

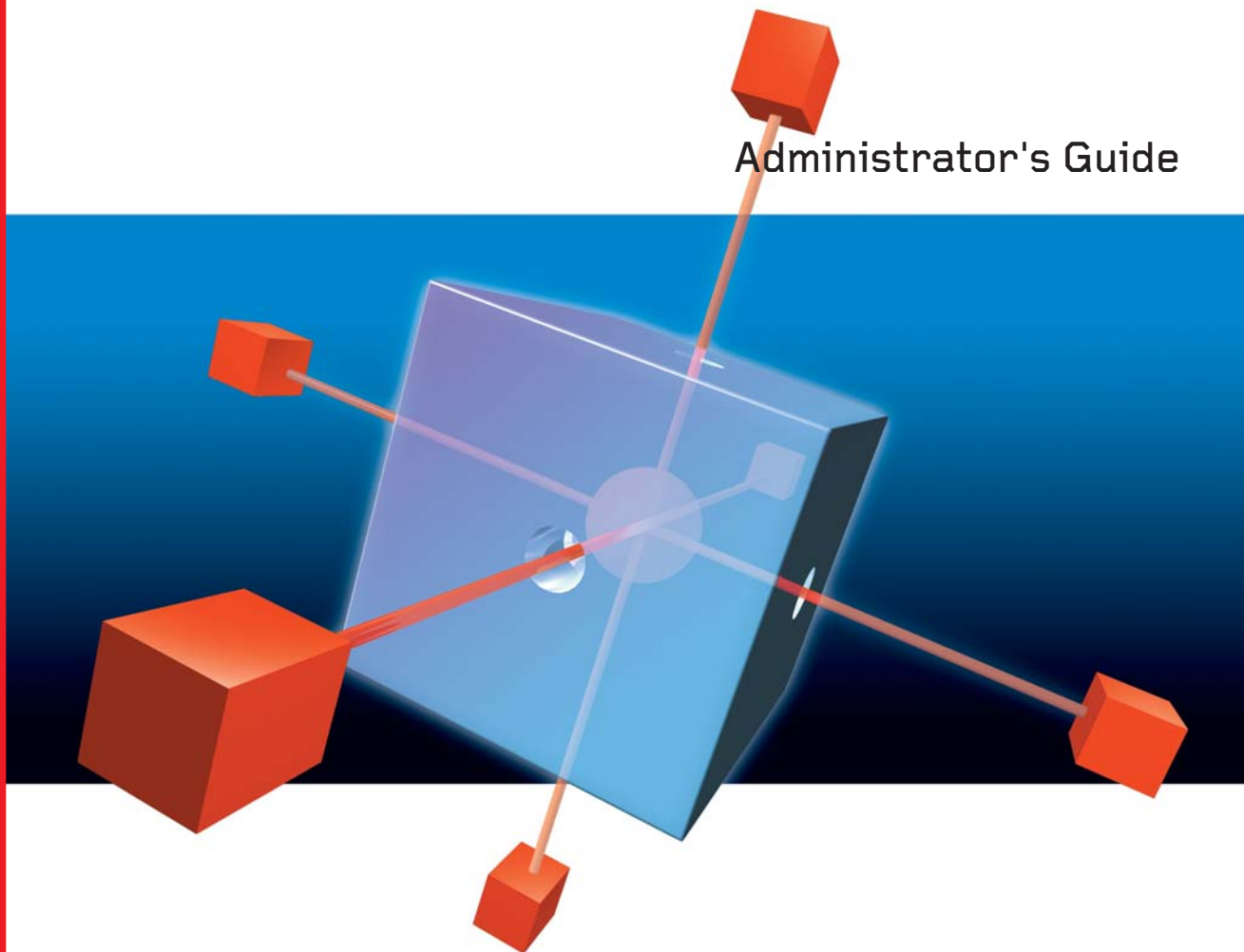
# TREND MICRO™

## OfficeScan™

## Corporate Edition 6

Comprehensive Security Protection for the Corporate Desktop

Administrator's Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Administrator's Guide, which are available from Trend Micro's Web site at:

[www.trendmicro.com/download/](http://www.trendmicro.com/download/)

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be reviewed on an annual basis at Trend Micro's then-current Maintenance fees.

Trend Micro, the Trend Micro t-ball logo, Control Manager, OfficeScan, ServerProtect, TrendLabs, and Trend Micro Damage Cleanup Services are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2004 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. OSEM61952/40617

Release Date: July, 2004

Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698; 6,119,165

The Administrator's Guide for Trend Micro OfficeScan Corporate Edition is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at [docs@trendmicro.com](mailto:docs@trendmicro.com). Your feedback is always welcome. Please evaluate this documentation on the following site:

[www.trendmicro.com/download/documentation/rating.asp](http://www.trendmicro.com/download/documentation/rating.asp)

# Contents

## **Chapter 1: What is OfficeScan™?**

What's New in OfficeScan 6.5 .....	1-2
New client-side features .....	1-2
New server-side features .....	1-3
OfficeScan Technology .....	1-3
Understanding viruses .....	1-4
How viruses spread .....	1-5
Understanding OfficeScan components .....	1-5
What you can do with OfficeScan .....	1-9
Benefits and capabilities .....	1-12
OfficeScan Server Architecture .....	1-15
OfficeScan server .....	1-15
OfficeScan client .....	1-17
Web console .....	1-20
Using the OfficeScan Documentation .....	1-20

## **Chapter 2: Planning for Deployment**

Deployment Methods .....	2-2
Overview of installation and deployment .....	2-2
Deploying OfficeScan Server .....	2-4
Determining the number of clients .....	2-4
Planning for network traffic .....	2-4
Planning the placement of program files .....	2-5
Determining the number of domains .....	2-6

Deciding how to deploy the client .....	2-6
Conducting a Pilot Deployment .....	2-6
Choosing a pilot site .....	2-7
Creating a rollback plan .....	2-7
Deploying your pilot .....	2-7
Evaluating your pilot deployment .....	2-7

## **Chapter 3: Deploying and Installing OfficeScan**

Installing OfficeScan Server .....	3-2
System requirements .....	3-2
Preparing for server installation .....	3-3
Full version and trial version .....	3-4
Required information .....	3-4
Registering OfficeScan .....	3-6
Using master installer to install OfficeScan server .....	3-6
Verifying a successful installation .....	3-13
Viewing OfficeScan and component license information .....	3-13
Activating a component license .....	3-13
Setting a Product Registration proxy .....	3-14
Default OfficeScan server settings .....	3-14
Upgrading OfficeScan .....	3-15
Upgrading from a previous version .....	3-15
Upgrading from a trial version .....	3-17
Verifying the upgrade .....	3-17
Uninstalling the OfficeScan Server .....	3-17
Installing OfficeScan Clients .....	3-19
System requirements .....	3-19
Installation using Trend Micro™ Vulnerability Scanner .....	3-20
OfficeScan client installation methods .....	3-20
Verifying a successful installation .....	3-35
Migrating to and Upgrading OfficeScan .....	3-40
Migrating from third-party antivirus applications .....	3-40

## **Chapter 4: Getting Started with OfficeScan**

Exploring the Web Console .....	4-2
Getting around the Web console .....	4-3
Other links on the console .....	4-8

---

Understanding the OfficeScan domain tree .....	4-8
Creating OfficeScan domains .....	4-9
Selecting OfficeScan domains and clients from the domain tree ..	4-9
Searching for clients .....	4-10
Refreshing the tree .....	4-11
Understanding the domain tree icons .....	4-11
Working with OfficeScan domains .....	4-12
Updating OfficeScan .....	4-13
Choosing an update source .....	4-13
Updating the server .....	4-14
Using Update Agent .....	4-17
Updating clients .....	4-20
Rolling back components .....	4-25
Verifying Client-Server Connection .....	4-26
Setting up Standard Notifications .....	4-26
Configuring standard alerts .....	4-27
Configuring outbreak alerts .....	4-29
Configuring the Scan Settings .....	4-31
Configuring Manual Scan .....	4-32
Configuring Real-time Scan .....	4-34
Configuring Scheduled Scan .....	4-36
Excluding files and folders from scanning .....	4-39
Running Scan Now .....	4-40
Granting Privileges to Clients .....	4-43
Importing and Exporting Policies .....	4-44
 <b>Chapter 5: Performing Additional Administrative Tasks</b>	
Changing the Web Console Password .....	5-2
Modifying Client Alert Messages .....	5-2
Configuring an Intranet Proxy .....	5-3
Changing OfficeScan Web Server Information .....	5-4
Removing Inactive Clients .....	5-4
Configuring the Quarantine Manager .....	5-5
Participating in the World Virus Tracking Program .....	5-6
 <b>Chapter 6: Managing Outbreaks</b>	
Using Outbreak Prevention .....	6-2

Blocking shared folders .....	6-2
Blocking ports .....	6-3
Denying write access to files and folders .....	6-6
Configuring client notification for outbreaks .....	6-7
Restoring network settings to normal .....	6-8
Configuring Virus Outbreak Monitor .....	6-9
Using Damage Cleanup Services .....	6-10
Running Cleanup Now .....	6-11

## **Chapter 7: Configuring Enterprise Client Firewall**

Understanding Enterprise Client Firewall .....	7-2
Understanding policies, exceptions, and profiles .....	7-2
Firewall defaults .....	7-4
Enterprise Client Firewall features .....	7-6
Deploying the Firewall .....	7-7
Verifying Deployment .....	7-10
Configuring Enterprise Client Firewall .....	7-11
Configuring policies .....	7-11
Configuring exceptions .....	7-12
Configuring profiles .....	7-14
Configuring Firewall Outbreak Monitor .....	7-16
Disabling the Firewall .....	7-17

## **Chapter 8: Viewing and Interpreting Logs**

Viewing and Interpreting Logs .....	8-2
Viewing virus logs .....	8-2
Deleting virus logs .....	8-3
Viewing server update logs .....	8-4
Viewing client update logs .....	8-4
Viewing system event logs .....	8-5
Viewing verify connection logs .....	8-6
Viewing Enterprise Client Firewall logs .....	8-6
Managing Logs .....	8-7

## **Chapter 9: Troubleshooting and Technical Support**

Client-server Communication .....	9-2
Incorrect Number of Clients on the Web Console .....	9-2

Incorrect Client Status on the Web Console .....	9-2
Incorrect Component Versions .....	9-3
Unsuccessful Installation from Web page or Remote Install .....	9-4
Client Icon Does Not Appear on Web Console After Installation .....	9-5
Issues During Migration from Third-party Antivirus Software .....	9-6
Client migration .....	9-6
Client Connection Time-out Occurs Frequently .....	9-8
Contacting Trend Micro .....	9-10
The Trend Micro Security Information Center .....	9-10
Known Issues .....	9-11
Contacting Technical Support .....	9-11
The Trend Micro Knowledge Base .....	9-12
Sending Suspicious Files to Trend Micro .....	9-12
About TrendLabsSM .....	9-13

## **Appendix A: Using OfficeScan Tools**

Administrative Tools .....	A-2
Database backup .....	A-3
Login Script Setup .....	A-4
Vulnerability Scanner .....	A-4
Server Tuner .....	A-9
Client Tools .....	A-10
Client Packager .....	A-10
Image Setup Utility .....	A-11
Restore Encrypted Files .....	A-11
Client Mover I .....	A-13
Touch Tool .....	A-14
Integrated Tools .....	A-15

## **Appendix B: Using Control Manager™ with OfficeScan**

Introducing Control Manager .....	B-2
What You Can do with Control Manager and OfficeScan .....	B-2
What is a Control Manager Agent? .....	B-3
Requirements for Installing the Agent .....	B-3
Required Information for Agent Installation .....	B-3
Obtaining the Public Encryption Key .....	B-4
Installing the Control Manager Agent .....	B-4



Accessing OfficeScan with Control Manager .....	B-7
Removing the Agent .....	B-7

## **Appendix C: Policy Server for Cisco™ NAC Primer**

Introduction to Trend Micro Policy Server for Cisco NAC .....	C-2
Understanding Components and Terms .....	C-2
Components .....	C-2
Terms .....	C-3
Cisco NAC Architecture .....	C-4
The Client Validation Sequence .....	C-5
Understanding the Policy Server .....	C-7
Understanding Policy Server policies and rules .....	C-8
Understanding Synchronization .....	C-14
Understanding Certificates .....	C-14
Understanding the CA certificate .....	C-16
Policy Server system requirements .....	C-16
Cisco Trust Agent (CTA) requirements .....	C-17
Accepted Cisco router models .....	C-18

## **Appendix D: Deploying Policy Server Cisco NAC**

Policy Server for NAC Deployment Overview .....	D-2
Enrolling the Cisco Secure ACS server .....	D-3
Exporting and Installing the CA Certificate .....	D-7
Preparing the Policy Server SSL Certificate .....	D-9
Deploying the Cisco Trust Agent .....	D-11
Verifying Cisco Trust Agent installation .....	D-12
Installing the Policy Server for Cisco NAC .....	D-13
Configuring the ACS Server .....	D-15
Configuring the Policy Server for Cisco NAC .....	D-16
Adding and removing Policy Servers .....	D-17
Viewing summary information for a Policy Server .....	D-18
Adding or editing OfficeScan servers .....	D-20
Configuring rules .....	D-22
Configuring policies .....	D-24
Using the client validation logs .....	D-26
Performing administrative tasks .....	D-28

## **Appendix E: Configuring OfficeScan with Add-ons and Third-party Software**

About Wireless Protection Manager .....	E-2
PDA system requirements .....	E-3
Installing Wireless Protection Manager .....	E-3
Using Wireless Protection Manager .....	E-5
Opening Wireless Protection Manager .....	E-5
Updating OfficeScan for Wireless .....	E-5
Downloading update components .....	E-6
Enabling and configuring proxy settings .....	E-6
Synchronizing with Your PDA .....	E-7
Working with logs .....	E-7
Overview of Check Point Firewall Architecture and Configuration ..	E-9
Integrating with OfficeScan .....	E-9
Configuring Check Point for OfficeScan .....	E-11
Installing SecureClient Support on the OfficeScan Client .....	E-12

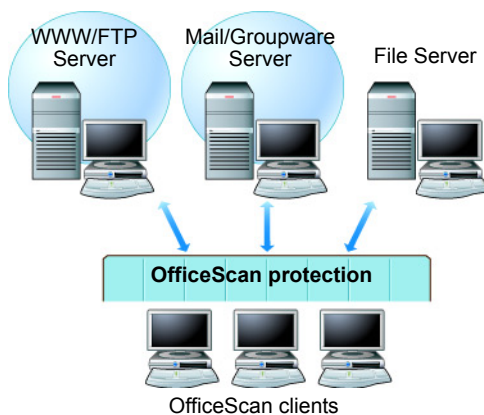
## **Appendix F: Glossary of Terms**



## What is OfficeScan™?

Trend Micro OfficeScan is a centrally managed antivirus solution for desktops, notebook computers, and servers. OfficeScan helps protect your organization's Windows™ NT/2000/XP/Server 2003 and Windows 95/98/Me computers from viruses and malicious code, including file viruses, macro viruses, and malicious Java™ applets and ActiveX™ controls.

The antivirus function of OfficeScan is provided through the client, which reports to and gets updates from the server. The OfficeScan Web console allows you to configure, monitor, and update clients.



**FIGURE 1-1 OfficeScan protection**

OfficeScan includes the following:

- OfficeScan server, which hosts the Web console, downloads updates from the Trend Micro ActiveUpdate server, collects and stores logs, and helps you control virus outbreaks
- OfficeScan client, which protects your Windows NT/2000/XP/Server 2003 and Windows 95/98/Me computers from viruses, Trojans, and other threats
- OfficeScan management console, also referred to as the Web console, which you use to manage your clients from one location

## What's New in OfficeScan 6.5

This version of OfficeScan inherits all the features of previous versions and provides the following new features:

### New client-side features

- **Enterprise Client Firewall** – helps protect OfficeScan clients from common network-based hacker attacks and network viruses
- **Update Agent** – redistributes the burden that updating components puts on the OfficeScan server. Allow specified clients to act as Update Agents- sources for

updated components. Other clients can receive updates from the Update Agents rather than the OfficeScan server.

- **Client access privileges (client security)** – control client user access to the OfficeScan client program folders and registry files. This prevents client users from deleting or altering the files necessary for the OfficeScan client program to function properly.

## New server-side features

- **Support for Policy Server for Cisco Network Admission Control (NAC)** – enforce antivirus policies on your OfficeScan clients by using Cisco NAC technology to identify at-risk computers. You can configure policies to modify OfficeScan client program settings based on analyses of client antivirus status.
- **Support for multi-server and remote server installation** – install or upgrade OfficeScan server on several server machines at the same time
- **Virus Outbreak Monitor** – use Virus Outbreak Monitor to observe the network for suspicious activity that may indicate infections
- **Manage policies** – import and export client policies, which include scan settings and privileges
- **Advanced Search** – when you want to modify client settings, you can search for specific clients based on a wide range of criteria, such as IP address, online status, and virus pattern file version
- **HTTP Server Selection** – install OfficeScan server on the included Apache 2.0.48 HTTP server or on a pre-installed Microsoft IIS server
- **SSL support** – enable Secure Socket Layer (SSL) for secure Web browser/Web server communications

## OfficeScan Technology

OfficeScan uses a reliable virus scanning and virus removal technology with the capabilities to help protect your network environment from malicious code.

## Understanding viruses

Tens of thousands of viruses 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.

Most computer viruses fall into the following categories:

- **ActiveX malicious code** – resides in Web pages that execute ActiveX controls
- **Boot sector viruses** – infects the boot sector of a partition or a disk
- **COM and EXE file infectors** – executable programs with .com or .exe extensions
- **Java malicious code** – operating system-independent virus code written or embedded in Java
- **Macro viruses** – encoded as an application macro and often included in a document
- **Trojan horses** – executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter
- **HTML, VBScript, or JavaScript viruses** – reside in Web pages and are downloaded through a browser
- **Worms** – a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email

## Network viruses

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the threats 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 machines, 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 disk-based file I/O scanning methods.

Enterprise Client Firewall works with a network virus pattern file to identify and block network viruses (see [Configuring Enterprise Client Firewall](#) on page 7-1 for more information on Enterprise Client Firewall).

## How viruses spread

In today's increasingly interconnected work place (email, the Internet, intranets, shared drives, FTP sites, removable drives, etc.) virus outbreaks can now occur suddenly. Whereas historically viruses typically spread by file and disk sharing, currently viruses can infect computers, mail systems, Web servers, and LANs through several different methods:

- Email, and email attachments
- Web traffic
- FTP traffic (file downloads)
- Shared network files and network traffic in general

## Understanding OfficeScan components

OfficeScan uses the following components to scan for, identify, and perform damage cleanup tasks to help protect and clean OfficeScan clients:

- **Client program:** the OfficeScan client program, which uses the virus pattern file and scan engine to identify infections and perform actions on infected files
- **Virus pattern file:** a file that helps OfficeScan identify virus signatures: unique patterns of bits and bytes that signal the presence of a virus (see [About the virus pattern file](#) on page 1-6 for more information)
- **Scan engine:** the engine OfficeScan uses to scan for viruses
- **Additional Threats pattern file:** a file that helps OfficeScan identify unique patterns of bits and bytes that signal the presence of a certain types of potentially undesirable files and programs, such as adware and spyware
- **Damage cleanup template:** used by the damage cleanup engine, this template helps identify Trojan files and processes so the engine can eliminate them
- **Damage cleanup engine:** the engine Damage Cleanup Services uses to scan for and remove Trojans and Trojan processes



- **Common firewall driver:** Enterprise Client Firewall uses the driver with the network virus pattern file to scan client machines for network viruses
- **Network virus pattern file:** like the virus pattern file, this file helps OfficeScan identify virus signatures
- **Cisco Trust Agent (if Policy Server for Cisco NAC is installed):** the program that enables communication between the OfficeScan client and routers supporting Cisco NAC

## About the virus pattern file

The Trend Micro scan engine uses an external data file, called the virus pattern file. It contains information that helps OfficeScan identify the latest viruses and other Internet threats such as Trojan horses, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly threat is discovered.

All Trend Micro antivirus programs using the ActiveUpdate function can detect the availability of a new virus pattern file on the Trend Micro server, and/or can be scheduled to automatically poll the server every week, day, or hour 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 virus 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 scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique “signature” or string of tell-tale characters that distinguish it from any other code, the virus experts at TrendLabs™ capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When a match is found, a virus has been detected and a notification is sent via an email message to the system administrator.

## Pattern file numbering

To allow you to compare the current pattern file in your software products to the most current pattern file available from Trend Micro, pattern files are assigned a version number.

There are two pattern file numbering systems currently in use at Trend Micro.

1. The traditional pattern file number is 3 digits, in the format *xxx*, for example, 786.
2. The new pattern file numbering system, which came into use during 2003, utilizes 6 digits, in the format *x.xxx.xx*.
  - The first digit is currently set to 1, indicating the new numbering system.
  - The next 3 digits represent the traditional pattern file number.
  - The last 2 digits provide additional information about the pattern file release for Trend Micro engineers.

Pattern release 786 in the new format might appear as 1.786.01.

Keep your pattern file updated to the most current version to safeguard against the most current threats.

## About 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, phishing 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 are developed and used for research

Rather than scan 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. If OfficeScan detects a virus, it can remove it and restore the integrity of the file.

The scan engine includes an automatic clean-up routine for old virus pattern files (to help manage disk space), as well as incremental pattern updates (to help manage bandwidth).

In addition, the scan engine is able to decrypt all major encryption formats (including MIME and BinHex). It also recognizes and scans common compression formats, including Zip, Arj, and Cab. OfficeScan also allows you to determine how many layers of compression to scan (up to a maximum of 20), for compressed files contained within a file.

It is important that the scan engine remain current with new threats. Trend Micro ensures this in two ways:

- Frequent updates to the virus pattern file, which can be downloaded and read by the engine without the need for any changes to the engine code itself (see [About the virus pattern file](#) on page 1-6)
- Technological upgrades in the engine software prompted by a change in the nature of virus threats, such as a rise in mixed threats like SQL Slammer

The Trend Micro scan engine is certified annually by international computer security organizations, including ICSA (International Computer Security Association).

