page 2-9
- *Component duplication process for Update Agents* on page 2-13

Server Update

Trend Micro updates the scan engine generally only during the release of a new OfficeScan version. However, Trend Micro releases pattern files regularly to keep your client protection current. Since pattern file updates are available regularly, OfficeScan uses a mechanism called **component duplication** that allows faster downloads of pattern files. See *Update Agent* on page 2-11 for more information.

- Trend Micro recommends updating daily to ensure both the server and clients have up-to-date components.
- If you use a proxy server to connect to the Internet, make sure you properly configure your proxy settings to download updates successfully. To configure proxy settings go to **Administration > Proxy Settings**.
- After updating, verify server update logs in **Logs > Server Update Logs**.

Server update methods

OfficeScan provides you the following component update methods for the server:

- **Scheduled update:** Configure the server to check its update source based on a schedule and automatically download any available updates. To configure scheduled update settings, go to **Updates > Server > Scheduled Update**.

- **Manual update:** Trend Micro recommends updating server components manually after installing/upgrading the OfficeScan server and whenever there is an outbreak. To manually update the server, go to **Updates > Server > Manual Update** or click **Update Server Now** on top of the main menu.

Server update source

Configure the server to download OfficeScan components from the Trend Micro ActiveUpdate server or from another source (**Updates > Server > Update Source**).

After the server downloads any available updates, it can automatically notify clients to update their components based on the settings you specified in **Updates > Networked Computers > Automatic Update**. If the component update is critical, let the server notify the clients at once by going to **Updates > Networked Computers > Manual Update**.

Note: If you do not specify a deployment schedule or event-triggered update settings in **Updates > Networked Computers > Automatic Update**, the server will download the updates but will not notify clients to update.

Component duplication process for the OfficeScan server

Updating a component as soon as a new version is available reduces the impact of component duplication on server performance. Therefore, make sure you download components regularly.

To help explain component duplication for the server, refer to the following scenario:

TABLE 2-3. Component duplication scenario

Full patterns on the OfficeScan server	Current version: 171					
	Other versions available:					
	169	167	165	163	161	159

TABLE 2-3. Component duplication scenario

Latest version on the ActiveUpdate server	Full pattern version: 175
	Incremental patterns: 173.175 171.175 169.175 167.175 165.175 163.175 161.175 159.175 157.175 155.175 153.175 151.175 149.175 147.175

1. The OfficeScan server compares its current full pattern version with the latest version on the ActiveUpdate server. If the difference between the two versions is 14 or less, the server only downloads the incremental pattern that accounts for the difference between the two versions.

   Note: If the difference is more than 14, the server automatically downloads the full version of the pattern file and 14 incremental patterns.

   To illustrate based on the example:

   - The difference between versions 171 and 175 is 2. In other words, the server does not have versions 173 and 175.
   - The server downloads incremental pattern 171.175. This incremental pattern accounts for the difference between versions 171 and 175.

2. The server merges the incremental pattern with its current full pattern to generate the latest full pattern.

   To illustrate based on the example:

   - On the server, OfficeScan merges version 171 with incremental pattern 171.175 to generate version 175.
   - The server has 1 incremental pattern (171.175) and the latest full pattern (version 175).

3. The server generates incremental patterns based on the other full patterns available on the server. If the server does not generate these incremental patterns, clients that missed downloading earlier incremental patterns automatically downloads the full pattern file, which will consequently generate more network traffic.

   To illustrate based on the example:

   - Because the server has pattern versions 169, 167, 165, 163, 161, 159, it can generate the following incremental patterns:

169.175 167.175 165.175 163.175 161.175 159.175

- The server does not need to use version 171 because it already has the incremental pattern 171.175.
- The server now has 7 incremental patterns:

  171.175 169.175 167.175 165.175 163.175 161.175 159.175
- The server keeps the last 7 full pattern versions (versions 175, 171, 169, 167, 165, 163, 161). It removes any older version (version 159).

4. The server compares its current incremental patterns with the incremental patterns available on the ActiveUpdate server. The server downloads the incremental patterns it does not have.

   To illustrate based on the example:

   - The ActiveUpdate server has 14 incremental patterns:

     173.175 171.175 169.175 167.175 165.175 163.175 161.175

     159.175 157.175 155.175 153.175 151.175 149.175 147.175
   - The OfficeScan server has 7 incremental patterns:

     171.175 169.175 167.175 165.175 163.175 161.175 159.175
   - The OfficeScan server downloads an additional 7 incremental patterns:

     173.175 157.175 155.175 153.175 151.175 149.175 147.175
   - The server now has all the incremental patterns available on the ActiveUpdate server.
5. The latest full pattern and the 14 incremental patterns are made available to clients.

Update Agent

If you identify "low-bandwidth" or "heavy traffic" sections of your network between clients and the OfficeScan server, you can assign OfficeScan clients to act as Update Agents, or update sources for other clients. This helps distribute the burden of deploying components to all clients.

If your network is segmented by location, and the network link between segments experiences a heavy traffic load, Trend Micro recommends allowing at least one client on each segment to act as an Update Agent.

Update Agent requirements and details

TABLE 2-4. Update Agent system requirements

Resource	Requirement
Operating system	Windows 2000, XP, Server 2003, Vista
Hardware	**Processor:** 800MHz Intel™ Pentium™ or equivalent **RAM:** • 512MB (Windows 2000, XP, Server 2003) • 1GB (Windows Vista) **Available disk space:** 700MB **Others:** Monitor that supports 800 x 600 resolution at 256 colors or higher
Update request capacity	Dependent on the computer's hardware specifications

Update Agent configuration

1. Grant clients the privilege to act as update agents in **Networked Computers > Client Management > Settings > Update Agent Settings**.
2. Select an update source from which the Update Agent can receive updated components.

   To enable Update Agents to get component updates from the OfficeScan server, go to **Updates > Networked Computers > Update Source**.

Note: Like the OfficeScan server, Update Agents also use component duplication when downloading components. See *Update Agent* on page 2-11 for more information.

3. In **Updates > Networked Computers > Update Source > Customized Update Source List**, specify the clients that will update from an Update Agent and then assign the corresponding Update Agent.

Note: The number of concurrent client connections that a single Update Agent can handle depends on the hardware specifications of the computer.

Component duplication process for Update Agents

1. The Update Agent compares its current full pattern version with the latest version on the update source. If the difference between the two versions is 14 or less, the Update Agent downloads the incremental pattern that accounts for the difference between the two versions.

Note: If the difference is more than 14, the Update Agent automatically downloads the full version of the pattern file.

2. The Update Agent merges the incremental pattern it downloaded with its current full pattern to generate the latest full pattern.
3. The Update Agent downloads all the remaining incremental patterns on the update source.
4. The latest full pattern and all the incremental patterns are made available to clients.

Client Update

To ensure that your clients stay protected from the latest security risks, update client components regularly. See *OfficeScan Components and Programs* on page 1-18 for a list of OfficeScan components. You cannot upgrade OfficeScan programs from the **Updates** menu in the Web console.

Note: For OfficeScan client program upgrade, see the Installation and Deployment Guide. For Cisco Trust Agent upgrade, go to **Cisco NAC > Agent Deployment**.

In addition to components, OfficeScan clients also receive updated configuration files automatically during client update. Clients need the configuration files to apply new settings. Each time you modify OfficeScan settings through the Web console, the configuration files change.

Before updating the clients, verify that the server has the latest components. For information on how to update the server, see *Server Update* on page 2-8.

Client update methods

You can initiate component update on clients using automatic or manual update. You can also grant users the privilege to manually update client components.

- **Automatic update:** Trend Micro recommends always using automatic update. It removes the burden placed on clients of performing manual updates and eliminates the risk of client computers not having up-to-date components.

  To configure automatic update settings, go to **Updates > Networked Computers > Automatic Update**. You can also configure clients to use proxy settings during automatic update. See *Proxy for Server Component Update* on page 2-4 for details.

  - **Event-triggered update:** The server can notify online clients to update components after it downloads the latest components, and offline clients when they restart and then connect to the server. Optionally initiate Scan Now (manual scan) on client computers after the update.

Note: If the OfficeScan server is unable to successfully send an update notification to clients after it downloads components, it automatically resends the notification after 15 minutes. The server continues to send update notifications up to a maximum of five times until the client responds. If the fifth attempt is unsuccessful, the server stops sending notifications. If you select the option to update components when clients restart and then connect to the server, component update will still proceed.

- **Schedule-based update:** Clients with the privilege to perform scheduled update check the client update source for updates based on the schedule that you specify. Before specifying the schedule, select the clients that can perform scheduled update.
  - To grant selected clients the privilege to enable/disable scheduled update, go to **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab **> Component Update Privilege**. When you grant the privilege, the default setting is to enable scheduled update. If the client user disables scheduled update from the client console, updating will not proceed on the update date and time you specified.
  - To automatically enable scheduled update without client user intervention, go to **Networked Computers > Client Management > Settings > Privileges and Other Settings > Other Settings** tab **> Update Settings**.

  For information on using schedule-based update with Network Address Translation, see *Client scheduled update with NAT* on page 2-17.

- **Manual update:** To initiate manual update, go to **Updates > Networked Computers > Manual Update**. Trend Micro recommends updating client components manually when client components are severely out-of-date and whenever there is an outbreak. Client components become severely out-of-date when the client fails to update components from the update source for an extended period of time.
- **Update Now on the client:** To grant client users the privilege to manually update client components, go to **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab **> Component Update Privileges**. After granting the privilege, the "Update Now" option becomes available when client users right-click the OfficeScan client icon in the system tray. You can also allow clients to use proxy settings during "Update Now". See *Proxy for Server Component Update* on page 2-4 for details.

Client update source

Clients get updates from the update source you specify in **Updates > Networked Computers > Update Source**. You can choose the OfficeScan server or a customized update source.

Update source priority

If OfficeScan clients are unable to update from the selected update source, they will try other sources. Update source priority is as follows:

1. The first entry on the customized update source list (if updating from customized sources), followed by the second entry, and so on.
2. The OfficeScan server (if you select to update from the standard update source directly or if you select to update from the OfficeScan server if all customized update sources are not available).
3. The Trend Micro ActiveUpdate server. This is the last available update source. If client computers have Internet connection, they can update components directly from the Trend Micro ActiveUpdate server. There are two ways to implement this option:
   a. Use the ActiveUpdate server as a backup source by going to **Networked Computers > Client Management > Settings > Privileges and Other Settings > Other Settings** tab **> Update Settings**.
   b. Force clients to update from the ActiveUpdate server (as the first choice). To do so, in **Updates > Networked Computers > Update Source**, add the ActiveUpdate server to the Customized Update Source List and make sure it is on top of the list. When you add the ActiveUpdate server as update source, you will need its URL, which is as follows:
   http://osce8-p.activeupdate.trendmicro.com/activeupdate. You cannot open this URL from your browser.

Tip: Trend Micro recommends using the ActiveUpdate server as the backup source. Forcing all clients to continually update from the ActiveUpdate server (as the first choice) could significantly consume network bandwidth between your local network and the Internet. Trend Micro recommends using this option only if you experience problems updating from the OfficeScan server or Update Agents.

Client scheduled update with NAT

The following issues may arise if your network uses Network Address Translation (NAT):

- Clients appear offline on the Web console.
- The OfficeScan server is not able to successfully notify clients of updates and configuration changes.

You can work around these issues by deploying updated components and configuration files from the server to the client with a scheduled update.

Do the following:

- Before installing OfficeScan client on client computers:
  - Configure the client update schedule in **Updates > Networked Computers > Automatic Update > Schedule-based Update**.
  - Grant clients the privilege to enable scheduled update in **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab **> Component Update Privilege**.
- If OfficeScan clients already exist on client computers:
  - Give clients the privilege to perform "Update Now" in **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab **> Component Update Privileges**.
  - Instruct users to manually update components on the client computer (by right-clicking the OfficeScan icon in the system tray and clicking "Update Now") to obtain the updated configuration settings.

When clients update, they will receive both the updated components and the configuration files.

Component Update Privileges and Settings

Configure update privileges and settings for selected clients in **Networked Computers > Client Management > Settings > Privileges and Other Settings**.

Privileges

TABLE 2-5. Component update privileges for selected client users

Option	Description	Client Console Navigation
Perform "Update Now"	Allows client users to manually update client components	Right-click the OfficeScan icon on the system tray and click "Update Now".
Enable scheduled update	Allows clients users to enable/disable scheduled update. Although users have the privilege to enable/disable scheduled update, they do not have the privilege to configure the actual schedule. You will have to specify the schedule in **Updates > Networked Computers > Automatic Update > Schedule-based Update**.	Right-click the OfficeScan icon on the system tray and click "{Enable/Disable} Scheduled Update".

Other settings

TABLE 2-6. Component update settings for selected client users

Option	Description	Client Console Navigation
Clients download updates from the Trend Micro ActiveUpdate Server	When initiating updates, OfficeScan clients first get updates from the update source specified on the **Updates > Networked Computers > Update Source** screen. If the update fails, the clients attempt to update from the OfficeScan server. Selecting this option enables clients to attempt to update from the Trend Micro ActiveUpdate server if the update from the OfficeScan server fails.	N/A
Enable scheduled update	This option allows you to enable/disable scheduled update on the selected clients.	N/A
Clients can update components but not upgrade the client program or deploy hot fixes	This option allows component updates to proceed but prevents hot fix deployment and client upgrade using all the upgrade methods. If you do not select this option, all clients simultaneously connect to the server to upgrade or install a hot fix. This may significantly affect server performance if you have a large number of clients. If you select this option, plan how to minimize the impact of client upgrade or hot fix deployment on the server and then execute your plan. See the *Installation and Deployment Guide* for more information about client upgrade methods.	N/A

Note on the "Enable scheduled update" options in the Privileges tab and Other Settings tab

There are two ways scheduled update is enabled/disabled on selected clients.

- Grant clients the privilege to enable/disable scheduled update.
- Enable/Disable scheduled update yourself without any user intervention.

You can select one or both options. See the next two tables for information about how these options work.

TABLE 2-7. Scheduled update scenario 1

Scheduled Update Option	State	Result
On the **Privileges** tab	Enabled (users have the privilege to enable/disable scheduled update)	If client users disable scheduled update, the OfficeScan client will NOT update components during the update schedule. Otherwise, the update will proceed.
On the **Other Settings** tab	Enabled OR Disabled	

TABLE 2-8. Scheduled update scenario 2

Scheduled Update Option	State	Result
On the **Privileges** tab	Disabled	The OfficeScan client will update components during the update schedule.
On the **Other Settings** tab	Enabled	

Component Rollback

Rolling back refers to reverting to the previous version of the Virus Pattern or 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.

Note: You can only roll back the Virus Pattern and Virus Scan Engine.

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 components, go to **Updates > Rollback**.

Scan Settings

To configure scan settings, on the Web console, go to **Networked Computers > Client Management > Settings > {Scan Type}**.

Grant client users the privilege to configure scan settings in **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab **> {Antivirus/Anti-spyware Privileges}**.

Scan Types

OfficeScan provides several types of scans to protect your clients from virus/malware and spyware/grayware.

Real-time Scan

OfficeScan scans files in real time. If OfficeScan detects no security risk, users can proceed to open or save the file. If OfficeScan detects a security risk, it displays a notification message, showing the name of the file and the specific security risk. You can configure notification messages that will display in **Notification > Client User Notifications**.

Manual Scan

Manual Scan for virus/malware starts immediately after a user launches it in the client console. The length of the scan depends on the number of files to scan and the client computer's hardware resources. The scan time and coverage for spyware/grayware depends on the scan method you or client users (with Manual Scan configuration privilege) specify. You can select the scan method to use in the Manual Scan Settings page in the Web console.

Scheduled Scan

Scheduled Scan has similar scan behavior as Manual Scan. The only difference is that Scheduled Scan runs automatically on the scheduled date and time. Use Scheduled Scan to automate routine scans on the client and improve scan management efficiency.

Scan Now

Scan Now and Manual Scan are the same type of scan. The only difference is that you initiate Scan Now remotely using the Web console, while users run Manual Scan locally on their client computers.

Virus/Malware Scan

This section provides you the available virus/malware scan options and settings.

Virus/Malware scan criteria

OfficeScan provides the following virus/malware scan criteria:

TABLE 2-9. Virus/Malware scan criteria

Scan Criteria	Options and Descriptions	Scan Type
Files to scan	Select one: • All scannable files: Scans all files that users open or save • File types scanned by IntelliScan: Scans only files known to potentially harbor malicious code, even those disguised by a harmless extension name. • Only files with extensions you specify	All types
Scan settings	Multiple selections:	
	• Scan boot area: Scans the boot sector of the client's computer's hard disk	Manual Scan, Scheduled Scan, Scan Now
	• Scan mapped drives and shared folders on the network: Scans any network drives or folders that are mapped to the client computer	Manual Scan, Real-time Scan
	• Scan hidden folders	Manual Scan
	• Use IntelliTrap: Blocks real-time compressed executable files and pairs them with other malware characteristics.	All types
	• Do not scan compressed files with more than the specified compression layers	All types
	• Scan floppy disk during system shutdown	Real-time Scan

TABLE 2-9. Virus/Malware scan criteria

Scan Criteria	Options and Descriptions	Scan Type
CPU usage	Select one: • High: No pausing between scans • Medium: Pause slightly between scans • Low: Pause longer between scans	Manual Scan, Scheduled Scan, Scan Now
User activity on files to scan	Select one: • Scan files being created/modified • Scan files being retrieved • Scan files being created/modified and retrieved See Table 2-10. for examples of user activities.	Real-time Scan
Schedule	Select one (and then select the start time of scan): • Daily • Weekly • Monthly	Scheduled Scan

TABLE 2-10. Real-time Scan behavior based on user activity

Activity	If the option selected is...		
	Scan files being created/modified	Scan files being retrieved	Scan files being created/modified and retrieved
Open a read-only file	Real-time Scan does not scan the file.	Real-time Scan scans the file.	Real-time Scan scans the file.
Copy or move a file from a directory excluded from scanning	Real-time Scan scans the file in the destination directory (if OfficeScan does not exclude this directory from scanning).	Real-time Scan does not scan the file in the destination directory	Real-time Scan scans the file in the destination directory (if OfficeScan does not exclude this directory from scanning).

Virus/Malware scan exclusions

To increase the performance of scanning and to skip scanning files causing false alarms, you can exclude certain files, file extensions, and directories. There are separate exclusion lists for Manual Scan, Real-time Scan, Scheduled Scan and Scan Now.

To configure scan exclusion settings, go to **Networked Computers > Client Management > Settings {Scan Type}**.

- For Manual Scan, Scheduled Scan and Scan Now, go to **Virus/Malware** tab **> Scan Exclusion**.
- For Real-time Scan, go to **Target** tab **> Scan Exclusion**.

OfficeScan automatically excludes the directories of the following Trend Micro products from scanning. If you have a Trend Micro product NOT listed below, you can manually add the product directories to the scan exclusion list.

- ScanMail™ for Microsoft Exchange (all versions except version 7)

  Note: If you use version 7, you can add the following folders to the exclusion list: \Smex\Temp, \Smex\Storage, \Smex\ShareResPool\

- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT
- InterScan™ Messaging Security Suite
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan VirusWall 3.53
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan E-mail VirusWall
- InterScan NSAPI Plug-in
- InterScan eManager 3.5x

Note: You can also configure OfficeScan to exclude Microsoft Exchange 2000/2003 directories from Manual Scan, Real-time Scan, Scheduled Scan and Scan Now by going to **Networked Computers > Global Client Settings > Virus/Malware Scan Settings**. For Microsoft Exchange 2007, you need to manually add the directory to the scan exclusion list. Refer to http://technet.microsoft.com/en-us/library/bb332342.aspx for scan exclusion details.

Global virus/malware scan settings

Configure global virus/malware scan settings in **Networked Computers > Global Client Settings**.

TABLE 2-11. Global virus/malware scan settings

Setting	Description
Configure scan settings for large compressed files	OfficeScan checks the file size and virus/malware count limit to determine whether to scan individual files contained in a compressed file. • **Do not scan files in the compressed file if the size exceeds __ MB:** OfficeScan does not scan any file that exceeds the limit. • **Stop scanning after OfficeScan detects __ viruses/malware in the compressed file:** When OfficeScan already detected the specified number of viruses/malware, it stops scanning the remaining un-scanned files in the compressed file. A large number of viruses/malware detected on a compressed file poses a huge threat and renders the file unsafe to access. Consider deleting the compressed file manually instead of letting the Virus Scan Engine take action on each of the infected files contained in the compressed file. • **Clean compressed files:** The scan action for viruses/malware detected on compressed files is "Clean".

TABLE 2-11. Global virus/malware scan settings

Setting	Description
Scan up to __ OLE layer(s)	Object Linking and Embedding (OLE) allows users to create objects with one application and then link or embed them in a second application.
Add Manual Scan to the Windows shortcut menu on client computers	Enabling this option allows users to scan files and folders by right-clicking a file or folder on the Windows desktop or in Windows Explorer and clicking **Scan with OfficeScan Client**.
Exclude the OfficeScan server database folder from Real-time Scan	By default, OfficeScan does not scan its own database. Trend Micro recommends retaining this setting to prevent any possible corruption of the database that may occur during scanning.
Exclude Microsoft Exchange server folders from scanning	OfficeScan does not scan Microsoft Exchange 2000/2003 server folders for viruses/malware during Manual Scan, Real-time Scan, Scheduled Scan and Scan Now. If you have both Antivirus and Web Threat Protection services activated, enabling this option also does not scan Microsoft Exchange folders for spyware/grayware during Real-time Scan. **Note:** For Microsoft Exchange 2007 folders, you need to manually add the folders to the scan exclusion list. See http://technet.microsoft.com/en-us/library/bb332342.aspx for scan exclusion details and *Virus/Malware scan exclusions* on page 2-25 for the procedure.

Virus/Malware scan actions

OfficeScan can take a number of actions against virus/malware based on the scan settings you specify in **Networked Computers > Client Management > Settings > {Scan Type} > Action** tab. You can use ActiveAction (the Trend Micro recommended scan actions) or customize scan actions for each virus/malware type. If you choose ActiveAction, you no longer need to specify scan actions for each virus/malware type. See *Viruses and Malware* on page 1-23 for information about each virus/malware type.

The following are the available scan actions:

TABLE 2-12. Available virus/malware scan actions

Scan Action	Description	Scan Type
Delete	Deletes an infected file	All types
Quarantine	Renames and then moves an infected file to the client computer's quarantine directory found in {OfficeScan client folder}\Suspect. When the client connects to the server, the client sends quarantined files to the server's quarantine directory. OfficeScan encrypts and renames quarantined files in the server computer. The default server quarantine directory is {OfficeScan server folder}\PCCSRV\Virus, which you can change by going to **Networked Computers > Client Management > Settings > {Scan Type} > Action** tab. You can also restore encrypted files.	All types
Clean	Cleans a cleanable file before allowing full access to the file, or lets the specified next action handle an uncleanable file. You can configure a second action if you choose Clean. OfficeScan will take this scan action if cleaning fails.	All types
Rename	Changes the infected file's extension to "vir". Users cannot open the file initially, but can do so if they associate the file with a certain application. A virus/malware may execute when opening the renamed infected file.	All types
Pass	Allows full access to the infected file without doing anything to the file. A user may copy/delete/open the file.	Manual Scan, Scheduled Scan, Scan Now
Deny Access	Denies access (copy, open) to the infected file. The client does not move the file to a different location (as opposed to Quarantine). Users can manually delete the file.	Real-time Scan

TABLE 2-13. Trend Micro recommended scan actions against virus/malware

Virus/ Malware Type	Real-time Scan		Manual Scan/Scheduled Scan/Scan Now	
	First Action	Second Action	First Action	First Action
Joke	Quarantine	N/A	Quarantine	N/A
Trojan	Quarantine	N/A	Quarantine	N/A
Virus	Clean	Quarantine	Clean	Quarantine
Test Virus	Deny Access	N/A	Pass	N/A
Packer	Quarantine	N/A	Quarantine	N/A
Others	Clean	Quarantine	Clean	Quarantine
Generic *	Pass	N/A	Pass	N/A

* Trend Micro flags this virus/malware type as suspicious based on some of its characteristics. The "Pass" scan action is only temporary. After determining if the virus/malware is a security risk or not, Trend Micro will change the scan action accordingly.