## Updating the scan engine

By storing the most time-sensitive virus information in the virus pattern file, 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:

- New scanning and detection technologies are incorporated into the software
- A new, potentially harmful virus is discovered that the scan engine cannot handle
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit the Trend Micro Web site:

<http://www.trendmicro.com>

## What you can do with OfficeScan

Perform key administrative tasks using the OfficeScan Web console:

- Analyze your network's protection against viruses
- Enforce antivirus policies
- Update your protection
- Perform virus scans from one location
- Quarantine infected files
- Control outbreaks on the network
- Manage OfficeScan domains and clients
- Protect clients from hacker attacks with Enterprise Client Firewall
- Protect your PDAs from viruses
- Evaluate client antivirus status and take action on at-risk clients

### Analyze your network's protection against viruses

OfficeScan can generate various types of logs, including virus logs, system event logs, update logs, and verify connection logs. Use these logs to verify update deployment, check client-server communication, and determine which computers are vulnerable to infection.

Also use these as a basis for designing and redesigning network protection, identifying which computers are at a higher risk of infection, and changing the antivirus settings accordingly for these computers.

### Enforce antivirus policies

OfficeScan provides three types of scans: Real-time Scan, Scheduled Scan, and Manual Scan. Enforce your organization's antivirus policies throughout the network by configuring the three types of scans based on these policies. Specify the types of files to scan and the action to take when OfficeScan finds a virus.

To ensure that uniform scan settings are applied to all clients, choose not to grant privileges to clients and lock the client program with a password to prevent users from removing or turning it off.

## Update your protection

Virus writers create new viruses and release them via different media everyday, especially the Internet. To ensure that you stay protected against the latest threats, you must periodically update the OfficeScan components. Trend Micro usually releases new virus pattern files on a weekly basis.

## Perform virus scans from one location

The Web console provides the option of performing Scan Now (Manual Scan) and configuring scheduled scans on clients to run during off-peak hours when network traffic is low.

## Quarantine infected files

You can specify a quarantine folder to control live viruses and infected files. OfficeScan then automatically forwards infected files to the quarantine folder.

## Control outbreaks on the network

Defining the criteria for an outbreak and setting up outbreak notifications allows you to quickly respond to outbreaks that may be developing on the network. When you receive an outbreak notification, enable Outbreak Prevention to prevent viruses from spreading.

By blocking shared folders and vulnerable ports and denying write access to files on clients, Outbreak Prevention helps stop outbreaks from overwhelming your network. Download the latest pattern file, and then perform Scan Now on all clients to remove any existing viruses.

## Manage OfficeScan domains and clients

A domain in OfficeScan is a group of clients that share the same configuration and run the same tasks. An OfficeScan domain is different from a Windows domain. There can be several OfficeScan domains in any given Windows domain.

Group clients into OfficeScan domains to simultaneously apply the same configuration to all domain members, making clients easier to manage.

## Protect clients from hacker attacks with Enterprise Client Firewall

Help protect OfficeScan Windows NT/2000/XP/Server 2003 clients from hacker attacks and network viruses by creating a barrier between the client machine and the network. Enterprise Client Firewall allows you to create customized policies and profiles to block or allow certain types of network traffic. Additionally, enable the Intrusion detection system to identify patterns in network packets that may indicate an attack on clients.

## Protect your PDAs from viruses

Viruses and other malicious code can infect your personal digital assistant (PDA) devices during beaming, synchronization, or Internet access. Protect your Palm™, Pocket PC™, or EPOC™ devices from these threats by installing OfficeScan for Wireless.

To install OfficeScan for Wireless on your Palm, Pocket PC, or EPOC device, open the client console and download Wireless Protection Manager.

For detailed instructions on how to install OfficeScan for Wireless, refer to the help topic *Protecting your PDA* on the OfficeScan client.

For more information on OfficeScan for Wireless, see [Configuring OfficeScan with Add-ons and Third-party Software](#) on page E-1. In Windows Explorer, you can also open the Quick Start Guide by double-clicking `Wireless Protection Manager Manual.pdf` in the `Trend Micro\Wireless Protection Manager` folder.

---

**Note:** To open `Wireless Protection Manager Manual.pdf`, you must have Adobe™ Reader™ installed. You can download Acrobat Reader for free from [www.adobe.com](http://www.adobe.com).

---

## Evaluate client antivirus status and take action on at-risk clients

The Trend Micro™ Policy Server for Cisco Network Admission Control (NAC) evaluates client antivirus status and determines what actions the clients should perform, such as updating components or enabling Real-time Scan, based on policies

you configure. Policy Server allows you to integrate OfficeScan clients with a Cisco NAC server and Network Access Devices, such as Cisco routers.

## **Benefits and capabilities**

OfficeScan brings many benefits to your organization by providing a comprehensive yet user-friendly method of managing your antivirus initiatives. The following is a summary of the advantages you can obtain with OfficeScan.

### **Single-console operation**

OfficeScan server allows you to manage your entire anti-virus system through a single Web console. The Web console is installed when you install OfficeScan server and uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

### **Virus Outbreak Monitor**

Virus Outbreak Monitor gets OfficeScan clients involved in virus-detection. Clients can notify the OfficeScan server when they detect suspicious activity occurring on the network. OfficeScan can then send an automatic notification message to the administrator to take proper action.

### **Outbreak Prevention**

With Outbreak Prevention, you can take preemptive steps to secure your network:

- Block shared folders to help prevent viruses from infecting files in shared folders
- Block ports to help prevent viruses from using vulnerable ports to infect files on the network
- Deny write access to files and folders to help prevent viruses from modifying files
- Create an alert message to display on OfficeScan clients when you create an outbreak prevention policy

### **Trend Micro IntelliScan**

IntelliScan is a new method of identifying files to scan. For executable files (for example, .zip and .exe), the true file type is determined based on the file content. For

non-executable files (for example, .txt), the true file type is determined based on the file header.

Using IntelliScan provides the following benefits:

- Performance optimization – IntelliScan does not affect crucial applications on the client because it uses minimal system resources
- Shorter scanning period – Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

## **Trend Micro ActiveAction**

Different types of viruses require different scan actions. Customizing scan actions for different types of viruses requires knowledge about viruses and can be a tedious task. ActiveAction is a set of pre-configured scan actions for viruses and other types of Internet threats. The recommended action for viruses is Clean, and the alternative action is Quarantine. The recommended action for Trojans and joke programs is Quarantine.

If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus, Trend Micro recommends using ActiveAction. Using ActiveAction provides the following benefits:

- Time saving and easy to maintain – ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- Updateable scan actions – Virus writers constantly change the way viruses attack computers. To help ensure that clients are protected against the latest threats and the latest methods of virus attacks, new ActiveAction settings are updated in virus pattern files.

## **Scanning for Additional Threats**

Your clients are at risk from threats other than viruses. Additional threats, including files and programs, can negatively affect the performance of the computers on your network.



---

**Note:** OfficeScan does not scan for these additional threats by default. Enable scanning for additional threats when configuring Manual Scan, Real-time Scan, Scheduled Scan, or Scan Now (see *Configuring the Scan Settings* on page 4-31).

---

OfficeScan can detect several types of additional threats, including the following:

- **Spyware** – software stored on client machines to gather data, such as user names and passwords, and transmits them to third parties
- **Adware** – similar to spyware, adware gathers user data, such as Web surfing preferences, that are commonly used for advertising purposes
- **Dialers** – software that changes client Internet settings and can force the client machine to dial pre-configured phone numbers through a modem
- **Joke program** – software that causes the client machine to behave abnormally, such as forcing the screen to shake
- **Hacking tools** – programs used to help hackers enter the client machine
- **Remote access tools** – programs used to help hackers access and control the client machine from a remote location
- **Password cracking applications** – software that can help hackers decipher user names and passwords
- **Others** – other types of threats not covered above

---

**Tip:** Trend Micro recommends enabling scanning for additional threats if users on your network do not require use of remote access or hacking tools.

---

## Trend Micro™ Damage Cleanup Services

Trend Micro Damage Cleanup Services (DCS) help restore your Windows system after a Trojan attack. A Trojan, like a virus, attacks your system (but unlike a virus, a Trojan cannot self-replicate).

When a Trojan is executed, you will likely experience unwanted system problems in operation, and sometimes loss of valuable data. These are indications that you should run Trend Micro Damage Cleanup Services on your system.

Two versions of Damage Cleanup Services are available at no charge – one for Trend Micro customers, and one for the general public. Download Damage Cleanup Services from the following Web site:

<http://www.trendmicro.com/download/dcs.asp>

Both versions do the following:

- terminate instances of Trojans in memory
- remove Trojan registry entries
- remove Trojan entries from system files
- scans for and delete Trojan copies in local hard drives

See *Using Damage Cleanup Services* on page 6-10 for more information on running DCS.

## Secure Web console communication

OfficeScan provides secure communications between the OfficeScan server and the Web console browser through Secure Socket Layer (SSL) technology.

OfficeScan server can generate a certificate for each Web console session, allowing the Web console browser to encrypt data based on Public Key Infrastructure (PKI) cryptography standards. The default time period for the certificate is three years.

## OfficeScan Server Architecture

OfficeScan is a two-tier application consisting of the following parts:

- The server, which hosts the Web console, downloads updates from an update source (such as the Trend Micro ActiveUpdate server), and provides updated components to clients.
- The client, which protects Windows NT/2000/XP/Server 2003 and Windows 95/98/Me computers from viruses, Trojans, and other malicious programs

### OfficeScan server

The OfficeScan server is the central repository for all client configurations, virus logs, and client software and updates.

The server performs these important functions:

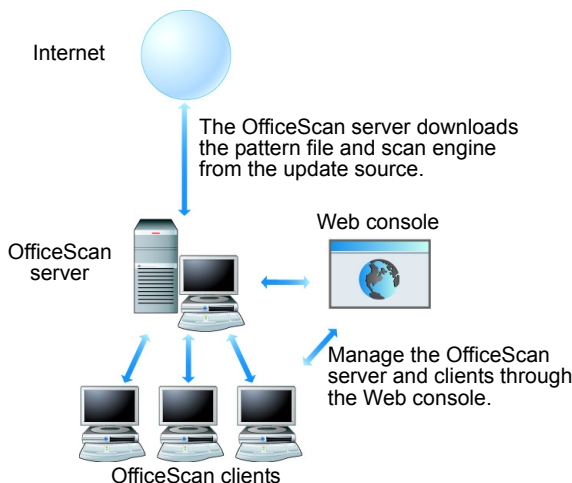
- It installs, monitors, and manages clients on the network
- It downloads virus pattern files, scan engines, and program updates from the Trend Micro update server, and then distributes them to clients

## **HTTP-based server**

The HTTP-based server is installed on a Windows NT, Windows 2000, Windows XP, or Windows Server 2003 with Internet Information Server™ (IIS) 4.0 or later. You may also install Apache Web server 2.0 or later on Windows 2000/XP/Server 2003 machines. The HTTP-based server is capable of providing real-time, bidirectional communication between the server and clients.

You can manage the clients from a Web browser-based Web console, which you can access from virtually anywhere on the network.

The server communicates with the client (and vice versa) via HyperText Transfer Protocol (HTTP). The HTTP-based server can only install HTTP-based clients. You cannot install an HTTP-based client if the client computer does not support TCP/IP (see Figure 1-2).



**FIGURE 1-2 How the HTTP-based server works**

## OfficeScan client

Protect Windows computers from viruses 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 [Client Mover I](#) on page A-13 for more information). 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 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 (see [Granting Privileges to Clients](#) on page 4-43 for more information).











There are two types of OfficeScan clients:

- Normal clients
- Roaming clients

## Normal clients

Normal clients are computers with the OfficeScan client installations and are stationary computers that maintain a continuous network connection with the server.

Icons that appear in a client's system tray indicate the status of the normal client. See Table 1-1 for a list of icons that appear on the normal client.

Icon	Description	Real-time Scan
	Normal client	Enabled
	Pattern file is outdated	Enabled
	Scan Now, Manual Scan, or Scheduled Scan is running	Enabled
	Real-time Scan is disabled	Disabled
	Real-time Scan is disabled and the pattern file is outdated	Disabled
	Real-time Scan Service is not running (red icon)	Disabled
	Real-time Scan Service is not running and the pattern file is outdated (red icon)	Disabled
	Disconnected from the server	Enabled
	Disconnected from the server and the pattern file is outdated	Enabled
	Disconnected from the server and Real-time Scan is disabled	Disabled

**TABLE 1-1. Icons that appear on a normal client**

## Roaming clients

Roaming clients are computers with the OfficeScan client installations and do not always maintain a constant network connection with the server (for example, notebook computers). These clients continue to provide antivirus protection, but have delays in sending their status to the server.







Assign roaming privileges to clients that are disconnected from the OfficeScan server for an extended period of time.

Roaming clients get updated only on these occasions:

- When the client performs Update Now
- When you configure automatic update deployment and select **Include roaming clients** on the **Automatic Deployment** screen

For more information on how to update clients, see [Updating clients](#) on page 4-20.

The status of a roaming client is indicated by icons that appear in its system tray. See Table 1-2 for a list of icons that appear on roaming clients.

Icon	Description	Real-time Scan
	Roaming client (blue icon)	Enabled
	Real-time Scan is disabled	Disabled
	Pattern file is outdated	Enabled
	Real-time Scan is disabled and the pattern file is outdated	Disabled
	Real-time Scan Service is not running (red icon)	Disabled
	Real-time Scan Service is not running and the pattern file is outdated (red icon)	Disabled

**TABLE 1-2. Icons that appear on roaming clients**

## Web console

The Web console is the central point for monitoring OfficeScan across the entire network, as well as for configuring server and client settings.

It gives you complete control over desktop and notebook computer antivirus settings. Use the Web console to do the following:

- Deploy the client program to desktop and notebook computers
- Group desktop and notebook computers into logical domains for simultaneous configuration and management
- Set scan configurations and start Manual Scan on a single computer or on multiple computers
- Receive notifications and view log reports for virus activities
- Receive notifications when viruses are detected on clients and send virus outbreak alerts via email, pager, SNMP Trap, or Windows Event Log
- Control outbreaks by configuring and enabling Outbreak Prevention

The Web console is installed when you install OfficeScan server. The Web console uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

Open the Web console from any computer on the network that has the required Web browser and communication protocols (see *System requirements for the Web console* on page 3-3).

## Using the OfficeScan Documentation

The documentation set for OfficeScan includes the following:

- **Administrator's Guide** – This guide helps you get “up and running” by introducing OfficeScan, assisting with installation planning, implementation, and configuration, and describing the main product functions. It also includes instructions on testing your installation using a harmless test file. The latest version of the Administrator's Guide is available in electronic form at the following location:

<http://www.trendmicro.com/download/>

- **Online help** – The purpose of online help is to provide descriptions for performing the main tasks, usage advice, and field-specific information, such as

valid parameter ranges and optimal values. Online help is accessible from the OfficeScan Web console.

- **Readme file** – The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and product release history.
- **Knowledge Base** – The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site:

<http://kb.trendmicro.com>





# Planning for Deployment

This chapter explains how to plan your network environment for the deployment of OfficeScan server and OfficeScan clients.

The topics discussed in this chapter include:

- *Deployment Methods* on page 2-2
- *Deploying OfficeScan Server* on page 2-4
- *Conducting a Pilot Deployment* on page 2-6

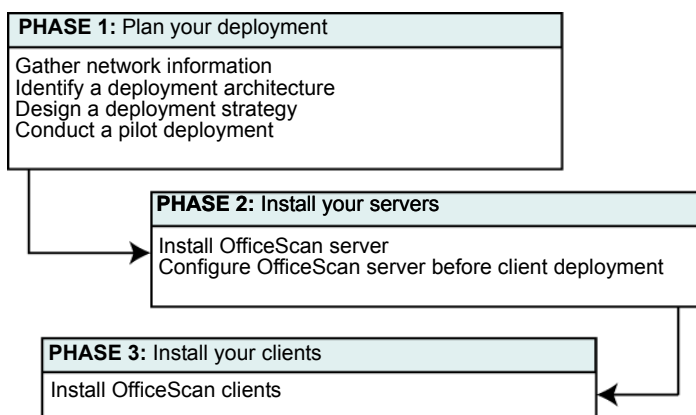
To take advantage of the benefits OfficeScan can bring your organization, you will need an understanding of the possible ways to deploy OfficeScan Server and OfficeScan clients. This section provides an overview of deployment architectures and strategies, network traffic planning, and an approach to pilot deployment.

# Deployment Methods

Deploying enterprise-wide, client-server software like OfficeScan requires careful planning and assessment.

## Overview of installation and deployment

This guide groups installation and deployment tasks into three phases. Each phase has corresponding sections that discuss in detail the tasks that you need to perform.



**FIGURE 2-1** Installation and deployment tasks

## Phase 1

During phase 1, plan how best to deploy OfficeScan by completing these tasks:

- Determine the number of clients
- Plan the placement of the program files
- Determine the number of domains
- Decide how to deploy the client

---

**Tip:** Trend Micro highly recommends conducting a pilot deployment before doing a full-scale deployment.

---

If you are deploying OfficeScan to multiple sites, you need to perform these additional tasks:

- Determine the number of sites
- Plan for network traffic
- Determine where you need to install the servers
- Decide how to deploy the server
- Decide how to deploy the clients

See *Deploying OfficeScan Server* on page 2-4 for details.

## Phase 2

During phase 2, start implementing the plan you have created in phase 1 for server installation. You complete this phase by performing the following tasks:

- Verify that your server meets the minimum system requirements
- Prepare for server installation
- Install your OfficeScan server
- Verify that the installation was successful
- Check if you need to modify the default settings (for example, scan settings and privileges) before deploying the clients

See *Installing OfficeScan Server* starting on page 3-2 for details.

## Phase 3

During phase 3, complete your installation and deployment by rolling out the client to your desktop and notebook computers. You complete this phase by performing the following tasks:

- Verify that the target computers meet the minimum system requirements
- Prepare for client installation
- Roll out your clients using Trend Micro tools or third-party tools

See *Installing OfficeScan Server* starting on page 3-2 for details.

## Deploying OfficeScan Server

This section provides information on deploying the OfficeScan server.

### Determining the number of clients

A client is a computer that has the OfficeScan client software installed on it. This includes desktop and notebook computers, including those that belong to users who telecommute or connect to the corporate network from their homes.

If you have a heterogeneous client base (that is, if your network has different Windows operating systems, such as Windows NT/2000/XP/Server 2003 and 95/98/Me), identify how many clients are using a specific Windows version. Use this information to decide which client deployment method will work best in your environment.

---

**Note:** A single OfficeScan server can manage up to 50,000 OfficeScan clients.

---

### Planning for network traffic

When planning for deployment, consider the network traffic that OfficeScan will generate. OfficeScan generates network traffic when the server and client communicate with each other.

The server generates traffic when it does the following:

- Connects to the Trend Micro update server to check for and download updated components
- Notifies clients to download updated components
- Notifies clients about configuration changes

The client generates traffic when it does the following:

- Starts up
- Performs scheduled update

- Switches between roaming mode and normal mode
- Performs Update Now

## **Network traffic during pattern file updates**

Significant network traffic is only generated when there is an updated version of the virus pattern file, scan engine, program, Additional Threats pattern file, firewall components and damage cleanup engine and template. To reduce network traffic generated during pattern file updates, OfficeScan uses a method called incremental update. Instead of downloading the full pattern file every time it is updated, only the new patterns that have been added since the last release are downloaded. These new patterns are merged with the old pattern file.

If clients are regularly updated, they only have to download the incremental pattern, which is around 500KB to 900KB. If clients are not regularly updated, they may have to download the full pattern, which is around 2.5MB to 3MB when compressed and 5MB when uncompressed.

Trend Micro releases new pattern files every week. However, if a particularly damaging virus is actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available.

## **Determining to install a dedicated server**

When selecting a server that will host OfficeScan, consider the following:

- How much CPU load is the server carrying?
- What other functions does the server perform?

If you are installing OfficeScan on a server that has other uses (for example, application server), Trend Micro recommends that you install on a server that is not running mission-critical or resource-intensive applications.

## **Planning the placement of program files**

During the OfficeScan server installation, specify where to install the program files on the clients. Either accept the default client installation path or modify it. Trend Micro recommends that you use the default settings, unless you have a compelling reason (such as insufficient disk space) to change them.

The default client installation path is:

C:\Program Files\Trend Micro\OfficeScan Client

## Determining the number of 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.

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

For ease of management, plan how many OfficeScan domains to create. You can group clients based on the departments they belong to or the functions they perform. Alternatively, you can group clients that are at a greater risk of infection and apply a more secure configuration to all of them.

## Deciding how to deploy the client

OfficeScan provides several client deployment methods. Determine which ones are most suitable for your environment. For a complete list of available client deployment methods, see [Installing OfficeScan Clients](#) on page 3-19.

For single site deployment, IT administrators can choose to deploy using Login Script Setup, wherein a program called `autopcc.exe` is added to the login script. When an unprotected client logs on to the domain, the server detects it and automatically deploys the client setup program. The OfficeScan client is deployed in the background and the client user does not notice the installation process.

In organizations where IT policies are strictly enforced, client installation via the internal Web page is recommended. The administrator sends out an instruction to users to visit an internal Web page where they can install the OfficeScan client with just a click of the button.

## Conducting a Pilot Deployment

Before performing a full-scale deployment, Trend Micro recommends that you first conduct a pilot deployment in a controlled environment. A pilot deployment provides

an opportunity to determine how features work and the level of support you will likely need after full deployment.

It also gives the installation team a chance to rehearse and refine the deployment process and test if your deployment plan meets your organization's business requirements.

Perform the following tasks to conduct a pilot deployment:

- Choose a pilot site
- Create a rollback plan
- Deploy your pilot
- Evaluate your pilot deployment

## Choosing a pilot site

Choose a pilot site that matches your production environment. Try to simulate the type of network topology that would serve as an adequate representation of your production environment.

## Creating a rollback plan

Trend Micro recommends creating a disaster recovery or rollback plan in case there are issues with the installation or upgrade process.

This process should take into account local corporate policies, as well as technical specifics.

## Deploying your pilot

Evaluate the different deployment methods (see [Deployment Methods](#) on page 2-2) to see which ones are suitable for your particular environment.

## Evaluating your pilot deployment

Create a list of successes and failures encountered throughout the pilot process. Identify potential pitfalls and plan accordingly for a successful deployment. This pilot evaluation plan can be rolled into the overall production deployment plan.





# Deploying and Installing OfficeScan

This chapter explains installation of OfficeScan Server and OfficeScan for clients. It also illustrates how to migrate and upgrade OfficeScan.

The topics discussed in this chapter include:

- *Installing OfficeScan Server* on page 3-2
- *Upgrading OfficeScan* on page 3-15
- *Uninstalling the OfficeScan Server* on page 3-17
- *Installing OfficeScan Clients* on page 3-19

# Installing OfficeScan Server

This section provides information on installing OfficeScan server.

## System requirements

The following are requirements to install the OfficeScan server:

- 300MHz Intel Pentium™ II processor or equivalent
- Operating system:
  - Microsoft™ Windows™ NT series (Service Pack 6a or above)
  - Windows 2000 Series (Service Pack 2 or above)
  - Windows XP (Professional Edition only, Service Pack 1 or above)
  - Windows Server 2003
- 128MB of RAM
- 300MB of disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft Internet Explorer 5.5 or later
- Web server:
  - Microsoft Internet Information Server (IIS)
    - on Windows NT: version 4.0
    - on Windows 2000: version 5.0
    - on Windows XP: version 5.1
    - on Windows Server 2003: version 6.0
  - Apache Web server 2.0 or later (for Windows 2000/XP [Service pack 1 or later]/Server 2003 only)
- Administrator or Domain Administrator access on the server machine
- File and printer sharing for Microsoft Networks installed on the server machine

---

**Note:** If you are planning to install the Cisco Trust Agent on the same computer as the OfficeScan server, do not install OfficeScan server on Windows Server 2003. See [Cisco Trust Agent \(CTA\) requirements](#) on page C-17 for more information on requirements for CTA.

---

## System requirements for the Web console

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

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

## Preparing for server installation

To help you deploy OfficeScan to your network smoothly, check the following items before installing the server:

- Where to run the setup program
- Required protocols
- Required rights
- Required restarts
- Required information
- Windows licenses
- TCP port for HTTP communication

## Required protocols

Before starting the installation, ensure that the server and clients have Transmission Control Protocol/Internet Protocol (TCP/IP) installed.

## Required rights

To install the server, you must have administrator or domain administrator rights to the target computer.

## Required restarts

Installing the OfficeScan server does not require you to restart the computer. After completing the installation, immediately configure the server, and then proceed to rolling out clients.

While installing the Web server, the setup program automatically stops and restarts the IIS service.

---

**WARNING!** *Make sure that you do not install the server on a computer that is running applications that might lock IIS, which will cause the installation to be unsuccessful.*

---

## Full version and trial version

When you install OfficeScan, you can install either a full version or a free, trial version:

- **Full version** – comes with technical support, virus pattern downloads, real-time scanning, and program updates for one year. You can renew a full version by purchasing a maintenance renewal.
- **Trial version** – provides real-time scanning and updates for 30 days. You can upgrade a trial version to a full version at any time.

---

**Note:** Both versions require an Activation Code to perform installation. If you do not have an Activation Code, register your version (see [Registering OfficeScan](#) on page 3-6)

---

## Required information

Have the following information ready before starting the installation:

- **Registration Key/Activation Code.** Your version of OfficeScan comes with a Registration Key. During installation, OfficeScan prompts you to enter the Activation Code and can redirect you to the Trend Micro Web site. Register your version of OfficeScan with the Registration Key and Trend Micro will provide you the Activation Code. If you do not have the Registration Key or Activation

Code, contact your Trend Micro sales representative (see [Contacting Technical Support](#) on page 9-11).

- **Proxy information.** If a proxy server handles Internet traffic on your network, you must type the proxy server information and your user name and password to be able to download the latest components, including the virus pattern file, scan engine and program from the Trend Micro update server. If you leave the proxy information blank during installation, you can still configure it on the OfficeScan console.
- **Console password.** To prevent unauthorized access to the OfficeScan Web console, specify a password that will be required of anyone who tries to open the console.
- **Custom client alert messages (optional).** When the OfficeScan client detects a virus on a computer during real-time scan or a firewall violation, an alert message appears. Customize the message that is displayed on the clients.
- **Client software installation path (optional).** Configure the client installation path where OfficeScan files will be copied to during client setup.

## Windows licenses

Make sure your organization has sufficient licenses for all clients to simultaneously connect to the server.

## TCP port for HTTP communication

Most hacker and virus attacks these days are delivered over HTTP. A large number of these attacks are directed at port 80, which is used in most organizations as the default Transmission Control Protocol (TCP) port for HTTP communication.

If your organization is currently using port 80 as its HTTP port, Trend Micro recommends using another port number that is less susceptible to hacker and virus attacks.

OfficeScan uses the same port number as your HTTP server's TCP port. Setup automatically retrieves this information when you install the OfficeScan server. If you are currently using port 80 as your HTTP port and want to change to another port number, do this before installing the OfficeScan server. Otherwise, reinstall the OfficeScan server to ensure successful client-server communication.

## Registering OfficeScan

You must register your version of OfficeScan to obtain an Activation Code. The registration process includes filling out an online form, which requires you to enter the Registration Key. Make sure you have the Registration Key that came in the OfficeScan package.

There are two ways to register Officescan:

- Register online before performing installation by visiting the following Trend Micro Web site:

`http://www.trendmicro.com/support/registration.asp`

- Register during installation by clicking **Register online** on the **Product Activation** screen (see *Using master installer to install OfficeScan server* on page 3-6).

Trend Micro sends the Activation Code to the email address you specify during registration.

## Using master installer to install OfficeScan server

Before running the OfficeScan setup program, try testing the server's fully-qualified domain name using the ping command in Windows to ensure that communication with it can be established. Also test the port number, IIS anonymous user logon, and the network's proxy settings.

---

**Note:** You need to remove the server program of your existing third-party antivirus software before installing the OfficeScan server.

---

---

**Note:** Close any running applications before installing the server. If you install while other applications are running, the installation process may take longer to complete.

---

### To install OfficeScan server:

1. Open the folder that contains the setup files and double-click **Setup** (SETUP.EXE). The **Welcome** screen appears.

2. Click **Next**. The **OfficeScan Software License Agreement** screen appears.
3. Read the agreement carefully, and then click **Yes** to agree to all the terms. The **Cisco NAC License Agreement** screen appears.
4. Read the agreement carefully, and then click **Yes** to agree to the all the terms. If you do not agree at this time, you cannot deploy Cisco NAC Policy Servers. You can choose not to agree at this time and later agree to this license on the OfficeScan server Web console. The **Choose Destination** screen appears.
5. Choose where to install or upgrade to this version of OfficeScan by clicking one of the following:
  - **I will install/upgrade OfficeScan Server on this computer**
  - **I will install/upgrade OfficeScan Server on a remote computer or on multiple computers**

If you selected to install on the current computer, the **Web Server** screen appears.

If you selected to install on a remote computer or on multiple computers, the **Choose Where to Install** screen appears. Do the following:

- a. Type the computer name or click **Browse** and select a computer on your network.
- b. Click **Add**. The computer name appears in the text box. Continue adding as many computers as necessary.

If you have a list of computer names saved as a text (.txt) file, click **Import list** and select the file.

To delete an entry in the list, select it and then click **Remove**.

- c. Click **Next**.

---

**Note:** If you are upgrading remotely, OfficeScan preserves the original settings from the previous installation, including the server name, proxy server information, and listening and HTTP port numbers. You cannot modify these settings during upgrade. Use the OfficeScan Web console to modify these settings.

---

6. Choose the Web server for the OfficeScan server:
  - **IIS server:** click **Install OfficeScan server on the IIS server** to install OfficeScan on an existing IIS installation



- **Apache 2.0:** click **Install OfficeScan server on Apache Web server 2.0** to install Apache 2.0 on an existing installation. If an Apache Web server version 2.0 or later installation is not found, Apache 2.0 will be installed automatically.

---

**Note:** OfficeScan will run on an Apache Web server only on Windows 2000/XP/Server 2003 machines.

---

7. Click **Next**. The **Server Information** screen appears.
8. Configure the following information:
  - **Server information:** click one of the following:
    - **Domain name:** verify the target server domain name. You can also use the server's fully qualified domain name (FQDN) if necessary to ensure successful client-server communication.
    - **IP address:** verify that the target server's IP address is correct. Clicking **IP address** is not recommended if the OfficeScan obtains an IP address from a DHCP server.

---

**Tip:** If the server has multiple network interface cards (NICs), Trend Micro recommends using one of the IP addresses, instead of the domain name or FQDN, to ensure successful client-server communication.

---

- If you selected to install OfficeScan on an IIS server, select one of the following in the **IIS Website** section:
  - **IIS default Web site** – click to install as an IIS default Web site (in the IIS default Web site folder)
  - **IIS virtual Web site** – click to install as an IIS virtual Web site (in the IIS virtual Web site folder)
- Under **Port number**, type a port to use as the server listening port.  
`http://{OfficeScan_server_name}:{port number}/officeScan`
- You also have the option of enabling Secured Socket Layer (SSL) security. Select the **Enable SSL** check box. Type the number of years to keep the SSL certificate valid (the default is 3 years) and type an SSL port number. If you enable SSL,

this port number will serve as the server's listening port. The OfficeScan server's address will be as follows:

```
https://{OfficeScan_server_name}:{port  
number}/officeScan
```

9. Click **Next**. A confirmation screen appears.

10. Verify the server information is correct and click **Yes**.

- If installing OfficeScan on the current computer (if you selected **I will install/upgrade OfficeScan Server on this computer** on the Choose Destination screen) the **Proxy Server** screen appears. Go to Step 11.
- If performing a remote install or installing on multiple computers (if you selected **I will install/upgrade OfficeScan Server on a remote computer or on multiple computers** on the **Choose Destination** screen), the **Target Server Analysis** screen appears. Do the following:
  - i. Click **Analysis**. The installer checks the computer to find out if it requires a new OfficeScan server program installation or an upgrade. You may need to type the administrator user name and password for that computer. If so, click **OK** after typing the information. The result appears under **Status** on the **Target Server Analysis** screen.

---

**Note:** If the installer cannot determine this information for any computers you selected, **Failed** appears under **Status**, and the installer will not install OfficeScan server on the selected computers. At least one computer must pass the analysis before the installation can continue.

---

ii. To save the list of computers you selected, click **Export** in the **Target Server Analysis** screen. The list is saved as a text file (.txt).

iii. Click **Next**.

11. If your organization uses a proxy server, type the required information such as the proxy address, port, and your user name and password for proxy server authentication. If your organization uses SOCKS 4, select the **Use SOCKS 4** check box.

Verify that the information you provided on the screen is correct. The OfficeScan server will use this information to connect to the Trend Micro update server and download updated components, such as pattern files and scan engines.

Click **Next** to continue. The **Administrator Account Password** screen appears.

12. Create OfficeScan administrator passwords for access to the Web console and for clients to unload/uninstall the client program. Confirm the passwords in the text boxes. This helps prevent unauthorized users from accessing the Web console and modifying your settings or removing the clients.
13. Click **Next**. The **Components Selection** screen appears.
14. Select the check boxes next to the components to install or enable:
  - **Install client protection to target OfficeScan server:** install the OfficeScan client program on the same machine you are installing the OfficeScan server

---

**Note:** The **Install client protections to target OfficeScan server** check box appears only if no installation of OfficeScan client exists on the machine. If an OfficeScan installation exists, the installer upgrades it automatically.  
You cannot install the OfficeScan client program on a machine running Trend Micro ServerProtect™ for Windows NT. Uninstall ServerProtect before installing OfficeScan client to the OfficeScan server machine.

---

- **Install Control Manager agent:** install the Control Manager agent to allow Control Manager to manage the OfficeScan server (see *Using Control Manager™ with OfficeScan* on page B-1 for more information)
- **Install Policy Server for Cisco NAC:** install Policy Server for Cisco NAC (see *Installing the Policy Server for Cisco NAC* on page D-13 for more information)
- **Enable Agent Deployment for Cisco NAC:** automatically deploy the Cisco Trust Agent when deploying OfficeScan clients

---

**Note:** Installation for Control Manager agent and Policy Server for Cisco NAC continues after OfficeScan server installation (see step Step 34).

---

15. Click **Next**. The **World Virus Tracking Program** screen appears.
16. Read the statement and click **Yes** to enroll in the World Virus Tracking Program or click **No** to decline to participate.
17. Click **Next**. The **Server Settings Finished** screen appears.
18. Click **Next**. The **Product Activation** screen appears.

19. Check if you have an OfficeScan Activation Code:
  - If you have the Activation Code for OfficeScan, click **Next**. The **Product Activation** screen appears.
  - If you do not have the Activation Code, click **Register online**. Your Web browser opens to the Trend Micro registration Web site.

Make sure you have the Registration Key that came with the OfficeScan package. Follow the instructions for new customer registration and Trend Micro will email you an Activation Code.
20. Type the Activation Codes for the following:
  - **Standard Antivirus:** to install OfficeScan Activation Code
  - **Damage Cleanup:** to install Damage Cleanup Services (optional)
21. Click **Next**. The **Product Registration Settings Finished** screen appears.
22. Confirm that the correct items will be installed.

---

**Note:** When you install OfficeScan server, Enterprise Client Firewall is also installed. If you do not want to install Enterprise Client Firewall, clear the Install Enterprise Client Firewall check box.

---

23. Click **Next**. The **Installation Path** screen appears.
24. Do the following to set an installation path:
  - Type an installation path
  - Click **Enable network scan for mapped drives and shared folders** to have OfficeScan client include mapped drives and shared folders during scanning
  - Modify the trusted port number so that it does not conflict with any other ports used in your internal network. This is a randomly generated port number through which the server will communicate with its clients.
25. Click **Next**. A confirmation screen appears.
26. Verify the port number and click **OK** to continue. The **Client Alert Message** screen appears.
27. Modify the default alert messages that appear on client machines if OfficeScan detects a virus, a firewall violation, and/or a network virus.
28. Click **Next**. The **Client Security Level** screen appears.
29. Click one of the following:

- **Normal:** assigns the access privileges already configured for the client Program Files and registry files to OfficeScan client files and OfficeScan client registries.
- **High:** restricts access privileges to OfficeScan client files and OfficeScan client registries.

---

**Note:** If you select **High**, the access permissions settings of the OfficeScan folders, files, and registries are inherited from the WINNT file (for client machines running Windows NT) or from the Program Files folder (for client machines running Windows 2000/XP/Server 2003).

---

30. Click **Next**. The **Client Settings Finished** screen appears.
31. Click **Next**. The **Select Program Folder** screen appears.
32. The Master Installer adds program icons to the folder listed under **Program Folder**. Modify it if necessary.
33. Click **Next**. The OfficeScan installation process commences. After installation completes, the **Shared Folder** screen appears.

If you selected **I will install/upgrade OfficeScan Server on a remote computer or on multiple computers** on the **Choose Destination** screen, a confirmation screen appears. Click **OK** to complete the installation.
34. Click **Next**. If you selected to install Control Manager agent or Policy Server for Cisco NAC, the installation commences (see *Installing the Control Manager Agent* on page B-4 and *Installing the Policy Server for Cisco NAC* on page D-13 for more information).
35. Click **Next**. The **Setup Complete** screen appears.

You have completed installing your OfficeScan server. Open the Web console or view the readme file by selecting the corresponding check box.
36. Click **Finish**.

---

**Note:** You can configure the OfficeScan settings using the Web console immediately after completing the installation and before deploying the clients. To start configuring basic OfficeScan settings, see *Getting Started with OfficeScan* on page 4-1.

---

## Verifying a successful installation

After completing the installation, verify that the OfficeScan server is properly installed.

**To verify the installation, do the following:**

- Look for the OfficeScan program shortcuts on the Windows **Start** menu of the OfficeScan server
- Check if OfficeScan is in the **Add/Remove Programs** list of the OfficeScan server's Control Panel
- Log on to the Web console with the server's URL:

`http://{OfficeScan_server_name}:{port number}/OfficeScan`

or if using SSL:

`https://{OfficeScan_server_name}:{port number}/OfficeScan`

where `{OfficeScan_server_name}` is the name or IP address you designated.

## Viewing OfficeScan and component license information

View detailed information about your licenses online, including the current license status.

**To view current license information and status:**

1. Open the OfficeScan Web console.
2. On the sidebar, click **Administration > Product License**. The **Product License** screen appears.
3. Click **View detailed license online** to see your license and click **Check Status Online** to see the status of your license.

## Activating a component license

If you did not activate components, such as Damage Cleanup Services, during OfficeScan installation, you can activate them from the Web console. You must register a component before using it. Ensure you have the component Activation Code or Registration Key.

**To activate a component:**

1. Click **Administration > Product License** on the sidebar, then click **Enter a new code** for the component you want to register. The **Enter a New Code** screen appears.
2. Enter the Activation Code and click **Activate**. If you do not have the Activation Code, click **Register Online** at the top of the screen and use the Registration Key to obtain an Activation Code.

## Setting a Product Registration proxy

If your network uses a proxy server to connect to the Internet, configure proxy settings to connect to the Product Registration server.

**To set the Product Registration proxy:**

1. Open the OfficeScan Web console.
2. On the sidebar, click **Administration > Product License > Product Registration Proxy**. The **Product Registration Proxy** screen appears.
3. Select the **Enable Internet Proxy** check box.
4. Type the address of the proxy server and its port number.
5. If your proxy server uses version 4 of the SOCKS protocol to handle Transmission Control Protocol (TCP), select the **Use SOCKS 4** check box.
6. If your proxy server requires a password, type your user name and password in the fields provided.
7. Click **Save** to save your settings.

## Default OfficeScan server settings

When you install OfficeScan server, the following default settings will apply. You may change the default settings to customize your installation.

- **Web Server – IIS Server**

A version of IIS server must already be installed on your computer if you keep the default selection.

If you select the Apache Web server and it is not already installed on your computer, OfficeScan installation automatically installs Apache Web server 2.0.48 (for Windows 2000/XP/Server 2003 only).

- **Components** – Standard Antivirus, Damage Cleanup

Standard antivirus protection installs the Trend Micro antivirus scan engine on client computers so client users can perform manual scans and have the maximum level of protection with real-time scan. Damage Cleanup installs the Trend Micro Damage Cleanup Services to remove remnants of Trojans that may exist on the system if an infection occurs.

- **Default Server Port** – 8080
- **SSL Port** – 4343
- **Target Directory** – C:\Program Files\Trend Micro\OfficeScan
- **Shared Folder Directory** – C:\Program Files\Trend Micro\OfficeScan\PCCSRV
- **Client-Server Port (Trusted Port)** – OfficeScan generates a random port number

OfficeScan server uses this port to communicate with OfficeScan clients. Ensure that this port does not conflict with your network environment.

- **Client Alert Message** – OfficeScan displays an alert message on a client whenever it detects a virus, Enterprise Client Firewall Violation, or when it determines a client is the source of an infection. A general message is provided for each during installation. If you do not want messages to appear, delete them. Create a new messages at any time through the Web console.

## Upgrading OfficeScan

You can upgrade to a full version of OfficeScan 6.5 from a previous version or from a trial version (see [Full version and trial version](#) on page 3-4 for more information on the differences between the full and trial versions).

### Upgrading from a previous version

Upgrading from a previous version of OfficeScan is a two-step process:

1. Back up `ofcscan.ini` and the database.



## 2. Upgrade the server using Master Upgrade.

---

**Tip:** Trend Micro recommends deleting all log files from the OfficeScan server before upgrading. If you want to preserve the log files, save them to another location first.

---

Client upgrade should be automated if you configured OfficeScan to automatically deploy updates to the clients whenever the server gets an update.

---

**Note:** This version of OfficeScan cannot be upgraded from Client/Server Suite or Client/Server/Messaging Suite.

---

## Backing up ofcscan.ini and the database

To ensure that you can easily restore your existing settings if the upgrade is unsuccessful, Trend Micro highly recommends backing up the `ofcscan.ini` file (where all settings are stored) and the database (where client records are stored).

Use the Database Backup Tool that came with your current version of OfficeScan. Refer to the documentation that was provided with your original OfficeScan installation. Information about Database backup is also available on page A-3.

## Upgrading using Master Upgrade

Master Upgrade refers to running the Master Installer to install a newer version of OfficeScan on the existing server. The upgrade procedure is very similar to installing OfficeScan with Master Installer. The only difference is that when specifying the server on which to install OfficeScan, you select your existing OfficeScan server. For more information on how to run Master Setup, see *Installing OfficeScan Server* on page 3-2).

---

**Note:** Upgrade OfficeScan server from any previous version of OfficeScan Corporate Edition. This does not include OfficeScan 6.0 for Small and Medium Businesses (SMB).

---

## Upgrading from a trial version

When your trial version is about to expire, OfficeScan displays a notification message on the **Summary** screen. You can upgrade from a trial version to the full version of OfficeScan through the Web console without losing any of your configuration settings. When you purchase a license to the full version, you will be given a Registration Key or an Activation Code.

### To upgrade from a trial version:

1. Open the OfficeScan Web console.
2. On the sidebar, click **Administration > Product License**. The **Product License** screen appears.
3. Click **Enter a new code**.
4. If you have an Activation Code, type it in the **New Activation Code** field and click **Activate**.

If you do not have an Activation Code, click Register Online and use the Registration Key to obtain an Activation Code.

## Verifying the upgrade

After upgrading OfficeScan, you can use the Trend Micro Vulnerability Scanner to check if you still have clients using the previous version. This tool checks computers for installed antivirus software and the versions they are using based on an IP address range you specify.

You can get Vulnerability Scanner from the `\PCCSRV\Admin\Utility\TMVS` folder of the OfficeScan server.

For more information on Vulnerability Scanner, see [Using Vulnerability Scanner to verify the client installation](#) on page 3-35 and [Vulnerability Scanner](#) on page A-4.

## Uninstalling the OfficeScan Server

OfficeScan uses an uninstall program to safely remove OfficeScan server from your computer. Remove all clients before removing the server.

**To remove the OfficeScan server:**

1. On the computer you used to install the server, click **Start > Programs > Trend Micro OfficeScan Server > Uninstall OfficeScan**.  
A confirmation screen appears.
2. Click **Yes**. Master Uninstaller, the server uninstallation program, prompts you for the administrator password.
3. Type the administrator password in the text box and click **OK**. Master Uninstaller then starts removing the server files. A confirmation message appears.
4. Click **OK** to close the uninstallation program.

## Installing OfficeScan Clients

This section provides information on installing OfficeScan clients.

### System requirements

The OfficeScan client has slightly different sets of requirements for Windows 95/95OSR2/98/Me, Windows NT/2000, and Windows XP/Server 2003.