Additional virus/malware scan action options

TABLE 2-14. Additional virus/malware scan action options

<table>
<tr><th colspan="3">Option</th><th>Scan Type</th></tr>
<tr><td colspan="3">Specify a quarantine directory
OfficeScan first stores quarantined files in the client computer's \Suspect folder and then sends the files to the designated quarantine directory.
Specify the quarantine directory in URL, UNC path, or absolute file path format. If you use UNC path, make sure the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this group.
Warning: If you specify an incorrect quarantine directory, the OfficeScan client keeps the files on the \Suspect folder until a correct quarantine directory is specified. In the server's virus/malware logs, the scan result is "Unable to send the quarantined file to the designated quarantine folder".
The quarantine directory can be any of the following:</td><td>All types</td></tr>
<tr><td>Quarantine Directory</td><td>Accepted Format</td><td>Example</td><td></td></tr>
<tr><td>A directory on the OfficeScan server computer</td><td>URL
UNC path</td><td>http://{osceserver} (This is the default directory.)
\\{osceserver}\ofcscan\Virus</td><td></td></tr>
<tr><td>A directory on another OfficeScan server computer (if you have other servers on your network)</td><td>URL
UNC path</td><td>http://{osceserver2}
\\{osceserver2}\ofcscan\Virus</td><td></td></tr>
<tr><td>Another computer on the network</td><td>UNC path</td><td>\\{computername}\temp</td><td></td></tr>
<tr><td>A different directory on the client computer</td><td>Absolute path</td><td>C:\temp</td><td></td></tr>
</table>

TABLE 2-14. Additional virus/malware scan action options

Option	Scan Type
Back up files before cleaning The backup directory on the client computer is OfficeScan Client\Backup. You can decrypt backup files. For information on decrypting backup files, see the online help.	All types
Display a notification message when virus/malware is detected To customize the notification message, go to **Notifications > Client User Notifications > Virus/Malware** tab.	Real-time Scan, Scheduled Scan

Spyware/Grayware Scan

This section provides you the available spyware/grayware scan options and settings.

Spyware/Grayware scan criteria

OfficeScan provides the following spyware/grayware scan criteria:

TABLE 2-15. Spyware/Grayware scan criteria

Scan Criteria	Options and Descriptions	Scan Type
Scan method	Select one: • Quick: Scans only computer areas commonly targeted by spyware/grayware • Full: Scans the entire computer	Manual Scan, Scheduled Scan, Scan Now
User activity on files to scan *	Select one: • Scan files being created/modified • Scan files being retrieved • Scan files being created/modified and retrieved See Table 2-10. for examples of user activities.	Real-time Scan

TABLE 2-15. Spyware/Grayware scan criteria

Scan Criteria	Options and Descriptions	Scan Type
Files to scan *	Select one: • All scannable files: Scans all files that users open or save • File types scanned by IntelliScan: Scans only files known to potentially harbor malicious code, even those disguised by a harmless extension name. • Only files with extensions you specify	Real-time Scan
Schedule	Select one (and then select the start time of scan): • Daily • Weekly • Monthly	Scheduled Scan

* Available only if you activate both Antivirus and Web Threat Protection services; not available if you only activate the Web Threat Protection service.

Spyware/Grayware scan exclusions

To increase the performance of scanning and to skip scanning files causing false alarms, you can exclude certain file extensions from spyware/grayware scan. There are separate exclusion lists for Manual Scan, Real-time Scan, Scheduled Scan and Scan Now.

To configure scan exclusion settings, go to **Networked Computers > Client Management > Settings {Scan Type}**.

- For Manual Scan, Scheduled Scan and Scan Now, go to **Spyware/Grayware** tab **> Scan Exclusion (File Extensions)**.
- For Real-time Scan, go to **Target** tab **> Scan Exclusion**.

Spyware/Grayware approved list

There may be certain applications and files that OfficeScan considers spyware or grayware, but which you still want to allow client computers to keep. You can configure the spyware/grayware approved list to prevent OfficeScan from scanning and treating these applications and files as spyware/grayware.

OfficeScan can accommodate a maximum of 1024 spyware/grayware in the approved list.

- To manage the spyware/grayware approved list, go to **Networked Computers > Client Management > Settings > Spyware/Grayware Approved List**.
- To add already detected spyware/grayware to the approved list, go to one of the following:
  - Networked Computers > Client Management > Logs > Spyware/Grayware Logs > Spyware/Grayware Log Criteria > Spyware/Grayware Logs > Add to Approved List
  - Logs > Networked Computer Logs > Security Risks > View Logs > Spyware/Grayware Logs > Spyware/Grayware Log Criteria > Spyware/Grayware Logs > Add to Approved List

Global spyware/grayware scan settings

Configure global spyware/grayware scan settings in **Networked Computers > Global Client Settings**.

The following are the available settings:

- **Enable assessment mode:** When in assessment mode, OfficeScan logs spyware/grayware detections but does not attempt to clean spyware/grayware components. Cleaning terminates processes or deletes registries, files, cookies and shortcuts. Trend Micro provides assessment mode to allow you to first evaluate whether spyware/grayware is legitimate or not and then take appropriate action based on your evaluation. For example, you can add legitimate spyware/grayware to the approved list.

Note: Assessment mode overrides any user-configured scan action. For example, even if you choose "Clean" as the scan action for Manual Scan, "Pass" remains as the scan action during assessment mode.

- **Scan for cookies:** OfficeScan does not scan cookies by default. Select this option if you consider cookies in your networked computers as potential security risks.

Spyware/Grayware scan actions

OfficeScan can take a number of actions against spyware/grayware based on the scan settings you specify in **Networked Computers > Client Management > Settings > {Scan Type} > Action** tab. Choose from the available scan actions in the Spyware/Grayware section of the screen. See *Spyware and Grayware* on page 1-25 for information about the types of spyware/grayware.

The following are the available scan actions:

TABLE 2-16. Available spyware/grayware scan actions

Scan Action	Description	Scan Type
Clean	Terminates processes or delete registries, files, cookies and shortcuts	Manual Scan, Real-time Scan, Scheduled Scan, Scan Now
Pass	Logs the spyware/grayware detection for assessment	Manual Scan, Scheduled Scan, Scan Now
Deny Access	Denies access (copy, open) to the detected spyware/grayware components	Real-time Scan

Additional spyware/grayware scan action option

TABLE 2-17. Additional spyware/grayware scan option

Option	Scan Type
Display a notification message when spyware/grayware is detected. To customize the notification message, go to **Notifications > Client User Notifications > Spyware/Grayware** tab.	Real-time Scan, Scheduled Scan

Scan Privileges

Grant selected client users the following scan privileges in **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab.

TABLE 2-18. Scan privileges for client users

Option	Description	Client Console Navigation
Configure Manual Scan, Real-time Scan and Scheduled Scan settings for virus/malware	Allows client users to configure their own virus/malware scan settings	Settings > {Scan Type}
Configure Manual Scan, Real-time Scan and Scheduled Scan settings for spyware/grayware	Allows client users to configure their own spyware/grayware scan settings	Settings > {Scan Type}
Stop Scheduled Scan	Allows client users to stop a running Scheduled Scan (for both virus/malware and spyware/grayware)	During Scheduled Scan, right-click the OfficeScan icon in the system tray and click "Stop Scheduled Scan".
Mail Scan privilege	Allows client users to manually scan their Microsoft Outlook mail messages and attachments for security risks	Mail Scan tab

Web Reputation Configuration

Configure Web Reputation settings in **Networked Computers > Web Reputation**.

Web Threats

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, Web threat creators constantly change the version or variant used. Because the Web threat is in a fixed location of a Web site rather than on an infected computer, the Web threat creator constantly modifies its code to avoid detection.

Reputation Score

A URL's "reputation score" determines whether it is a Web threat or not. Trend Micro calculates the score using proprietary metrics.

- Trend Micro considers a URL "a Web threat", "very likely to be a Web threat", or "likely to be a Web threat" if its score falls within the range set for one of these categories.
- Trend Micro considers a URL safe to access if its score exceeds a defined threshold.

Security Levels

There are four security levels that determine whether OfficeScan will allow or block access to a URL.

- **High:** Blocks URLs that are unrated, a Web threat, very likely to be a Web threat, or likely to be a Web threat
- **Medium:** Blocks URLs that are unrated, a Web threat, or very likely to be a Web threat
- **Medium-low:** Blocks URLs that are a Web threat or very likely to be a Web threat
- **Low:** Blocks only URLs that are a Web threat

For example, if you set the security level to Low, OfficeScan only blocks URLs considered a "Web threat". Remember that as you set the security level higher, the Web threat detection rate improves but the possibility of false positives also increases.

The security levels are eventually referenced by Web Reputation policies.

Web Reputation Policies and Computer Location

In many organizations, employees use both desktop and notebook computers to perform their tasks. Since notebook computers connect to multiple networks and employees physically carry them past the organization's gateway, OfficeScan needs to extend Web threat protection to them even when they disconnect from your network. Web Reputation policies ensure client computer protection regardless of location.

OfficeScan checks a client computer’s gateway IP address to determine its location and then applies a specific Web Reputation policy to the computer. OfficeScan considers a computer "internal" if its gateway IP address matches any of the IP addresses you specify in the Computer Location screen on the Web console, and "external" if otherwise.

Trend Micro recommends enforcing a stricter policy on external computers. Trend Micro also recommends disabling Web Reputation for internal computers if you already use a Trend Micro product with Web Reputation capability (such as InterScan Gateway Security Appliance and InterScan Web Security Appliance).

Approved URLs

Approved URLs bypass Web Reputation policies; OfficeScan does not block these URLs even if the Web Reputation policy is set to block them. Add URLs that you consider safe to the approved URL list.

Web Reputation Logs

You can allow clients on both internal and external computers to send Web Reputation logs to the server. Do this if you want to analyze URLs that OfficeScan blocks and take appropriate action on URLs you think are safe to access.

Chapter 3

Managing Networked Computers

Topics in this chapter:

OfficeScan Firewall

The OfficeScan firewall uses policies, exceptions, and profiles to organize and customize methods for protecting networked computers. For an overview of the OfficeScan firewall, see *OfficeScan Firewall* on page 1-7.

Note: Trend Micro recommends uninstalling other software-based firewall applications on OfficeScan clients before deploying and enabling OfficeScan firewall. Multiple vendor firewall installations on the same computer may produce unexpected results.

The following steps are necessary to successfully use the OfficeScan firewall:

1. **Create a policy:** The policy allows you to select a security level that blocks or allows traffic on networked computers and enables firewall functions.
2. **Add exceptions to the policy:** Exceptions allow clients to deviate from a policy. With exceptions, you can specify clients, and allow or block certain types of traffic, despite the security level setting in the policy. For example, you can block all traffic for a set of clients in a policy, but create an exception that allows HTTP traffic so clients can access a Web server.
3. **Create and assign profiles to clients:** The firewall profile includes a set of client attributes. Each profile is associated with a policy. When a client matches the attributes specified in the profile, the associated policy is triggered.

Policies

You can configure firewall policies and exceptions in **Networked Computers > Firewall > Policies**.

Policies include the following:

- **Security level:** A general setting that blocks or allows all inbound and/or all outbound traffic on the client computer
- **Firewall features:** Enable/Disable the OfficeScan firewall, the Intrusion Detection System (IDS), and the firewall violation notification message. See *Intrusion Detection System* on page 1-8 for more information on IDS.

- **Policy exception list:** A list of configurable exceptions to block or allow various types of network traffic

Policy Exceptions

Exceptions include more specific settings to allow or block different kinds of traffic based on client computer port number(s) and IP address(es). You can configure a list of exceptions to associate with each policy. The exceptions in the list override the **Security level** setting in a policy.

Types of firewall policy exception

- **Restrictive:** Blocks only specified types of network traffic and applies to policies that allow all network traffic. An example use of a restrictive policy exception is blocking client ports commonly vulnerable to attack, such as ports that Trojan programs often use.
- **Permissive:** Allows only specified types of network traffic and applies to policies that block all network traffic. For example, you may want to permit clients to access only the OfficeScan server and a Web server. To do this, allow traffic from the trusted port (used to communicate with the OfficeScan server) and the port the client uses for HTTP communication.
  - Client listening port (trusted): **Networked Computers > Client Management > Status**. The port number is under **Basic Information**.
  - Server listening (trusted) port: **Administration > Connection Settings**. The port number is under **Connection Settings for Networked Computers**.

Firewall policy exception settings

- **Action:** Blocks or allows traffic that meets the exception criteria
- **Direction:** Inbound or outbound network traffic on the client computer
- **Protocol:** The type of traffic: TCP, UDP, ICMP
- **Port(s):** Ports on the client computer on which to perform the action
- **Client computer IP addresses:** The IP addresses of computers on the network to which the traffic criteria apply

Firewall policy exception template editor

You can edit exceptions in the Exception Template Editor and apply them to all existing policies or you can edit exceptions that apply to an individual policy.

Configuring exceptions: an example

During an outbreak you may choose to block all client traffic, including the HTTP port (port 80). However, if you still want to grant the blocked clients access to the Internet, you can add the Web proxy server to the exception list.

Profiles

You can configure firewall profiles and alternate servers in **Networked Computers > Firewall > Profiles**.

Firewall profiles provide flexibility by allowing you to choose the attributes that a client or group of clients must have before applying a policy. Profiles include the following:

- **Associated policy:** Each profile uses a single policy
- **Client attributes:** Clients with the following attributes apply the associated policy:
  - **IP address:** A client that has a specific IP address, an IP address that fall within a range of IP addresses, or an IP address belonging to a specified subnet
  - **Domain:** A client that belongs to a certain OfficeScan domain
  - **Computer:** A client with a specific computer name
  - **Platform:** A client running a specific platform
  - **Logon name:** Clients to which specified users have logged on
  - **Client status:** If a client is online or offline

  Select any combination of client attributes to specify client computers.

- **User privileges:** Allow or prevent client users from doing the following:
  - Changing the security level specified in a policy
  - Editing the exception list associated with a policy

Note: These privileges apply only to clients that match the attributes specified in the profile. You can assign other firewall privileges to selected client users by going to **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab. See *Firewall Privileges on page 3-8* for more information.

OfficeScan applies OfficeScan firewall profiles to clients in the order in which the profiles appear in the profile list. For example, if a client matches the first profile, OfficeScan applies to the client the actions configured for that profile. OfficeScan ignores the other profiles configured for that client.

The more exclusive a policy, the more you need to position it at the top of the list. For example, policies you create for a single client should be at the top, followed by those for a range of clients, a network domain, and all clients.

Alternate servers

You can edit the list of alternate servers, which are computers that act as substitutes for the OfficeScan server when it applies firewall profiles. An alternate server can be any computer on your network.

OfficeScan makes the following assumptions when you enable alternate servers:

- Clients connected to alternate servers are online, even if the clients cannot communicate with the OfficeScan server.
- Firewall profiles applied to online clients also apply to clients connected to alternate servers.

Default Settings

OfficeScan firewall provides default policies, exceptions, and profiles to give you a basis for initiating your client firewall protection strategy. The default settings include common conditions that may exist on your clients, such as installations for the Cisco NAC Trust Agent and the need to access the ScanMail for Microsoft Exchange Web console.

TABLE 3-1. Default firewall policies

Policy Name	Security Level	Client settings	Exceptions	Recommended use
All access	Low	Enable firewall	None	Use to allow clients unrestricted access to the network
Cisco Trust Agent for Cisco NAC	Low	Enable firewall	Allow incoming/ outgoing UDP traffic through port 21862	Use when clients have a Cisco Trust Agent (CTA) installation
Communication Ports for TMCM	Low	Enable firewall	Allow all incoming/outgoing TCP/UDP traffic through ports 80 and 10319	Use when clients have an MCP agent installation
ScanMail for Microsoft Exchange (SMEX) console	Low	Enable firewall	Allow all incoming/outgoing TCP traffic through port 16372	Use when clients need to access the SMEX console
InterScan Messaging Security Suite (IMSS) console	Low	Enable firewall	Allow all incoming/outgoing TCP traffic through port 80	Use when clients need to access the IMSS console

TABLE 3-2. Default firewall policy exceptions

Exception Name	Action	Protocol	Port	Direction
DNS	Allow	TCP/UDP	53	Incoming and outgoing
NetBIOS	Allow	TCP/UDP	137,138,139,445	Incoming and outgoing
HTTPS	Allow	TCP	443	Incoming and outgoing
HTTP	Allow	TCP	80	Incoming and outgoing
Telnet	Allow	TCP	23	Incoming and outgoing
SMTP	Allow	TCP	25	Incoming and outgoing
FTP	Allow	TCP	21	Incoming and outgoing
POP3	Allow	TCP	110	Incoming and outgoing

Note: None of the default exceptions specify clients. If you use any of the default exceptions, specify the clients to which you want the exceptions to apply.

TABLE 3-3. Default firewall profile

Profile Name	Policy used	Applied to clients
All clients profile	All access	Unspecified

Firewall Privileges

Go to **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab to grant client users the privilege to do the following:

- View the Firewall tab in the client console
- **Enable/Disable the OfficeScan firewall, the Intrusion Detection System, and the firewall violation notification message:** You cannot override user-specified settings from the OfficeScan server Web console.

  If you do not enable the features, the firewall settings you configure from the OfficeScan server Web console display under **Network card list** on the client console.
- **Allow clients to send firewall logs to the OfficeScan server:** If you select this option, configure the log sending schedule in **Networked Computers > Global Client Settings**. The schedule only applies to clients with firewall log sending privilege.

Firewall Testing

To help ensure that the OfficeScan firewall works properly, perform a test on a client or group of clients. See the online help for the testing procedure.

WARNING! *Test OfficeScan client program settings in a controlled environment only. Do not perform tests on client computers connected to your network or to the Internet. Doing so may expose client computers to viruses, hacker attacks, and other risks.*

Firewall: How to Disable

Use the OfficeScan Web console to disable the OfficeScan firewall on clients. You need to create a new policy that does not enable the firewall and then apply the policy to clients. See the online help for the procedure.

You can also disable the firewall for all clients by deactivating it in the **Administration > Product License** screen.

Outbreak Protection

OfficeScan provides several methods to manage outbreaks on your network. These include enabling OfficeScan to monitor the network for suspicious activity, blocking critical client computer ports and folders, sending outbreak alert messages to clients, and cleaning up infected computers.

Outbreak Prevention

Use Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients.

WARNING! *Configure the Outbreak Prevention settings carefully during an outbreak. Incorrect configuration may cause unforeseen network issues.*

Once you enable Outbreak Prevention, verify that a green check mark appears in the **OPP** column of the selected clients on the client tree.

After disabling outbreak prevention, scan your networked computers for security risks to ensure that the outbreak has been contained.

Outbreak Prevention Policies

Limit/Deny access to shared folders

You can either allow read-only or deny full access to shared folders on your network to prevent security risks from spreading through the shared folders.

Block ports

During outbreaks, you can block vulnerable ports that viruses/malware might use to gain access to client computers.

WARNING! *Configure Outbreak Prevention settings carefully. Blocking ports that are in use makes network services that depend on them unavailable. For example, if you block the trusted port, OfficeScan cannot communicate with the client for the duration of the outbreak.*

You can modify the following settings of entries on the **Port Blocking Settings** list:

- **Traffic direction:** Block incoming and/or outgoing traffic
- **Port number:** Modify the number of any port or enter a range of ports for each entry in the list
- **Traffic protocol:** Specify TCP, UDP or both
- **Comments:** Add any comments to describe the entry on the list

Deny write access to files and folders

Viruses/Malware can modify or delete files and folders on the host computers. You can configure OfficeScan to prevent viruses/malware from modifying or deleting files and folders on client computers during an outbreak.

Post-outbreak Task

When you are confident that an outbreak has been contained and that OfficeScan already cleaned or quarantined all infected files, you can restore your network settings to normal by disabling Outbreak Prevention.

If you do not restore your network settings manually, OfficeScan automatically restores these settings after the number of hours specified in **Automatically restore network settings to normal after { } hours** on the Outbreak Prevention Settings screen. The default setting is 48 hours.

Client Notifications

Configure client user notifications to inform or remind users about events that require their attention (such as security risk detection), and instruct them how to perform the necessary actions.

Security Risk Notifications

OfficeScan can display notification messages on selected client computers to inform users of security risks detected on the computer. The messages display immediately after the following instances:

- Real-time Scan and Scheduled Scan detect virus/malware and spyware/grayware.
- The OfficeScan firewall detects a firewall policy violation.
- OfficeScan blocks a URL that violates a Web Reputation policy.

You can modify the default messages for the different security risks by clicking the tabs in the **Notifications > Client User Notifications** screen and entering the new messages in the text boxes provided.

Note: For information about the notifications that OfficeScan can send to you and other OfficeScan administrators, see *Administrator Notifications* on page 4-7.

Virus/Malware notification

- Clients only display the virus/malware notification message if configured to do so. You can configure this setting in **Networked Computers > Client Management > Settings > {Real-time or Scheduled Scan Settings} > Action** tab. Only the clients you selected in the client tree (when you click **Networked Computers > Client Management**) will display the message.

- You can choose to display a notification message if a virus/malware originated from the client user's computer. To do so, go to **Notifications > Client User Notifications > Virus/Malware** tab. Select the check box under Virus/Malware Infection Source, specify an interval for sending notifications and optionally modify the default notification message. This notification message displays only if you enable Windows Messenger Service. You can check the status of this service in the Services screen (**Control Panel > Administrative Tools > Services > Messenger**).

Spyware/Grayware notification

Clients only display the spyware/grayware notification message if configured to do so. You can configure this setting in **Networked Computers > Client Management > Settings > {Real-time or Scheduled Scan Settings} > Action** tab. Only the clients you selected in the client tree (when you click **Networked Computers > Client Management**) display the message.

Firewall violation notification

Clients only display the firewall violation notification message if configured to do so and if outbound traffic violates the firewall settings. You can configure this setting in **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab.

Web Reputation notification

Clients only display the Web Reputation notification message if configured to do so. You can configure this setting in **Networked Computers > Client Management > Settings > Privileges and Other Settings > Other Settings** tab. Only the clients you selected in the client tree (when you click **Networked Computers > Client Management**) display the message.

After the notification message displays, another message displays in the client computer's browser, informing users to report the URL to the OfficeScan administrator if they think the URL is safe to access.

Other Notifications

OfficeScan can also display notifications during the following instances. Enable these notifications by going to **Networked Computers > Global Client Settings**.

- If the Virus Pattern remains outdated after a certain number of days
- If client users need to restart their computers to load a kernel mode driver

  After installing a hot fix or an upgrade package that contains a new version of a kernel mode driver, the driver's previous version may still exist on the computer. The only way to unload the previous version and load the new one is to restart the computer. After restarting the computer, the new version automatically installs and no further restart is necessary.

  The notification message displays on the client computer after installing the hot fix or upgrade package.

Client-Server Connection Verification

OfficeScan represents the client connection status in the client tree using icons. However, certain conditions may prevent the client tree from displaying the correct client connection status. For example, if you accidentally unplug the network cable of a client computer, the client will not be able to notify the server that it is now offline. This client will still appear as online in the client tree.

You can verify client-server connection manually or by schedule by going to **Networked Computers > Connection Verification**.

Note: You cannot select specific domains or clients and then verify their connection status. OfficeScan verifies the connection status of all its registered clients.