#### System requirements for the Windows 95/98/Me client

To install the client to Windows 95/98/Me computers, they must have the following:

- 133MHz Intel™ Pentium™ processor or equivalent
- Microsoft Windows 95/98/98 SE/Me
- 64MB of RAM
- 80MB of disk space
- Monitor that supports 640 x 480 resolution at 256 colors or higher
- Microsoft Internet Explorer 4.01 or later
- Microsoft Internet Explorer 5.0 or later if need to perform Web setup

#### System requirements for the Windows NT/2000 client

To install the client to Windows NT (with Service Pack 6a) or Windows 2000 (with Service Pack 2 or later) computers, they must have the following:

- 150MHz Intel Pentium processor or equivalent
- Microsoft Windows NT 4.0 Workstation/Server with SP6a or above, Windows 2000 Server/Advanced Server/Professional with SP2 or above
- 64MB of RAM
- 80MB of disk space
- Monitor that supports 640 x 480 resolution at 256 colors or higher
- Microsoft Internet Explorer 4.01 or later
- Microsoft Internet Explorer 5.0 or later if need to perform Web setup

## System requirements for the Windows XP/Server 2003

To install the client to Windows XP (Home or Professional Edition with Service Pack 1) and Windows Server 2003 computers, they must have the following:

- 300MHz Intel Pentium processor or equivalent
- 128MB of RAM
- 80MB of disk space
- Monitor that supports 800 x 600 resolution at 256 colors
- Microsoft Internet Explorer 6.0 or later if need to perform Web setup

## Installation using Trend Micro™ Vulnerability Scanner

Use Trend Micro Vulnerability Scanner to identify desktop and notebook computers on your network that are not protected against viruses. This tool checks computers on your network for installed antivirus software based on an IP address range you specify.

Get Vulnerability Scanner from the \PCCSRV\Admin\Utility\TMVS folder of the OfficeScan server.

For more information on Vulnerability Scanner, see *Vulnerability Scanner* on page A-4.

## OfficeScan client installation methods

OfficeScan provides several methods to deploy the client. This section discusses the various deployment methods to help you decide which is most suitable for your environment.

Install OfficeScan client with any of the following methods:

- **Internal Web page** – instruct the users in your organization to go to the internal Web page and download the client setup files
- **Login Script Setup** – automate the installation of the OfficeScan client to unprotected computers when they log on to the network
- **Client Packager** – deploy the client setup or update files to client via email. This is especially useful for low-bandwidth remote offices

- **Windows Remote Install** – install the client program on all Windows NT/2000/XP/Server 2003 clients from your Web console
- **From a client disk image** – create an image of an OfficeScan client and make clones of it to other computers on your network
- **Vulnerability Scanner (TMVS)** – install the client program on all Windows Windows 2000/Server 2003 clients with the Trend Micro Vulnerability Scanner
- **Microsoft System Management Server (SMS)** – use Microsoft System Management Server (SMS) to distribute the client program

Table 3-1 summarizes the benefits of each client deployment method.

	Web page	Login scripts	Client packager	Windows Remote Install	Client image setup	TMVS	Microsoft SMS
Suitable for deployment across the WAN	No	No	Yes	Yes	Yes	Yes	Yes
Suitable for centralized administration and management	No	Yes	No	Yes	Yes	No	Yes
Requires client user intervention	Yes	No	Yes	No	No	Yes	Yes
Requires IT resource	No	Yes	Yes	Yes	Yes	Yes	Yes
Suitable for mass deployment	No	Yes	Yes	No	Yes	Yes	Yes
Bandwidth consumption	Low, if scheduled	High, if clients are started at the same time	Low, if scheduled	Low, if scheduled	Low, if scheduled	Low, if scheduled	Low, if scheduled

**TABLE 3-1 OfficeScan client deployment tools**

To use any of these client deployment methods, you must have local admin rights to the target computers.

If you use any of these client deployment methods, your clients will inherit the default settings of OfficeScan, unless you modify them after installing the server.

## Installing from an internal Web page

If you installed OfficeScan server to a computer running Windows NT, Windows 2000, Windows XP, or Windows Server 2003 with Internet Information Server (IIS) 4.0 or later or Apache 2.0.48 (only on Windows 2000/XP/Server 2003 machines), users can install the client from the internal Web server created during master setup.

This is a convenient way to deploy the OfficeScan client. You only have to instruct users to go to the internal Web page and download the client setup files.

---

**Tip:** Use Vulnerability Scanner to see which clients have not followed the instructions to install from the Web console (see [Vulnerability Scanner](#) on page A-4 for more information).

---

Users must have Microsoft Internet Explorer 5.0 or later with the security level set to allow ActiveX controls to successfully download the client setup files. Email your users the following instructions to install the OfficeScan client from the internal Web server.

### To install from the internal Web page:

1. Open an Internet Explorer window and type one of the following:

- **OfficeScan server with SSL:**


`https://{OfficeScan_server_name}:{port}/officescan/console/clientinstall`

- **OfficeScan server without SSL:**

`http://{OfficeScan_server_name}:{port}/officescan/console/clientinstall`

Alternatively, click the **Click here** link under **Install OfficeScan Client** on the main page of the OfficeScan server Web console.

2. Click **Install Now** to start installing the OfficeScan client.

The client installation starts. Once installation is completed, the screen displays the message, "Client installation is complete". To verify a successful installation, check if the OfficeScan client icon  appears in the Windows system tray.

## Installing with Login Script Setup

Use Login Script Setup to automate the installation of the OfficeScan client on unprotected computers when they log on to the network. Login Script Setup adds a program called `autopcc.exe` to the server login script. `Autopcc.exe` performs the following functions:

- Determines the operating system of the unprotected computer and installs the appropriate version of the OfficeScan client
- Updates the scan engine, virus pattern file, Damage Cleanup Services components, Additional Threats pattern file, and program files

---

**Note:** Client computers must have Windows Active Directory installed before performing OfficeScan client installation.

---

### To add `autopcc.exe` to the login script using Login Script Setup:

1. On the computer you used to run the server installation, click **Programs > Trend Micro OfficeScan server {Server Name} > Login Script Setup** from the Windows **Start** menu.

The Login Script Setup utility loads. The console displays a tree showing all domains on your network.

2. Browse for the Windows NT/2000/Server 2003 whose login script you want to modify, select it, and then click **Select**. The server must be a primary domain controller and you must have administrator access.

Login Script Setup prompts you for a user name and password.

3. Type your user name and password. Click **OK** to continue.

The **User Selection** screen appears. The **Users** list shows the computers that log on to the server. The **Selected users** list shows the users whose computer login script you want to modify.

- To modify the login script of a single or multiple users, select them from the **Users** and then click **Add**
- To modify the login script of all users, click **Add All**
- To exclude a user whose computer you previously modified, select the name in the **Selected users** and click **Delete**
- To reset your choices, click **Delete All**



4. Click **Apply** when all the target users are in the **Selected users** list.  
A message appears, informing you that you have modified the server login scripts successfully.
5. Click **OK**. The Login Script Setup utility will return to its initial screen.
  - To modify the login scripts of other servers, repeat steps 2 to 4
  - To close Login Script Setup, click **Exit**

When an unprotected computer logs on to the servers whose login scripts you modified, `autopcc.exe` will automatically install the client to it.

### Installing with Windows NT/2000/Server 2003 scripts

If you already have an existing login script, Login Script Setup will append a command that executes `autopcc.exe`; otherwise, it creates a batch file called `ofcscan.bat` (which contains the command to run `autopcc.exe`).

Login Script Setup appends the following at the end of the script:

```
\\{Server_name}\ofcscan\installation_path
```

where:

- `{Server_name}` is the computer name or IP address of the computer where the OfficeScan server is installed
- `ofcscan` is the OfficeScan directory on the server
- `installation_path` is the directory where you installed the server files (by default, the `PCCSRV` folder)

The Windows 2000 login script is on the Windows 2000 server (through a net logon shared directory), under:

```
\\Windows 2000 server\system  
drive\WINNT\SYVOL\domain\scripts\ofcscan.bat
```

The Windows NT login script is on the Windows NT server (through a net logon shared directory), under:

```
\\Windows NT server\system  
drive\windir\system32\repl\export\scripts\ofcscan.bat  
  
\\Windows NT server\system  
drive\windir\system32\repl\import\scripts\ofcscan.bat
```

The Windows 2003 login script is on the Windows 2003 server (through a net logon shared directory), under:

```
\\Windows 2003 server\system  
drive\windir\sysvol\domain\scripts\ofcscan.bat
```

## Installing with Client Packager

Client Packager is a tool that can compress setup and update files into a self-extracting file to simplify delivery via email, CD-ROM, or similar media. It also includes an email function that can open your Microsoft™ Outlook address book and allow you to send the package from within the Client Packager console.

When users receive the package, all they have to do is double-click the file to run the setup program. OfficeScan clients you install using Client Packager report to the server where Client Packager created the setup package. This tool is especially useful when deploying the client setup or update files to clients in low-bandwidth remote offices.

Client Packager can create two types of self-extracting files:

- **Executable** – this common file type has an .exe extension
- **Microsoft Installer Package Format (MSI)** – this file type has an .msi extension and conforms to Microsoft's installer package specifications. For more information on MSI, see the Microsoft Web site ([www.microsoft.com](http://www.microsoft.com)).

---

**Tip:** Trend Micro recommends using Active Directory to deploy an MSI package with **Computer Configuration** instead of **User Configuration**. This helps ensure that the MSI package will be installed regardless of which user logs on to the machine.

---

---

**Note:** Install **Microsoft Outlook** to use the Client Packager send mail option. Windows Installer 2.0 is necessary for clients to run an MSI package.

---

### To create a package with Client Packager:

1. On the OfficeScan server, open Windows Explorer.
2. Browse to \PCCSRV\Admin\Utility\ClientPackager.
3. Double-click ClnPack.exe to run the tool. The Client Packager console opens.

---

**Note:** You must run the program from the OfficeScan server only.

---

4. Under **Target operating system**, select the operating system for which you want to create the package.

The options are **Windows 95/98/Me** and **Windows NT/2000/XP/Server 2003**.



5. Select from among the following installation options under **Install**:
- **Silent Mode** – creates a package that installs on the client machine in the background, unnoticeable to the client without showing an installation status window
  - **MSI Package** – creates a package that conforms to the Microsoft Installer Package Format
  - **Disable Prescan (only for fresh-install)** – disables the normal file scanning that OfficeScan performs before starting setup
  - **Force overwrite with latest version**: overwrites old versions with the latest version (this check box is enabled only when you select **Update** for **Package type**). This option appears only when creating a package for Windows NT/2000/XP/Server 2003.
  - **Update Agent**: gives the client the ability to act as an Update Agent

---

**Note:** If you select MSI Package, the package file has an .msi extension; otherwise, it has an .exe extension. The MSI package is for Active Directory deployment only. For local installation, create an .exe package.

---

6. Under **Components**, select the components to include in the installation package:
- **Program** – all components (if you select Program, Client Packager automatically selects the other components)
  - **Scan engine** – the latest scan engine on the OfficeScan server
  - **Virus pattern/Additional Threats pattern** – the latest virus pattern file and Additional Threats pattern file on the OfficeScan server (Additional threats include spyware, adware, keyloggers and other undesirable applications)
  - **Common Firewall Driver** – the driver for Enterprise Client Firewall

- **Network Virus Pattern** – the latest pattern file specifically for network viruses
  - **DCE/DCT** – the latest Damage Cleanup Service engine and template on the OfficeScan server
7. Select the OfficeScan client utilities to include in the package:
    - **POP3 Mail Scan** – performs a virus scan on the client's Post Office Protocol 3 (POP3) mail messages and attachments as they are downloaded from the mail server
    - **Outlook Mail Scan** – performs a virus scan on the client's Microsoft Outlook folders
    - **Wireless Protection** – an antivirus module to protect your Personal Digital Assistants (PDA). This is not available with Silent Mode or MSI packages.
    - **Check Point SecureClient** – support for Check Point SecureClient for Windows NT/2000/XP/Server 2003
  8. Ensure that the location of the ofcscan.ini file is correct next to **Source file**.
  9. To modify the path, click  to browse for the ofcscan.ini file. By default, this file is located in the \PCCSRV folder of the OfficeScan server.
  10. In **Output file**, click  to specify the file name (for example, ClientSetup.exe) and the location to create the client package.
  11. Click **Create** to build the client package. When Client Packager finishes creating the package, the message "Package created successfully." appears. To verify successful package creation, check the output directory you specified.
  12. Send the package to your users via email, or copy it to a CD or similar media and distribute among your users.

---

**WARNING!** *You can only send the package to the OfficeScan clients which report to the server where the package was created. Do not send the package to OfficeScan clients that report to other OfficeScan servers.*

---

## Sending the package via email

Microsoft Outlook is necessary to use the Client Packager email function.

**To send the package from the console:**

1. Click **Send mail**. The **Choose Profile** window appears.
2. Choose a profile name from the list and click **OK**.
3. Enter the user name and password required to access Outlook on your computer.
4. The **Send mail** screen opens with the default subject and message. Click **To** and specify the recipients of the package. Client Packager opens your Microsoft Outlook address book. Click **Cc** or **Bcc** to furnish copies to other recipients in your organization.
5. Edit the default subject and message (optional) and click **Send**.

---

**Note:** If the Client Packager is unable to find your Microsoft Outlook address book, an error message is displayed when you click **Send mail**, **To**, **Cc**, or **Bcc**.

---

## Installing with Windows Remote Install

Remotely install the OfficeScan client to Windows NT/2000/XP (Professional Edition Only) and Server 2003 computers connected to the network, and install to multiple computers at the same time. To use Windows Remote Install, you need administrator rights for the target computers.

---

**Note:** You cannot use Windows Remote Install to install OfficeScan client on machines running Windows XP Home Edition.

---

**To install with Windows Remote Install:**

1. From the OfficeScan Web console sidebar, click **Clients > Remote Install** on the OfficeScan server sidebar.  
The **Remote Install** screen appears. The domains and computers list displays all the Windows domains on your network.
2. From the list of computers, select a client, and then click **Add >>**. OfficeScan prompts you for a user name and password to the target computer. You need administrator rights to the target computer.
3. Type your user name and password, and then click **Login**. The target computer appears in the selected computers list.

4. Repeat these steps until the list displays all the Windows computers to install OfficeScan client.
5. Click **Install** to install the client to your target computers. A confirmation box appears.
6. Click **Yes** to confirm that you want to install the client to the target computers. A progress screen appears as OfficeScan copies the program files to each target computer.
7. When OfficeScan completes the installation to a target computer, the installation status will appear in the **Result** field of the selected computers list, and the computer name appears with a green check mark.

---

**Note:** Windows Remote Install will not install OfficeScan client on a machine already running OfficeScan server.

---

## Installing from a client disk image

Disk imaging technology allows you to create an image of an OfficeScan client and make clones of it to other computers on your network.

Each client installation needs a Globally Unique Identifier (GUID), so that the server can identify your clients individually. Use an OfficeScan program called `imgsetup.exe` to create a different GUID for each of the clones.

---

**Note:** The computers you are installing to must have the same Windows platform type as the source computer. There are two types of Windows platforms: Windows 95/98/Me and Windows NT/2000/XP/Server 2003. For example, if the source OfficeScan client machine is running Windows XP, you can only create clones for computers running Windows NT, 2000, XP, or Server 2003, not Windows 95, 98 or Me.

---

### To create a disk image of an OfficeScan client:

1. Obtain disk imaging software.
2. Install the OfficeScan client to a computer. You will use this client as the source of the disk image.

3. Copy `ImgSetup.exe` to this computer from the OfficeScan server's `\PCCSRV\Admin\Utility\ImgSetup` folder.
4. Run `imgsetup.exe` on this computer. A RUN registry key will be created under `HKEY_LOCAL_MACHINE`.
5. Create a disk image of the OfficeScan client using your disk imaging software.
6. Restart the clone. `ImgSetup.exe` will automatically start and create one new GUID value. The client will report this new GUID to the server and the server will create a new record for the new client.

---

**WARNING!** *To avoid having two computers with the same name in the OfficeScan database, remember to manually change the computer name or domain name of the cloned OfficeScan client.*

---

## Installing with Vulnerability Scanner

The Trend Micro Vulnerability Scanner (TMVS) can search for unprotected computers on your network and install OfficeScan client on them.

---

**Note:** You can use Vulnerability Scanner on machines running Windows 2000 or Server 2003; however, the machines cannot be running Terminal Server.

You cannot install OfficeScan clients with Vulnerability Scanner if an OfficeScan server installation is present on the same machine.

---

### To install OfficeScan client with Vulnerability Scanner:

1. In the drive where you installed OfficeScan server, open the following directories: **OfficeScan > PCCSRV > Admin > Utility > TMVS**. Double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears.
2. Click **Settings**. The **Settings** screen appears.
3. Under **OfficeScan server Setting (for Install and Log Report)**, type the OfficeScan server name and port number.
4. Select the **Auto-Install OfficeScan Client for unprotected computer** check box.

5. Click **Start** to begin checking the computers on your network and begin OfficeScan client installation.

---

**Note:** Refer to the online help for complete information on how to use and configure this tool.

---

## Installing the client using Microsoft SMS

You can also install the client using Microsoft System Management Server (SMS). However, you must have Microsoft BackOffice SMS installed on the server.

Installing the client using Microsoft SMS is a two-step process:

1. Create the setup package
2. Distribute or “advertise” the package to the target computers

---

**Note:** The following instructions are applicable if you are using Microsoft SMS 2.0 and SMS 2003.

---

There are different methods to create a package based on the location of the SMS and OfficeScan servers:

- local drive: the SMS server and the OfficeScan server are on the same machine
- remote location: the SMS server and the OfficeScan server are on different machines

### To create the setup package on the local drive:

1. Open the SMS Administrator console.
2. On the **Tree** tab, click **Packages**.
3. On the **Action** menu, click **New > Package From Definition**. The **Welcome** screen of the **Create Package From Definition Wizard** appears.
4. Click **Next**. The **Package Definition** screen appears.
5. Click **Browse**. The **Open** screen appears.
6. Browse for the package description file (PDF) on the server. The location of the PDF depends on the operating system of the target clients. The PDF for the Windows NT/2000/XP/Server 2003 client is in



\PCCSRV\PCCNT\Disk1\setup.pdf. The PDF for the Windows 95/98/Me client is in \PCCSRV\PCC95\Disk1\setup.pdf.

7. Select the PDF for the target clients, and then click **OK**.

The package name for the PDF you have selected appears on the **Package Definition** screen. If you selected the PDF for the Windows NT/2000/XP/Server 2003 Server client, it will show “OfficeScan Client NT/2K/XP/Server 2003 setup 6.5”. If you selected the PDF for the Windows 95/98/Me client, it will show “OfficeScan Client 95/98/Me setup 6.5”.

8. Click **Next**. The **Source Files** screen appears.

9. Click **Always obtain files from a source directory**, and then click **Next**.

The **Source Directory** screen appears, displaying the name of the package you are creating and the source directory.

10. Click **Local drive on site server**.

11. Click **Browse** and select the source directory where the PDF file is located.

12. Click **Next**. The wizard creates the package. When it completes the process, the name of the package appears on the SMS Administrator console.

#### **To create a setup package on a remote location:**

1. On the OfficeScan server, use Client Packager to create a setup package with an .exe extension. (the .msi package is not supported). See [Installing with Client Packager](#) on page 3-25.

2. On the computer where you want to store the source, create a shared folder.

3. Browse for the package description file (PDF).

The location of the PDF depends on the operating system of your target clients. The PDF for the Windows NT/2000/XP/Server 2003 client is in \PCCSRV\PCCNT\Disk1\setup.pdf. The PDF for the Windows 95/98/ME client is in \PCCSRV\PCC95\Disk1\setup.pdf.

4. Copy the installation package you created with Client Packager and the setup.pdf file to the shared folder.

5. Open the setup.pdf file with a text editor, and change the IS-CmdLine and CommandLine parameters to the package name (for example: IS-CmdLine=package\_name.exe).

6. Open the SMS Administrator console.

7. On the **Tree** tab, click **Packages**.

8. On the **Action** menu, click **New > Package From Definition**. The **Welcome** screen of the **Create Package From Definition Wizard** appears.
9. Click **Next**. The **Package Definition** screen appears.
10. Click **Browse**. The **Open** screen appears.
11. Browse for the package description file (PDF), which is located in the shared folder you created.
12. Click **Next**. The **Source Files** screen appears.
13. Click **Always obtain files from a source directory**, and then click **Next**. The **Source Directory** screen appears.
14. Click **Network path (UNC name)**.
15. Click **Browse** and select the source directory where the PDF file is located (the shared folder you created).
16. Click **Next**. The wizard creates the package. When it completes the process, the name of the package appears on the SMS Administrator console.

**To distribute the package to target computers:**

1. On the **Tree** tab, click **Advertisements**.
2. On the **Action** menu, click **All Tasks > Distribute Software**. The **Welcome** screen of the **Distribute Software Wizard** appears.
3. Click **Next**. The **Package** screen appears.
4. Click **Distribute an existing package**, and then click the name of the setup package you created.
5. Click **Next**. The **Distribution Points** screen appears.
6. Select a distribution point to which you want to copy the package, and then click **Next**. The **Advertise a Program** screen appears.
7. Click **Yes** to advertise the client setup package, and then click **Next**. The **Advertisement Target** screen appears.
8. Click **Browse** to select the target computers. The **Browse Collection** screen appears.
9. Click the collection to which you want to distribute the setup package.
  - If you created a client setup package for Windows NT/2000/XP/Server 2003, click **All Windows NT Systems**.

- If you created a client setup package for Windows 98, click **All Windows 98 Systems**.

---

**Note:** To distribute the client setup package to Windows Me computers, you must create a new collection. For instructions on how to create a new collection, refer to the Microsoft SMS documentation.

---

10. Click **OK**. The **Advertisement Target** screen appears again.
11. Click **Next**. The **Advertisement Name** screen appears.
12. In the text boxes, type a name and comments for the advertisement, and then click **Next**. The **Advertise to Subcollections** screen appears.
13. Choose whether to advertise the package to subcollections. You can choose to **Advertise the program only to members of the specified collection** or **Advertise the program to members of subcollections as well**.
14. Click **Next**. The **Advertisement Schedule** screen appears.
15. Specify when to advertise the client setup package by typing or selecting the date and time in the list boxes.  
  
If you want Microsoft SMS to stop advertising the package on a specific date, click **Yes. This advertisement should expire**, and then specify the date and time in the **Expiration date and time** list boxes.
16. Click **Next**. The **Assign Program** screen appears.
17. Click **Yes, assign the program**, and then click **Next**.

Microsoft SMS creates the advertisement and displays it on the SMS Administrator console.

When Microsoft SMS distributes the advertised program (that is, the OfficeScan client program) to target computers, a screen will pop up on each target computer. Instruct users to click **Yes** and follow the instructions provided by the wizard to install the OfficeScan client to their computers.

### **Known issues when installing with Microsoft SMS:**

- "Unknown" appears in the Run Time and Disk Space columns of the SMS console.
- If the installation is unsuccessful, the installation status may still show that the installation is complete on the SMS program monitor. For instructions on how to

verify if the installation was successful, see *Verifying a successful installation* on page 3-13.

## Verifying a successful installation

Use Vulnerability Scanner to detect installed antivirus solutions, search for unprotected computers on your network, and install OfficeScan client. To determine if computers need protection, Vulnerability Scanner pings ports that antivirus solutions normally use.

## Using Vulnerability Scanner to verify the client installation

You can also automate Vulnerability Scanner by creating scheduled tasks. For information on how to automate Vulnerability Scanner, see the OfficeScan online help.

You can run Vulnerability Scanner on the server or on any Windows 2000 computer on the network. To run Vulnerability Scanner on a computer other than the server, copy the TMVS folder from the \PCCSRV\Admin\Utility folder of the server to the computer.

---

**Note:** You can use Vulnerability Scanner on machines running Windows 2000 or Server 2003; however, the machines cannot be running Terminal Server.

---

### To verify client installation using Vulnerability Scanner:

1. In the drive where you installed OfficeScan server, open the following directories: **OfficeScan > PCCSRV > Admin > Utility > TMVS**. Double-click **TMVS.exe**. The **Trend Micro Vulnerability Scanner** console appears.
2. Click **Settings**. The **Settings** screen appears.
3. Under **Product Query**, select the **OfficeScan** check box and specify the port that the server uses to communicate with clients.
4. Under **Description Retrieval Settings**, click the retrieval method to use. Normal retrieval is more accurate, but it takes longer to complete.

If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting the **Retrieve computer descriptions when available** check box.

5. If you want to automatically send the results to yourself or to other administrators in your organization, select the **Email results to the system administrator** check box under **Alert Settings**. Then, click **Configure** to specify your email settings.
  - In **To**, type the email address of the recipient
  - In **From**, type your email address. If you are sending it to other administrators in your organization, this will let the recipients know who sent the message
  - In **SMTP server**, type the address of your SMTP server. For example, type `smtp.company.com`. The SMTP server information is required
  - In **Subject**, type a new subject for the message or accept the default subjectClick **OK** to save your settings.
6. To display an alert on unprotected computers, click the **Display alert on unprotected computers** check box. Then, click **Customize** to set the alert message. The **Alert Message** screen appears. Type a new alert message in the text box or accept the default message, and then click **OK**.
7. To save the results as a comma-separated value (CSV) data files, select the **Automatically save the results to a CSV file** check box. By default, Vulnerability Scanner saves CSV data files in the TMVS folder. If you want to change the default CSV folder, click **Browse**, select a target folder on your computer or on the network, then click **OK**.
8. You can enable Vulnerability Scanner to ping computers on the network to get their status. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout text** boxes.
9. To remotely install OfficeScan Client and send a log to the server, type the OfficeScan server name and port number. If you want to automatically remotely install OfficeScan client, select the **Auto-install OfficeScan Client for unprotected computers** check box.
10. Click **Install Account** to configure the account. The **Account Information** screen appears. Type user name and password that permits installation. Click **OK**.
11. If you want to send logs to the OfficeScan server, select the **Report log to OfficeScan server** check box.

12. Click **OK** to save your settings. The **Vulnerability Scanner** console appears.

**To run a manual vulnerability scan on a range of IP addresses:**

1. Under **IP Range to Check**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers. Note the Vulnerability Scanner only supports a class B IP address range (for example: 168.212.1.1 to 168.212.254.254).
2. Click **Start** to begin checking the computers on your network. The results appear in the **Results** table under the **Manual Scan** tab.

---

**Note:** You can also run Vulnerability Scanner at the command prompt. For more information, see the Vulnerability Scanner online help.

---

**To run a vulnerability scan on computers requesting IP addresses from a DHCP server:**

1. Click the **DHCP Scan** tab in the **Results** box. The **DHCP Start** button appears.
2. Click **DHCP Start**. Vulnerability scanner begins listening for DHCP requests and performing vulnerability checks on computers as they log on to the network.

## Testing the client installation with the EICAR test script

Trend Micro recommends testing your product and confirming that it works by using the EICAR test script. EICAR, the European Institute for Computer Antivirus Research, developed the test script as a safe way to confirm that antivirus software is properly installed and configured. Visit the EICAR Web site for more information:

<http://www.eicar.org>

The EICAR test script is an inert text file with a .com extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software will react to it as if it were a virus. Use it to simulate a virus incident and confirm that email notifications, HTTP scanning, and virus logs work properly.

---

**WARNING!** *Never use real viruses to test your antivirus installation.*

---

**To test the client installation with the EICAR test script:**

1. Make sure Real-time scan is enabled on the client.

2. Copy the following string and paste it into Notepad or any plain text editor:  
`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. Save the file as EICAR.com to a temp directory. OfficeScan should immediately detect the file.
4. To test other computers on your network, attach the EICAR.com file to an email message and send it to one of the computers.

---

**Note:** Trend Micro also recommends testing a zipped version of the EICAR file. Using compression software, zip the test script and perform the steps above.

---

#### **To test the client installation HTTP scanning capability:**

- Download the EICAR.com test script from either of the following URLs:

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

`http://www.eicar.org/anti\_virus\_test\_file.htm`

OfficeScan should show that it detected the EICAR test file.

## **Removing the client**

There are two ways to remove the OfficeScan program from the clients:

- Remove the client from the OfficeScan Web console
- Remove the client using its uninstallation program

---

**Note:** If the client also has a Cisco Trust Agent (CTA) installation, uninstalling the OfficeScan client program may or may not remove CTA. This depends on the settings you configured for the client for Cisco Agent Deployment (see *Deploying the Cisco Trust Agent* on page D-11).

---

## **Removing the client from the OfficeScan Web console**

You can remove the client program from computers on the network using the Web console. Note that removing the client program also removes virus protection on selected clients.

---

**WARNING!** *Removing the OfficeScan client may expose the client computer(s) to virus threats.*

---

### To remove the client using Uninstall Now

1. On the OfficeScan Web console sidebar, click **Clients**. The domain tree for **Clients** screen appears.
2. Click the domains or clients on which you want to run Uninstall Now by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Uninstall Clients**. The **Uninstall Clients** screen appears.
4. Under **Computer**, select the clients to remove, and then click **Start Notification**. The server sends a request to the client to run the client uninstallation program.

### To stop notifications

To stop notifications to clients that have not yet started the client uninstallation program, do the following:

1. Select the clients that you no longer want to remove.
2. Click **Stop Notification**. Clients that have not yet started the client uninstallation program will skip the request. However, clients that are already running the uninstallation program do not stop the uninstallation procedure.

## Removing the client using its uninstallation program

If you granted users the privilege to remove the client program, instruct them to run the client uninstallation program from their computers. For more information, see [Granting Privileges to Clients](#) on page 4-43.

### To run the client uninstallation program:

1. On the Windows **Start** menu, click **Programs > Trend Micro OfficeScan Client > Uninstall OfficeScan Client**. The **OfficeScan Client Uninstallation** screen appears and prompts for the uninstall password.
2. Type the uninstall password, and then click **OK**. The **OfficeScan Client Uninstallation** screen shows the progress of the uninstallation.

You may need to restart your computer to complete the uninstallation.



## Migrating to and Upgrading OfficeScan

If you are using third-party antivirus software or an older version of OfficeScan, you can easily migrate or upgrade to this version OfficeScan. This section helps you perform migration and upgrade by enumerating the tasks that you need to perform and provides detailed instructions on how to do them.

In this section, you will learn about the following topics:

- Migrating from third-party antivirus applications
- Upgrading from a previous version

### Migrating from third-party antivirus applications

Migrating from third-party antivirus software to OfficeScan is a two-step process: the installation of the OfficeScan server, followed by the migration of the clients.

However, there may be other procedures that you need to complete, depending on your environment.

To help you migrate to OfficeScan, follow these guidelines:

1. Plan the migration
2. Pilot the migration
3. Install the OfficeScan server
4. Migrate the clients

#### Plan your migration

As with deployment, you need to plan how you will migrate existing antivirus software to OfficeScan. Trend Micro recommends planning the following for migration:

- Set a migration schedule
- Form a team that will handle the migration
- Identify which segments of your network will be migrated and when
- Decide on the best method to migrate the clients
- Create a rollback plan in case you encounter difficulties

Trend Micro recommends planning the migration on a non-working day or during off-peak hours to ensure that the process will not interfere with your organization's normal operations. If migrating a large client base, you may also want to stage the migration into segments to facilitate the process. Migrating 500 clients simultaneously is easier than migrating 20,000 clients.

## Pilot your migration

Perform a small scale migration before doing a full-scale rollout. Choose a pilot site that matches your production environment, install the server, and then use different methods to migrate the clients.

Evaluate the results of the pilot migration, identify potential difficulties, and decide which client migration methods work best in your environment.

## Install the OfficeScan server

The next step is to install the OfficeScan server. Before installing, verify that the server meets the system requirements. You need to remove the server program of your existing third-party antivirus software before installing the OfficeScan server.

For instructions on how to install the OfficeScan server, refer to [Installing OfficeScan Server](#) on page 3-2.

OfficeScan cannot remove the server program of your existing third-party, client/server antivirus application.

## Manual client migration

To remove third-party antivirus applications and install the OfficeScan client automatically, perform any of the following:

- Install from the internal Web page
- Install with Login Script Setup (`autopcc.exe`)
- Install with Windows NT Remote Install

For instructions on how to use these methods, refer to [Installing OfficeScan Clients](#) on page 3-19. The procedures for deploying and migrating clients are similar, except for the fact that when migrating the clients, third-party antivirus applications are removed from your computers before the OfficeScan client installation.

## Automatic client migration

Automatic client migration refers to replacing existing third-party antivirus software with the OfficeScan client. The client setup program automatically removes the third-party software on your client computers and replaces it with the OfficeScan client.

Refer to Table 3-2 for a list of third-party applications that OfficeScan can automatically remove.

Vendor	Product Name	Version	Platform
Ahnlab™	V3 Pro™	2000 Deluxe	Windows NT
Ahnlab	V3 Pro	98 Deluxe	Windows 98
Ahnlab	V3 Pro	98	Windows 9x
Computer Associates™	eTrust InoculateIT™	6.0	Windows NT and 9x
Computer Associates	InocuLAN™	5, 4.53	Windows NT and 9x
Computer Associates	Cheyenne AntiVirus™	9x	Windows 9x
Computer Associates	Cheyenne AntiVirus	NT	Windows NT
F-Secure™	Anti-Virus™	4.04, 4.08, 4.3, 5.3	Windows NT and 9x
F-Secure	Anti-Virus	BackWeb	Windows NT
F-Secure	Anti-Virus	Management Agent	Windows NT
Hauri™	ViRobot™	2000 Professional	Windows NT and 9x
Intel™	LANDesk Virus Protect™	5.0	Windows NT and 9x
McAfee™	Dr. Solomon™	4.0.3	Windows 98
McAfee	Dr. Solomon	4.0.3 NT	Windows NT
McAfee	Dr. Solomon	7.77, 7.95 NT	Windows NT and 9x
McAfee	ePolicy Orchestrator™	Agent 1000, Agent 2000	Windows NT and 9x
McAfee	VirusScan	Enterprise 7.0	NT, 2000, XP
McAfee	VirusScan	ASaP	9x, Me, NT, 2000, XP
McAfee	VirusScan	6.01, 6.02	Windows NT

Vendor	Product Name	Version	Platform
McAfee	VirusScan	NT	Windows NT
McAfee	VirusScan™	MSPlus98	Windows 9x
McAfee	VirusScan	TC	Windows NT and 9x
McAfee	VirusScan	4.5, 4.51, 5.15, 5.16, 5.21, 6.01	Windows NT and 9x
McAfee	NetShield™	NT 4.03a, 4.5	Windows NT
Panda Software™	Antivirus™	Local Networks	Windows NT and 9x
Panda Software	Antivirus	6.0	Windows NT and 9x
Panda Software	Antivirus	Windows NT WS	Windows NT
Sophos™	Anti-Virus	3.37, 3.47, 3.5x	Windows NT and 9x
Symantec	Norton AntiVirus	2003, 2002, 2001, 2000	Windows NT and 9x
Symantec	Norton AntiVirus	2003 Cht	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition™	8.0 (2002)	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	7.5, 7.51, 7.6,	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	2001	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	2000	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	7.0	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	6.524	Windows 9x
Symantec	Norton AntiVirus Corporate Edition	5.0, 5.31, 5.32	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	2.0	Windows NT
Tegam™	ViGUARD™	9.25e	Windows NT

**TABLE 3-2**      **Third-party applications that OfficeScan can automatically remove**

## Verify the migration

After migrating to OfficeScan, Trend Micro recommends the Trend Micro Vulnerability Scanner (TMVS) to check if you still have clients using the previous antivirus application. This tool checks your computers for installed antivirus software and the versions they are using based on an IP address range you specify.

You can get Vulnerability Scanner from the `\PCCSRV\Admin\Utility\TMVS` folder of the OfficeScan server.

# Getting Started with OfficeScan

This chapter explains how to use the OfficeScan web console and how to configure basic settings.

The topics discussed in this chapter include:

- *Exploring the Web Console* on page 4-2
- *Updating OfficeScan* on page 4-13
- *Verifying Client-Server Connection* on page 4-26
- *Setting up Standard Notifications* on page 4-26
- *Configuring the Scan Settings* on page 4-31
- *Running Scan Now* on page 4-40
- *Granting Privileges to Clients* on page 4-43
- *Importing and Exporting Policies* on page 4-44

## Exploring the Web Console

When you install OfficeScan server, you also install the Web console, which uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

### To open the Web console:

1. On any computer on the network, open a Web browser and type `http://{OfficeScan_Server_Name}:{port number}/officescan` in the address bar.  
If using SSL, type `https://{OfficeScan_Server_Name}:{port number}/officescan` in the address bar.
2. The browser displays the OfficeScan login screen.

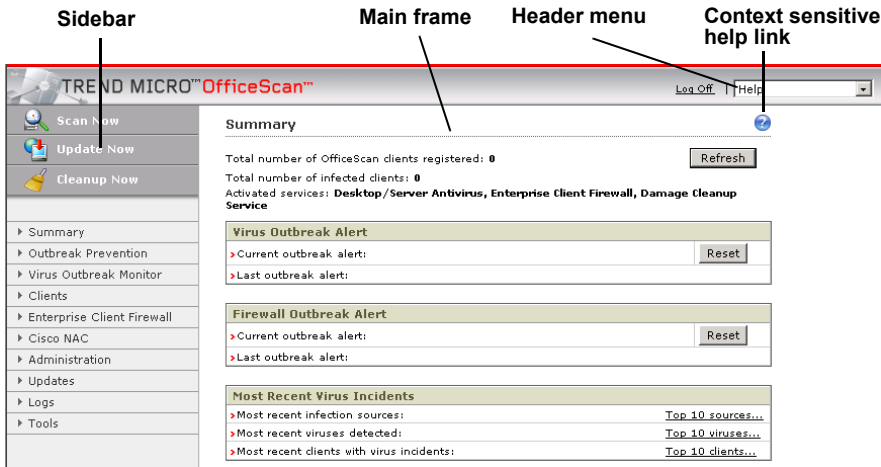


**FIGURE 4-1.** The browser displays the Welcome screen of the Web console.

3. Type your password in the **Password** text box, and then click **Enter**. The browser displays the **Summary** screen of the Web console.

## Getting around the Web console

There are two main parts to the Web console: the sidebar and the main frame. The sidebar groups tasks that you perform into sections. **Cleanup Now** and **Scan Now**, for example, are tasks to run under the section **Clients** (see Figure 4-2).



**FIGURE 4-2** The browser displays the Welcome screen of the Web console

When you click a task on the sidebar, the main frame displays the information that you need to perform the task or opens another screen that you use to perform the task.

The sidebar contains shortcuts to **Scan Now**, **Update Now**, and **Cleanup Now**. Click **Scan Now** to perform a manual scan on computers that you suspect to be infected. Click **Update Now** to check the Trend Micro update server for the latest updated components, including virus pattern files, scan engine and program, Damage Cleanup scan engine and template, and Additional Threats pattern files. Click **Cleanup Now** to run Damage Cleanup Services on selected clients to check for Trojans.



The following table summarizes the tasks to perform for each category on the sidebar:

<b>Summary</b>	
Summary	View a summary of the outbreak status, recent virus incidents, and the update and connection status of clients.

<b>Outbreak Prevention</b>	
Deploy Now	Apply Outbreak Prevention to control an outbreak that may be developing on your network.
Restore	Deactivate Outbreak Prevention to restore your network settings to normal after an outbreak is contained.

<b>Virus Outbreak Monitor</b>	
Virus Outbreak Monitor	Enable Virus Outbreak Monitor if you want OfficeScan to send you a message in the event that clients detect excessive network traffic.

<b>Clients</b>	
Scan Options	Configure Real-time Scan, Manual Scan, and Scheduled Scan options.
Client Privileges	Grant users privileges to modify individual scan settings, update components, remove or unload the client and access OfficeScan client program folders, files, and registries.
Export/Import	Import and export scan settings and Outbreak Prevention settings.
Scan Now	Perform a manual scan for viruses on selected clients from the Web console. Configure the action that OfficeScan takes on infected files under Manual Scan in the Scan Options section.
Cleanup Now	Search specifically for Trojans on selected clients using Damage Cleanup Services.
Uninstall Clients	Remove the client program from client computers.

View Status	View client information, including its privileges and the versions of its components, such as virus pattern file, scan engine and program, DCS engine and template, and Additional Threats pattern file.
Notify Install	Notify users via email to install OfficeScan client.
Remote Install	Install the client software to Windows NT/2000/XP/Server 2003 computers remotely using the Web console. Install to multiple computers at the same time without having to physically go to each computer.
Verify Connection	Check the connection status of clients manually or automatically.
Global Client Settings	Configure optional and advanced settings for clients, including scan settings, alert settings, reserved disk space and watchdog settings, Scheduled Update settings, and connection settings.

<b>Enterprise Client Firewall</b>	
Profile List	Configure a list of profiles to apply to client Enterprise Client Firewall settings.
Policy List	Configure profiles that apply to Enterprise Client Firewall policies.
Firewall Outbreak Monitor	Enable and configure alert criteria that may signal an intrusion on client machines. Also create an alert message to send to administrators when an alert is triggered.

<b>Cisco NAC</b>	
Policy Servers	Manage a list of Policy Servers on your network.
Agent Deployment	Install or uninstall the Cisco Trust Agent on OfficeScan client machines.
Client Certificate	Import the client certificate to authenticate end user clients with the Cisco Secure Access Control Server (ACS).

<b>Administration</b>	
Set Console Password	Change the password to the Web console periodically to prevent unauthorized users from modifying your settings or removing the clients.
Standard Alert	Send alerts to administrators in your organization whenever OfficeScan detects a virus on any client.
Outbreak Alert	Send alerts to administrators in your organization when OfficeScan determines that conditions on your network have met specified outbreak criteria.
Client Alert Message	Modify the message that is displayed on the clients whenever OfficeScan detects a virus, a Enterprise Client Firewall violation, or a computer that is the source of an infection.
Intranet Proxy	Configure intranet proxy settings if a your network uses a proxy server for internal communications.
Web Server	Update OfficeScan server's name, IP address and HTTP port number.
Inactive Clients	Automatically remove inactive clients to ensure that the domain tree displays only active clients.
Quarantine Manager	Set both the capacity of the quarantine folder and the maximum allowable size of quarantined files.
Product License	Activate and check the status of component product licenses.
World Virus Tracking	Choose if to participate in the World Virus Tracking Program, which is designed to help Trend Micro gather and report virus-scanning results from customers worldwide.

<b>Updates</b>	
Server Update	Manually or automatically update the components on the server as well as configure your proxy settings to download updates from the Trend Micro update server.

Client Deployment	Update the clients manually or automate the deployment of updates.
Rollback	Revert the pattern file or scan engine to the previous version if you encounter problems after deploying it.


<b>Logs</b>	
Virus Logs	View a list of viruses that have infected clients on the network, with details about each infection.
Update Logs	View the time and date that the server and clients received updates and a list of what components they updated. Use these logs to keep track of the server's update history and to verify that updates were successfully deployed to clients.
System Event Logs	View system events that have occurred on the server, such as shutdown and startup. Use these logs to verify that the server is running smoothly and that the services necessary for OfficeScan to work on the network are running.
Verify Connection Logs	View verify connection logs to determine the connection status between the server and clients.
Enterprise Client Firewall Logs	Request clients to send Enterprise Client Firewall logs to the OfficeScan server. View these logs to determine if there are any attacks directed at your OfficeScan clients taking place on your network.
Log Maintenance	To conserve disk space on the server, set a schedule to delete logs.

<b>Tools</b>	
Administrative Tools	View tools that can help you manage the server and clients.
Client Tools	View tools that can enhance the performance of the clients.

## Other links on the console

The Web console also has other links that you use to log off the console, open the online help, and view virus information. These are located at the upper right corner and below the main frame.

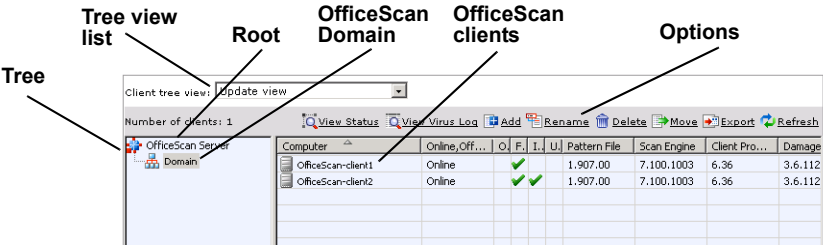
Header links	
Log Off	Click to end your session. Logging off the Web console prevents unauthorized users from modifying the settings or removing clients.
Help	Select one of the following from the menu
Contents and Index	Select to open the online help system.
Knowledge Base	Select to open the Trend Micro online knowledge base to view FAQs and updated product information, access customer support, and register your version of OfficeScan.
Security Info	Select to display the Trend Micro Security Information page to read about the latest virus threats.
Sales	Select to display the Trend Micro sales Web page to contact your regional sales representative.
Support	Select to display the Trend Micro support Web page to submit questions and find answers to common questions about Trend Micro products.
About	Select to display the About page, which contains an overview of the product and tells you how to check the version of your components.