Check the client tree again to verify the client connection status or view the connection verification logs in **Logs > Networked Computer Logs > Connection Verification**.

Client Privileges and Other Settings

Configure privileges and other settings specific to certain clients in **Networked Computers > Client Management > Settings > Privileges and Other Settings**.

TABLE 3-4. Privileges and settings for selected clients

Setting	Description
PRIVILEGES	
Roaming privilege	Allow clients to be on roaming mode. See *Roaming clients* on page 1-14 for details.
Antivirus, Anti-spyware Scheduled Scan and Mail Scan privileges	Allows client users to configure their own scan settings. See *Scan Privileges* on page 2-35 for details.
Firewall privileges	See *Firewall Privileges* on page 3-8 for details.
Toolbox privilege	Displays the **Toolbox** tab on the client console. The Toolbox tab allows users to install Check Point SecureClient Support. OfficeScan provides a tool that allows Check Point SecureClient to check if the client Virus Pattern and Virus Scan Engine are current.
Proxy setting privilege	Allows client users to configure proxy settings. OfficeScan uses user-configure proxy settings only on the following instances: • When clients perform "Update Now". See *Client update methods* on page 2-14 for information on the "Update Now" feature. • When users disable, or OfficeScan cannot detect, automatic proxy settings. See *Proxy configuration* on page 3-18 for more information.
Component update privileges	Allows client users to configure their own component update settings. See *Other settings* on page 2-19 for details.

TABLE 3-4. Privileges and settings for selected clients

Setting	Description
Client uninstallation	Allows users to uninstall the OfficeScan client with or without a password To initiate silent client uninstallation from the Web console, go to **Networked Computers > Client Management > Tasks > Client Uninstallation**.
Client unload	Allows users to temporarily stop the OfficeScan client with or without a password
OTHER SETTINGS	
Update settings	See *Other settings* on page 2-19 for details.
Web Reputation settings	Displays a notification message on the client computer if OfficeScan blocks a URL that violates a Web Reputation policy
Client security	Allows or restricts users from accessing OfficeScan client files and registries If you select High, the access permission settings of the OfficeScan folders, files, and registries will be the same as the Program Files folder settings of client computers running Windows 2000/XP/Server 2003. Therefore, if the permissions settings (Security settings in Windows) of the Program Files folder are set to allow full read/write access, selecting High still allows users full read/write access to the OfficeScan client folders, files, and registries.
Client console access restriction	Users are not able to access the client console from the system tray or Windows Start menu but can do so from the OfficeScan client installation folder. OfficeScan runs in the background and continues to provide protection from security risks.

Global Client Settings

OfficeScan applies global client settings to all clients or only to clients with certain privileges. Configure global client settings in **Networked Computers > Global Client Settings**.

TABLE 3-5. Global client settings

Setting	Description
Virus/Malware scan settings	See *Global virus/malware scan settings* on page 2-26 for details.
Spyware/Grayware scan settings	See *Global spyware/grayware scan settings* on page 2-33 for details.
Firewall log settings	You can grant certain clients the privilege to send firewall logs to the OfficeScan server. You can configure the log sending schedule in this section. Only clients with the privilege to send firewall logs will use the schedule. See *Firewall Privileges* on page 3-8 for information on firewall privileges that you can grant selected clients.
Alert settings	See *Other Notifications* on page 3-13 for details.

TABLE 3-5. Global client settings

Setting	Description
Reserved disk space and Watchdog settings	• **Watchdog service:** Restarts the OfficeScan client immediately if it terminates unexpectedly, which may happen if the client is under attack by a hacker. Malicious programs known as retro-viruses, like WORM_KLEZ.h, retaliate against antivirus solutions by shutting down key antivirus processes and deleting some files used by an antivirus solution. This enables them to infect using an old virus, hence the name "retro-virus". The OfficeScan Watchdog service (OfcDog.exe) protects the status of the OfficeScan client by doing the following: • Monitoring the status of NT Real-time Scan (NtRtScan.exe) and OfficeScan NT Listener (TmListen.exe). If these OfficeScan processes are not running and not stopped by a normal system process, the Watchdog service restarts them. It also writes an event log on the client computer and sends the log to the server. • Locking all .exe and .dll files in the OfficeScan client directory to prevent other programs and even the user from modifying or deleting them. The Watchdog service is, by default, randomly named to help prevent other programs from terminating it. • **Anti-hacking mode:** Gives the Watchdog service a random name. This helps prevent any security risk from identifying the service and terminating it. • **Reserve { } MB of disk space for updates:** Allocates a certain amount of client disk space for hot fixes, pattern files, scan engines, and program updates. OfficeScan reserves 60MB of space by default.
Network virus log consolidation	Clients send only network virus logs once every hour. For more information about network viruses, see *Viruses and Malware* on page 1-23.

TABLE 3-5. Global client settings

Setting	Description
Virus/Malware log bandwidth setting	OfficeScan consolidates virus log entries when detecting multiple infections from the same virus/malware over a short period of time. OfficeScan may detect a single virus/malware multiple times, quickly filling the virus/malware log and consuming network bandwidth when the client sends log information to the server. Enabling this feature helps reduce both the number of virus/malware log entries made and the amount of network bandwidth clients consume when they report virus log information to the server.
Proxy configuration	Manually configuring proxy settings may be a complicated task for many end users. Use automatic proxy settings to ensure that correct proxy settings are applied without requiring any user intervention. When enabled, automatic proxy settings are the primary proxy settings when clients update components either through automatic update or Update Now. For information on automatic update and Update Now, see *Client update methods* on page 2-14. If clients cannot connect using the automatic proxy settings, client users with the privilege to configure proxy settings can use user-configured proxy settings. Otherwise, connection using the automatic proxy settings will fail. **Note:** Proxy authentication is not supported. • **Automatically detect settings:** Automatically detects the administrator-configured proxy settings by DHCP or DNS. • **Use automatic configuration script:** Uses the proxy auto-configuration (PAC) script set by the network administrator to detect the appropriate proxy server.
Client grouping	This option groups clients in the client tree by NetBIOS, Active Directory or DNS domain.

Client Settings Management

You may want many OfficeScan clients to have the same scan and/or client privilege settings. OfficeScan allows you to save (export) a specific client's scan settings and privileges and then replicate (import) them to multiple clients. This provides an easy way to configure identical settings on many clients.

You cannot export the scan and privilege settings of multiple clients. You can only export the settings of a single client, a domain, or the root.

To import and export settings, go to **Networked Computers > Client Management > Settings > {Import** or **Export} Settings**.

Cisco NAC

Trend Micro Policy Server for Cisco Network Admission Control (NAC) evaluates the status of antivirus components on OfficeScan clients. Policy Server configuration options give you the ability to configure settings to perform actions on at-risk clients to bring them into compliance with your organization's antivirus initiative.

These actions include the following:

- Instruct client computers to update their OfficeScan client components.
- Enable Real-time Scan.
- Perform Scan Now.
- Display a notification message on client computers to inform users of the antivirus policy violation.

To help you analyze the performance of your antivirus policies, view Policy Server logs, which record information such as the time the Policy Server evaluated clients and the result of the evaluations.

Note: For additional information on Cisco NAC technology, see the Cisco Web site at www.cisco.com/go/nac.

Cisco NAC is discussed in detail in the following chapters:

- *Understanding Policy Server for Cisco NAC* on page 5-1
- *Deploying Policy Server for Cisco NAC* on page 6-1

Chapter 4

Managing the OfficeScan Server

Topics in this chapter:

Trend Micro Control Manager

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services, third-party antivirus and content security products at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for managed products and services throughout the network.

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

See *Managing OfficeScan Using Control Manager* on page 7-1 for more information.

Logs

OfficeScan keeps comprehensive logs about security risk detections, events, and updates. Use these logs to assess your organization's protection policies and to identify clients at a higher risk of infection or attack. Also use these logs to check client-server connection and verify if component update is successful or not.

Networked Computer Logs

Security risk logs

Security risks include virus/malware, spyware/grayware, firewall violations and Web threats.

For spyware/grayware logs, you can add detected spyware/grayware to the approved list if you consider them safe. For more information on the approved list, see *Spyware/Grayware approved list* on page 2-33.

For firewall violation logs, you have the option to first notify clients to send the logs to the server to ensure that the most up-to-date logs are available to you. OfficeScan clients that have OfficeScan firewall enabled store firewall events in a log on the client computer. View these logs to analyze OfficeScan firewall performance.

Component update logs

OfficeScan clients send virus pattern update logs to the server. In the Component Update Progress screen, you can view the number of clients updated for every 15-minute interval and the total number of clients updated.

Connection verification logs

OfficeScan keeps connection verification logs to allow you to determine whether or not the OfficeScan server can communicate with all of its registered clients. OfficeScan creates a log entry each time you verify client-server connection from the Web console. See *Client-Server Connection Verification* on page 3-13.

Spyware/Grayware restore logs

After cleaning spyware/grayware, OfficeScan clients back up spyware/grayware data, which the OfficeScan server can restore anytime if you consider the spyware/grayware safe. Spyware/Grayware logs show you the restore result.

Server Update Logs

OfficeScan keeps logs for all events related to component updates on the OfficeScan server. View the logs to verify that OfficeScan successfully downloaded the components required to keep your protection current.

System Event Logs

OfficeScan also records events related to the server program, such as shutdown and startup. Use these logs to verify that the OfficeScan server and services work properly.

OfficeScan logs the following events:

OfficeScan Master Service and Database Server:

- Master Service started
- Master Service stopped successfully
- Master Service stopped unsuccessfully
- Database Server restarted

Outbreak notifications for firewall violation and shared folder sessions:

- Log type (IDS logs, Firewall logs, Network Virus logs) exceeded
- Number of shared folder sessions in the last {number of minutes}

Database backup:

- Database backup successful
- Database backup failed
- Database backup cancelled

Log Deletion

To keep the size of your logs from occupying too much space on your hard disk, you can configure OfficeScan to delete logs manually or based on a schedule.

Licenses

You can view and renew OfficeScan product service licenses from the Web console. You can also activate a new service you wish to use.

If you activate the Antivirus service, you can enable/disable the OfficeScan firewall. The Antivirus service also includes support for Cisco NAC and outbreak prevention.

Note: You can enable the OfficeScan firewall during installation. If you disable firewall, OfficeScan hides all firewall functions in the server and client.

OfficeScan allows you to activate multiple licenses for a product service. View all the licenses (both active and expired) for a service from the Web console.

The status of your licenses appears at the top of the **Administration > Product License** screen. Reminders display during the following instances:

Full version

- 30 days before grace period ends
- When the license expires and grace period elapses

Note: During this time, you will not be able to obtain technical support and perform component update. The scan engines will still scan computers using out-of-date components. These out-of-date components may not be able to protect you completely from the latest security risks.

Evaluation (Trial) version

- When the license expires

Note: During this time, OfficeScan disables component updates, scanning, and all client features.

OfficeScan Database Backup

The OfficeScan server database contains all OfficeScan settings, including scan settings and privileges. If the server database becomes corrupted, you can easily restore it if you have a backup. You can back up the database manually at any time or configure a backup schedule.

When backing up the database, OfficeScan automatically helps defragment the database and repairs any possible index file corruption.

Tip: Trend Micro recommends configuring a schedule for automatic backup. Back up the database during non-peak hours when server traffic is low.

WARNING! *Do not perform the backup with any other tool or software. Configure database backup from the OfficeScan Web console only.*

To restore the database backup files:

1. Stop the OfficeScan Master Service.
2. Overwrite the database files in \PCCSRV\HTTPDB with the backup files.
3. Restart the OfficeScan Master Service.

OfficeScan Web Server Information

During OfficeScan server installation, the master Setup program automatically sets up a Web server (IIS or Apache Web server) that enables networked computers to connect to the OfficeScan server. You can configure the Web server to which both networked computer clients will connect.

If you modify the Web server settings externally (for example, from the IIS management console), you must also make the changes in OfficeScan to ensure it maintains server-client communication and that you can still gain access to the Web console. For example, if you change the IP address of the server for networked computers manually or if you assign a dynamic IP address to it, you need to reconfigure the server settings of OfficeScan.

Administrator Notifications

OfficeScan can notify you and other OfficeScan administrators in your organization whenever it detects a security risk on any client or during a security risk outbreak. Configure notification settings in **Notifications > Administrator Notifications**.

Note: To configure notification settings that display on client computers, see *Client Notifications* on page 3-11.

OfficeScan sends notifications through the following:

- Email
- Pager
- SNMP trap
- Windows NT Event Log

Standard Notifications

OfficeScan comes with a set of default notification messages that you and other administrators receive whenever it detects virus/malware or spyware/grayware on client computers. Modify these messages to suit your requirements.

Configure OfficeScan to send a notification when it detects a security risk, or only when the action on the security risk is unsuccessful and therefore requires your intervention.

Outbreak Notifications

Configure OfficeScan to notify you and other OfficeScan administrators of security risk outbreaks on your network. Define the outbreak criteria based on the number of security risk detections and the detection period. OfficeScan sends the notification when the number of detections is exceeded during the detection period. For example if you specify 100 as the number of detections, OfficeScan sends the notification after it detects the 101st instance of a virus/malware.

Responding to an outbreak is very critical. Unless you take corrective action, an outbreak can spread quickly throughout and beyond your network.

Web Console Password

The Web console is password-protected to prevent unauthorized users from modifying OfficeScan settings or removing the client program from networked computers. During installation, the OfficeScan Setup program requires you to specify a Web console password; however, you can modify your password from the Web console by going to **Administration > Console Password**.

If you forget the console password, contact Trend Micro technical support for instructions on how to gain access to the Web console. The only other alternative is to uninstall and reinstall OfficeScan.

Inactive Clients

When you use the client uninstallation program to remove the client program from a computer, the program automatically notifies the server. When the server receives this notification, it removes the client icon in the client tree to show that the client does not exist anymore.

However, if you use other methods to remove the client, such as reformatting the computer hard drive or deleting the client files manually, OfficeScan will not be aware of the removal and it will display the client as inactive. If a user unloads or disables the client for an extended period of time, the server also displays the client as inactive.

To have the client tree display active clients only, you can configure OfficeScan to automatically remove inactive clients from the client tree.

Quarantine Manager

Whenever the OfficeScan client detects a security risk and the scan action is quarantine, it encrypts the infected file, moves it to the local quarantine folder, and then sends it to the OfficeScan server. The server also encrypts the infected file to prevent it from infecting other files.

Default locations of the quarantine folder:

Client: {OfficeScan installation folder}\OfficeScan Client\SUSPECT

Server: {OfficeScan installation folder}\OfficeScan\PCCSRV\Virus

The default OfficeScan installation folder is C:\Program Files\Trend Micro.

Note: If the OfficeScan client is unable to send the encrypted file to the OfficeScan server for any reason, such as a network connection problem, the encrypted file remains in the client quarantine folder. The client will attempt to resend the file when it connects to the OfficeScan server.

You can configure the capacity of the quarantine folder and the maximum file size of an infected file for quarantine. For more information, see *Additional virus/malware scan action options* on page 2-30.

Administrative and Client Tools

OfficeScan includes a set of tools to accomplish various OfficeScan tasks, including server configuration and client management.

There are two types of OfficeScan tools. Please note that you cannot run any of these tools from the Web console. For detailed information about these tools and how to use them, see the online help.

- **Administrative tools:** Developed to help you configure the server and manage clients
  - **Login Script Setup:** Automates the installation of the OfficeScan client to unprotected computers when they log on to the network
  - **Vulnerability Scanner:** Detects installed antivirus solutions and searches for unprotected computers on your network

    - **Server Tuner:** Optimizes the performance of OfficeScan servers
- **Client tools:** Developed to help enhance the performance of the client program
    - **Client Packager:** Compresses OfficeScan client Setup and update files into a self-extracting file to simplify the delivery to clients using email, CD-ROM, or similar media
    - **Image Setup Utility:** Creates an image of an OfficeScan client and makes clones of it to other computers on your network
    - **Restore Encrypted Files:** Unencrypts an infected file that OfficeScan encrypted to retrieve necessary information from the file
    - **Client Mover:** If you have more than one OfficeScan server on the network, transfers clients from one OfficeScan server to another
    - **Touch Tool:** Synchronizes the time stamp of one file with the time stamp of another file or with the system time of the computer
    - **ServerProtect Normal Server Migration Tool:** Migrates the ServerProtect™ Normal Server program to the OfficeScan client

Note: Some tools available in previous versions of OfficeScan are not available in this version. Please contact your support provider if you need to use a specific tool not listed above.

The World Virus Tracking Program

You can send security risk scanning results to the World Virus Tracking Program to better track trends in security risk outbreaks. Your participation in this program can benefit the attempt to better understand the development and spread of security risks.

When you installed OfficeScan, the OfficeScan installer asks you whether or not you want to participate in the World Virus Tracking Program. You can change the setting from the Web console anytime.

To view the current Trend Micro virus map, visit http://www.trendmicro.com/map.

Chapter 5

Understanding Policy Server for Cisco NAC

Topics in this chapter:

Components and Terms

The following is a list of the various components and the important terms you need to become familiar with to understand and use Policy Server for Cisco NAC.

Components

The following components are necessary in the Trend Micro implementation of Policy Server for Cisco NAC:

TABLE 5-1. Policy Server for Cisco NAC components

Component	Description
Cisco Trust Agent (CTA)	A program installed on a client computer that allows it to communicate with other Cisco NAC components
OfficeScan client computer	A computer with the OfficeScan client program installed. To work with Cisco NAC, the client computer also requires the Cisco Trust Agent.
Network Access Device	A network device that supports Cisco NAC functionality. Supported Network Access Devices include a range of Cisco routers, firewalls, and access points, as well as third-party devices with Terminal Access Controller Access Control System (TACACS+) or the Remote Dial-In User Service (RADIUS) protocol. For a list of supported devices, see *Supported Platforms and Requirements* on page 5-19.
Cisco Secure Access Control Server (ACS)	A server that receives OfficeScan client antivirus data from the client through the Network Access Device and passes it to an external user database for evaluation. Later in the process, the ACS server also passes the result of the evaluation, which may include instructions for the OfficeScan client, to the Network Access Device.
Policy Server	A program that receives and evaluates OfficeScan client antivirus data. After performing the evaluation, the Policy Server determines the actions the OfficeScan client should carry out and then notifies the client to perform the actions.
OfficeScan server	Reports the current Virus Pattern and Virus Scan Engine versions to the Policy Server, which uses this information to evaluate the OfficeScan client's antivirus status.

Terms

Become familiar with the following terms related to Policy Server for Cisco NAC:

TABLE 5-2. Terms related to Policy Server for Cisco NAC

Term	Definition
Security posture	The presence and currency of antivirus software on a client. In this implementation, security posture refers to whether or not the OfficeScan client program exists on client computers, the status of certain OfficeScan client settings, and whether or not the Virus Scan Engine and Virus Pattern are up-to-date.
Posture token	Created by the Policy Server after OfficeScan client validation. It includes information that tells the OfficeScan client to perform a set of specified actions, such as enabling Real-time Scan or updating antivirus components.
Client validation	The process of evaluating client security posture and returning the posture token to the client
Policy Server rule	Guidelines containing configurable criteria the Policy Server uses to measure OfficeScan client security posture. A rule also contains actions for the client and the Policy Server to carry out if the security posture information matches the criteria (see *Policy Server Policies and Rules* on page 5-9 for detailed information).
Policy Server policy	A set of rules against which the Policy Server measures the security posture of OfficeScan clients. Policies also contain actions for clients and the Policy Server to carry out if the criteria in the rules associated with the policy do not match the security posture (see *Policy Server Policies and Rules* on page 5-9 for detailed information).
Authentication, Authorization, and Accounting (AAA)	Describes the three main services used to control end-user client access to computer resources. Authentication refers to identifying a client, usually by having the user enter a user name and password. Authorization refers to the privileges the user has to issue certain commands. Accounting refers to a measurement, usually kept in logs, of the resources utilized during a session. The Cisco Secure Access Control Server (ACS) is the Cisco implementation of an AAA server.

TABLE 5-2. Terms related to Policy Server for Cisco NAC

Term	Definition
Certificate Authority (CA)	An authority on a network that distributes digital certificates for the purposes of performing authentication and securing connections between computers and/or servers.
Digital Certificates	An attachment used for security. Most commonly, certificates authenticate clients with servers, such as a Web server, and contain the following: user identity information, a public key (used for encryption), and a digital signature of a Certificate authority (CA) to verify that the certificate is valid.
Remote Authentication Dial-In User Service (RADIUS)	An authentication system requiring clients to enter a user name and password. Cisco Secure ACS servers support RADIUS.
Terminal Access Controller Access Control System (TACACS+)	A security protocol enabled through AAA commands used for authenticating end-user clients. Cisco ACS servers support TACACS+.

Cisco NAC Architecture

Figure 5-1 illustrates a basic Cisco NAC architecture with the components described above.

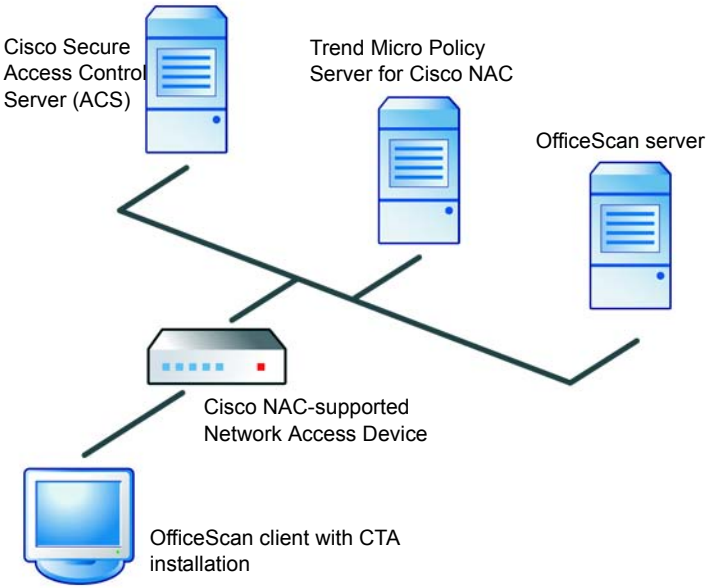


FIGURE 5-1 Basic Cisco NAC architecture

The OfficeScan client in Figure 5-1 has a CTA installation and is only able to access the network through a Network Access Device that supports Cisco NAC. The Network Access Device is between the client and the other Cisco NAC components.

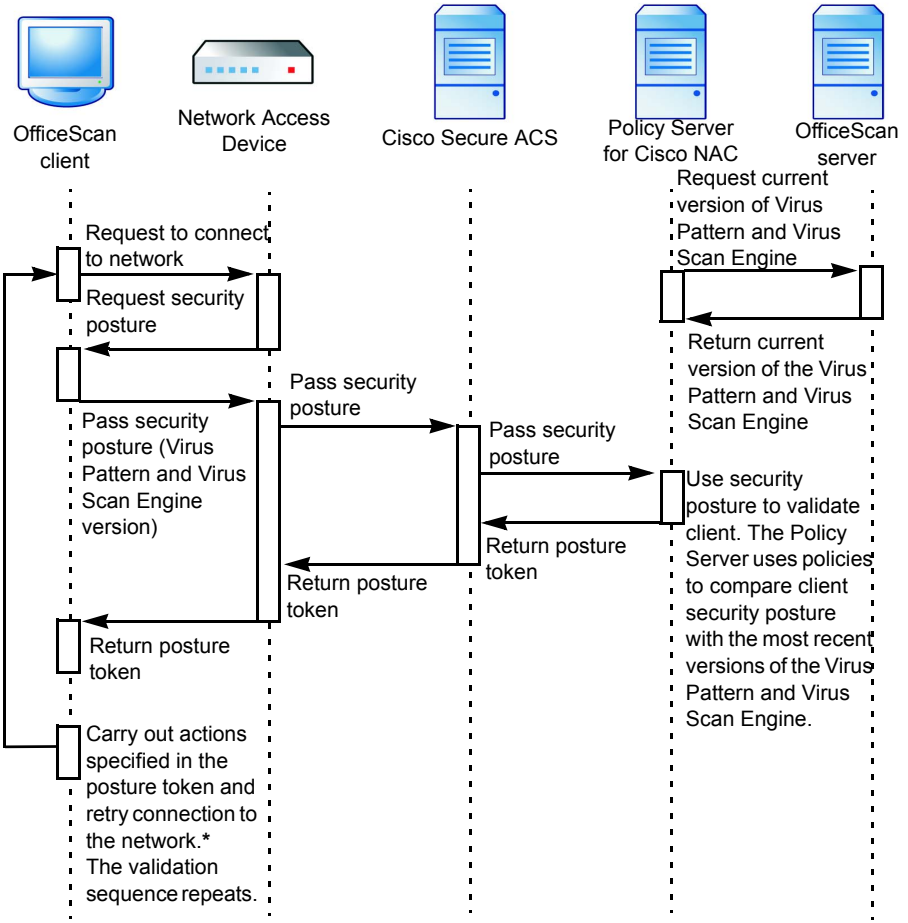
Note: The architecture of your network may differ based on the presence of proxy servers, routers, or firewalls.