Links below the main frame	
	Click this icon to open the online help system (not available on every screen).

## Understanding the OfficeScan domain tree

The OfficeScan domain tree is a Java-based tree that displays OfficeScan domains and clients on the network. It appears in the main frame when you click **Outbreak**

**Prevention, Clients, or Logs**, or when you select **Go to Client Console** in the Enterprise Client Firewall Profile Editor.



**FIGURE 4-3** The OfficeScan client domain tree

### Creating OfficeScan domains

OfficeScan uses existing Windows domains on the network when initially assigning clients to OfficeScan domains.

For example, a network currently has a Windows domain called 'YourCompany' with three computers named 'A', 'B', and 'C'. When you install OfficeScan on these three computers, it will automatically create an OfficeScan domain called 'YourCompany' and populate it with these three computers.

You can also create new OfficeScan domains, modify the structure of the OfficeScan domain tree, or change the OfficeScan domain names so that they suit your organization's virus management policy.

---


**Tip:** Group clients with similar virus protection requirements together in the same OfficeScan domain. This simplifies the task of applying OfficeScan settings to multiple clients.

---

### Selecting OfficeScan domains and clients from the domain tree

Select OfficeScan domains or clients to simultaneously apply settings.

- To select a single OfficeScan domain or client, click the OfficeScan domain or client name.

- To select multiple, adjacent OfficeScan domains or clients, click the first OfficeScan domain or client in the range, hold down the SHIFT key, and then click the last domain or client in the range.
- To select a range of non-adjacent OfficeScan domains or clients, click the first OfficeScan domain or client in the range. Hold down the CTRL key and then click the OfficeScan domains or clients that you want to select.
- To select all clients that report to the server, click the root icon .

## Searching for clients

To search for clients, use either of the following two methods:

### To do a simple search:

1. Type a client name in the **Simple Search** text field.

---

**Note:** If you do not know the entire client name, type part of the name. OfficeScan selects the first client name in the list that matches what you typed.

---

2. Click **Search**. A list of matching clients will appear highlighted in the domain tree.

### To do an advanced search:

1. Click **Advanced Search**. The Advanced Search screen appears.
2. Search for clients based on three types of criteria:
  - a. **Basic**
    - **IP range** – click and type a range of client IP addresses
    - **IP Segment** – click and type a portion of an IP address starting with the first octet. The search will return all computers with IP addresses containing that entry. For example, typing 10.5 will return all computers in the IP address range 10.5.0.0 to 10.5.255.255.
    - **Platforms** – click and select the client platforms
    - **Domain** – click and select a client domain from the list
    - **MAC Address** – type a MAC address range (in hexadecimal notation)
  - b. **Version**

For the following, select either **Earlier than** or **Earlier than and including** from the list and type a version number in the text box:


- **Scan Engine version**
- **Virus Pattern File version**
- **Client Program version**
- **Damage Cleanup template version**
- **Damage Cleanup engine version**
- **Additional Threats pattern version**

c. **Status**

- **Connected** – select a connection status: **Online**, **Offline**, or **Roaming**
- **Outbreak Prevention**– select either **Activated** or **Normal** mode
- **Infected client** – select and type the number of infected clients






3. Click **OK**. A list of matching clients will appear in the domain tree.

## Refreshing the tree

To refresh the domain tree, click the refresh icon  .

## Understanding the domain tree icons

The following icons indicate the status of clients in OfficeScan domains.

Windows 95/98/Me clients	Description	Windows NT/2000/XP/Server 2003 clients and servers
	OfficeScan domains: double-click to display clients that belong to this domain	
	Normal client/server	
	Client with Update Agent installation	



## Working with OfficeScan domains

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

For ease of management, group clients based on the departments to which they belong or the functions they perform. Also group clients that are at a greater risk of infection, so you can apply a more secure configuration to all of them in just one setting.

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

By default, OfficeScan creates domains based on existing Windows domains and refers to each client according to its computer name. Delete or rename the domains that OfficeScan has created for you, or create a new domain. You can even transfer clients from one domain to another.

### To add an OfficeScan domain:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click **Add** in the main frame. The **Add Domain** screen appears.
3. Type a name for the OfficeScan domain to add, and then click **OK**. The new OfficeScan domain appears in the domain tree.

### To move OfficeScan client:

1. On the sidebar, click **Clients**. The domain tree appears.
2. Select the client that you want to move, and then click **Move**. The **Move Clients** screen appears. Alternatively, drag and drop the client to another OfficeScan domain.
3. Do one of the following:
  - To move clients to another OfficeScan domain:
    - i. Select the OfficeScan domain to move the client under **Move selected client(s) to another Domain**.
    - ii. Click **OK**. The client appears under the OfficeScan domain you have selected.
  - To move clients to another OfficeScan server:

- i. Enter the server name, port number, and client communication port under **Move selected client(s) to another OfficeScan Server**.
- ii. Click **OK**.

**To delete OfficeScan domain:**

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. In the OfficeScan domain tree, click the OfficeScan domain to delete. The clients that belong to the OfficeScan domain are displayed.
3. Move the clients to other OfficeScan domains. Do this by dragging and dropping the clients to other domains.
4. When the OfficeScan domain is empty, click **Delete**. A confirmation screen appears.
5. Click **Ok**.

**To rename OfficeScan domain:**

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the OfficeScan domain to rename, and then click **Rename**. The **Rename Domain** screen appears.
3. Type a new name for the OfficeScan domain, and then click **OK**. The new OfficeScan domain appears in the domain tree.

## Updating OfficeScan

To help ensure that clients stay protected against the latest virus threats, regularly update the OfficeScan components. Do the following to configure OfficeScan to perform updates:

1. Configure the OfficeScan server for updates
2. If you are using Update Agents, specify which clients act as agents and configure agent settings (see [Using Update Agent](#) on page 4-17 for more information)
3. Configure OfficeScan clients to receive updates from an update source

## Choosing an update source

When choosing the location(s) from where to update clients, consider the bandwidth of the sections of your network that are between clients and the update source(s) (see

*Planning for network traffic* on page 2-4 for more information on how updates affect network traffic). The following table describes different component update options and recommends when to use them:.

Update option	Description	Recommendation
ActiveUpdate server > OfficeScan server > clients.	The OfficeScan server receives updated components from the ActiveUpdate server (or other update source) and deploys them directly to clients.	Use this method if there are <b>no</b> sections of your network between the OfficeScan server and clients you identify as 'low-bandwidth'.
ActiveUpdate server > OfficeScan server > Update Agents > clients	The OfficeScan server receives updated components from the ActiveUpdate server (or other update source) and deploys them directly to Update Agents, which deploy the components to clients.	Use this method to balance the traffic load on your network if there are sections of your network between the OfficeScan server and clients you identify as 'low-bandwidth'.
ActiveUpdate server > Update Agents > clients	Update Agents receive updated components directly from the ActiveUpdate server (or other update source) and deploy them to clients.	Use this method only if you are experiencing 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 are experiencing 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.

## Updating the server

Update components by configuring the server to download component updates from the Trend Micro update server. After the server downloads any available updates, it

deploys them to clients based on the deployment schedule you specified on the **Automatic Deployment** screen under **Updates > Client Deployment**.

Trend Micro updates components on a daily (and in some cases hourly) basis to endure that client protection stays current.

---

**Tip:** Trend Micro recommends updating the server daily to help ensure OfficeScan server has current component versions.

---

OfficeScan provides these methods of updating the server:

- Configure automatic scheduled updates for the server
- Update the server manually

## Configuring automatic scheduled updates

Configure the server to regularly check the update server and automatically download any available updates. Because clients normally get updates from the server, using automatic update is an easy and effective way of ensuring that your protection against viruses is always current.

### To update the server based on a schedule:

1. On the sidebar, click **Updates > Server Update > Automatic Update**. The **Automatic Update** screen appears.
2. Select the **Enable scheduled update of the OfficeScan server** check box.
3. In the **Components** box, select the components to update.
4. Under **Update schedule**, specify a schedule when to perform scheduled update.
  - **Hourly** – click to perform scheduled updates every hour
  - **Daily** – click to perform scheduled updates every day
  - **Weekly** – click to perform scheduled updates once a week. You must select a day from the list.
  - **Monthly** – click to perform scheduled updates once a month. You must select a date from the list.

Regardless of the selection, specify when to perform scheduled updates in the **Time** lists.

5. Under **Update Source**, select the location from where to download the update. Select either the **Trend Micro ActiveUpdate server** or **Other update source** and type in the source's URL.
6. To have the server continue retrying if an update attempt fails, select the **Retry update if update attempt fails** check box under **Program Update Retry**.  
In the **Number of attempts** list, select the number of times that the server will attempt the update.  
In the **Interval** list, select the time interval, in minutes, before the server continues to retry the update attempt.
7. Click **Save** to save your settings.

## Updating the server manually

Also update the components on the server manually. Trend Micro recommends updating the server manually immediately after deploying OfficeScan and whenever there is a virus outbreak.

### To update the server manually:

1. On the sidebar, click **Updates > Server Update > Manual Update**. The **Manual Update** screen appears, showing your current components, their version numbers, and the most recent update dates.
2. Under **Update Source**, choose whether to receive updates from the update server or from another source and type the source URL.
3. Click **Update**. The server checks the Trend Micro update server for updated components. If there are available updates, they appear on the **Available Updates From Trend Micro** screen, with the component names and version numbers.
4. Select the check boxes for the components to update.
5. Click **Update**. The server downloads the updated components.

---

**Note:** If you do not specify a deployment schedule on the **Automatic Deployment** screen under **Client Deployment**, the server will download the updates but will not deploy them to clients.

---

To check if you have specified a download schedule, click **Updates > Server Update > Automatic Update** on the sidebar. The **Automatic Update** screen appears showing the update schedule.

---

**Note:** If there are proxy servers on your network, make sure the proxy settings are properly configured (see *Configuring Internet Proxy settings* on page 4-17).

---

## Configuring Internet Proxy settings

The Web console uses two proxy settings: one for server-client communication on the local area network (intranet) and one for the server when it connects to the Internet to download updates from the Trend Micro ActiveUpdate server.

If your network uses a proxy server to connect to the Internet, you must configure the OfficeScan Internet proxy settings for your server to download updates from the Trend Micro update server or other update source.

### To set the Internet proxy:

1. On the sidebar, click **Updates > Server > Internet Proxy**. The **Internet Proxy** screen appears.
2. Select the **Use a proxy server** check box.
3. Type the address of the proxy server and its port number.
  - If the proxy server uses version 4 of the SOCKS protocol to handle Transmission Control Protocol (TCP), select the **Use SOCKS 4** check box.
4. If the proxy server requires a password, type your user name and password in the fields provided.
5. Click **Save** to save your settings.

## Using Update Agent

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

For example, 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.

---

**Note:** Only Windows NT/2000/XP/Server 2003 clients can act as Update Agents. Ensure that Update Agent machines have at least 15 Megabytes of available disk space.

---


Configuring Update Agents is a three-step process:

1. Grant clients the privilege to act as update agents (see *Specifying a client as an Update Agent* on page 4-18)
2. Select an update source from which the Update Agent can receive updated components (see *Selecting an update source for the agents* on page 4-19)
3. Select which clients you want to update from the Update Agent and set the Update Agents as the client update source.

## Specifying a client as an Update Agent

For clients to act as Update Agents, you must first grant them the privilege to do so.


### To specify a client as an Update Agent:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to which to grant Scheduled Update privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon .
3. On the sidebar, click **Client Privileges**. The **Client Privileges** screen appears.
4. Under Update, select the **Act as Update Agent** check box.

---

**Note:** If you select multiple clients, you cannot modify the **Act as Update Agent** privilege. To change this privilege for multiple clients at one time, create and export a policy for Client privilege settings (see *Granting Privileges to Clients* on page 4-43). Then select multiple clients and import the policy. The Client privilege settings, including the **Act as Update Agent** privilege, are applied to all selected clients.

---

5. Click **Save**. Clients that act as update agents appear with the  icon in the domain tree.

## Selecting an update source for the agents

Enable Update Agents to get their component updates from the OfficeScan server on the **Update Agent** screen. If you do not enable Update Agents to get component updates from the OfficeScan server, they receive updates from the source specified on the **Update Source** screen.

### To select where Update Agents get their updates:

1. On the sidebar, click **Updates > Client Deployment > Update Agent**. The **Update Agent** screen appears.
2. Click the **Always update from standard update source (OfficeScan server)** to have agents always get updates from the OfficeScan server.

To have agents get updates from the sources specified on the **Update Source** screen, clear the check box (see [Selecting an update source](#) on page 4-20 for more information).

3. Click **Save**.

## Setting an Update Agent as a client update source

To have OfficeScan clients get their updates from one or more Update Agents, add the Update Agent(s) to the Customized update source list in the **Update Source** screen. You can also specify (by IP address) which clients receive updates from any update source.

### To set an Update Agent as a client update source:

1. On the sidebar, click **Updates > Client Deployment > Update Source**. The **Update Source** screen appears.
2. Click **Customized Update Source**.
3. In the **Customized Update Source** list, click **Add**. The **Add IP Range and Update Source** screen appears.
4. Type a range of IP addresses of clients that you want to receive updates from an Update Agent.
5. Next to **Update Source**, click **Update Agent** and select an agent from the list.

---

**Note:** The clients you granted the privilege to act as Update Agents appear in the list. If any Update Agents are missing, apply the **Act as Update Agent**



privilege to the clients in the **Client Privileges** screen (see *Specifying a client as an Update Agent* on page 4-18).

---

6. Click **Save**.

## Updating clients

To help ensure that clients stay protected from the latest virus threats, regularly update their components. The clients get updates from the server, which downloads updates from the Trend Micro ActiveUpdate server.

Before updating the clients, verify that the server has the latest components. For information on how to update the server, refer to *Updating the server* on page 4-14.

Trend Micro periodically updates the scan engine and program. On the other hand, Trend Micro updates virus pattern files every week and more often during virus outbreaks to help ensure that clients are protected from new virus threats.

---

**Tip:** Trend Micro recommends updating the server daily to help ensure OfficeScan server has current component versions.

---

OfficeScan provides these methods of updating clients:

- Automatic Deployment
- Manual Deployment
- Update Now on the client

Except for using Update Now on the client, these methods can update all components on the client (see *Understanding OfficeScan components* on page 1-5 for descriptions of each component).

## Selecting an update source

First select a source from which clients can receive component updates.

### To select an update source:

1. On the sidebar, select **Updates > Client Deployment > Update Source**. The **Update Source** screen appears.
2. Select an update source:

- Click **Standard update source** to have clients update from the OfficeScan server

- Click **Customized Update Source** to have clients update from the first update source on the **Customized update source** list. If the Trend Micro update server is not on the list, you must add it. The default address is:

`http://officescan-p.activeupdate.trendmicro.com/activeupdate`

If updating from an Update Agent, you must also add the agent to the list (see *Using Update Agent* on page 4-17 for more information on Update Agents).

Do the following to modify the **Customized Update Source List**:

- i. Click **Add** or **Edit**. The **IP Range and Update Source** screen appears.
- ii. Add the range of client IP address that will receive updates from this source.
- iii. Click an **Update Source**:
  - **Update Agent** – click and specify an Update Agent from the list. Select which clients act as Update Agents in the **Client Privileges** screen (see *Using Update Agent* on page 4-17 for more information).
  - **Specified** – click and type the IP address of an update source

3. Click **Save**. The **Update Source** screen appears.

4. Click **Notify All Client(s)**.

---

**Note:** You can add a maximum of 96 update sources to the Customized update source list.

---

## Updating clients using Automatic Deployment

Automating client updates is an easy and effective way of ensuring that clients always get the latest components from the server. Trend Micro recommends automating client updates to help protect clients from the latest virus threats.

**To update clients using Automatic Deployment:**

1. On the sidebar, click **Updates > Client Deployment > Automatic Deployment**. The **Automatic Deployment** screen appears.

2. Under **Event-triggered Deployment**, select when to deploy the updates and whether to scan the client:
  - **Deploy to clients immediately after the OfficeScan server downloads a new component**  
Also, decide whether to include roaming client(s).
  - **Deploy to clients (For OfficeScan clients only and excluding roaming clients) when they are restarted**
  - **Scan the computer after update:** select to scan OfficeScan clients after the update to help ensure that the client was not infected. Click one of the following:
    - Perform Cleanup Now and Scan Now
    - Perform Cleanup Now

---

**Tip:** Trend Micro recommends specifying an update schedule. If you do not specify a schedule, the clients will only be updated if you perform manual deployment from the console.

---

3. Under **Schedule to Deploy**, select the **Enable scheduled deployment from OfficeScan server or customized update source** check box to specify an update schedule. Ensure that you grant clients the privilege to enable a schedule update under **Clients > Client Privileges**.
4. Select how often to perform scheduled deployment. Click one of the following:
  - **Hours** – to deploy every { } hours. Select a number of hours
  - **Daily** – to deploy daily. Select the start time and the length of deployment time
  - **Weekly** – to deploy weekly. Select a day
5. Click **Save**.

## Updating clients using Manual Deployment

Update clients manually by deploying updated components on the server to the clients using Manual Deployment.


**To update clients using Manual Deployment:**

1. On the sidebar, click **Updates > Client Deployment > Manual Deployment**. The **Manual Deployment** screen appears.
2. Under **Deployment Target**, choose to update all clients whose components are out of date or choose specific clients:
  - To update all online clients, including roaming clients with functional connections to the server, click **Select clients with out-of-date components** and select the **Include roaming client(s)** check box
  - To update specific clients, click **Manually select clients** and do the following:
    - i. Click **Select** to choose specific clients. The **Manual Deployment** screen shows the client tree.
    - ii. Click the clients you want to update or click the root icon to update all clients.
3. After selecting all clients to update, click **Notify**. The server starts notifying each client to download the updates.

**Updating clients using Update Now**

Instruct users to update the client components by performing Update Now on the client. Performing Update Now updates components from the specified update source to the client. Users can also download update components directly from the Trend Micro update server, if you grant users this privilege.

**To allow users to download from the Trend Micro ActiveUpdate server:**

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to which to grant Scheduled Update privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon .
3. On the sidebar, click **Client Privileges**. The **Client Privileges** screen appears.
4. Under **Update**, select the **Download from the Trend Micro ActiveUpdate server** check box.
5. Click **Save** to grant the privilege to the selected domains or clients.
6. On the sidebar, click **Updates, Client Deployment**, and then **Update Source**. The **Update Source** screen appears.

7. Click **Customized Update Source**. Clients will update from the first update source on the **Customized update source** list. If the Trend Micro update server is not on the list, you must add it. The default address is:  
`http://officescan-p.activeupdate.trendmicro.com/activeupdate`

**To perform Update Now on the client:**

1. Right-click the OfficeScan icon in the system tray of the OfficeScan client machine. The OfficeScan shortcut menu appears.
2. Click **Update Now!**. The **Update Now Settings** screen appears.
3. If your network requires you to use a proxy server, click **Use a proxy server** check box and enter the proxy server settings.
4. Click **Update Now**. A status screen appears showing the progress of the component download.

## Verifying a successful update

Check the client update logs to verify that an update has been successfully deployed.

**To view the Client Update Logs:**

1. On the sidebar, click **Logs > Update Logs > Client Update**. The **Client Update Logs** screen appears.
2. Select the number of results to view on each page from the **Display results per page** list.
3. To sort the table, click on the **Time/Date** or **Update Components** column headings.
4. To view the progress of a particular update, click **View** under the **Progress** column. The **Client Update Progress** screen appears, displaying the number of clients updated for every 15-minute interval and the total number clients updated.
5. To view the details of a particular update, click **View** under the **Detail** column. The **Client Update Detail** screen appears.

## Rolling back components

Rolling back refers to reverting to the previous version of a virus pattern file or scan engine. If the pattern file or scan engine that you are using is not functioning properly, roll back these components.

OfficeScan uses two types of scan engines: one for Windows NT/2000/XP/Server 2003 clients and one for Windows 95/98/Me clients. You need to roll back these two types of scan engines separately. The rollback procedures for both types of scan engines are the same.


---

**Note:** OfficeScan retains only the current and the previous versions of the scan engine and the last five pattern files.

---

### To roll back the pattern file or scan engine:

1. On the sidebar, click **Updates > Rollback**. The **Rollback** screen appears showing the current versions of your virus pattern file and scan engine, and the previous versions of these components, if any.
2. Click **Synchronize with Server** under the appropriate section. The **Rollback** screen shows the client domain tree.

To select all domains and clients, click the root icon . You can also search for clients by selected criteria, as well as change the client tree view. To select multiple, adjacent clients, click the first client in the range, hold down the SHIFT key, and then click the last client in the range.
3. Click **Notify** to roll back the pattern file or scan engine on the selected clients. A confirmation screen appears.

Click **Back** to return to the original **Rollback** screen.
4. If an older version pattern file exists on the server, you can roll back both the client and the server. Click **Rollback server and clients**. The **Rollback** screen appears.
  - a. Select the clients to roll back.
  - b. Click **Notify** to roll back the pattern file on the selected clients.

The server notifies the selected clients to roll back the pattern file to synchronize with the server.

## Verifying Client-Server Connection

Verify OfficeScan client-server connection to help ensure that all your clients will have the correct configuration, including scan settings and privileges. Verify client-server connection manually or automatically from the Web console.

### To verify the client-server connection:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Verify Connection**. The **Verify Connection** screen appears.
4. To verify client-server connection manually, click **Verify Now** under **Manual Verification**.
5. To verify client-server connection automatically, click the **Scheduled Verification** tab and select the **Enable scheduled verification** check box. Choose from these options:
  - **Once** – click to perform only one connection verification
  - **Hourly** – click to verify the client-server connection every hour
  - **Daily** – click to verify the client-server connection every day
  - **Weekly** – click to verify the client-server connection every week and select a day from the listIf you clicked **Once**, **Daily**, or **Weekly**, select a time for the verification to begin under **Start time**.
6. Click **Save** to save the verification schedule.

Check the client tree again to verify that the client status changed. Also, view the verify connection log for a summary of your connection verification. See [Viewing verify connection logs](#) on page 8-6 for more information.

## Setting up Standard Notifications

The latest Internet-aware viruses, if left unchecked, can spread quickly throughout your organization and overwhelm network resources. Set up notifications for

OfficeScan to inform you about viruses it detects or any outbreak that may be developing on the network.