The Client Validation Sequence

Client validation refers to the process of evaluating an OfficeScan client's security posture and returning instructions for the client to perform if the Policy Server considers it to be at-risk. The Policy Server validates an OfficeScan client by using configurable rules and policies.

Figure 5-2 illustrates the sequence of events that occurs when an OfficeScan client attempts to access the network:

1. The Cisco Network Access Device starts the validation sequence by requesting the security posture of the client when it attempts to access the network.
2. The Network Access Device then passes the security posture to the ACS server.
3. The ACS server passes the security posture to the Policy Server, which performs the evaluation.
4. In a separate process, the Policy Server periodically polls the OfficeScan server for Virus Pattern and Virus Scan Engine version information to keep its data current. It then uses a policy you configure to perform a comparison of this information with the client security posture data.
5. Following that, the Policy Server creates a posture token, and passes it back to the OfficeScan client.
6. Finally, the client performs the actions configured in the posture token.



* The client retries to access the network when the Network Access Device timer expires. See your Cisco router documentation for information on configuring the timer.

FIGURE 5-2 Network access validation sequence

The Policy Server

The Policy Server is responsible for evaluating the OfficeScan client's security posture and for creating the posture token. It compares the security posture with the latest versions of the Virus Pattern and Virus Scan Engine received from the OfficeScan server to which the client is a member. It returns the posture token to the Cisco Secure ACS server, which in turn passes it to the client from the Cisco Network Access Device.

Installing additional Policy Servers on a single network can improve performance when a large number of clients simultaneously attempt to access the network. These Policy Servers can also act as a backup if a Policy Server becomes inoperable. If there are multiple OfficeScan servers on a network, the Policy Server handles requests for all OfficeScan servers registered to it. Likewise, multiple Policy Servers can handle requests for a single OfficeScan server registered to all the Policy Servers. Figure 5-3 illustrates the relationship of multiple OfficeScan servers and Policy Servers.

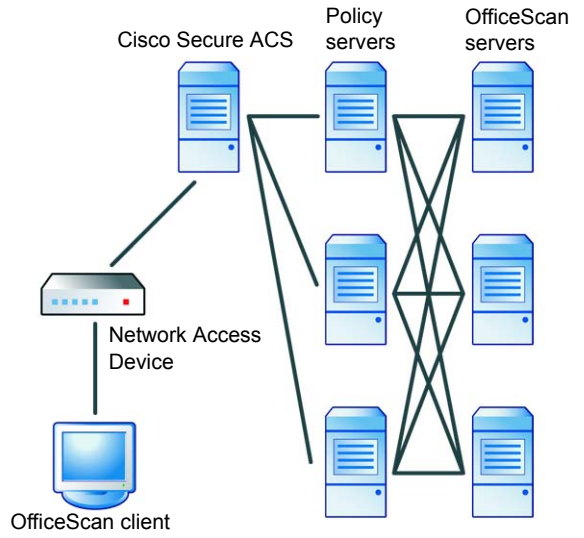


FIGURE 5-3 Multiple Policy Server/OfficeScan server relationship

You can also install the Policy Server on the same computer as the OfficeScan server.

Policy Server Policies and Rules

Policy Servers use configurable rules and policies to help enforce your organization's security guidelines.

Rules include specific criteria that Policy Servers use to compare with the security posture of OfficeScan clients. If the client security posture matches the criteria you configure in a rule, the client and server carry out the actions you specify in the rule (see *Policy Server and OfficeScan client actions* on page 5-11).

Policies include one or more rules. Assign one policy to each registered OfficeScan server on your network for both outbreak mode and normal mode (see *Outbreak Prevention* on page 3-9 for more information on network modes).

If the OfficeScan client security posture matches the criteria in a rule that belongs to the policy, the OfficeScan client carries out the actions you configure in the rule. However, if the client security posture does not match any of the criteria in any of the rules associated with the policy, you can still configure default actions in the policy for the client and server to carry out (see *Policy Server and OfficeScan client actions* on page 5-11).

Tip: If you want certain clients in an OfficeScan domain to have different outbreak and normal mode policies from other clients in the same domain, Trend Micro suggests restructuring the domains to group clients with similar requirement (see *OfficeScan Domains* on page 2-3).

Rule Composition

Rules include security posture criteria, default responses associated with clients, and actions that clients and the Policy Server perform.

Security posture criteria

Rules include the following security posture criteria:

- **Client machine state:** If the client computer is in the booting state or not
- **Client Real-time Scan status:** If Real-time Scan is enabled or disabled
- **Client scan engine version currency:** If the Virus Scan Engine is up-to-date
- **Client virus pattern file status:** How up-to-date the Virus Pattern is. The Policy Server determines this by checking one of the following:
  - If the Virus Pattern is a certain number of versions older than the Policy Server version
  - If the Virus Pattern became available a certain number of days prior to the validation

Default responses for rules

Responses help you understand the condition of OfficeScan clients on your network when client validation occurs. The responses, which appear in the Policy Server client validation logs, correspond to posture tokens. Choose from the following default responses:

- **Healthy:** The client computer conforms to your security policies and is not infected.
- **Checkup:** The client needs to update its antivirus components.
- **Infected:** The client computer is infected or is at risk of infection.
- **Transition:** The client computer is in the booting state.
- **Quarantine:** The client computer is at high risk of infection and requires quarantine.
- **Unknown:** Any other condition

Note: You cannot add, delete, or modify responses.

Policy Server and OfficeScan client actions

If the client security posture matches the rule criteria, the Policy Server can carry out the following action:

- Creates an entry in a Policy Server client validation log (see *Client Validation Logs* on page 6-19 for more information)

If the client security posture matches the rule criteria, the OfficeScan client can carry out the following actions:

- Enable client Real-time Scan so the OfficeScan client can scan all opened or saved files (see *Real-time Scan* on page 2-21 for more information)
- Update all OfficeScan components (see *Component Updates* on page 2-6 for more information)
- Scan the client (Scan Now) after enabling Real-time Scan or after an update
- Display a notification message on the client computer

Default Rules

Policy Server provides default rules to give you a basis for configuring settings. The rules cover common and recommended security posture conditions and actions. The following rules are available by default:

TABLE 5-3. Default rules

Rule Name	Matching Criteria	Response if Criteria Matched	Server Action	Client Action
Healthy	Real-time Scan status is enabled and Virus Scan Engine and Virus Pattern are up-to-date.	Healthy	None	None

TABLE 5-3. Default rules

Rule Name	Matching Criteria	Response if Criteria Matched	Server Action	Client Action
Checkup	Virus Pattern version is at least one version older than the version on the OfficeScan server to which the client is registered.	Checkup	Create entry in client validation log	• Update components • Perform automatic Cleanup Now on the client after enabling Real-time Scan or after an update • Display notification message on the client computer **Note:** If you use this rule, Trend Micro recommends using automatic deployment. This helps ensure that clients receive the latest Virus Pattern immediately after the OfficeScan downloads new components.
Transition	Client computer is in the booting state.	Transition	None	None
Quarantine	Virus Pattern version is at least five versions older than the version on the OfficeScan server to which the client is registered.	Quarantine	Create entry in client validation log	• Update components • Perform automatic Cleanup Now and Scan Now on the client after enabling Real-time Scan or after an update • Display notification message on the client computer

TABLE 5-3. Default rules

Rule Name	Matching Criteria	Response if Criteria Matched	Server Action	Client Action
Not protected	Real-time Scan status is disabled.	Infected	Create entry in client validation log	• Enable client Real-time Scan • Display notification message on the client computer

Policy Composition

Policies include of any number of rules and default responses and actions.

Rule enforcement

Policy Server enforces rules in a specific order, which allows you to prioritize your rules. You can change the order of rules, add new ones, and remove existing ones from a policy.

Default responses for policies

As with rules, policies include default responses to help you understand the condition of OfficeScan clients on your network when client validation occurs. However, the default responses are associated with clients only when client security posture does NOT match any rules in the policy.

The responses for policies are the same as those for rules (see *Default responses for rules* on page 5-10 for the list of responses).

Policy Server and OfficeScan client actions

The Policy Server enforces rules to clients by subjecting client posture information to each of the rules associated with a policy. Rules are applied in a top-down manner based on the rules in use specified on the Web console. If the client posture matches any of the rules, the action corresponding to the rule is deployed to the client. If no rules match, the default rule applies and the action corresponding to the default rule is deployed to clients.

Default Outbreak Mode Policy evaluates OfficeScan clients using the "Healthy" rule. It forces all clients that do not match this rule to immediately implement the actions for the "Infected" response.

Default Normal Mode Policy evaluates OfficeScan clients using all the non-"Healthy" rules (Transition, Not Protected, Quarantine, CheckUp). It classifies all clients that do not match any of these rules as "healthy" and applies the actions for the "Healthy" rule.

Default Policies

Policy Server provides default policies to give you a basis for configuring your settings. Two policies are available, one for normal mode and one for outbreak mode.

Policy name: Default Normal Mode Policy

- Default rules associated with policy: Transition, Not protected, Quarantine, and Checkup
- Response if none of the rules match: Healthy
- Server action: None
- Client action: None

Policy name: Default Outbreak Mode Policy

- Default rules associated with policy: Healthy
- Response if none of the rules match: Infected
- Server action: Create entry in client validation log
- Client action:
  - Enable client Real-time Scan
  - Update components
  - Perform Scan Now on the client after enabling Real-time Scan or after an update
  - Display a notification message on the client computer

Synchronization

Regularly synchronize the Policy Server with registered OfficeScan servers to keep the Policy Server versions of the Virus Pattern, Virus Scan Engine, and server outbreak status (normal mode or outbreak mode) up-to-date with those on the OfficeScan server. Use the following methods to perform synchronization:

- **Manually:** Perform synchronization at any time on the Summary screen (see *Summary Information for a Policy Server* on page 6-17).
- **By schedule:** Set a schedule to have OfficeScan perform synchronization (see *Administrative Tasks* on page 6-20).

Certificates

Cisco NAC technology uses the following digital certificates to establish successful communication between various components:

TABLE 5-4. Cisco NAC certificates

Certificate	Description
ACS certificate	Establishes trusted communication between the ACS server and the Certificate Authority (CA) server. The Certificate Authority server signs the ACS certificate before you save it on the ACS server.
CA certificate	Authenticates OfficeScan clients with the Cisco ACS server. The OfficeScan server deploys the CA certificate to both the ACS server and to OfficeScan clients (packaged with the Cisco Trust Agent).
Policy Server SSL certificate	Establishes secure HTTPS communication between the Policy Server and ACS server. The Policy Server installer automatically generates the Policy Server SSL certificate during Policy Server installation. **Note:** The Policy Server SSL certificate is optional. However, Trend Micro recommends using it to ensure that only encrypted data transmits between the Policy Server and ACS server.

Figure 5-4 illustrates the steps involved in creating and deploying ACS and CA certificates:

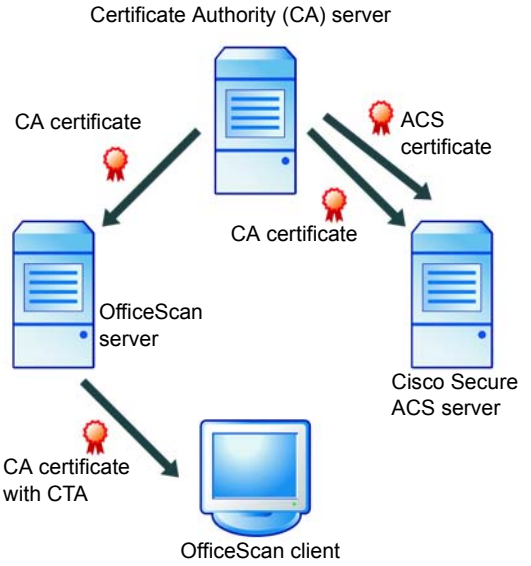


FIGURE 5-4 ACS and CA certificate creation and deployment

1. After the ACS server issues a certificate signing request to the CA server, the CA issues a certificate (the ACS certificate). The ACS certificate then installs on the ACS server. See *Cisco Secure ACS Server Enrolment* on page 6-3 for more information.
2. A CA certificate is exported from the CA server and installed on the ACS server. See *CA Certificate Installation* on page 6-3 for detailed instructions.
3. A copy of the same CA certificate is saved on the OfficeScan server.
4. The OfficeScan server deploys the CA certificate to clients with the CTA. See *Cisco Trust Agent Deployment* on page 6-8 for detailed instructions.

The CA Certificate

OfficeScan clients with CTA installations authenticate with the ACS server before communicating client security posture. Several methods are available for authentication (see your Cisco Secure ACS documentation for details). For example, you may already have enabled computer authentication for Cisco Secure ACS using Windows Active Directory, which you can configure to automatically produce an end user client certificate when adding a new computer in Active Directory. For instructions, see Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows.

For users with their own Certificate Authority (CA) server, but whose end user clients do not yet have certificates, OfficeScan provides a mechanism to distribute a root certificate to OfficeScan clients. Distribute the certificate during OfficeScan installation or from the OfficeScan Web Console. OfficeScan distributes the certificate when it deploys the Cisco Trust Agent to clients (see *Cisco Trust Agent Deployment* on page 6-8).

Note: If you already acquired a certificate from a Certificate Authority or produced your own certificate and distributed it to end user clients, it is not necessary to do so again.

Before distributing the certificate to clients, enroll the ACS server with the CA server and then prepare the certificate (see *Cisco Secure ACS Server Enrolment* on page 6-3).

Policy Server System Requirements

Before installing Policy Server, check if the computer meets the following requirements:

Operating System

- Microsoft Windows 2000 Professional (Service Pack 2 or above)
- Microsoft Windows 2000 Server (Service Pack 2 or above)
- Microsoft Windows 2000 Advanced Server (Service Pack 2 or above)

- Microsoft Windows XP Professional (Service Pack 1 or above)
- Microsoft Windows Server 2003 Standard
- Microsoft Windows Server 2003 Enterprise
- Microsoft Windows Cluster Server 2000

Hardware

- 300MHz Intel Pentium II processor or equivalent
- 128MB of RAM
- 300MB of available disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher

Web Server

- Microsoft Internet Information Server (IIS) versions 5.0 or 6.0
- Apache Web server 2.0 or later (for Windows 2000/XP/Server 2003 only)

Web Console

To use the OfficeScan server management (Web) console, the following are required:

- 133MHz Intel Pentium processor or equivalent
- 64MB of RAM
- 30MB of available disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft Internet Explorer 5.5 or later

Cisco Trust Agent (CTA) Requirements

Before deploying Cisco Trust Agent to client computers, check if the computers meet the following requirements:

Operating System

- Microsoft Windows NT 4.0
- Windows 2000 Professional and Server with Service Pack 4
- Windows XP Professional (up to Service Pack 2)
- Windows Server 2003

Hardware

- 200MHz single or multiple Intel Pentium processors
- 128MB of RAM for Windows NT and 2000
- 256MB of RAM for Windows XP and 2003
- 5MB of available disk space (20MB recommended)

Others

- Windows Installer 2.0 or later

Supported Platforms and Requirements

The following platforms support the Cisco NAC functionality:

TABLE 5-5. Supported platforms and requirements

Supported Platform	Models	IOS Images	Minimum Memory/Flash
Routers			
Cisco 830, 870 series	831, 836, 837	IOS 12.3(8) or later	48MB/8MB
Cisco 1700 series	1701, 1711, 1712, 1721, 1751, 1751-V, 1760	IOS 12.3(8) or later	64MB/16MB
Cisco 1800 series	1841	IOS 12.3(8) or later	128MB/32MB
Cisco 2600 series	2600XM, 2691	IOS 12.3(8) or later	96MB/32MB

TABLE 5-5. Supported platforms and requirements

Supported Platform	Models	IOS Images	Minimum Memory/Flash
Cisco 2800 series	2801, 2811, 2821, 2851	IOS 12.3(8) or later	128MB/64MB
Cisco 3600 series	3640/3640A, 3660-ENT series	IOS 12.3(8) or later	48MB/16MB
Cisco 3700 series	3745, 3725	IOS 12.3(8) or later	128MB/32MB
Cisco 3800 series	3845, 3825	IOS 12.3(8) or later	256MB/64MB
Cisco 7200 series	720x, 75xx	IOS 12.3(8) or later	128MB/48MB
VPN Concentrators			
Cisco VPN 3000 Series	3005 - 3080	V4.7 or later	N/A
Switches			
Cisco Catalyst 2900	2950, 2970	IOS 12.1(22)EA5	N/A
Cisco Catalyst 3x00	3550, 3560, 3750	IOS 12.2(25)SEC	N/A
Cisco Catalyst 4x00	Supervisor 2+ or higher	IOS 12.2(25)EWA	N/A
Cisco Catalyst 6500	6503, 6509, Supervisor 2 or higher	CatOS 8.5 or later	Sup2 - 128MB, Sup32 - 256MB, Sup720 - 512MB
Wireless Access Points			
Cisco AP1200 Series	1230	N/A	N/A

Chapter 6

Deploying Policy Server for Cisco NAC

Topics in this chapter:

Note: This chapter includes basic instructions to set up and configure Policy Server for Cisco NAC. For more information about configuring and administering Cisco Secure ACS servers and other Cisco products, see the most recent Cisco documentation available at the following Web site: http://www.cisco.com/univercd/home/home.htm

Policy Server for NAC Deployment Overview

Follow the procedure below to deploy the Policy Server for Cisco NAC:

1. **Install the OfficeScan server:** Install the OfficeScan server on the network (see the *Installation and Deployment Guide*).
2. **Install OfficeScan clients:** Install the OfficeScan client program on all clients whose antivirus protection you want Policy Server to evaluate (see the *Installation and Deployment Guide*).
3. **Enroll the Cisco Secure ACS server:** Establish a trusted relationship between the ACS server and a Certificate Authority (CA) server by having the ACS server issue a certificate signing request. Then save the CA-signed certificate (called the ACS certificate) on the ACS server (see *Cisco Secure ACS Server Enrolment* on page 6-3).
4. **Export and install a CA certificate:** Export the CA certificate to the ACS server and store a copy on the OfficeScan server. This step is only necessary if you have not deployed a certificate to clients and the ACS server (see *CA Certificate Installation* on page 6-3).
5. **Deploy the Cisco Trust Agent and CA certificate:** Deploy the Cisco Trust Agent and the CA certificate to all OfficeScan clients so clients can submit security posture information to the Policy server (see *Cisco Trust Agent Deployment* on page 6-8).
6. **Install the Policy Server for Cisco NAC:** Install the Policy Server for Cisco NAC to handle requests from the ACS server (see *Policy Server for Cisco NAC Installation* on page 6-12).
7. **Export an SSL certificate from the Policy Server:** Export an SSL certificate from the Policy Server to the Cisco ACS server to establish secure SSL communications between the two servers (see *Policy Server for Cisco NAC Installation* on page 6-12).
8. **Configure the ACS server:** Configure the ACS server to forward posture validation requests to the Policy Server (see *ACS Server Configuration* on page 6-15).
9. **Configure the Policy Server for NAC:** Create and modify Policy Server rules and policies to enforce your organization's security strategy for OfficeScan clients (see *Policy Server for Cisco NAC Configuration* on page 6-15).

Note: The following procedures are for reference only and may be subject to change depending on updates to either the Microsoft and/or Cisco interfaces.

Before performing any of the tasks in this chapter, verify that the Network Access Device(s) on your network are able to support Cisco NAC (see *Supported Platforms and Requirements* on page 5-19). See the device documentation for set up and configuration instructions. Also, install the ACS server on your network. See your Cisco Secure ACS documentation for instructions.

Cisco Secure ACS Server Enrolment

Enroll the Cisco Secure ACS server with the Certificate Authority (CA) server to establish a trust relationship between the two servers. The following procedure is for users running a Windows Certification Authority server to manage certificates on the network. Refer to your vendor documentation if using another CA application or service and see your ACS server documentation for instructions on how to enroll a certificate.

CA Certificate Installation

The OfficeScan client authenticates with the ACS server before it sends security posture data. The CA certificate is necessary for this authentication to take place. First, export the CA certificate from the CA server to both the ACS server and the OfficeScan server, then create the CTA agent deployment package. The package includes the CA certificate (see *The CA Certificate* on page 5-17 and *Cisco Trust Agent Deployment* on page 6-8).

Perform the following to export and install the CA certificate:

- Export the CA certificate from the Certificate Authority server
- Install it on the Cisco Secure ACS server
- Store a copy on the OfficeScan server

Note: The following procedure is for users running a Windows Certification Authority server to manage certificates on the network. Refer to your vendor documentation if you use another Certification Authority application or service.

To export and install the CA certificate for distribution:

1. Export the certificate from the Certification Authority (CA) server:
   a. On the CA server, click **Start > Run**. The Run screen opens.
   b. Type **mmc** in the **Open** box. A new management console screen opens.
   c. Click **File > Add/Remove Snap-in**. the **Add/Remove Snap-in** screen appears.
   d. Click **Certificates** and click **Add**. The **Certificates snap-in** screen opens.
   e. Click **Computer Account** and click **Next**. The Select Computer screen opens.
   f. Click **Local Computer** and click **Finish**.
   g. Click **Close** to close the **Add Standalone Snap-in** screen.
   h. Click **OK** to close the **Add/remove Snap-in** screen.
   i. In the tree view of the console, click **Certificates > Trusted Root > Certificates**.
   j. Select the certificate to distribute to clients and the ACS server from the list.
   k. Click **Action > All Tasks > Export...** The Certificate Export Wizard opens.

l. Click **Next**.

m. Click **DER encoded binary x.509** and click **Next**.

n. Enter a file name and browse to a directory to which to export the certificate.

o. Click **Next**.

p. Click **Finish**. A confirmation window displays.

q. Click **OK**.

2. Install the certificate on Cisco Secure ACS.

   a. Click **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

   b. Type the full path and file name of the certificate in the **CA certificate file** field.

   c. Click **Submit**. Cisco Secure ACS prompts you to restart the service.

   d. Click **System Configuration > Service Control**.

   e. Click **Restart**. Cisco Secure ACS restarts.

   f. Click **System Configuration > ACS Certificate Management > Edit Certificate Trust List**. The Edit Certificate Trust List screen appears.

   g. Select the check box that corresponds to the certificate you imported in step b and click **Submit**. Cisco Secure ACS prompts you to restart the service.

   h. Click **System Configuration > Service Control**.

   i. Click **Restart**. Cisco Secure ACS restarts.

3. Copy the certificate (.cer file) to the OfficeScan server computer so you can deploy it to the client with the CTA (see *Cisco Trust Agent Deployment* on page 6-8 for more information).

Note: Store the certificate on a local drive and not on mapped drives.

Policy Server SSL Certificate Preparation

To establish a secure SSL connection between the ACS server and the Policy Server, prepare a certificate especially for use with SSL. The Policy Server Setup program automatically generates the SSL certificate.

To prepare the Policy Server SSL certificate for distribution:

1. Export the certificate from the Certification Store on mmc.

   If the Policy server runs IIS:

   a. On the Policy Server, click **Start > Run**. The Run screen opens.

   b. Type **mmc** in the **Open** box. A new management console screen opens.

   c. Click **Console > Add/Remove Snap-in**. the Add/Remove Snap-in screen appears.

   d. Click **Add**. The **Add Standalone Snap-ins** screen appears.

   e. Click **Certificates** and click **Add**. The **Certificates snap-in** screen opens.

   f. Click **Computer Account** and click **Next**. The Select Computer screen opens.

   g. Click **Local Computer** and click **Finish**.

   h. Click **Close** to close the **Add Standalone Snap-in** screen.

   i. Click **OK** to close the **Add/remove Snap-in** screen.

   j. In the tree view of the console, click **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.

k. Select the certificate from the list.

Note: Check the certificate thumbprint by double-clicking the certificate and selecting **Properties**. The thumbprint should be the same as the thumbprint for the certificate located in the IIS console.

To verify this, open the IIS console and right click either **virtual Web site** or **default Web site** (depending on the Web site on which you installed Policy Server) and then select **Properties**. Click **Directory Security** and then click **View Certificate** to view the certificate details, including the thumbprint.

---

l. Click **Action > All Tasks > Export...** The Certificate Export Wizard opens.

m. Click **Next**.

n. Click **DER encoded binary x.509** or **Base 64 encoded X.509** and click **Next**.

o. Enter a file name and browse to a directory to which to export the certificate.

p. Click **Next**.

q. Click **Finish**. A confirmation window displays.

r. Click **OK**.

If the Policy server runs Apache 2.0:

a. Obtain the certificate file server.cer. The location of the file depends on which server, the OfficeScan server or the Policy Server, you installed first:

- If you installed OfficeScan server before installing Policy Server, the file is in the following directory: C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\certificate
- If you installed Policy Server before installing OfficeScan server, the file is in the following directory: C:\Program Files\Trend Micro\OfficeScan\PolicyServer\Private\certificate

b. Copy the certificate file to the ACS server.

2. Install the certificate on Cisco Secure ACS.
   a. On the ACS Web console, click **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.
   b. Type the full path and file name of the certificate in the **CA certificate file** field.
   c. Click **Submit**. Cisco Secure ACS prompts you to restart the service.
   d. Click **System Configuration > Service Control**.
   e. Click **Restart**. Cisco Secure ACS restarts.

Cisco Trust Agent Deployment

The Cisco Trust Agent (CTA) enables communication between OfficeScan clients and Network Access Devices that support Cisco NAC. After installing and deploying the OfficeScan server and OfficeScan clients, deploy the CTA to OfficeScan clients from the Web console. The CTA deployment package includes the CA certificate you saved on the OfficeScan server (see *CA Certificate Installation* on page 6-3).

Note: Install Windows Installer 2.0 or later on client computers before deploying the agent.

To deploy CTA to clients from the OfficeScan Web console:

1. Open the OfficeScan server Web console.
2. Do one of the following:
   - If you already distributed certificates to clients, go to Step 3.
   - If you have not yet distributed certificates to clients, do the following:
     i. Click **Cisco NAC > Client Certificate**. The Import Client Certificate screen appears.
     ii. Type the full path and file name of the prepared CA certificate stored on the server. For instructions on preparing a CA certificate, see *CA Certificate Installation* on page 6-3.
     iii. Click **Import**. The certificate information appears.

Note: If you did not accept the terms of the Cisco License Agreement during installation of the OfficeScan server, you cannot deploy the agent. When you click **Agent Deployment**, the license information appears again. Read the license agreement and click **Yes** to agree to the terms.

3. Click **Agent Deployment** in the menu. The client tree appears.
4. Select the clients or domains to which to deploy the CTA and click **Deploy Agent**. The **Agent Installation/Uninstallation** screen appears.
5. Click **Install/Upgrade Cisco Trust Agent** and then click **Apply to All Clients**.
6. Click **Close**.

Note: If the client to which you deploy the agent is not online when you click **Install Cisco Trust Agent**, OfficeScan automatically fulfills the task request when the client becomes online.

If you already prepared a CA certificate before installing the OfficeScan server, you can deploy CTA during OfficeScan server installation. The option to deploy CTA is in the Install Other OfficeScan Programs screen of master Setup. For instructions on installing the OfficeScan server, see the *Installation and Deployment Guide*.

To deploy the CTA to clients using the OfficeScan server master installer:

1. In the Install Other OfficeScan Programs screen, select **Cisco Trust Agent for Cisco NAC**.
2. Do one of the following:
   - If you have already distributed certificates to Cisco Secure NAC end user clients, click **Next**.
   - If you need to distribute certificates to clients:
     i. Click **Import Certificate**.
     ii. Locate and select the prepared certificate file and click **OK**. For instructions on preparing a certificate file, see *CA Certificate Installation* on page 6-3.
     iii. Click **Next**.
3. Continue with OfficeScan server installation.

Cisco Trust Agent Upgrade and Deployment

If your Cisco NAC Access Control Server (ACS) is version 4.0 or later, you must upgrade the Cisco Trust Agent to version 2.0 or later.

To upgrade CTA:

1. On the main menu, click **Cisco NAC > Agent Management**.
2. Click **Use {CTA version)**. The OfficeScan server upgrades the agent on the server.
3. On the main menu, click **Agent Deployment > Deploy Agent**.
4. Click **Install/Upgrade Cisco Trust Agent** to manually deploy the agent to your OfficeScan clients.
5. Click **Apply to Future Clients Only** to save the settings without deploying the agent or **Apply to All Clients** to deploy the agent.

To manually replace the CTA package:

You can manually replace the CTA package on the OfficeScan server if there is a specific version you want to use.

1. In the CTA version you want to use, copy the CTA .msi file to the following folder:

   {OfficeScan installation folder}\OfficeScan\PCCSRV\Admin\Utility\CTA\CTA-Package

   OR

   {OfficeScan installation folder}OfficeScan\PCCSRV\Admin\Utility\CTA\CTA-Supplicant-Package
2. Copy the following files to {OfficeScan installation folder}\OfficeScan\PCCSRV\Admin\Utility\CTA\PosturePlugin: TmabPP.dll, tmabpp.inf and TmAbPpAct.exe.
3. In the Web console, go to **Cisco NAC > Agent Management** and click **Use {CTA version}**.

After agent upgrade, the files will be zipped to PostureAgent.zip as a CTA deployment package under {OfficeScan installation folder}OfficeScan\PCCSRV\download\Product.

Cisco Trust Agent Installation Verification

After deploying the CTA to clients, verify successful installation by viewing the client tree. The client tree contains a column titled **CTA Program**, which is visible in the **Update**, **View All**, or **Antivirus** views. Successful CTA installations contain a version number for the CTA program.

You can also verify that the processes ctapsd.exe, ctaEoU.exe, ctatransapt.exe and ctalogd.exe are running on the client computer.

Policy Server for Cisco NAC Installation

There are two ways to install Policy Server:

- The Policy Server installer located on the Enterprise CD
- The OfficeScan server master installer (this installs both OfficeScan server and the Policy Server on the same computer)

Note: The master installer installs both the OfficeScan server and Policy Server Web console on a Web server you specify: IIS or Apache. If the installer does not find an Apache server on the system, or if an existing Apache server installation is not version 2.0 or above, the installer automatically installs Apache version 2.0.

The ACS server, Policy Server, and OfficeScan server must be on the same network segment to ensure effective communication.

WARNING! *Before installing the Apache Web server, refer to the Apache Web site for the latest information on upgrades, patches, and security issues:* www.apache.org.

To install Policy Server for Cisco NAC using the Policy Server installer:

1. Log on to the computer to which you will install Policy Server for Cisco NAC.
2. Locate the Policy Server for Cisco NAC installer package on the Enterprise CD.
3. Double-click setup.exe to run the installer.
4. Follow the installation instructions.

You can install the Policy Server to the OfficeScan server computer.

To install Policy Server for Cisco NAC from the OfficeScan server master installer:

1. In the Install Other OfficeScan Programs screen of the OfficeScan server master installer, select **Policy Server for Cisco NAC**.
2. Click **Next**.
3. Continue with OfficeScan server installation.
4. When the Welcome screen for Trend Micro Policy Server for Cisco NAC appears, click **Next**. The Policy Server for Cisco NAC License Agreement screen appears.
5. Read the agreement and click **Yes** to continue. The Choose Destination Location screen appears.
6. Modify the default destination location if necessary by clicking **Browse...** and selecting a new destination for the Policy Server installation.
7. Click **Next**. The Web Server screen appears.
8. Choose the Web server for the Policy Server:
   - **IIS server:** Click to install on an existing IIS Web server installation
   - **Apache 2.0 Web server:** Click to install on an Apache 2.0 Web server
9. Click **Next**. The Web Server Configuration screen appears.
10. Configure the following information:
    - If you selected to install Policy Server on an IIS server, select one of the following:
      - **IIS default Web site:** Click to install as an IIS default Web site
      - **IIS virtual Web site:** Click to install as an IIS virtual Web site

- Next to **Port**, type a port that will serve as the server listening port.

Note: When the Policy Server and OfficeScan server are on the same computer and uses the same Web server, the port numbers are as follows:
Apache Web server/IIS Web server on default Web site: Policy Server and OfficeScan server share the same port
Both on IIS Web server on virtual Web site: Policy Server default listening port is 8081 and the SSL port is 4344. The OfficeScan server default listening port is 8080 and the SSL port is 4343.

- If you selected to install Policy Server on an IIS server, you also have the option of using Secured Socket Layer (SSL). Type the SSL port number and the number of years to keep the SSL certificate valid (the default is 3 years). If you enable SSL, this port number will serve as the server's listening port. The Policy Server's address will be as follows:
  - http://{Policy Server name}:{port number} or
  - https://{Policy Server name}:{port number} (if you enable SSL)

11. Click **Next**.
12. Specify the Policy Server console password and click **Next**.
13. Specify the ACS Server authentication password and click **Next**.
14. Review the installation settings. If satisfied with the settings, click **Next** to start the installation. Otherwise, click **Back** to go to the previous screens.
15. When the installation is complete, click **Finish**.
    The OfficeScan server master installer will continue.

ACS Server Configuration

To allow Cisco Secure ACS to pass authentication requests to the Policy Server for Cisco NAC, add the Policy Server for Cisco NAC in **External Policies** for the external user database to use for authentication. See your ACS server documentation for instructions on how to add the policy server in a new external policy.

Note: You can configure the ACS server to perform functions such as blocking client access to the network. These ACS functions are beyond the scope of the Trend Micro Policy Server for Cisco NAC implementation and are not in this document. See your ACS documentation for details on configuring other ACS functions.

Policy Server for Cisco NAC Configuration

After installing OfficeScan and the Policy Server, and deploying both the OfficeScan client and the Cisco Trust Agent, configure the Policy Server for Cisco NAC. To configure a Policy Server, access the Policy Server Web console from the OfficeScan Web console by going to **Cisco NAC > Policy Servers** and clicking the Policy Server link.

This section describes the following aspects of Policy Server configuration:

- *Policy Server Configuration from OfficeScan* starting on page 6-16 describes how to manage Policy Servers on the OfficeScan Web console.
- *Summary Information for a Policy Server* starting on page 6-17 shows you how to get an overview of Policy Servers on your network.
- *Policy Server Registration* starting on page 6-18 is the first step in configuring Policy Servers.
- *Rules* starting on page 6-18 shows you how to create and edit rules that comprise policies.
- *Policies* starting on page 6-19 shows you how to create and edit policies that ultimately determine how Policy Server measures client security posture.

- *Client Validation Logs* starting on page 6-19 gives an overview of how to use logs to understand the security posture status of clients on your network.
- *Administrative Tasks* starting on page 6-20 describes how to change the Policy Server password and set a schedule for synchronization.

Policy Server Configuration from OfficeScan

The first step in configuring Policy Servers is to add the installed Policy Servers to the OfficeScan server. This allows you to open the Policy Server Web console from the OfficeScan Web console.

To add a Policy Server:

1. On the main menu of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The Policy Servers screen appears displaying a list of all Policy Servers.
2. Click **Add**. The Policy Server screen displays.
3. Type the full Policy Server address and port number the server uses for HTTPS communication (for example: https://policy-server:4343/). Also type an optional description for the server.
4. Type a password to use when logging in the Policy Server Web console and confirm the password.
5. Click **Add**.

To delete a Policy Server:

1. On the main menu of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The Policy Servers screen appears displaying a list of all Policy Servers.
2. Select the check box next to the Policy Server to delete.
3. Click **Delete**.

Note: To validate all clients on your network, add all OfficeScan servers to at least one Policy Server.

Summary Information for a Policy Server

The Summary screen contains information about the Policy Server including configuration settings for policies and rules, client validation logs, and OfficeScan servers registered to a Policy Server.

The IP address and port number of the Policy Server for Cisco NAC appears at the top of the Summary screen.

The **Configuration Summary** table displays the number of OfficeScan servers registered to the Policy Server, the Policy Server policies, and the rules that compose the policies.

To view and modify Configuration Summary details for a Policy Server:

1. On the main menu of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The Policy Servers screen appears displaying a list of all Policy Servers.
2. Click the server name of the Policy Server whose details you want to view. The Summary screen appears showing the **Configuration Summary** table.
3. Click the link next to the item whose configuration settings you want to view:
   - **Registered OfficeScan server(s):** The OfficeScan servers currently on the network
   - **Policies:** The Policy Server policies registered OfficeScan servers can use
   - **Rule(s):** The Policy Server rules that comprise policies

Tip: If you want multiple Policy Servers on your network to have the same settings, including the same rules and policies, export and then import settings from one server to another.

Trend Micro recommends configuring the same settings on all Policy Servers on your network to maintain a consistent antivirus policy.

To synchronize the Policy Server with registered OfficeScan servers:

In the summary screen, click **Synchronize with OfficeScan**. The Summary - Synchronization Results screen appears showing the following read-only information:

- **OfficeScan server name:** The host name or IP address and port number of the registered OfficeScan servers
- **Synchronization Result:** Indicates if the synchronization was successful or not
- **Last Synchronized:** The date of the last successful synchronization

For more information on synchronization, see *Synchronization* on page 5-15.

Policy Server Registration

Register the Policy Server with at least one OfficeScan server so the Policy Server can obtain Virus Pattern and Virus Scan Engine version information (see *Network access validation sequence* on page 5-7 for information on the role the OfficeScan server performs in the validation process).

Note: For Policy Server to validate all clients on your network, add all OfficeScan servers to at least one Policy Server.

Add a new OfficeScan server or edit the settings of an existing one from the OfficeScan servers screen, which you can access by going to the Policy Server Web console and clicking **Configurations > OfficeScan servers**.

Rules

Rules are the building blocks of policies and comprise policies. Configure rules as the next step in Policy Server configuration (see *Rule Composition* on page 5-9 for more information).

To access the Web console screens for Cisco ACS rules, go to the Policy Server Web console and click **Configurations > Rules** on the main menu.

Policies

After configuring new rules or ensuring that the default rules are suitable for your security enforcement needs, configure policies registered OfficeScan servers can use (see *Policy Composition* on page 5-13 for more information).

Add a new Cisco NAC policy or edit an existing one to determine the rules currently enforced and to take action on clients when client security posture does not match any rules.

To access the Web console screens for Cisco ACS policies, go to the Policy Server Web console and click **Configurations > Policies** on the main menu.

Client Validation Logs

Use the client validation logs to view detailed information about clients when they validate with the Policy Server. Validation occurs when the ACS server retrieves client security posture data and sends it to the Policy Server, which compares the data to policies and rules (see *The Client Validation Sequence* on page 5-6).

Note: To generate client validation logs, when adding or editing a new rule or policy, select the check box under **Server-side actions**.

To access the Web console screens for Cisco ACS logs, go to the Policy Server Web console and click **Logs > View Client Validation Logs** on the main menu.

Client Log Maintenance

The Policy Server archives client validation logs when they reach a size you specify. It can also delete log files after a specified number of log files accumulates. Specify the way Policy Server maintains client validation logs by clicking **Logs > Log Maintenance** on the Policy Server Web console.

Administrative Tasks

Perform the following administrative tasks on the Policy Server:

- **Change password:** Change the password configured when adding the Policy Server (see *Policy Server Configuration from OfficeScan* on page 6-16)
- **Configure a synchronization schedule:** The Policy Server needs to periodically obtain the version of the Virus Pattern and Virus Scan Engine on the OfficeScan server to evaluate OfficeScan client security posture. Therefore, you cannot enable or disable scheduled synchronization. By default, the Policy Server synchronizes with the OfficeScan server(s) every five minutes (see *Synchronization* on page 5-15 for more information).

Note: You can manually synchronize the Policy Server with the OfficeScan server at any time on the Summary screen (see *Summary Information for a Policy Server* on page 6-17).

To access the Web console screens for Cisco ACS administration tasks, go to the Policy Server Web console and click Administration on the main menu.

Chapter 7

Managing OfficeScan Using Control Manager

Topics in this chapter:

Control Manager Basic Features

Trend Micro Control Manager manages OfficeScan servers deployed across your organization's local and wide area networks. It can also manage other antivirus and content security products and services.

TABLE 7-1. Control Manager features

Feature	Description
Centralized configuration	The Product Directory and cascading management structure allow you to coordinate security risk response efforts from a single management console. This helps ensure consistent enforcement of your organization's security risk protection policies.
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging security risk outbreak.
Secure communication infrastructure	Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol. Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
Secure configuration and component download	These features allow you to configure secure management console access and component download.
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager management console users. User accounts define what the user can see and do on a Control Manager network. Track account usage through user logs.
Command tracking	This feature allows you to monitor all commands executed using the Control Manager management console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.

TABLE 7-1. Control Manager features

Feature	Description
On-demand product control	Manage OfficeScan servers in real time. Control Manager immediately sends configuration modifications made on the management console to OfficeScan servers. For example, system administrators can run Manual Scan from the management console, which is indispensable during a virus outbreak.
Centralized update control	Update OfficeScan components from the management console.
Centralized reporting	Get an overview of OfficeScan's performance using comprehensive logs and reports.

Trend Micro Management Communication Protocol

Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for OfficeScan. MCP replaces Trend Micro Management Infrastructure (TMI) as the way Control Manager communicates with OfficeScan. MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and two-way communication support
- Single sign-on (SSO) support

Reduced Network Loading and Package Size

TMI uses an application protocol based on XML. Even though XML provides a degree of extensibility and flexibility in the protocol design, the drawbacks of applying XML as the data format standard for the communication protocol consist of the following:

- XML parsing requires more system resources compared to the other data formats such as CGI name-value pair and binary structure (the program leaves a large footprint on your OfficeScan server).
- The agent footprint required to transfer information is much larger in XML compared with other data formats.
- Data processing performance is slower due to the larger data footprint.
- Packet transmissions take longer and the transmission rate is less than other data formats.

MCP's data format resolves these issues. The MCP's data format is a BLOB (binary) stream with each item composed of name ID, type, length and value. This BLOB format has the following advantages:

- **Smaller data transfer size compared to XML:** Each data type requires only a limited number of bytes to store the information. These data types are integer, unsigned integer, Boolean, and floating point.
- **Faster parsing speed:** With a fixed binary format, each data item can be easily parsed one by one. Compared to XML, the performance is several times faster.
- **Improved design flexibility:** Design flexibility is also been considered since each item is composed of name ID, type, length and value. There will be no strict item order and compliment items can be present in the communication protocol only if needed.

In addition to applying binary stream format for data transmission, more than one type of data can be packed in a connection, with/or without compression. This type of data transfer strategy preserves network bandwidth and creates improved scalability.

NAT and Firewall Traversal Support

With limited addressable IPs on the IPv4 network, NAT (Network Address Translation) devices have become widely used to allow more end-point computers to connect to the Internet. NAT devices achieve this by forming a private virtual network to the computers attached to the NAT device. Each computer that connects to the NAT device will have one dedicated private virtual IP address. The NAT device will translate this private IP address into a real world IP address before sending a request to the Internet. This introduces some problems since each connecting computer uses a virtual IP and many network applications are not aware of this behavior. This usually results in unexpected program malfunctions and network connectivity issues.

For products that work with TMCM 2.5/3.0 agents, one pre-condition is assumed. The server relies on the fact that the agent is reachable by initiating a connection from the server to the agent. This is a so-called two-way communication product, since both sides can initiate network connection with each other. This assumption breaks when the agent sits behinds a NAT device (or the Control Manager server sits behind a NAT device) since the connection can only route to the NAT device, not the product behind the NAT device (or the Control Manager server sitting behind a NAT device). One common workaround is that a specific mapping relationship is established on the NAT device to direct it to automatically route the in-bound request to the respective agent. However, this solution needs user involvement and it does not work well when large-scale product deployment is needed.

The MCP deals with this issue by introducing a one-way communication model. With one-way communication, only the agent initiates the network connection to the server. The server cannot initiate connection to the agent. This one-way communication works well for log data transfers. However, the server dispatching of commands occurs under a passive mode. That is, the command deployment relies on the agent to poll the server for available commands.

HTTPS Support

The MCP integration protocol applies the industry standard communication protocol (HTTP/HTTPS). HTTP/HTTPS has several advantages over TMI:

- A large majority of people in IT are familiar with HTTP/HTTPS, which makes it easier to identify communication issues and find solutions those issues
- For most enterprise environments, there is no need to open extra ports in the firewall to allow packets to pass
- Existing security mechanisms built for HTTP/HTTPS, such as SSL/TLS and HTTP digest authentication, can be used.

Using MCP, Control Manager has three security levels:

- **Normal security:** Control Manager uses HTTP for communication
- **Medium security:** Control Manager uses HTTPS for communication if HTTPS is supported and HTTP if HTTPS is not supported
- **High security:** Control Manager uses HTTPS for communication

One-way and Two-way Communication Support

MCP supports one-way and two-way communication.

One-way communication

NAT traversal has become an increasingly more significant issue in the current real-world network environment. To address this issue, MCP uses one-way communication. One-way communication has the MCP agent initiating the connection to and polling of commands from the server. Each request is a CGI-like command query or log transmission. To reduce the network impact, the connection is kept alive and open as much as possible. A subsequent request uses an existing open connection. Even if the connection is dropped, all connections involving SSL to the same host benefit from session ID cache that drastically reduces re-connection time.

Two-way communication

Two-way communication is an alternative to one-way communication. It is still based on one-way communication, but has an extra channel to receive server notifications. This extra channel is also based on the HTTP protocol. Two-way communication can improve real-time dispatching and processing of commands from the server by the MCP agent.

Single Sign-on (SSO) Support

Through MCP, Control Manager 3.5 now supports single sign-on (SSO) functionality for OfficeScan and other Trend Micro products. This feature allows users to sign on to Control Manager and access OfficeScan without having to log on to the OfficeScan console.

MCP Agent Heartbeat

To monitor the status of OfficeScan, the MCP agent polls Control Manager based on a schedule. Polling occurs to indicate the status of the OfficeScan server and to check for commands from Control Manager to the OfficeScan server. The Control Manager management console then presents the product status. This means that the OfficeScan server status is not a real-time, moment-by-moment reflection of the network's status. Control Manager checks the status of each OfficeScan server in a sequential manner in the background and changes its status to offline when a fixed period of time elapses without a heartbeat.