Configure OfficeScan to send these types of alerts:

- Standard alerts
- Outbreak alerts

## Configuring standard alerts

Send alerts to yourself or other administrators in your organization whenever OfficeScan detects a virus on any client. Standard alerts inform you whenever a virus incident occurs on a client machine.

To ensure that recipients get the alerts, OfficeScan provides multiple ways of sending alerts. Send standard alerts through the following:

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

OfficeScan includes the following information in all alert messages by default, except pager alerts:

- Computer name
- User name
- Domain name
- File path of the infected file
- Virus name
- Date and time of detection
- Scan action and result

### To send alerts via email:

1. On the sidebar, click **Administration > Standard Alert > Email Notification**. The **Email Notification** screen appears.
2. Select the **Enable notification via email** check box and fill in these fields:
  - **SMTP** – type the domain name of the mail server



- **Port number** – type the port number that the OfficeScan server uses to communicate with the mail server (default is 25)
- **To** – type the destination email address
- **From** – type the name of the sender
- **Subject** – type the subject of the alert
- **Message** – type the alert message

3. Click **Save** to save the settings.

**To send alerts via pager:**

1. On the sidebar, click **Administration > Standard Alert > Pager Notification**. The **Pager Notification** screen appears.
2. Select the **Enable notification via pager** check box.
3. Type both the pager number to which to send the alert message and the COM (communications) port to which your modem is connected.
4. Type a message in the **Message** text box.
5. Click **Save** to save the settings.

**To send alerts via SNMP Trap:**

1. On the sidebar, click **Administration > Standard Alert > SNMP Trap**. The **SNMP Trap** screen appears.
2. Select the **Enable notification via SNMP Trap** check box.
3. Type the IP address for SNMP trap notifications and the community name.
4. Type a message in the **Message** text box.
5. Click **Save** to save the settings.

**To send alerts to the Windows NT Event Log:**

1. On the sidebar, click **Administration > Standard Alert > NT Event Log**. The **NT Event Log** screen appears.
2. Select the **Enable notification via NT Event Log** check box.
3. Type a message in the **Message** text box.
4. Click **Save** to save the settings.

## Configuring outbreak alerts

An outbreak refers to a sudden increase in the incidence of viruses on the network. In OfficeScan, you define the criteria for outbreaks; that is, how many virus incidents within a certain period of time constitutes an outbreak. Responding to an outbreak is critical. Unless you take corrective action, an outbreak can spread quickly throughout and beyond the network.

To help you respond to outbreaks that may be developing on the network, send outbreak alerts to administrators whenever the outbreak criteria is met.

When OfficeScan sends an outbreak alert, use Outbreak Prevention to control the outbreak on the network. For more information on Outbreak Prevention, see [Using Outbreak Prevention](#) on page 6-2.

OfficeScan provides the following ways to send alerts:

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

### To send alerts via email:

1. On the sidebar, click **Administration > Outbreak Alert > Email Notification**. The **Email Notification** screen appears.
2. Select the **Enable notification via email** check box.
3. Under **Outbreak Criteria**, define how many virus incidents within a certain period of time constitute an outbreak.

---

**Tip:** Trend Micro recommends declaring an outbreak if OfficeScan detects 100 viruses in 24 hours (the default values).

---

4. Under **Alert Message Settings**, fill in these fields:
  - **SMTP** – type the domain name of the mail server
  - **Port number** – type the port number that the OfficeScan server uses to communicate with the mail server (default is 25)
  - **To** – type the destination email address
  - **From** – type the name of the sender

- **Subject** – type the subject of the alert
  - **Message** – type the alert message
5. Select the information to include in the email body under **Alert Information to Include**.
  6. Click **Save** to save the settings.

---

**To send alerts via pager:**

1. On the sidebar, click **Administration > Outbreak Alert > Pager Notification**. The **Pager Notification** screen appears.
2. Select the **Enable notification via pager** check box.
3. Under **Outbreak Criteria**, define how many virus incidents within a certain period of time constitute an outbreak.

---

**Tip:** Trend Micro recommends declaring an outbreak if OfficeScan detects 100 viruses in 24 hours (the default values).

---

4. Type both the pager number to which to send the alert message and the COM (communications) port number to which the modem is connected.
5. Type a message in the **Message** text box.
6. Click **Save** to save the settings.

**To send alerts via SNMP trap:**

1. On the sidebar, click **Administration > Outbreak Alert > SNMP Trap**. The **SNMP Trap** screen appears.
2. Select the **Enable notification via SNMP Trap** check box.
3. Under **Outbreak Criteria**, define how many virus incidents within a certain period of time constitute an outbreak.

---

**Tip:** Trend Micro recommends declaring an outbreak if OfficeScan detects 100 viruses in 24 hours (the default values).

---

4. Type the IP address of the network management station to use for SNMP trap notifications and the community name.
5. Type a message in the **Message** text box.

6. Click **Save** to save the settings.

**To send alerts to the Windows NT Event Log:**

1. On the sidebar, click **Administration > Outbreak Alert > NT Event Log**. The **NT Event Log** screen appears.
2. Select the **Enable notification via NT Event Log** check box.
3. Type a message in the **Message** text box.
4. Click **Save** to save the settings.

## Configuring the Scan Settings

OfficeScan provides three types of scans: Real-time Scan, Scheduled Scan, and Manual Scan. Enforce your organization's antivirus policies throughout the network by configuring the three types of scans based on these policies. Specify the types of files to scan and the action to take when a virus is found.

If you do not configure the scan settings, clients will scan files using the default settings of OfficeScan. The default scan settings provide an adequate level of protection for most environments.

Exclude files and folders from scans to save time or to skip problem files that trigger false alarms. File and folder exclusion applies to all types of scans. For information on how to exclude files and folders, see [Excluding files and folders from scanning](#) on page 4-39.

---

**Note:** Enabling scanning of Additional Threats may generate a large amount of incident logs and alerts. OfficeScan may frequently detect several commonly used applications, such as Hotbar, and interpret them as spyware/adware. To prevent OfficeScan from detecting commonly used applications, add the application files to the Exclusion List for all types of scans (see [Scanning for Additional Threats](#) on page 1-13 for more information on the types of threats OfficeScan can recognize).

---

Use IntelliScan to help determine which files to scan for potential threats and ActiveAction to utilize a set of Trend Micro pre-configured scan actions for viruses and other types of threats (see [Trend Micro IntelliScan](#) on page 1-12 and [Trend Micro ActiveAction](#) on page 1-13 for more information).

## Configuring Manual Scan

Also called Scan Now, manual scan occurs momentarily after being invoked and scans all files specified. The length of the scan depends on the number of files you are scanning and the computer's hardware resources.

### To configure Manual Scan:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to which to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Options > Manual Scan**. The **Manual Scan Settings** screen appears.
4. Under **Scan Target**, specify the files to scan:
  - **All scannable files** – click to scan all files that the client opens or saves
  - **Use IntelliScan – True file type identification** – click to use IntelliScan
  - **Scan files with the following extensions** – click to manually specify the files to scan based on their extensions:  
.ARJ, .ASP, .BAT, .BIN, .BOO, .CAB, .CHM, .CLA, .CLASS, .COM, .CSC, .DAT, .DLL, .DOC, .DOT, .DRV, .EML, .EXE, .GZ, .HLP, .HTA, .HTM, .HTML, .HTT, .INI, .JAR, .JS, .JSE, .LNK, .LZH, .MDB, .MPD, .MPP, .MPT, .MSG, .MSO, .NWS, .OCX, .OFT, .OVL, .PDF, .PHP, .PIF, .PL, .POT, .PPS, .PPT, .PRC, .RAR, .REG, .RTF, .SCR, .SHS, .SYS, .TAR, .VBE, .VBS, .VSD, .VSS, .VST, .VXD, .WML, .WSF, .XLA, .XLS, .XLT, .XML, .Z, and .ZIP
  - **Scan compressed files** – select to scan compressed files that are stored on the client. In the **Up to { } layers of compression** list, select the maximum number of compression layers to scan.
  - **Enable Exclusion list** – select to exclude certain directories, files and extensions from scanning. Click **Enable Exclusion List** to go to the Exclusion List screen to configure exclusion settings. See [Excluding files and folders from scanning on page 4-39](#).
  - **Scan memory (not applicable to Windows NT/2000/XP/Server 2003 clients)** – select to scan the Random Access Memory (RAM) of the client
  - **Scan boot area** – select to scan the boot sector of the hard disk on the client

- **Scan hidden folders** – select to include hidden folders in any scan
  - **Scan for Additional Threats** – select to scan for software that installs components that record Web surfing habits (includes adware, spyware, keyloggers, and dialers)
  - **Scan mapped drives and shared folders on the network** – click to scan all mapped drives and shared folders on the network
5. Under **Scan Action**, specify how to handle Internet threats when OfficeScan detects them.
- **Use ActiveAction – recommended actions by file type** – click to use ActiveAction
  - **Use Customized scan action** – click to manually specify how to handle different types of Internet threats when OfficeScan detects them
  - **Use the same action for all malware types** – click to handle all types of Internet threats in the same manner

In the **Action1** and **Action2** lists, select the action to perform on infected files:

- **Pass** – take no action on the file
- **Delete** – delete the file
- **Rename** – rename the file to identify it as infected
- **Quarantine** – move the file to the quarantine directory
- **Clean** – clean the file of the virus

---

**Tip:** Trend Micro recommends selecting **Clean**. Save a copy of the files before cleaning, select the **Back up files before cleaning** check box.

---

OfficeScan performs **Action 2** only if **Action 1** is not successful.

- In **Quarantine directory**, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path to store the infected files.  
For example: HTTP://<OfficeScan\_server\_name>
6. Click **Save** to save the manual scan settings.

---

**Note:** If you clicked the root icon before setting the manual scan settings, another button named **Apply to All** will appear beside **Save**. If you want all existing and future clients to have these manual scan settings, click **Apply to All**.

---

## Configuring Real-time Scan

Set OfficeScan to scan a file in real-time whenever it is opened or saved. If OfficeScan does not detect a virus, the user can proceed with opening or saving the file. If it does detect a virus, OfficeScan displays an alert message, showing the name of the infected file and the virus name.

The performance of real-time scanning depends on its settings. Optimize the performance of real-time scans by specifying certain file types that are vulnerable to viruses or by limiting the maximum number of compression layers to scan.

### To configure Real-Time Scan:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Options > Real time Scan**. The **Real-time Scan Settings** screen appears.
4. Select the **Enable Real-time Scan** check box.
5. Under **Scan Target**, specify incoming or outgoing files.
  - **Scan incoming file** – select to scan only files the user is saving
  - **Scan outgoing file** – select to scan only files the user is opening
  - **Scan incoming and outgoing file** – select to scan both incoming and outgoing files (files the client user is saving and/or opening)

Select the types of files to scan:

- **All scannable files** – click to scan all files that the client opens or saves
- **Use IntelliScan – all essential file types** – click to use IntelliScan
- **Scan files with the following extensions** – click to manually specify the files to scan based on their extensions:

.ARJ, .ASP, .BAT, .BIN, .BOO, .CAB, .CHM, .CLA, .CLASS, .COM, .CSC, .DAT, .DLL, .DOC, .DOT, .DRV, .EML, .EXE, .GZ, .HLP, .HTA, .HTM, .HTML, .HTT, .INI, .JAR, .JS, .JSE, .LNK, .LZH, .MDB, .MPD, .MPP, .MPT, .MSG, .MSO, .NWS, .OCX, .OFT, .OVL, .PDF, .PHP, .PIF, .PL, .POT, .PPS, .PPT, .PRC, .RAR, .REG, .RTF, .SCR, .SHS, .SYS, .TAR, .VBE, .VBS, .VSD, .VSS, .VST, .VXD, .WML, .WSF, .XLA, .XLS, .XLT, .XML, .Z, and .ZIP

- **Scan compressed files** – select to scan compressed files that are stored on the client. In the **Up to { } layers of compression** list, select the maximum number of compression layers to scan.
  - **Enable Exclusion list** – select to exclude certain directories, files and extensions from scanning. Click the **Enable Exclusion List** link to go to the Exclusion List screen to configure exclusion settings. See *Excluding files and folders from scanning on page 4-39*.
  - **Scan boot area (not applicable to Windows NT/2000/XP/Server 2003 clients)** – select to scan the boot sector of the hard disk on the client
  - **Scan during system shutdown** – select to run Real-time Scan every time the client is shut down
  - **Scan for Additional Threats** – select to scan for software that installs components that record Web surfing habits (includes adware, spyware, keyloggers, and dialers)
  - **Scan mapped drives and shared folders on the network** – click to scan all mapped drives and shared folders on the network
6. Under **Scan Action**, specify how to handle Internet threats when OfficeScan detects them.
- **Display an alert message on the client when a virus is detected** – select to have an alert message pop up on the client
  - **Use ActiveAction – recommended actions by file type** – click to use ActiveAction
  - **Use Customized scan action** – click to manually specify how to handle different types of Internet threats
- In the **Action1** and **Action2** lists, select the action to perform on infected files.



- **Use the same action for all malware types** – click to handle all types of Internet threats in the same manner

In the **Action1** and **Action2** lists, select the action to perform on infected files.

- **Pass** – take no action on the file
- **Delete** – delete the file
- **Rename** – rename the file to identify it as infected
- **Quarantine** – move the file to the quarantine directory
- **Clean** – clean the file of the virus

---

**Tip:** Trend Micro recommends selecting **Clean**. To save a copy of the files before cleaning, select the **Back up files before cleaning** check box.

---

OfficeScan performs **Action 2** only if **Action 1** is not successful.

- In **Quarantine directory**, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path to store the infected files.

For example: HTTP://<OfficeScan\_server\_name>

7. Click **Save** to save your manual scan settings.

---

**Note:** If you clicked the root icon before setting the manual scan settings, another button named **Apply to All** will appear beside **Save**. If you want all existing and future clients to have these manual scan settings, click **Apply to All**.

---

## Configuring Scheduled Scan

A scheduled scan completely scans specified files at the time and frequency configured. Use scheduled scan to automate routine scans on the clients and improve virus management efficiency.

### To configure Scheduled Scan:

1. On the sidebar, click **Clients**. The domain tree for the **Client** screen appears.

2. Click the domains or clients to which to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Options > Scheduled Scan**. The **Scheduled Scan Settings** screen appears.
4. Select the **Enable Scheduled Scan** check box.
5. Under **Schedule**, specify when to perform scheduled scans:
  - **Daily** - click to perform scheduled scan every day
  - **Weekly** - click to perform scheduled scan once a week. You must select a day from the list
  - **Monthly** - click to perform scheduled scan once a month. You must select a date from the list

Regardless if you click **Daily**, **Weekly**, or **Monthly**, you must specify a time to perform a scheduled scan in the **Start time** list boxes.

6. Under **Scan Target**, specify the files to scan by selecting the check boxes and clicking the options.
  - **All scannable files** – click to scan all files that the client opens or saves
  - **Use IntelliScan – all essential file types** – click to use IntelliScan
  - **Scan files with the following extensions** – click to manually specify the files to scan based on their extensions:
 

.ARJ, .ASP, .BAT, .BIN, .BOO, .CAB, .CHM, .CLA, .CLASS, .COM, .CSC, .DAT, .DLL, .DOC, .DOT, .DRV, .EML, .EXE, .GZ, .HLP, .HTA, .HTM, .HTML, .HTT, .INI, .JAR, .JS, .JSE, .LNK, .LZH, .MDB, .MPD, .MPP, .MPT, .MSG, .MSO, .NWS, .OCX, .OFT, .OVL, .PDF, .PHP, .PIF, .PL, .POT, .PPS, .PPT, .PRC, .RAR, .REG, .RTF, .SCR, .SHS, .SYS, .TAR, .VBE, .VBS, .VSD, .VSS, .VST, .VXD, .WML, .WSF, .XLA, .XLS, .XLT, .XML, .Z, and .ZIP
  - **Scan compressed files** – select to scan compressed files that are stored on the client. In the **Up to { } layers of compression** list, select the maximum number of compression layers to scan.
  - **Enable Exclusion list** – Select to exclude certain directories, files and extensions from scanning. Click the **Enable Exclusion List** link to go to the Exclusion List screen to configure exclusion settings. See [Excluding files and folders from scanning on page 4-39](#).

- **Scan memory (not applicable to Windows NT/2000/XP/Server 2003 clients)** – select to scan the Random Access Memory (RAM) of the client
  - **Scan boot area** – select to scan the boot sector of the hard disk on the client
  - **Scan for Additional Threats** – select to scan for software that installs components that record Web surfing habits (includes adware, spyware, keyloggers, and dialers)
7. Under **Scan Action**, specify how to handle Internet threats when OfficeScan detects them.
- **Display an alert message on the client when a virus is detected** – select to have an alert message pop up on the client
  - **Use Customized scan action** – click to manually specify how to handle different types of Internet threats  
In the **Action1** and **Action2** lists, select the action to perform on infected files.
  - **Use the same action for all malware types** – click to handle all types of Internet threats in the same manner  
In the **Action1** and **Action2** lists, select the action to perform on infected files:
    - **Pass** – take no action on the file
    - **Delete** – delete the file
    - **Rename** – rename the file to identify it as infected
    - **Quarantine** – move the file to the quarantine directory
    - **Clean** – clean the file of the virus

---

**Tip:** Trend Micro recommends selecting **Clean**. To save a copy of the files before cleaning, select the **Back up files before cleaning** check box.

---

OfficeScan performs **Action 2** only if **Action 1** is not successful.

8. Click **Save** to save your manual scan settings.

---

**Note:** If you clicked the root icon before setting the manual scan settings, another button named **Apply to All** will appear beside **Save**. If you want all existing and future clients to have these manual scan settings, click **Apply to All**.

---

## Excluding files and folders from scanning

To increase the performance of scanning or to skip files that are causing false alarms, you can exclude certain files and folders from scanning. The files and folders you add to the exclusion list will be skipped by manual scan, real-time scan, and scheduled scan.


### To exclude files and folders from scanning:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Select the domains or clients on which to configure the scan options by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Options**. Next, click the type of scan to perform (manual, real time, scheduled). The settings screen for that scan type appears.
4. In that settings screen, select the check box next to **Enable Exclusion list**. Click the **Enable Exclusion list** link. The **Execution List** screen appears.
5. To exclude all folders containing Trend Micro products and components, select the **Exclude from scanning the directories where Trend Micro products are installed** check box.
6. To exclude specific directories, type the directory names under **Enter the directory path (E.g. c:\temp\ExcludeDir)** and click **Add**.
7. To exclude specific files by file name, type the file names under **Enter the file name or file name with full path (E.g. ExcludeDoc.hlp; c:\temp\excldir\ExcludeDoc.hlp)** and click **Add**.

---

**Note:** All subdirectories in the directory path you specify will also be excluded.

---

8. Specify the files to exclude based on their extensions.  
To use specified extensions, select the extensions to protect and click .

To specify an extension that is not in the list, type it in the text box, and then click **Add**.

9. To apply this setting to all future clients that will belong to the domain you selected, click **Save**.
  - To apply this setting to all existing and future clients that belong and will belong to the domain you selected, click **Apply to All**
  - If you only selected a client or clients in Step 1, only **Save** will appear

---

**Note:** If Microsoft Exchange Server is running on your client machines, Trend Micro recommends excluding all Microsoft Exchange Server folders from scanning.

---

## Running Scan Now

Run Scan Now on clients remotely using the Web console. In addition to turning on Real-time Scan and configuring Scheduled Scan, Trend Micro recommends running Scan Now on computers you suspect to be infected.

### To run Scan Now:

1. On the sidebar, click **Clients**. The domain tree for the **Client** screen appears.
2. Click the domains or clients on which to run Scan Now by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Now**. The **Scan Now** screen appears, displaying the clients or domains you selected.
4. Under **Computer**, select the clients on which to run Scan Now, and then click **Start Notification**. The server sends a request to the client to run Scan Now using the pre-configured settings.

### To change Scan Now settings:

1. Click **Scan Now Settings**. The **Scan Now Settings** screen appears.
2. Under **Scan Target**, specify the files to scan:
  - **All scannable files** – click to scan all files that the client opens or saves
  - **Use IntelliScan – all essential file types** – click to use IntelliScan

- **Scan files with the following extensions** – click to manually specify the files to scan based on their extensions:  
 .ARJ, .ASP, .BAT, .BIN, .BOO, .CAB, .CHM, .CLA, .CLASS, .COM, .CSC, .DAT, .DLL, .DOC, .DOT, .DRV, .EML, .EXE, .GZ, .HLP, .HTA, .HTM, .HTML, .HTT, .INI, .JAR, .JS, .JSE, .LNK, .LZH, .MDB, .MPD, .MPP, .MPT, .MSG, .MSO, .NWS, .OCX, .OFT, .OVL, .PDF, .PHP, .PIF, .PL, .POT, .PPS, .PPT, .PRC, .RAR, .REG, .RTF, .SCR, .SHS, .SYS, .TAR, .VBE, .VBS, .VSD, .VSS, .VST, .VXD, .WML, .WSF, .XLA, .XLS, .XLT, .XML, .Z, and .ZIP
  - **Enable Exclusion list** – Select to exclude certain directories, files and extensions from scanning. Click the **Enable Exclusion List** link to go to the Exclusion List screen to configure exclusion settings. See [Excluding files and folders from scanning on page 4-39](#).
  - **Scan memory (not applicable to Windows NT/2000/XP/Server 2003 clients)** – select to scan the Random Access Memory (RAM) of the client
  - **Scan boot area** – select to scan the boot sector of the hard disk on the client
  - **Scan for Additional Threats** – select to scan for software that installs components that record Web surfing habits (includes adware, spyware, keyloggers, and dialers)
  - **Scan compressed files** – select to scan compressed files that are stored on the client. In the **Up to { } layers of compression** list, select the maximum number of compression layers to scan.
3. Under **Scan Action**, specify how to handle Internet threats when OfficeScan detects them.
- **Use ActiveAction – recommended actions by file type** – click to use ActiveAction
  - **Use customized scan action** – click to manually specify how to handle different types of Internet threats  
 In the **Action1** and **Action2** lists, select the action to perform on infected files.
  - **Use the same action for all malware types** – click to handle all types of Internet threats in the same manner.  
 In the **Action1** and **Action2** lists, select the action to perform on infected files.

- **Pass** – take no action on the file
- **Delete** – delete the file
- **Rename** – rename the file to identify it as infected
- **Quarantine** – move the file to the quarantine directory
- **Clean** – clean the file of the virus

---

**Tip:** Trend Micro recommends selecting **Clean**. To save a copy of the files before cleaning, select the **Back up files before cleaning** check box.