Active heartbeats are not the only means Control Manager has for determining the status of OfficeScan. The following also provide Control Manager with the OfficeScan server status:

- Control Manager receives logs from the OfficeScan server. Once Control Manager receives any type of log from the OfficeScan server successfully, this implies that the OfficeScan server works fine.
- In two-way communication mode, Control Manager actively sends out a notification message to trigger the OfficeScan server to retrieve the pending command. If Control Manager connects to the OfficeScan server successfully, the product works fine and this event counts as a heartbeat.

- In one-way communication mode, the MCP agent periodically sends query commands to Control Manager. This periodic query behavior works like a heartbeat and is treated as such by Control Manager.

The MCP agent heartbeats implement with the following ways:

- **UDP:** If OfficeScan can reach the server using UDP, this is the most lightweight, fastest solution available. However, this does not work in NAT or firewall environments. Also OfficeScan cannot make sure that Control Manager does indeed receive the request.
- **HTTP/HTTPS:** To work under a NAT or firewall environment, a heavyweight HTTP connection can transport the heartbeat.

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the OfficeScan server applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can be uploaded to Control Manager along with the heartbeat. The data usually contains OfficeScan server activity information to display on the console.

The Schedule Bar

Use the schedule bar in the Communicator Scheduler screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

Blue slots denote Working status or the hours that the Communicator sends information to the Control Manager server. White slots indicate Idle time. Define Working or Idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity. The sample schedule bar below shows only two inactive hours:

The active periods specified by the bar are from 0:00 A.M. to 7:00 A.M, 8:00 A.M to 3:00 PM, and from 6:00 P.M. to 12:00 P.M.

The Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest Communicator status information and the need to manage system resources. Trend Micro's default settings are satisfactory for most situations. However consider the following points when you customize the heartbeat setting:

TABLE 7-2. Heartbeat recommendations

Heartbeat Frequency	Recommendation
Long-interval Heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status on the Control Manager management console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).
Short-interval Heartbeats (below 60 minutes)	Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.

OfficeScan Registration

OfficeScan is a standalone product and registering it to Control Manager is not required. However, by registering to Control Manager, you gain the benefits explained earlier in this chapter.

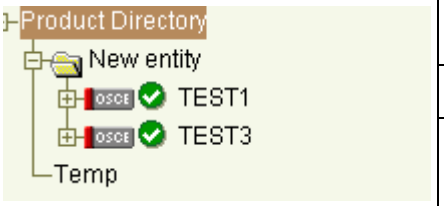
Refer to the OfficeScan online help for the registration procedure. After registration, do the following:

1. Open the Control Manager management console.
2. In **Main Menu**, click **Products**.
3. On the left most menu, select **Managed Products** from the list and then click **Go**.
4. Check to see that the OfficeScan server displays.

OfficeScan Management

Indirectly administer one or more OfficeScan servers through the Product Directory. Use the Directory Manager to customize the Product Directory organization.

TABLE 7-3. The Control Manager Product Directory

Product Directory Tree	Icon	Description
		New entity or user-defined folder name
		The OfficeScan server
		Connection status

Arrange the Product Directory using the Directory Manager. Use descriptive folders to group your OfficeScan servers according to their protection type and the Control Manager network administration model.

Product Directory

Take care when planning the structure of the Product Directory because it affects the following:

- **User access:** When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. Carefully plan the Product Directory since you can only grant access to a single segment. For example, granting access to the root segment grants access to the entire Product Directory.
- **Deployment planning:** Control Manager deploys component and program updates based on Deployment Plans. These plans deploy to Product Directory folders. A well-structured directory will therefore simplify the designation of recipients.
- **Outbreak Prevention Policy (OPP) deployment:** OPP deployment depends on Deployment Plans for efficient distribution of the policy.

Product Directory Tasks

Accessing an OfficeScan default folder

Newly registered OfficeScan servers usually appear in the **New entity** folder depending on the user account specified during the agent installation. Control Manager determines the default folder for the OfficeScan server by the privileges of the user account specified during installation.

Accessing Product Directory

Use the Product Directory to administer OfficeScan registered with the Control Manager server.

Note: Viewing and accessing the folders in the Product Directory depends on the Account Type and folder access rights used to log on to the management console.

To access the Product Directory:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.

Refreshing the Product Directory

To refresh the Product Directory, in the Product Directory, click the **Refresh** icon on the upper right corner of the left menu.

Deploying new components using the Product Directory

Manual deployments allow you to update OfficeScan components on demand. This is useful especially during security risk outbreaks.

Download new components before deploying them to OfficeScan servers.

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired folder or OfficeScan server.
4. On the working area, click the **Tasks** tab.
5. Select **Deploy pattern files/cleanup templates** or **Deploy engines**.
6. Click **Next**.
7. Click **Deploy Now** to start the manual deployment of new components.
8. Monitor the progress through Command Tracking.
9. Click the **Command Details** link to view details of component deployment.

Viewing OfficeScan status summaries

The Product Status screen displays the security risk protection status of all OfficeScan servers and other managed products.

There are two ways to view the OfficeScan status summary:

- Through the Home page
- Through the Product Directory

To access through the Home page:

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through Product Directory:

1. Click **Products** on the main menu.
2. On the left-hand menu, select the desired folder or OfficeScan server.
   - If you click an OfficeScan server, the Product Status tab displays the OfficeScan server's summary.
   - If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays the summary for the entire Control Manager system.

Note: By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last month available in the **Display summary for** list.

OfficeScan Configuration

You can configure OfficeScan servers either individually or in groups according to folder division. Perform group configuration using the folder **Configuration** tab.

Note: When performing group configuration, verify that you want all OfficeScan servers in the group to have the same configuration. Otherwise, add OfficeScan servers that should have the same configuration to Temp to prevent overwriting the settings of other servers.

The Configuration tab shows either the product's Web console or a Control Manager-generated console.

To configure OfficeScan:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired OfficeScan server or folder.
4. On the working area, click the **Configuration** tab.

5. Select OfficeScan from the Select product list.

Note: Step 4 is necessary when you use the folder Configuration tab.

6. At the Select configuration list, select the OfficeScan feature to access or configure.
7. Click **Next**. The OfficeScan Web console appears.

OfficeScan Task Management

Use the **Tasks** tab to invoke available actions to OfficeScan. You can perform the following tasks on OfficeScan:

- Configuration replication
- Deploy engines
- Deploy license profiles
- Deploy pattern files/cleanup templates
- Deploy program files
- Enable Real-time Scan
- Start Scan Now

Deploy the latest pattern file or scan engine to OfficeScan servers with outdated components. To successfully do so, the Control Manager server must have the latest components from the Trend Micro ActiveUpdate server. Perform manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to OfficeScan:

1. Access the Product Directory.
2. On the left-hand menu, select the desired OfficeScan server or folder.
3. On the working area, click the **Tasks** tab.
4. Select the task from the **Select task** list.
5. Click **Next**.
6. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

OfficeScan Logs

Use the **Logs** tab to query and view logs for a group or specific OfficeScan server.

To query and view OfficeScan server logs:

1. Access the Product Directory.
2. On the left-hand menu, select the desired OfficeScan server or folder.
3. On the working area, click the **Logs** tab.
4. Select the client log type:

   Event Logs:

   a. Provide the following search parameters:

TABLE 7-4. Search parameters for event logs

Parameter	Description
Severity	Refers to the degree of information available. The options are: Critical, Warning, Information, Error, Unknown. Select the check box of your chosen parameter.
Incident	Refers to events. The options are: All events, Virus outbreak, Module update, Service On, Service Off, Security violation, Suspicious Outbreak, Device Status.
Product	If you select a folder, this list shows the OfficeScan servers belonging to the folder. To view information on all OfficeScan servers, select **All**.
Logs for	View all logs, or only those that the OfficeScan server generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range. If you chose Specified range, select the appropriate month, day, and year for the Start date and End date.
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity.
Sort order	Sort results in ascending and descending order.

b. Click **Display Logs** to begin the query and display the query results.

Security Logs:

a. Select a query category and click **Query**.

b. Provide the following search parameters:

TABLE 7-5. Search parameters for security logs

Parameter	Description
Logs for	View all logs, or only those that the OfficeScan server generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range. If you chose Specified range, select the appropriate month, day, and year for the Start date and End date.
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity.
Sort order	Sort results in ascending and descending order.

c. Click **Display Logs** to begin the query. The Query Result screen displays the results in a table format.

5. The **Generated at entity** column of the result table indicates the Control Manager server time.

OfficeScan Recovery After Removal

The following scenarios can cause Control Manager to delete OfficeScan from the Product Directory:

- Reinstalling the Control Manager server and selecting the Delete existing records and create a new database option. This option creates a new database using the name of the existing one.
- Replacing the corrupted Control Manager database with another database of the same name
- Accidentally deleting the OfficeScan server using the Directory Manager

If a Control Manager server's OfficeScan server records are lost, the agents on OfficeScan still "know" where they are registered to. The agent will automatically re-register itself after 8 hours or when the service restarts.

To recover OfficeScan removed from the Product Directory, open the OfficeScan Web console, go to **Administration > Control Manager Settings**, and click **Update Settings**.

The Search Facility

Use the Search button to quickly:

- Add a specific or a group of OfficeScan servers to Temp
- Find and locate a specific OfficeScan server in the Product Directory

To search for a folder or OfficeScan server:

1. Access Product Directory.
2. On the left menu, click **Search**.
3. On the working area, provide the following search parameters:

TABLE 7-6. Search parameters

Parameter	Description
Search for	Select the object of the search from the drop down list. Search for managed OfficeScan servers or Communicators based on their name, folder name, or computer name.
Keyword	This allows you to search for the object by name. Select **Case sensitive** to narrow down the search results.
Status	Select the appropriate connection status, for the Communicator or managed OfficeScan server The options are: All, Active, Inactive, Abnormal, Product Active, and Product Inactive. Choose **All** to search for objects regardless of the connection status.
Product	Select OfficeScan Corporate Edition from the list.

4. Click **Begin Search** to start searching.
5. Control Manager presents the search results in a table format. You may opt to directly create the temp sub-folder where the search results will be grouped.

Directory Manager

After the registering to Control Manager, the OfficeScan server first appears in the Product Directory under the default folder.

Use the Directory Manager to customize the Product Directory organization to suit your administration model needs.

The Directory allows you to create, modify, or delete folders, and move OfficeScan between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the OfficeScan server belonging to each folder. Consider the following factors when planning and implementing your folder and OfficeScan server structure:

- Product Directory
- User Accounts
- Deployment Plans

Group OfficeScan servers according to geographical or administrative reasons.

To access the Directory Manager:

1. Access Product Directory.
2. On the left-hand menu, click **Directory Manager**.

The Directory Manager Options

Directory Manager provides the following options: New Folder, Delete, Rename, Undo, Redo, Cut, Paste, and Reset.

Use these options to manipulate and organize OfficeScan servers in your Control Manager network.

To use and apply changes in Directory Manager:

- Right-click a folder or OfficeScan server to open a pop-up menu that presents a list of actions you can perform.
- Click **+** or the folder to display the OfficeScan server belonging to a folder.
- Press **Enter** or click anywhere when you rename a folder.
- Click **Save** to apply your changes and update the Directory Manager organization.
- Click **Reset** to discard changes that are not yet saved.

Directory Manager Tasks

Creating a folder

Group OfficeScan into different folders to suit your organization's Control Manager network administration model.

To create a folder:

1. Access the Directory Manager.
2. On the working area, right-click where you want to create a new folder. If this is your first time to build the tree, right-click the Root folder.
3. Select **New folder** from the pop-up menu. Control Manager creates a new sub-folder under the main folder.
4. Type a name for the new folder or use the default name and then press **Enter**.
5. Click **Save**.

Except for the New entity folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, _, {, >, }, and ~), numbers (0 to 9), or alphabet characters (a/A to z/Z).

Renaming a folder or OfficeScan

To rename a folder or OfficeScan server:

1. Access Directory Manager.
2. On the working area, right-click the folder or OfficeScan server you want to rename and then select **Rename** from the pop-up menu. The folder/OfficeScan server name becomes an editable field.
3. Type a name for the new folder or use the default name and then press **Enter**.
4. Click **Save**.

Note: Renaming an OfficeScan server only changes the name stored in the Control Manager database. There are no effects to the product.

Moving folders or OfficeScan server

To transfer or move a folder or OfficeScan server to another location:

1. Access Directory Manager.
2. On the working area, select the folder or OfficeScan server you want to move.
3. Do one of the following:
   - Drag-and-drop the folder or OfficeScan server to the target new location
   - Cut and paste the folder or OfficeScan server to the target new location
4. Click **Save**.

Deleting user-defined folders

Take caution when deleting user-defined folders in the Directory Manager. You may accidentally delete an OfficeScan server which causes it to unregister from the Control Manager server.

To delete a user-defined folder:

1. Access the Directory Manager.
2. On the working area, right-click the folder you want to delete and then select **Delete** from the pop-up menu.
3. Click **Save**.

Note: You cannot delete the New entity folder.

Temp

Temp, a collection of OfficeScan server shortcuts, allows you to focus your attention on specific servers without changing the Product Directory organization. Use Temp to deploy updates to groups of products with outdated components.

Consider the following issues when using Temp:

- Control Manager deletes all OfficeScan server shortcuts when you log off from the management console.
- You can only add an OfficeScan server to Temp if you can see it in the Product Directory. You cannot make shortcuts to servers that you cannot access.

Temp Usage

You can manipulate OfficeScan servers in Temp the same way you would in the Product Directory. The folders and OfficeScan servers belonging to Temp have the same folder and OfficeScan server-level controls. However, Control Manager determines the actions you can perform on the OfficeScan server according to your user account's access rights.

You can use Temp for the following purposes:

- Issue commands to groups of OfficeScan servers using folder-level access rights.
- Select a specific OfficeScan server, and then use the available Product Directory tabs to perform an action.

To access Temp:

1. Access Product Directory.
2. On the left most menu, click **Temp**.

Temp-related Tasks

Adding OfficeScan to Temp

There are three methods to add OfficeScan to Temp:

- From the Search results
- From the Product Directory
- Add OfficeScan with outdated components based on the Status Summary page

Trend Micro recommends that you add several OfficeScan servers at once to Temp using the last method. The Status Summary screen provides information as to which OfficeScan use outdated components. It simplifies component updates on groups of OfficeScan belonging to different folder groups.

Note: Adding OfficeScan servers to Temp only allows you to determine servers with outdated components; doing so does not trigger automatic deployment.

To add from the Search results:

1. Click **Products** on the main menu.
2. On the left-hand menu, click **Search**.
3. On the working area, search for OfficeScan servers or folders.
4. Specify a sub-folder name in the **Temp sub-folder for managed products** field for the Temp sub-folder that will contain the OfficeScan server shortcuts.

Note: Step 4 is optional. If you want to create multiple folder levels belonging to Temp, specify \{folder name level1}\{sub-folder name level2} in the Temp sub-folder for entities field.

5. Click **Add**. Control Manager adds OfficeScan from the search results to Temp.

To add from the Product Directory:

1. Access the Product Directory.
2. On the left-hand menu, select the OfficeScan server you want to add to Temp.
3. Press "+" on the numeric keypad.

To add OfficeScan with outdated components based on the Status Summary page:

1. Access Product Directory.
2. On the left-hand menu, select the desired Product Directory folder.
3. On the working area, click the **Product Status** tab.
4. At the Component Status table, click one of the numeric links indicating the number of outdated OfficeScan servers. Depending on the link you clicked, the Virus Pattern Status (Outdated) and Scan Engine Status (Outdated) opens displaying the computer name, product name, product version, and outdated component version.
5. Click **Add to Temp** in the status page. Control Manager adds OfficeScan servers to Temp using folders named after the page from which they were added. For example, Control Manager places OfficeScan added from the Scan Engine Status (Outdated) page under the Scan Engine Status (Outdated) folder.

Note: Clicking **Add to Temp** only adds the OfficeScan server shown on the status page. If the list of OfficeScan servers spans more than one screen, click **Add to Temp** on all screens to add all servers with outdated components.

---

6. Click **Back** to return to the Status Summary page, and then proceed to the next outdated component. Repeat the instructions until Control Manager adds all the outdated OfficeScan severs to Temp.

Removing OfficeScan From Temp

To remove an OfficeScan server from Temp:

1. Access Product Directory.
2. On the left-hand menu, click **Temp**.
3. From the available OfficeScan servers on the Temp list, select the folder or OfficeScan server shortcut that you want to remove.
4. Press "-" in the numeric keypad.

Note: Control Manager removes OfficeScan server shortcuts in Temp when you log off from the management console.

Removing OfficeScan from Temp will neither disconnect OfficeScan nor uninstall the MCP agent from the Control Manager server.

Component Download and Deployment

Update Manager is a collection of functions that help you update components on your Control Manager network. Trend Micro recommends updating components to remain protected against the latest security risks.

The following are the components to update:

- **Pattern files/Cleanup templates:** Includes the following:
  - Virus Pattern
  - Spyware Pattern
  - Virus Cleanup Template
  - Spyware Active-monitoring Pattern
  - IntelliTrap Pattern
  - IntelliTrap Exception Pattern
  - Common Firewall Pattern

- **Engines:** Includes the following:
  - Virus Scan Engine (32-bit and 64-bit versions)
  - Spyware Scan Engine (32-bit and 64-bit versions)
  - Venus Spy Trap Engine (32-bit and 64-bit versions)
  - Virus Cleanup Engine (32-bit and 64-bit versions)
  - Anti-rootkit Driver (32-bit version)
- **Product program:** Product-specific components (for example, Service Pack releases)

Note: Only registered users can perform component update. For more information, see the Control Manager online help Registering and Activating your Software > Understanding product activation topic.

To minimize Control Manager network traffic, disable the download of components not used by OfficeScan.

Update Manager

Update Manager provides functions that help you update the components of your Control Manager network.

Updating the Control Manager network involves two steps:

- Downloading components: You can do this manually or by schedule
- Deploying components: You do this manually or by schedule

Manual Downloads

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

This is the Trend Micro recommend method of configuring manual downloads. Manually downloading components requires multiple steps:

Tip: Ignore steps 1 and 2 if you have already configured your deployment plan and configured your proxy settings.

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download settings

Step 5: Configure the automatic deployment settings

Step 6: Complete the manual download

To manually download components:

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.

FIGURE 7-1. Deployment Plan screen

3. On the working area, click **Add New Plan**.

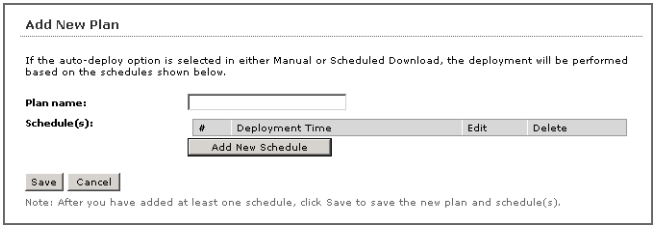


FIGURE 7-2. Add New Plan screen

4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.
5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.

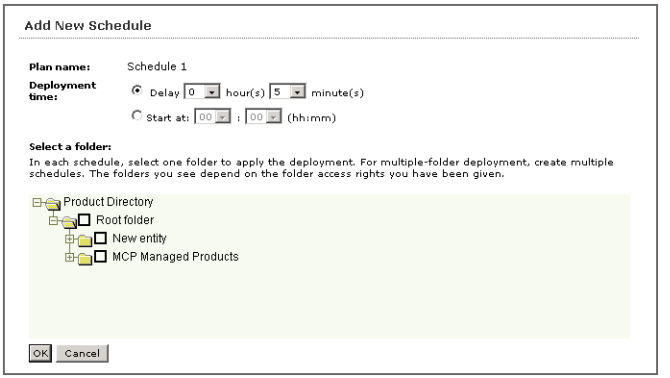


FIGURE 7-3. Add New Schedule screen

6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay:** After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at:** Performs the deployment at a specific time

     Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the OfficeScan servers under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

1. Click **Administration > System Settings**. The System Settings screen appears.

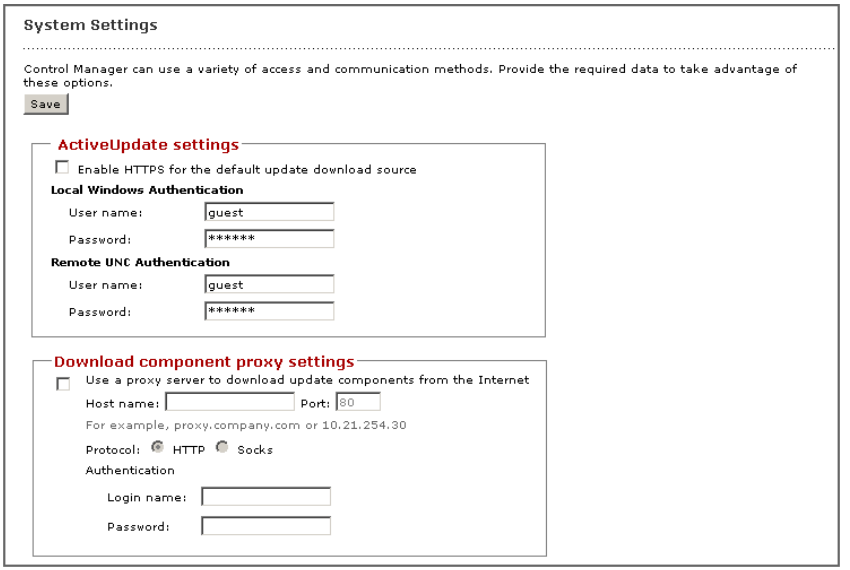


FIGURE 7-4. System Settings screen

2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:
   - HTTP
   - SOCKS
6. Type a login name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration > Update Manager > Manual Download**. The Manual Download screen appears.

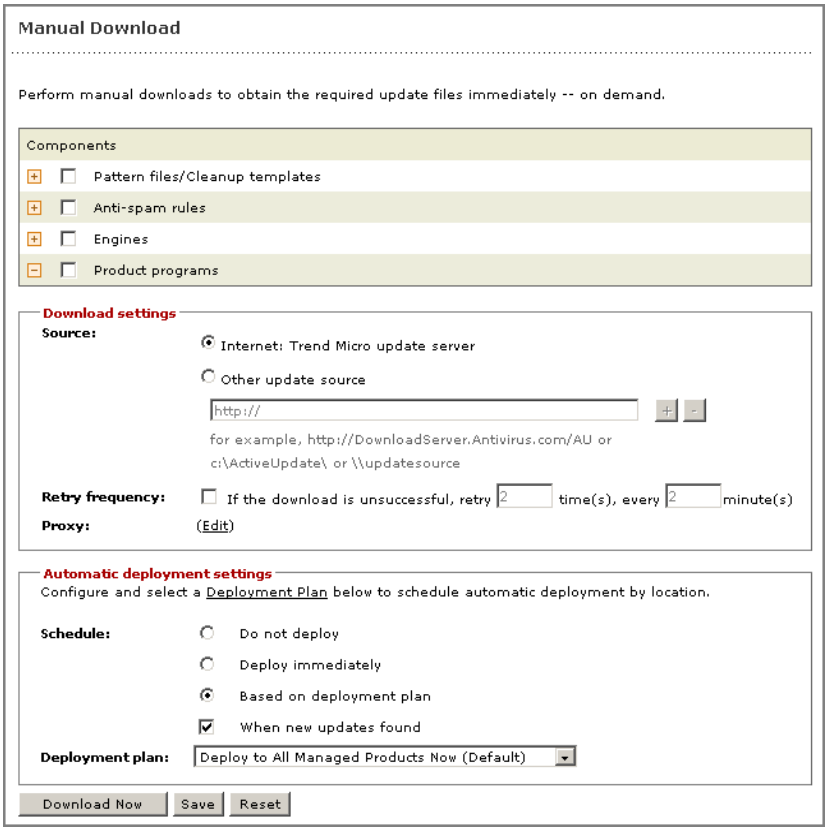


FIGURE 7-5. Manual Download screen

2. From the Components area select the components to download.
   a. Click the + icon to expand the component list for each component group.
   b. Select the OfficeScan components to download. See *OfficeScan Components and Programs* on page 1-18 for more information.

Step 4: Configure the download settings

1. Select the update source:
   - **Internet: Trend Micro update server:** Download components from the Trend Micro ActiveUpdate server.
   - **Other update source:** Type the URL of the update source in the accompanying field.

     After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.
2. Select **Retry frequency** and specify the number or retries and duration between retries for downloading components.

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save**, your settings will be lost.

---

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 5: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:
   - **Do not deploy:** Components download to Control Manager, but do not deploy to OfficeScan. Use this option under the following conditions:
     - Deploying to individual OfficeScan servers
     - Testing the updated components before deployment

- **Deploy immediately:** Components download to Control Manager, then deploy to OfficeScan servers.
- **Based on deployment plan:** Components download to Control Manager, but deploy to OfficeScan servers based on the schedule you select.
- **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to OfficeScan servers based on the schedule you select.

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save**, your settings will be lost.

2. From the **Deployment plan** list, select a deployment plan after components download to Control Manager.
3. Click **Save**.

Step 6: Complete the manual download

1. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.
2. Click the **Command Details** to view details from the Command Details screen.
3. Click **OK** to return to the Manual Download screen.

Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire day(s) or for a certain time every day.

This feature is particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

To configure scheduled download exceptions:

1. Click **Administration** on the main menu.
2. On the left-hand menu under Update Manager, click **Scheduled Download Exceptions**.
3. Do the following:
   - To schedule a daily exception, under Daily schedule exceptions, select the check box of the day(s) to prevent downloads, and then select the **Do not download updates on the specified day(s)** check box. Every week, all downloads for the selected day(s) are blocked.
   - To schedule an hourly exception, under Hourly schedule exceptions, select the hour(s) to prevent downloads, and then select the **Do not download updates on the specified hour(s)** check box. Every day, all downloads for the selected hours are blocked.
4. Click **Save**.

Scheduled Downloads

Configure scheduled downloading of components to keep your components up-to-date and your network secure. Control Manager supports granular component downloading. You can specify the component group and individual component download schedules. All schedules are autonomous of each other. Scheduling downloads for a component group downloads all components in the group.

Use the Scheduled Download screen to obtain the following information for components currently in your Control Manager system:

- **Frequency:** Shows how often the component is updated
- **Enabled:** Indicates if the schedule for the component is either enabled or disabled
- **Update Source:** Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download schedule

Step 5: Configure the download settings

Step 6: Configure the automatic deployment settings

Step 7: Enable the schedule and save settings

To configure and enable scheduled downloads:

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.

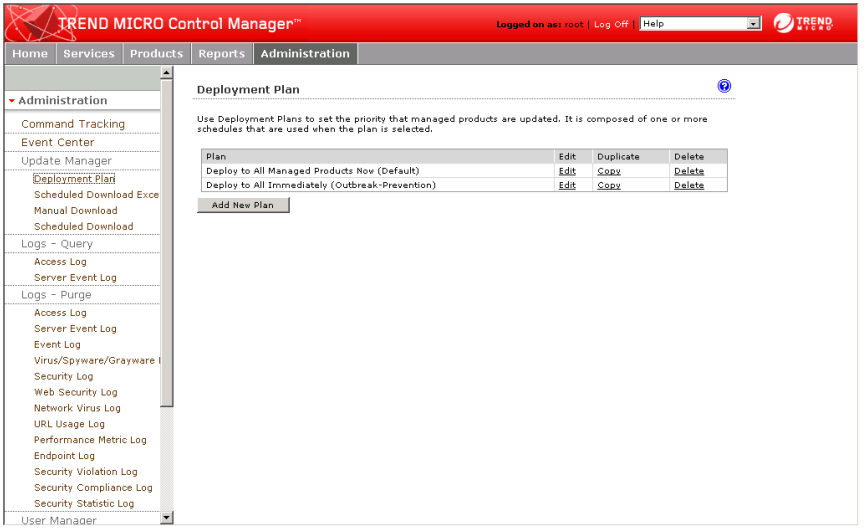


FIGURE 7-6. Deployment Plan screen

3. On the working area, click **Add New Plan**.

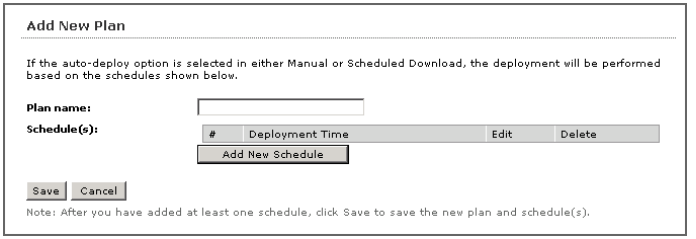


FIGURE 7-7. Add New Plan screen

4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.
5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay:** After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at:** Performs the deployment at a specific time

     Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the OfficeScan servers under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

1. Click **Administration > System Settings**. The System Settings screen appears.

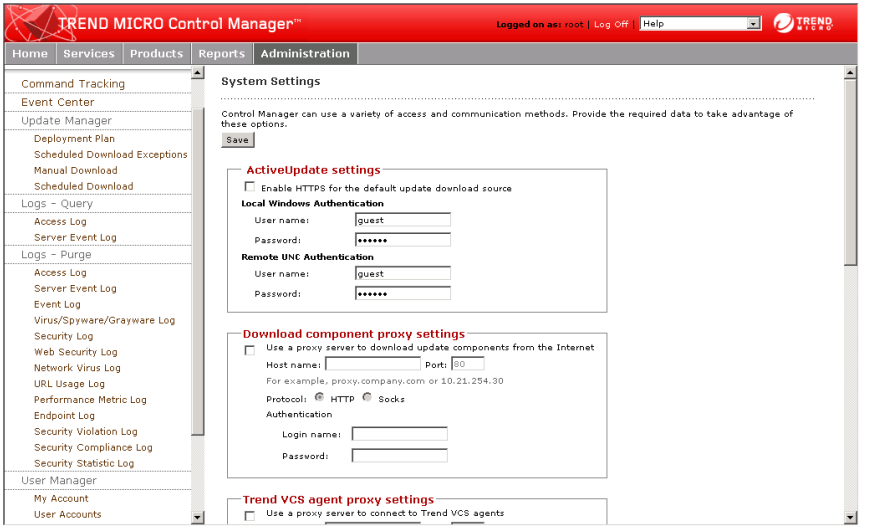


FIGURE 7-8. System Settings screen

2. In the **Download component proxy settings** area, select the **Use a proxy server to download update components from the Internet** check box.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:
   - HTTP
   - SOCKS
6. Type a login name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration > Update Manager > Scheduled Download**. The Scheduled Download screen appears.

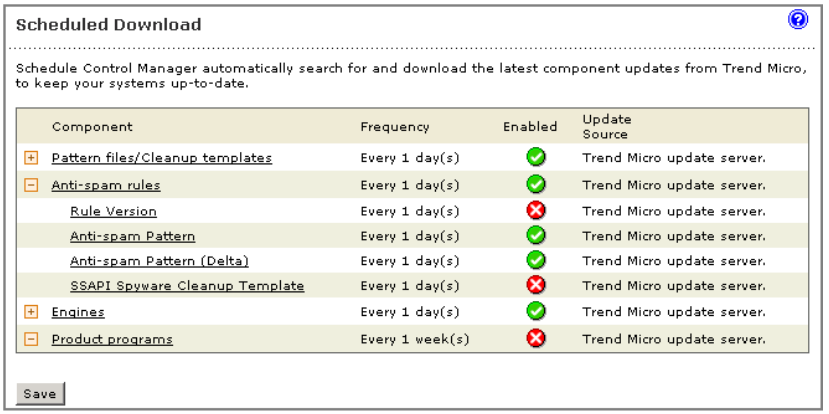


FIGURE 7-9. Scheduled Download screen

2. From the Components area select the components to download.
   a. Click the + icon to expand the component list for each component group.
   b. Select the OfficeScan components to download. See *OfficeScan Components and Programs* on page 1-18 for more information.

The {Component Name} screen appears.

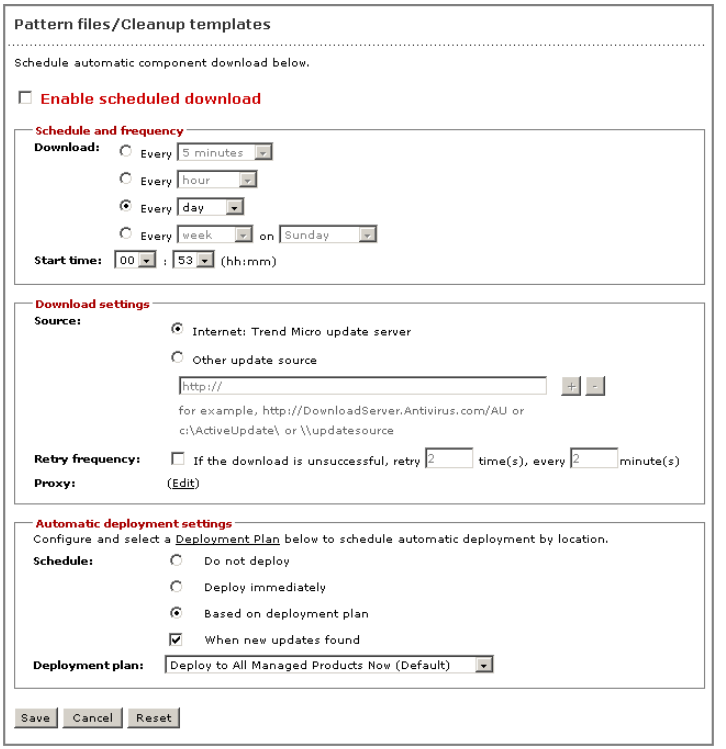


FIGURE 7-10. {Component Name} screen

Step 4: Configure the download schedule

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.
2. Define the download schedule. Select a frequency and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minute, hour, day, or week.
3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.

Step 5: Configure the download settings

1. Select the update source:
   - **Internet: Trend Micro update server:** Download components from the Trend Micro ActiveUpdate server.
   - **Other update source:** Type the URL of the update source in the accompanying field.

     After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.
2. Select **Retry frequency** and specify the number or retries and duration between retries for downloading components.

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save**, your settings will be lost.

---

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 6: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:
   - **Do not deploy:** Components download to Control Manager, but do not deploy to OfficeScan servers. Use this option under the following conditions:
     - Deploying to individual OfficeScan servers
     - Testing the updated components before deployment
   - **Deploy immediately:** Components download to Control Manager, then deploy to OfficeScan servers.
   - **Based on deployment plan:** Components download to Control Manager, but deploy to OfficeScan servers based on the schedule you select.

- **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to OfficeScan servers based on the schedule you select.

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save**, your settings will be lost.

2. From the **Deployment plan** list, select a deployment plan after components download to Control Manager.
3. Click **Save**.

Step 7: Enable the schedule and save settings

1. Click the status button in the Enabled column.
2. Click **Save**.

Reports

A Control Manager **report** is an online collection of figures about security risk events that occur on the Control Manager network. The Enterprise edition provides the Control Manager reports.

Control Manager 3.5 categorizes reports according to the following types:

- Local reports
- Global reports

Note: You can only configure the **Global Report Profile** option through the parent server management console.

Local Reports

Local reports are reports about OfficeScan servers administered by the parent server. Local reports do not include reports generated by child servers. Use the Global Report options to view reports about OfficeScan servers administered by child servers registered to the parent server.

Use Local Reports screen to view available one-time-only and scheduled local report profiles.

To access Local Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Local Report Profile**.

Note: When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Global Reports

Global reports are reports about OfficeScan servers administered by child servers as well as the parent server.

Use Global Reports screen to view available one-time-only and scheduled global report profiles.

To access Global Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Global Report Profile**.
3. When multiple reports are available, sort reports according to Report Profile or Last Created date.

Note: Only the parent server can display the global report profiles.

When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Report Templates

A report template outlines the look and feel of Control Manager reports. In particular, a template defines which sections appear in a report:

- Headers
- Report body
- Footers

Note: In Control Manager 3.5 spyware/grayware are no longer considered viruses. This change affects the virus count in all original virus related reports.

To generate these reports, click **Reports** on the main menu, then click **Create Report Profile** under Local Report Profile on the navigation menu. In the Contents tab that appears in the working area, you can enter a report name, an optional report title and an optional report description. Use the **Report Category** list to peruse the categories of reports listed below. Clicking a mark into a check box includes the associated report in the final exported report file.

Control Manager 3.5 also provides 18 templates stored in {root}\Program Files\Trend Micro\Control Manager\Reports as Crystal Report version 9 files (*.rpt). These templates also apply to Local and Global reports.

Report Profiles

A **profile** lays out the content (template and format), target, frequency, and recipient of a report. You can view reports in the following file formats:

- **RTF:** Rich text format; use a word processor (for example, Microsoft Word) to view *.RTF reports
- **PDF:** Portable document format; use Adobe™ Reader™ to view *.PDF reports

- **ActiveX™:** ActiveX documents; use a Web browser to view reports in ActiveX format

Note: Control Manager cannot send reports in ActiveX format as email attachments.

- **RPT:** Crystal Report format; use Crystal Smart Viewer to view *.RPT reports

After generating the report, Report Server launches the default viewer for that report file format. For RPT reports, you must have the Crystal Smart Viewer installed.

Report-related Tasks

Creating a report profile

Creating a report profile is a five-step process. Creating local or global reports, the process stays very similar. The process to create a report profile is as follows:

Step 1: Select whether to create a local or global report

Step 2: Configure the Contents tab settings

Step 3: Configure the Targets tab settings

Step 4: Configure the Frequency tab settings

Step 5: Configure the Recipient tab settings

To create local or global report profile:

Step 1: Select whether to create a local or global report

1. Click **Reports** on the main menu.
2. Take one of the following actions:
   - To create a local report profile, click **Local Report Profile** under Reports.
   - To create a global report profile, click **Global Report Profile** under Reports.

3. On the left menu under Local Report Profile or Global Report Profile, click **Create Report Profile**.

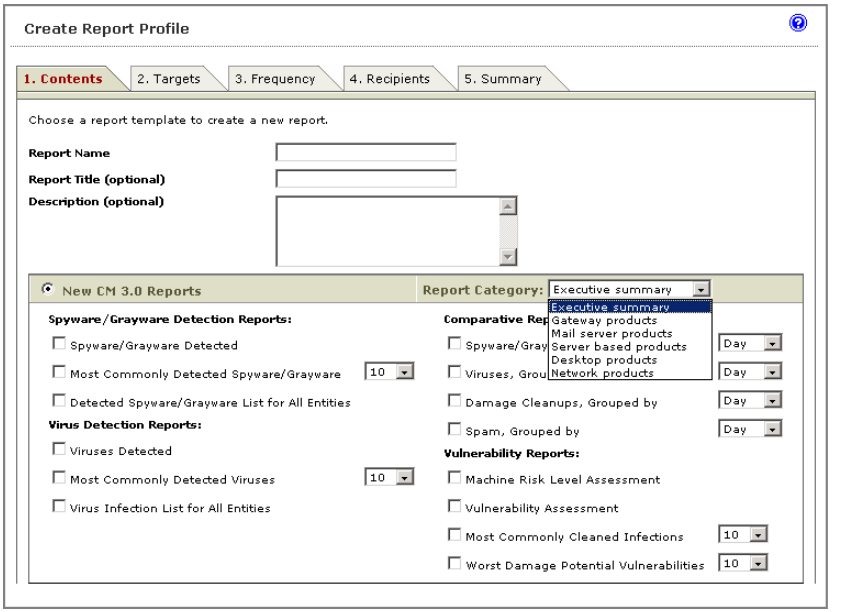


FIGURE 7-11. Create Report Profile screen, Contents tab

Step 2: Configure the Contents tab settings

1. In the working area under the **Contents** tab, type a name for the report in the **Report name** field to identify the profile on the Local Reports screen.
2. Type a title for the report in the **Report Title** field (optional).
3. Type a description of the report profile in the **Description** field (optional).
4. Select **Desktop Products** from the **Report Category** list.
5. Select the report type, the specific reports to generate, and the output format.

6. Click **Next** to proceed to the **Targets** tab.

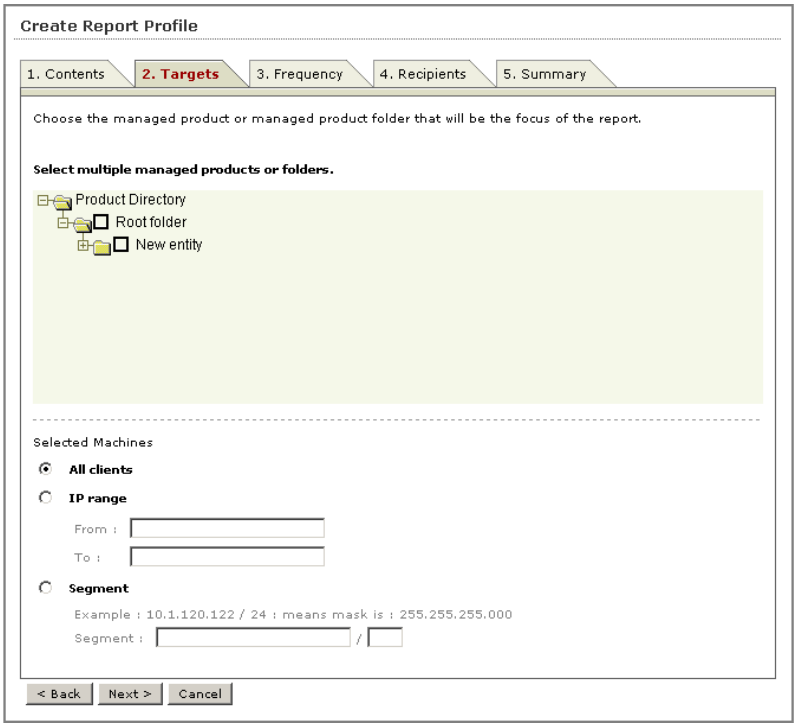


FIGURE 7-12. Create Report Profile screen, Targets tab

Step 2: Configure the Contents tab settings

1. On the working area under the **Targets** tab, select the target of the local or global report profile:
   - Select the OfficeScan server or folders. The profile only contains information about the OfficeScan or folders selected.
   - Select the child servers. The profile only contains information about the child servers selected. Select the parent server to include all child servers' managed OfficeScan servers in the profile.

2. Select the computers that the report will include:
   - **All clients:** All clients the selected OfficeScan server protects
   - **IP range:** Select the IP range of the clients you want to include in the report
   - **Segment:** Select the IP range and segment of the clients you want to include in the report
3. Click **Next** to proceed to the **Frequency** tab.

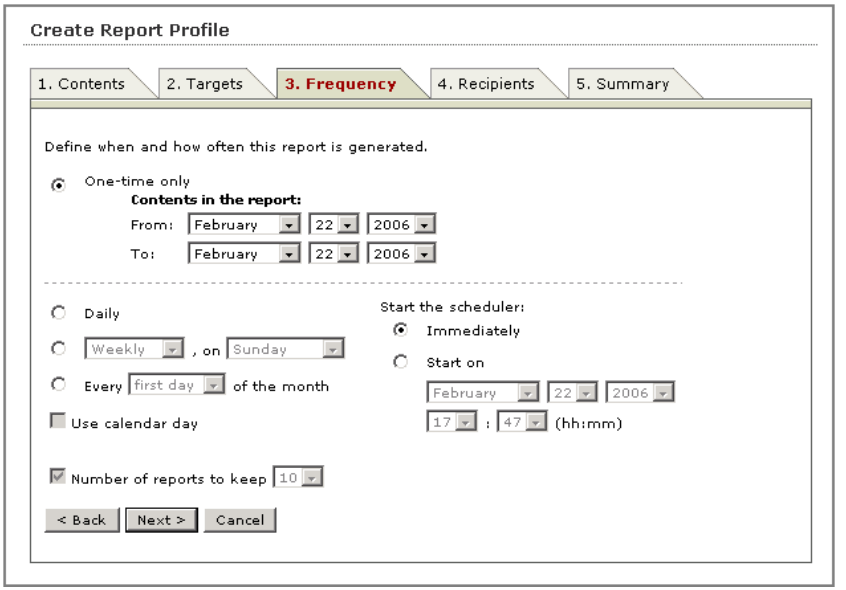


FIGURE 7-13. Create Report Profile screen, Frequency tab

Step 4: Configure the Frequency tab settings

1. On the working area under the **Frequency** tab, specify how often Control Manager generates this report. You have the following options:
   - **One-time only:** Provides information you specified in the From and To dates
   - **Daily:** Contains information from the creation time (12:00 AM yesterday) up to the current time
   - **Weekly or Bi-weekly:** Contains 7 or 14 days worth of information; select the day of the week that will trigger the report server to generate a report
   - **Monthly:** Contains 30 days worth of information; select the day of the month (first, 15th, or last day) that will trigger the report server to generate a report
   - **Use calendar day:** If checked, the start time is 00:00:00 of the first day and the end time is 00:00:00 of the day before generation

     If it is not checked, the start time is the same generation hour of the first day and end time is the generation hour of the day when generation occurs
2. Under **Start the scheduler**, specify when the Report Server starts collecting information for this report. Select one of the following:
   - **Immediately:** The report server collects information as soon as you save the report profile
   - **Start at:** The report server collects information at the specified date and time
3. For scheduled reports, click **Number of reports to keep** and then specify the instance Control Manager will maintain on the server.

Note: Control Manager automatically enables a scheduled report profile. To temporarily disable generating reports, navigate to the Local or Global Scheduled Reports screen, and then clear the check box adjacent to the scheduled report profile.

---

4. Click **Next** to proceed to the **Recipient** tab.

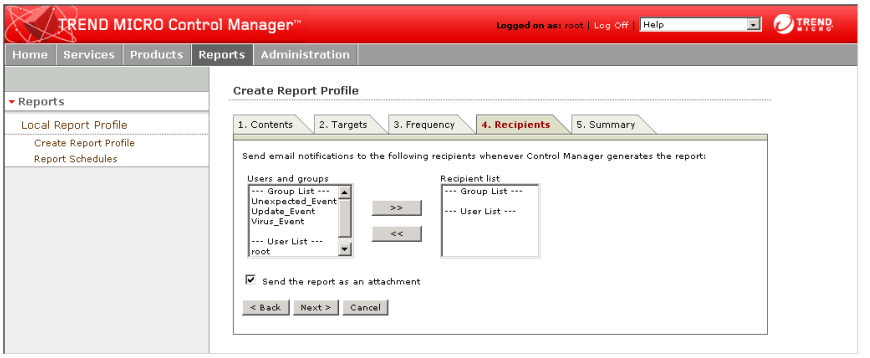


FIGURE 7-14. Create Report Profile screen, Recipients tab

Step 5: Configure the Recipient tab settings

1. On the working area under the **Recipients** tab, select recipients from the existing Control Manager users and groups.
   - Use >> to add recipients from the **Users and groups** list to the Recipient list.
   - Use << to remove recipients from the **Recipient** list.
2. Click **Send the report as an attachment** to send the report as an attachment. Otherwise, recipients will only receive an email notification about the report generated.

3. Click **Next** to proceed to the Summary tab.

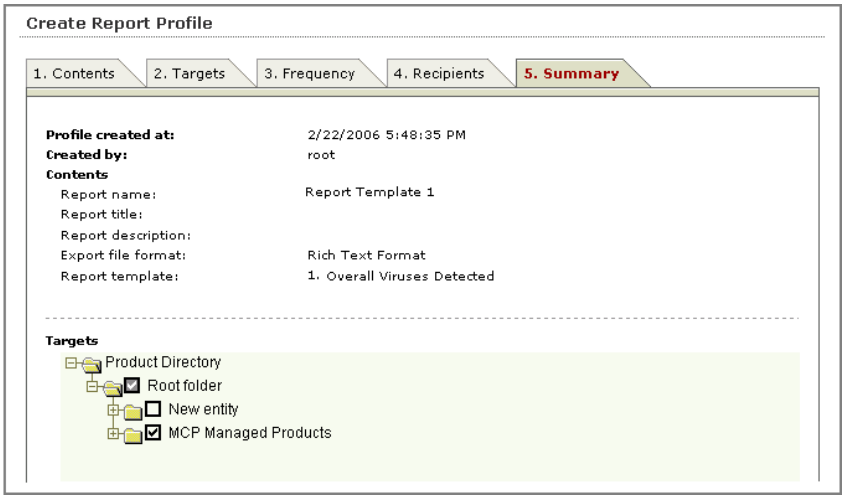


FIGURE 7-15. Create Report Profile screen, Summary tab

4. On the working area under the **Summary** tab, review the profile settings and then click **Finish** to save the profile.

Reviewing report profile settings

Use the Profile Summary screen to review profile settings.

To access Profile Summary and review report profiles:

- Access Local or Global Reports

  On the working area under the Profile Summary column, click **View Profile**.
- Access Local or Global Scheduled Reports

  On the working area under the Profile Summary column, click **View Profile**.

Enabling scheduled report profiles

By default, Control Manager enables scheduled profiles upon creation. In an event that you disable a profile (for example, during database or agent migration), you can re-enable it through the Scheduled Local Reports or Scheduled Global Reports screen.

To enable scheduled report profiles:

1. Access Local or Global Scheduled Reports.
2. On the working area under Report Profiles column, click the profile check box.

   Click the check box adjacent to Report Profiles to select or deselect all profiles.
3. Click **Enable**.

Note: The options to enable, disable, and edit one-time-only profiles are not available because Control Manager generates these reports only once.

Generating on-demand scheduled reports

The Report Server generates scheduled reports based on the date and time you specified. When the date and time has not yet commenced, use **Run Now** to create scheduled reports on demand.

To generate on-demand scheduled reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
   - To create a local report profile, click **Local Report Profile** on the left menu under Reports
   - To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the Available Reports column, click the corresponding **View** link.

4. On the Available Reports for {profile name} under **Generate a {Frequency} report starting from**, specify the starting month, day, and year.
5. Click **Run Now**.

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the **View** link adjacent to the report becomes available.

Viewing generated reports

Aside from sending and then viewing reports as email attachments, you can also use the Local Report Profile or Global Report Profile screen to view the available local or global reports.

To view reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
   - To create a local report profile, click **Local Report Profile** on the left menu under Reports
   - To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the Available Reports column, click the corresponding **View** link.

   On the Available Reports for {profile name}, you can sort reports according to **Submission Time** or **Stage Completion Time.**
4. Under the Status column, click **View Report**. The default program used to open the file format opens.

Chapter 8

FAQs and Troubleshooting Resources

Topics in this chapter:

Frequently Asked Questions (FAQs)

Component Updates

What is the maximum number of clients that an Update Agent can manage?

The number depends on the hardware specifications of the Update Agent. However, since the OfficeScan server will only notify 250 OfficeScan clients at a time and keep the notification queue on 250 for the time being, the estimate is one Update Agent will not handle over 250 downloading processes concurrently.

Even on one Update Agent instance, the maximum is 250 update requests.

What is the maximum number of update sources for each OfficeScan client?

The maximum number of update sources is 64. This information is available in the ous.ini file in the \OfficeScan\PCCSRV folder.

What are the alternative options if component update from an Update Agent fails?

The OfficeScan client gets the updates from the OfficeScan server. If the update from the OfficeScan server fails, clients with the privilege can get updates from the ActiveUpdate server.

Server Management

Which files and folders should I add to the scan exclusion list to prevent problems with Microsoft Exchange and ScanMail for Microsoft Exchange operations?

For Microsoft Exchange 2000/2003, you do not need to add folders to the scan exclusion list. Simply go to **Networked Computers > Global Client Settings > Virus/Malware Scan Settings** and select **Exclude Microsoft Exchange server folders from scanning**.

If you use Microsoft Exchange 2007, refer to the following page for scan exclusion details:

http://technet.microsoft.com/en-us/library/bb332342.aspx.

For ScanMail for Microsoft Exchange, all ScanMail for Microsoft Exchange versions, except version 7, are automatically excluded from scanning. You do not need to manually add these versions' folders to the exclusion list.

If you use version 7, add the following folders to the exclusion list:

- \Smex\Temp
- \Smex\Storage
- \Smex\ShareResPool\

Does OfficeScan allow the migration of ServerProtect for Microsoft Windows settings when migrating multiple Normal Servers to the OfficeScan server?

No. In this release, the OfficeScan server inherits the ServerProtect key features like multiple Scheduled Scans and settings during migration.

How can I disable Secure Sockets Layer (SSL)?

1. Delete the OfficeScan folder on the virtual directory or default Web site.
2. Open a command prompt and go to the PCCSRV folder.
3. Type the following: svrinst -setvirdir -disablessl
4. Open the Internet Information Services (IIS) console and verify if the OfficeScan virtual directory has been recreated.
5. Right-click the OfficeScan site or folder.
   - If OfficeScan has been installed on a separate virtual site, remove port 4343 indicated in the SSL port.
   - If OfficeScan is installed under the default Web site, remove port 443.
6. Save the changes.
7. Change the OfficeScan link in the **Start** menu.
   a. Go to the PCCSRV folder.
   b. Look for the file with the Internet Explorer icon (aside from the readme file).
   c. Check the properties under the **Web Document** tab.
   d. Change the URL as follows.
      - If installed under the default Web site: http://{server name}/officescan
      - If installed under another Web site: http://{server name}:8080/officescan
8. Launch the OfficeScan Web console to verify if SSL has been disabled.

Does the OfficeScan server provide authentication when it writes to or reads from CodeBase 6.5?

No. The dbserver.exe process is the only OfficeScan component that interfaces with the CodeBase database. It only accesses the database, and thus does not need to provide a user name and password.

When receiving information (such as component versions) from the OfficeScan client, the OfficeScan server sends the information to Dbserver.exe. The Dbserver.exe then modifies the client record on the database to reflect the component information for the client.

How can I prevent overwriting the OfficeScan client's exception list when I deploy a new firewall profile?

Open the Web console and go to **Networked Computers > Firewall > Profiles**. In the screen, make sure to disable the option **Overwrite client security level/exception list**.

Client Management

What are offline and inactive clients?

An offline client does not have functional connection with the OfficeScan server. This occurs for various reasons, such as when the client computer is unplugged, disabled, removed, or turned off.

A client becomes "inactive" if it remains offline for a certain number of days. To determine the number of days, open the Web console and go to **Administration > Inactive Clients**.

Debug Logs

How can I enable debug logging for the OfficeScan server and client?

Refer to *OfficeScan Server Logs* on page 8-5 and *OfficeScan Client Logs* on page 8-11.

Troubleshooting Resources

This section provides you a list of resources you can use to troubleshoot OfficeScan server and client issues.

Refer to the troubleshooting section of the server online help for solutions to OfficeScan issues you may encounter. Some of the solutions provided in the online help direct you to the Trend Micro Knowledge Base. Please make sure you have Internet connection to open the Knowledge Base.

Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) collects necessary debugging information from a customer's product whenever problems occur. It automatically turns the product's debug status on and off and collects necessary files according to problem categories. Trend Micro uses this information to troubleshoot problems related to the product.

To obtain this tool and relevant documentation, contact your Support provider.

OfficeScan Server Logs

Aside from logs available on the Web console, you can use other types of logs (such as debug logs) to troubleshoot product issues.

WARNING! *Debug logs may affect server performance and consume a large amount of disk space. Enable debug logging only when necessary and promptly disable it if you no longer need debug data. Remove the log file if the file size becomes huge.*

Some of the OfficeScan server logs are as follows:

Debug log using LogServer.exe

To enable debug logging for the OfficeScan server, Trend Micro Vulnerability Scanner, and Policy Server:

1. Log on to the Web console.
2. On the banner of the Web console, click the "C" in "MICRO".
3. Specify debug log settings and then click **Save**. The default file name is ofcdebug.log.
4. Check the log file in the default location: \PCCSRV\Log.

To disable debug logging for the OfficeScan server, Trend Micro Vulnerability Scanner, and Policy Server:

1. Log on to the Web console.
2. On the banner of the Web console, click the "C" in "MICRO".
3. Unmark **Enable debug log** and then click **Save**.

To enable debug logging for server installation and upgrade:

You can enable debug logging before performing the following tasks:

- Uninstall and then install the server again.
- Upgrade OfficeScan 8.0 to a new version.
- Perform remote installation/upgrade (Debug logging is enabled on the computer where you launched Setup and not on the remote computer.)

1. Copy the "LogServer" folder located in \PCCSRV\Private to C:\.
2. Create a file named ofcdebug.ini with the following content:

   [debug]

   DebugLevel=9

   DebugLog=C:\LogServer\ofcdebug.log
3. Save ofcdebug.ini to C:\LogServer.
4. Perform the appropriate task (that is, uninstall/reinstall the server, upgrade to a new server version, or perform remote installation/upgrade).
5. Check ofcdebug.log in C:\LogServer.

Local installation/upgrade log

File name: OFCMAS.LOG

Location: %windir%

Remote installation/upgrade log

On the computer where you launched Setup:

File name: ofcmasr.log

Location: %windir%

On the target computer:

File name: OFCMAS.LOG

Location: %windir%

Component update log

File name: TmuDump.txt

Location: \PCCSRV\Web\Service\AU_Data\AU_Log

To get detailed server update information:

1. Create a file named aucfg.ini with the following content:
   [Debug]
   level=-1
   [Downloader]
   ProxyCache=0
2. Save the file to \PCCSRV\Web\Service.
3. Restart the OfficeScan Master Service.

To stop collecting detailed server update information:

1. Delete aucfg.ini.
2. Restart the OfficeScan Master Service.

Client Packager log

To enable logging for Client Packager creation:

1. Modify ClnExtor.ini in \PCCSRV\Admin\Utility\ClientPackager as follows:
   [Common]
   DebugMode=3
2. Check ClnPack.log in C:\.

To disable logging for Client Packager creation:

Open ClnExtor.ini and change the "DebugMode" value from 3 to 0.

ServerProtect Normal Server Migration Tool debug log

To enable debug logging for ServerProtect Normal Server Migration Tool:

1. Create a file named ofcdebug.ini file with the following content:

   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9
2. Save the file to C:\.
3. Check ofcdebug.log in C:\.

To disable debug logging for ServerProtect Normal Server Migration Tool:

Delete ofcdebug.ini.

VSEncrypt debug log

OfficeScan automatically creates the debug log (VSEncrypt.log) in the user account's temporary folder. For example, C:\Documents and Settings\{User name}\Local Settings\Temp.

Control Manager MCP Agent debug log

Debug files on the OfficeScan server's \PCCSRV\CMAgent folder:

- Agent.ini
- Product.ini
- The screenshot of the Control Manager Settings page
- ProductUI.zip

To enable debug logging for the MCP Agent:

1. Modify product.ini in \PCCSRV\CmAgent as follows:

   [Debug]

   debugmode = 3

   debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log

2. Restart the OfficeScan Control Manager Agent service from the Windows Services screen.
3. Check CMAgent_debug.log in C:\.

To disable debug logging for the MCP Agent:

1. Open product.ini and delete the following:

   debugmode = 3

   debuglevel= 3

   debugtype = 0

   debugsize = 10000

   debuglog = C:\CMAgent_debug.log
2. Restart the OfficeScan Control Manager service.

Virus Scan Engine debug log

To enable debug logging for the Virus Scan Engine:

1. Open the Registry Editor (regedit.exe).
2. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters.
3. Change the value of "DebugLogFlags" to "00003eff".
4. Perform the steps that led to the scanning issue you encountered.
5. Check TMFilter.log in %SystemRoot%.

To disable debug logging for the Virus Scan Engine:

Restore the value of "DebugLogFlags" to "00000000".

OfficeScan Client Logs

You can use client logs (such as debug logs) to troubleshoot client issues.

WARNING! *Debug logs may affect client performance and consume a large amount of disk space. Enable debug logging only when necessary and promptly disable it if you no longer need debug data. Remove the log file if the file size becomes huge.*

Some of the OfficeScan client logs are as follows:

Debug log using LogServer.exe

To enable debug logging for the OfficeScan client:

1. Create a file named ofcdebug.ini with the following content:

   [Debug]
   Debuglog=C:\ofcdebug.log
   debuglevel=9
   debugLevel_new=D
   debugSplitSize=10485760
   debugSplitPeriod=12
   debugRemoveAfterSplit=1

2. Send ofcdebug.ini to client users, instructing them to save the file to C:\.

   LogServer.exe automatically runs each time the client computer starts. Instruct users NOT to close the LogServer.exe command window that opens when the computer starts as this prompts OfficeScan to stop debug logging. If users close the command window, they can start debug logging again by running LogServer.exe located in \OfficeScan Client.
3. For each client computer, you can check ofcdebug.log in C:\.

To disable debug logging for the OfficeScan client:

Delete ofcdebug.ini.

Fresh installation log

File name: OFCNT.LOG

Locations:

- %windir% for all installation methods except MSI package
- %temp% for the MSI package installation method

Upgrade/Hot fix log

File name: upgrade.log

Location: \OfficeScan Client\Temp

Damage Cleanup Services debug log

To enable debug logging for Damage Cleanup Services:

1. Open TSC.ini in \OfficeScan Client.
2. Modify the following line as follows: DebugInfoLevel=3
3. Check TSCDebug.log in \OfficeScan Client\debug.

To disable debug logging for Damage Cleanup Services:

Open TSC.ini and change the "DebugInfoLevel" value from 3 to 0.

Mail Scan log

File name: SmolDbg.txt

Location: \OfficeScan Client

Client connection log

File name: Conn_YYYYMMDD.log

Location: \OfficeScan Client\ConnLog

Client update log

File name: Tmudump.txt

Location: \OfficeScan Client\AU_Data\AU_Log

To get detailed client update information:

1. Create a file named aucfg.ini with the following content:
   [Debug]
   level=-1
   [Downloader]
   ProxyCache=0
2. Save the file to \OfficeScan Client.
3. Reload the client.

To stop collecting detailed client update information:

1. Delete aucfg.ini.
2. Reload the client.

Outbreak Prevention debug log

File name: OPPLogs.log

Location: \OfficeScan Client\OppLog

OfficeScan firewall debug log

To enable debug logging for the Common Firewall Driver:

1. Add the following data in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters:

   Type: DWORD value (REG_DWORD)

   Name: DebugCtrl

   Value: 0x111
2. Restart the computer.
3. Check cfw-log.txt in C:\.

To disable debug logging for the Common Firewall Driver:

1. Delete "DebugCtrl" in the registry key.
2. Restart the computer.

To enable debug logging for the OfficeScan NT Firewall service:

1. Create a file named Tmpfw.ini with the following content:

   [debug]

   debug_on=yes

   debug_level=90

   log_path=C:\TmPfw.log
2. Save the file to \OfficeScan Client.
3. Reload the client.
4. Check TmPfw.log in C:\.

To disable debug logging for the OfficeScan NT Firewall service:

1. Open Tmpfw.ini and change the "debug_on" value from "yes" to "no".
2. Reload the client.

Web Reputation debug log

To enable debug logging for the Web Reputation feature:

1. Edit TmProxy.ini located in \OfficeScan Client as follows:

   [debug]

   debug_on=yes

   debug_level=90

   log_path=C:\TmProxy.log
2. Reload the client.
3. Check TmProxy.log in C:\.

To disable debug logging for the Web Reputation feature:

1. Open TmProxy.ini and change the "debug_on" value from "yes" to "no".
2. Reload the client.

Transport Driver Interface (TDI) debug log

To enable debug logging for TDI:

1. Add the following data in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters:

   Type: DWORD value (REG_DWORD)

   Name: Debug

   Value: 1111 (Hexadecimal)

   Type: String value (REG_SZ)

   Name: LogFile

   Value: C:\tmtdi.log
2. Restart the computer.
3. Check tmtdi.log in C:\.

To disable debug logging for TDI:

1. Delete "Debug" and "LogFile" in the registry key.
2. Restart the computer.

Chapter 9

Contacting Trend Micro

Topics in this chapter:

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: 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:

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

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: virusresponse@trendmicro.com, and specify "Phish or Disease Vector" as the Subject.
- Use the Web-based submission form: 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

Configuring OfficeScan with Third-party Software

Topics in this appendix:

Overview of Check Point Architecture and Configuration

You can fully integrate OfficeScan installations with Check Point™ SecureClient™ using Secure Configuration Verification (SCV) within the Open Platform for Security (OPSEC) framework. Please familiarize yourself with Check Point SecureClient OPSEC documentation before reading this section. Documentation for OPSEC can be found at www.opsec.com.

Check Point SecureClient has the capability to confirm the security configuration of computers connected to the network using Secure Configuration Verification (SCV) checks. SCV checks are a set of conditions that define a securely configured client system. Third-party software can communicate the value of these conditions to Check Point SecureClient.

Check Point SecureClient then compares these conditions with conditions in the SCV file to determine if the client is considered secure.

SCV checks are regularly performed to ensure that only securely configured systems are allowed to connect to the network.

SecureClient uses Policy Servers to propagate SCV checks to all clients registered with the system. The administrator sets the SCV checks on the Policy Servers using the SCV Editor.

The SCV Editor is a tool provided by Check Point that allows you to modify SCV files for propagation to client installation. To run the SCV Editor, locate and run the file SCVeditor.exe on the Policy Server. In the SCV Editor, open the file local.scv in the folder C:\FW1\NG\Conf (replace C:\FW1 with the installation path for the Check Point firewall if different from the default).

For specific instructions on opening and modifying an SCV file with the SCV Editor, see *Check Point for OfficeScan Configuration* on page A-4.

OfficeScan Integration

OfficeScan client periodically passes the Virus Pattern number and Virus Scan Engine number to SecureClient for verification. SecureClient then compares these values with values in the client local.scv file.

This is what the local.scv file looks like if you open it in a text editor:

```
(SCVObject
    :SCVNames (
        : (OfceSCV
            :type (plugin)
            :parameters (
                :CheckType (OfceVersionCheck)
                :LatestPatternVersion (701)
                :LatestEngineVersion (7.1)
                :PatternCompareOp (">=")
                :EngineCompareOp (">=")
```

```
                    )
                )
            )
            :SCVPolicy (
                : (OfceSCV)
            )
            :SCVGlobalParams (
                :block_connections_on_unverified (true)
                :scv_policy_timeout_hours (24)
            )
)
```

In this example, the SCV check will allow connections through the firewall if the pattern file version is 701 or later, and the scan engine number is 7.1 or later. If the scan engine or pattern file is earlier, all connections through the Check Point firewall get blocked. Modify these values using the SCV Editor on the local.scv file on the Policy Server.

Note: Check Point does not automatically update the pattern file and scan engine version numbers in the SCV file. Whenever OfficeScan updates the scan engine or pattern file, you need to manually change the value of the conditions in the local.scv file to keep them current. If you do not update the scan engine and pattern versions, Check Point will authorize traffic from clients with earlier pattern files or scan engines, creating a potential for new viruses to infiltrate the system.

Check Point for OfficeScan Configuration

To modify the local.scv file, you need to download and run the SCV Editor (SCVeditor.exe).

To configure the Secure Configuration Verification file:

1. Download SCVeditor.exe from the Check Point download site at: www.checkpoint.com/techsupport/ng/fp3_updates.html#opsecsdk

   The SCV Editor is part of the OPSEC SDK package.
2. Run SCVeditor.exe on the Policy Server. The SCV Editor console opens.
3. Expand the **Products** folder and select **user_policy_scv**.
4. Click **Edit > Product > Modify**, and then type **OfceSCV** in the **Modify** box. Click **OK**.

> **Note:** If your local.scv file already contains product policies for other third-party software, create a new policy by clicking **Edit > Product > Add**, and then typing **OfceSCV** in the **Add** box.

5. Now add five parameters. To add a parameter, click **Edit > Parameters > Add**, and then type a **Name** and **Value** in the corresponding boxes. Table A-1 lists the parameter names and values. Parameter names and values are case-sensitive, and you must type them in the order given in Table A-1.

TABLE A-1. SCV file parameter names and values

Name	Value
CheckType	OfceVersionCheck
LatestPatternVersion	{current pattern file number}
LatestEngineVersion	{current scan engine number}
LatestPatternDate	{current pattern file release date}
PatternCompareOp	>=

TABLE A-1. SCV file parameter names and values

Name	Value
EngineCompareOp	>=
PatternMismatchMessage	
EngineMismatchMessage	

Type the most current pattern file number and scan engine number in place of the text in curly braces in Table A-1. You can view the latest virus pattern and scan engine versions for clients by clicking **Update & Upgrade** on the main menu of the OfficeScan Web console. The pattern version number will appear to the right of the pie chart representing the percentage of clients protected.

6. Select **Block connections on SCV unverified**.
7. Click **Edit > Product > Enforce**.
8. Click **File > Generate Policy File** to create the file. Select the existing local.scv file to overwrite it.

SecureClient Support Installation

If you have users that connect to the office network from a Virtual Private Network (VPN), and they have both Check Point SecureClient and the OfficeScan client installed on their computers, you can ask them to install SecureClient support. This module allows SecureClient to perform SCV checks on VPN clients, ensuring that only securely configured systems are allowed to connect to the network.

Users can verify that they have Check Point SecureClient installed on their computers by checking for the  icon in the system tray or for an item named **Check Point SecureClient** on the **Add/Remove Programs** screen of Windows.

To install SecureClient support:

1. Open the client console.
2. Click the **Toolbox** tab.
3. Under **Check Point SecureClient Support**, click **Install/Upgrade SecureClient support**. A confirmation screen appears.
4. Click **Yes**. The client connects to the server and downloads the module. When download is complete, the message "Register OfficeScan SCV" appears.
5. Click **OK**.

Appendix B

Glossary

Terms and Definitions

Term	Description
Dynamic Host Control Protocol (DHCP)	A device, such as a computer or switch, must have an IP address to connect to a network, but the address does not have to be static. A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network.
Dynamic IP Address (DIP)	A Dynamic IP address is an IP address assigned by a DHCP server. The MAC address of a computer will remain the same, however, the DHCP server may assign a new IP address to the computer depending on availability.
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.

Term	Description
File Transfer Protocol (FTP)	FTP is a standard protocol used for transporting files from a server to a client over the Internet. Refer to Network Working Group RFC 959 for more information.
Hyper Text Transfer Protocol (HTTP)	HTTP is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet.
HTTPS	Hypertext Transfer Protocol using Secure Socket Layer (SSL).
Internet Control Message Protocol (ICMP)	Occasionally a gateway or destination host uses ICMP to communicate with a source host, for example, to report an error in datagram processing. ICMP uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and implemented by every IP module. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.
Internet Protocol (IP)	"The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)
Ping	A utility that sends an ICMP echo request to an IP address and waits for a response. The Ping utility can determine if the computer with the specified IP address is online or not.
Secure Socket Layer (SSL)	SSL is a scheme proposed by Netscape Communications Corporation to use RSA public-key cryptography to encrypt and authenticate content transferred on higher-level protocols such as HTTP, NNTP, and FTP.
SSL certificate	A digital certificate that establishes secure HTTPS communication

Term	Description
SOCKS 4	A TCP protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model.
Telnet	Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.
Transmission Control Protocol (TCP)	A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols that support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.
User Datagram Protocol (UDP)	A connectionless communication protocol used with IP for application programs to send messages to other programs. Refer to DARPA Internet Program RFC 768 for information.

Index

T

U

V

W