---

OfficeScan performs **Action 2** only if **Action 1** is not successful.

4. Click **Save** to save the Manual Scan settings.

---

**Note:** If you clicked the root icon before setting the manual scan settings, another button named **Apply to All** will appear beside **Save**. If you want all existing and future clients to have these manual scan settings, click **Apply to All**.

---

#### **To stop Scan Now:**

1. Select the clients on which to stop Scan Now.
2. Click **Stop Scan**.

#### **To stop notifications:**

1. Select the clients you no longer want to run Scan Now.
2. Click **Stop Notification**. Clients that have not yet started Scan Now will skip the request. However, clients that are already running Scan Now will not be affected. To stop Scan Now on these clients, click **Stop Scan**.

---

**Note:** Scan Now and manual scan are the same type of scan. The only difference is that you run Scan Now remotely from the Web console, while users run manual scan locally on the clients.

---

## Granting Privileges to Clients

You have the option of granting users privileges to modify individual scan settings, update components, and remove or unload the client. This is a way of sharing control over individual client settings.

However, to enforce uniform antivirus policy throughout the organization, Trend Micro recommends granting limited privileges to users. This will ensure that scan settings are not modified or clients are not removed or unloaded without your permission.

### To grant privileges to clients:

1. On the sidebar, click **Clients**. The domain tree for the **Client** tree appears.
2. Click the domains or clients to which to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Client Privileges**. The **Set Client Privileges** screen appears.
4. Select the privileges to grant users. Configure the following areas:
  - **Antivirus** – select the check boxes for the scan privileges to grant users
  - **Enterprise Client Firewall** – select the check boxes to allow clients to view the Enterprise Client Firewall tab and enable or disable Enterprise Client Firewall, the Intrusion Detection System, and the Enterprise Client Firewall alert message
  - **Mail Scan** – select the check boxes for the mail scan privileges to grant users
  - **Toolbox** – select the check boxes to display a toolbox tab and grant users privileges to different client tools
  - **Proxy Setting** – select the check box to allow the user to use a proxy
  - **Update** – select the check boxes for the update privileges to grant users. You can allow client to **Perform Update Now**, **Download from the Trend Micro update server**, **Enable scheduled update**, or **Act as an Update Agent**.

---

**Note:** Enable scheduled update is applicable only if you enable scheduled deployment on the **Automatic Deployment** screen, under **Updates > Client**



**Deployment** (see *Updating clients using Automatic Deployment* on page 4-21 for more information).

---

- **Uninstallation** – To allow users to remove the client without requiring a password, click **Allow the client user to uninstall OfficeScan client**. To allow only users with the uninstall password to be able to remove the client, click **Require a password for the client user to uninstall OfficeScan client**, and then type an uninstall password in the text box.
- **Unloading** – To allow users to unload (or turn off) the client without requiring a password, click **Allow the client user to unload OfficeScan**. To allow only users with the unload password to be able to turn off the client, click **Require a password for the client user to unload OfficeScan client**, and then type an unload password in the text box.
- **Client Security** – To allow clients read/write access to the OfficeScan client folders, files, and registries on client machines, click **Normal**. To restrict clients from accessing OfficeScan client folders, files, and registries, click **High**.

If you select **High**, the access permissions settings of the OfficeScan folders, files, and registries is inherited from the WINNT file (for client machines running Windows NT) or from the Program Files folder (for client machines running Windows 2000/XP/Server 2003).

Therefore, if the permissions settings (**Security** settings in Windows) of the WINNT file or Program Files folder are set to allow full read/write access, selecting **High** still allows clients full read/write access to the OfficeScan client folders, files, and registries.

---

**Note:** If you clicked the root icon before setting privileges, another button named **Apply to All** will appear beside **Apply**. If you want all existing and future clients to have this set of privileges, click **Apply to All**.

---

## Importing and Exporting Policies

You may want many OfficeScan clients to have the same scan settings and/or client privilege settings (including the ability to act as an Update Agent). OfficeScan allows you to save (export) client scan and privilege policies as a .dat file and later import

the file to multiple clients. This provides an easy way to configure identical settings on many clients.

---

**Tip:** If you grouped clients with similar virus protection requirements into a domain, Trend Micro recommends configuring the settings of one client, exporting its policy, and importing the policy file to the remainder of the clients in the domain (see *Creating OfficeScan domains* on page 4-9 for information and suggestions on creating domains).


---

---

**Note:** You cannot import policies from clients running other versions of OfficeScan.

---

**To export client settings to a policy file:**

1. On the sidebar, click **Clients > Export/Import**. The domain tree for the **Clients** screen appears.
2. Click the domain or client whose scan and privilege settings you want to export by clicking the corresponding icon in the domain tree. To select the settings for the root domain, click the root icon . You can also search for clients by selected criteria, as well as change the client tree view.

---


**Note:** 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.

---

3. On the sidebar, click **Export settings**. The **Export Settings** screen appears.
4. Click any of the scan or privilege settings links to view and modify the settings for the clients or domains you selected.
5. Click **Export** to save the settings as a policy (a .dat file).
6. Click **Save** and then specify the location to which you want to save the .dat file.
7. Click **Save** again to save the file.

**To import client policies:**

1. On the sidebar, click **Clients > Export/Import**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to which you want to import the policy by clicking the corresponding icons in the domain tree. To select all domains and clients,

click the root icon . You can also search for clients by selected criteria, as well as change the client tree view. To select multiple, adjacent clients, click the first client in the range, hold down the SHIFT key, and then click the last client in the range.

3. On the sidebar, click **Import policy**. The **Import Policy** screen appears.
4. Click **Browse** to find the .dat policy file on your computer and click **Import**. The **Import Policy** screen appears, showing a summary of the settings.
5. Click any of the scan or privilege settings links to view details regarding those settings. If you selected a domain in the domain tree, select the **Apply to children** check box to import the policies to all clients under that domain.
6. Click **Apply to Target** to import the selected policy files. A confirmation screen appears showing that your policy has imported successfully.

# Performing Additional Administrative Tasks

During OfficeScan server installation, you configured settings such as the Web console password and the Web server IP address. If the need arises, you can still modify many of these settings through the Web console at any time.

The topics discussed in this chapter include:

- *Changing the Web Console Password* on page 5-2
- *Modifying Client Alert Messages* on page 5-2
- *Configuring an Intranet Proxy* on page 5-3
- *Changing OfficeScan Web Server Information* on page 5-4
- *Removing Inactive Clients* on page 5-4
- *Configuring the Quarantine Manager* on page 5-5
- *Participating in the World Virus Tracking Program* on page 5-6

## Changing the Web Console Password

To prevent unauthorized users from modifying your settings or removing the client program from your computers, the Web console is password-protected. The OfficeScan master setup program requires you to specify a Web console password; however, you can modify your password from the Web console.

### To change the console password:

1. On the sidebar, click **Administration > Set Console Password**. The **Set Console Password** screen appears.
2. Type your current password in the **Old password** text box.
3. Type your new password (maximum 24 characters) in the **New password** text box, and then retype that password in the **Confirm password** text box.
4. Click **Save**.

---

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

---

## Modifying Client Alert Messages

OfficeScan can display alert messages on client machines to inform users of the following events on their computers:

- **Virus infections** – appears on client machines when OfficeScan detects a virus
- **Enterprise Client Firewall violations** – appears on client machines when you enable the Enterprise Client Firewall alert message (see [Configuring policies on page 7-11](#))
- **Infection source detections** – appears on client machines when OfficeScan detects that the machine is the source of a spreading virus infection

OfficeScan provides a default message for each and allows you to change them during OfficeScan installation (see [Using master installer to install OfficeScan server on page 3-6](#)). You can also modify them on the **Client Alert Message** screen.

**To modify the alert messages:**

1. Click **Administration > Client Alert Message** on the sidebar. The **Client Alert Message** screen appears.
2. Modify the default messages.
3. Under **Client Alert Message for Infection Source**, select the **Show warning describing source of infection** check box to display this warning message on the client.
4. OfficeScan displays one warning message on the client for each virus that originated from the client. If it detects more than one virus, it displays multiple warning messages. However, you can limit the number of messages displayed by setting a time interval between messages. Next to **Minimum interval**, select the minimum number of minutes OfficeScan waits between displaying another warning message (the default is 1 minute). If OfficeScan detects multiple viruses originating from the client within this time interval, it will not display additional warning messages.
5. Click **Save**.

## Configuring an Intranet Proxy

Server-client communications on the intranet do not normally require a proxy server. However, if your network uses a proxy server for internal communications, you can also set OfficeScan to use an intranet proxy. OfficeScan prompted you to configure the intranet proxy settings during installation; however, you can change them on the **Intranet Proxy** screen (see *Using master installer to install OfficeScan server* on page 3-6).

**To set the intranet proxy:**

1. On the sidebar, click **Administration > Intranet Proxy**. The **Intranet Proxy** screen appears.
2. Select the **Enable Intranet Proxy** check box.
3. Type the name of the proxy server and its port number. If the proxy server uses version 4 of the SOCKS protocol to handle Transmission Control Protocol (TCP), select the **Use SOCKS 4** check box.
4. If the proxy server requires a user name and password, type them in the fields provided.

5. Click **Save**.

## Changing OfficeScan Web Server Information

The Web server allows you to use the Web console to perform key administrative tasks for OfficeScan. During master setup, the installation program automatically sets up a Web server. As soon as master setup is complete, you can start using the Web console to configure OfficeScan.

However, 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 manually or if you assign a dynamic IP address to it, you need to reconfigure the Web server settings of OfficeScan.

---

**Note:** If your server obtains a dynamic IP address, Trend Micro recommends using the fully-qualified domain name (FQDN) of the server (instead of its IP address). This ensures that when your server obtains a different IP address, clients will still be able to find it using its FQDN.

---

### To configure the Web server:

1. On the sidebar, click **Administration > Web Server**. The **Web Server** screen appears.
2. Type the domain name or IP address of the OfficeScan server.
3. Type the port number that the OfficeScan server uses.
4. Click **Save**.

## Removing 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 domain tree to show that the client does not exist anymore.

However, if the client is removed using other methods, 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 domain tree only display active clients, you can configure OfficeScan to automatically remove inactive clients from the domain tree.

**To automatically remove inactive clients:**

1. On the sidebar, click **Administration > Inactive Clients**. The **Inactive Clients** screen appears.
2. Select the **Enable automatic removal of inactive clients** check box.
3. Select how many days should pass before OfficeScan considers a client inactive.
4. Click **Save**.

## Configuring the Quarantine Manager

Whenever a client detects an Internet threat in a file and the scan action for that type of threat is quarantine, OfficeScan encrypts the infected file and sends it to the quarantine folder on the server. OfficeScan encrypts the infected file to prevent it from infecting other files. The default location of quarantine folder is as follows:

```
OfficeScan\PCCSRV\Virus
```

For more information on configuring scan settings and to change the location of the quarantine folder, see [Configuring the Scan Settings](#) on page 4-31 and select any type of scan. From the Quarantine Manager screen, you can configure the capacity of the quarantine folder and the maximum individual file size for every infected file that can be stored in it.

**To configure the quarantine folder:**

1. On the sidebar, click **Administration > Quarantine Manager**. The **Quarantine Manager** screen appears.
2. To set the capacity of the quarantine folder, type a new value (in Megabytes) in the **Quarantine folder capacity** text box. The default capacity is 10240MB.



3. To set the maximum size for an infected file that can be stored in the quarantine folder, type a new value in the **Maximum size for a single file** text box. The default maximum file size is 64MB.

4. Click **Save**.

To delete all existing files in the quarantine folder, click **Delete All Quarantined Files**.

## Participating in the World Virus Tracking Program

You can send virus scanning results from your OfficeScan installation to the World Virus Tracking Program to better track trends in virus outbreaks. Your participation in this program can benefit the attempt to better understand the development and spread of virus infections. The OfficeScan installer asks you whether or not you want to participate in the World Virus Tracking Program; however, you can change this setting at any time (see *Using master installer to install OfficeScan server* on page 3-6 for more information on the installation procedure).

### To save Virus Tracking Program participation settings:

1. On the sidebar, click **Administration > World Virus Tracking**. The **World Virus Tracking Program** screen appears.
2. Read the disclaimer and click **Yes** to participate in the World Virus Tracking Program or click **No** to decline participation.
3. Click **Save**.

To view the current Trend Micro virus map, click Virus Map or enter the following address in your Web browser:

`http://www.trendmicro.com/map`

# Managing Outbreaks

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

The topics discussed in this chapter include:

- *Using Outbreak Prevention* on page 6-2
- *Configuring Virus Outbreak Monitor* on page 6-9
- *Using Damage Cleanup Services* on page 6-10



## Using Outbreak Prevention

Use Outbreak Prevention to block specific shared folders ports, and to deny write access to specified files and folders on selected clients. Also configure an alert message that appears on OfficeScan client machines.

---

**WARNING!** *Enable Outbreak Prevention only when there is a virus outbreak. Configure the Outbreak Prevention settings carefully. Incorrect configuration may cause unforeseen network issues.*

---

Once you enable Outbreak Prevention, verify that Outbreak Prevention the client icons in the domains you selected appear as  or .

## Blocking shared folders

During virus outbreaks, Trend Micro recommends blocking shared folders on the network to prevent viruses from spreading through the shared folders. Many types of viruses gain access to computers through shared folders.

### To block shared folders:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon. You can also search for clients by selected criteria, as well as change the client tree view.
3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Under **Outbreak prevention settings**, select **Block shared folders**.
5. To configure the shared folder blocking settings, click **Settings**. The **Shared Folder Blocking** screen appears.
6. Under **Shared Folder Blocking Settings**, specify the access privilege to shared folders when you enable Outbreak Prevention. Click one of the following:
  - **Read access only**
  - **No read or write access**

7. Click **Save** to save your settings.
8. Click **Back** to return to the **Outbreak Prevention Settings** screen.
9. Click **Activate Settings** to enable Outbreak Prevention on the selected domains or clients.
10. The **Outbreak Prevention** screen appears, showing the current outbreak prevention settings.

## Blocking ports

During virus outbreaks, block vulnerable ports that viruses and Trojans might use to gain access to clients. You may block all ports or specific ports on your workstations.

### To block ports:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Under **Outbreak prevention settings**, select the **Block ports** check box.
5. To configure the port blocking settings, click **Settings**. The **Port Blocking** screen appears.
6. To block the trusted port, which the server and client use for communication, select the **Block trusted port** check box.

---

**WARNING!** *If you block the Trusted port, OfficeScan cannot communicate with the client for the duration of the outbreak.*

---

7. To add ports to block, click **Add Ports**. The **Add Ports to Block** screen appears.
8. Specify which ports to block. Click one of the following:
  - **Block all ports (Including ICMP)** – click to block all ports, including the ICMP, which is an extension of Internet Protocol (IP), and supports packets containing error, control, and informational messages.

---

**Note:** Clicking **Block all ports (including ICMP)** will block all ports except the trusted port. To block the trusted port, select the **Block trusted ports** check box on the **Port Blocking** screen.

---

- **Block specified ports** – click to specify the ports to block. Click one of the following:
  - **Commonly used ports** – click to block port numbers that are normally used for popular Internet services; for example, port 80 for Web (HTTP), port 25 for Email (SMTP). If you click **Commonly used ports**, select at least one port number to have OfficeScan save your port blocking settings.
  - **All Trojan ports** – click to block all ports that are known to be vulnerable to Trojan attacks
  - **Specify a port number or port range between 1 and 65535** – click to specify the direction of traffic to block and the port range or port numbers

To block incoming traffic, select **Incoming traffic**.

To block outgoing traffic, select **Outgoing traffic**

Click either **Port range** or **Port number(s)**. If you click **Port range**, type a range of port numbers between 1 and 65535 in the text boxes. If you click **Port number(s)**, type the port numbers to block in the text box. Separate entries with commas.

From the **Protocol** list, select the communication method to block from the drop-down list. Select Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or both.

In **Comments**, type optional information, such as reasons for blocking the ports you specified

- **Ping protocol (Reject ICMP)** – click to block ICMP packets, such as ping
9. Click **OK**. A confirmation screen appears.
  10. Click **OK**. The **Port Blocking** screen appears, showing a summary of the port blocking settings, including the blocked ports, protocol, comments, and traffic direction.

11. Click **Back** to return to the **Outbreak Prevention** screen.
12. Click **Activate Settings** to enable Outbreak Prevention on the selected domains or clients. The **Outbreak Prevention** screen appears, showing your current outbreak prevention settings.


To modify existing port blocking settings, see the next section *Modifying port blocking settings* on page 6-5.

## Modifying port blocking settings

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

**To modify the existing settings of an individual port from the Port Blocking screen:**

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Under **Outbreak prevention settings**, select the **Block ports** check box.
5. To configure the port blocking settings, click **Settings**. The **Port Blocking** screen appears.
6. Click the  icon under the **Edit** column for the port entry you want to edit. The **Port Blocking Setting** screen appears.
7. Select whether to block incoming and/or outgoing traffic.
8. Click **Port range** and type the port numbers to block all ports within a range or click **Port number(s)** and type one or more individual port numbers to block a set of ports.

9. Modify the protocol used by the port(s) by selecting **TCP**, **UDP**, or **TCP/UDP** from the **Protocol** menu.
10. Type a description in the port(s) **Comments** field, which typically provides a descriptive name for the port(s).
11. Click **OK**. A confirmation screen appears.
12. Click **OK** again to return to the **Port Blocking** screen.

## Denying write access to files and folders

Some viruses modify or delete files and folders on host computers. Configure OfficeScan to prevent viruses from modifying or deleting files and folders on clients during a virus outbreak by denying write access to files and folders.

### To deny write access to files and folders:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Under **Outbreak prevention settings**, select **Deny write files and folders**.
5. To configure the shared folder blocking settings, click **Settings**. The **Deny Write Settings** screen appears.
6. To deny write access to specific directories and files with specific extensions, type the path of the directory to protect in **Directory path**. For example, type `C:\temp`. Type the absolute path for the directory. If typing multiple paths, separate entries with semicolons (;).


Next, click **Add**. The path appears under **Protected directories**. Before continuing, make sure all the directories to protect appear under **Protected directories**.

---

**Note:** All subdirectories in the directory path you specify will also be protected.

---

7. Specify the files in the **Protected directories** list to deny write access based on their extensions. Click one of the following:
  - **All files in the protected directories**
  - **Files in the protected directories with the following extensions**

To use specified extensions, select the extensions to protect from **Extensions list** and click .

To specify an extension that is not in the list, type it in the text box, and then click **Add**. If typing multiple extensions, separate entries with semicolons (;).

To protect specific files, type the full file names under **Files to Protect**.
8. Click **Save** to save the settings. A confirmation screen appears.
9. Click **OK**. The directory path to protect is visible under **Protected Directories** in the **Deny Write Settings** screen.
10. Click **Back** to return to the **Outbreak Prevention Settings** screen.
11. Click **Activate Settings** to enable Outbreak Prevention on the selected domains or clients. The **Outbreak Prevention** screen appears, showing the current outbreak prevention settings.

## Configuring client notification for outbreaks

Enabling Outbreak Prevention can prevent users from gaining access to network resources. To inform users that Outbreak Prevention has been enabled, display outbreak notifications on clients.

### To display outbreak notifications on clients:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Select the **When OPP is enabled, display the following message on the OfficeScan clients** check box.
5. Accept the default message or type a new message in the text box.



6. Click **Activate Settings** to save your settings.

---

**Note:** You can also configure outbreak alerts to send to yourself or OfficeScan administrators via Email, pager, SNMP trap, or Windows NT event log (*Configuring outbreak alerts* on page 4-29).



---

## Restoring network settings to normal

After verifying that an outbreak has been contained and that all infected files have been cleaned or quarantined, restore network settings to normal by disabling Outbreak Prevention.

### To restore network settings to normal:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Restore**. The **Restore Outbreak Prevention Settings** screen appears.
4. To inform users that the outbreak has ended, select the **When manual outbreak prevention settings are disabled, display the following message on the OfficeScan clients** check box. Either accept the default message or type a new one in the text box.
5. Click **Restore to normal**.
6. The **Outbreak Prevention** screen displays a message that Outbreak Prevention is disabled on the selected domains and computers.

To verify that Outbreak Prevention is disabled, check if the client icons in the domains you selected no longer appear as  or .

---

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

---

## Configuring Virus Outbreak Monitor

After infecting a host on a network, many types of viruses attempt to drop files on target computers. This action creates a session on the target machine. Therefore, monitoring the number of simultaneous sessions on your network is an effective method of detecting viruses.

OfficeScan clients notify the OfficeScan server when they detect sessions. Whenever the number of concurrent sessions exceeds a specified amount, OfficeScan server can send an alert message to the administrator, who can take proper action.

### To configure Virus Outbreak Monitor:

1. Click **Virus Outbreak Monitor** in the sidebar. The **Virus Outbreak Monitor** screen appears.
2. Select the **Enable Virus Outbreak Monitor** check box.
3. Under **Alert Criteria for Virus Outbreak Monitor**, type both the minimum number of network sessions and time period (in minutes) during which they are detected. These criteria will determine when to send an alert message.

---

**Tip:** In determining the number of network sessions, Trend Micro suggests taking the number of clients divided by 10 (#clients/10) for every three minutes.

---

4. To send an alert message, select the **Send a notification via email if alert criteria are met** check box.
5. If you enable an alert message, fill in these fields under **Alert message settings**:
  - **SMTP** – type the domain name of the mail server
  - **Port Number** – type the port number that the OfficeScan server uses to communicate with the mail server (default is 25)
  - **To** – type the destination email address
  - **From** – type the name of the sender
  - **Subject** – type the subject of the alert
  - **Message** – type the alert message
6. Click **Save** to save the settings.

**To export Virus Outbreak Monitor records:**

1. Click **Virus Outbreak Monitor** in the sidebar. The **Virus Outbreak Monitor** screen appears.
2. Click the link that displays the **Network sessions recorded** under **Current Status**. The **Virus Outbreak Monitor Records** screen appears.
3. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. A confirmation screen appears.

Click **Open** to view the file in your spreadsheet application without saving it.

---

**Note:** Use a spreadsheet application to view CSV data files.

---

## Using Damage Cleanup Services

OfficeScan also helps protect Windows computers against Trojans (or Trojan horse programs) using a built-in Trojan cleaner called Damage Cleanup Services (DCS).

A Trojan is a malicious program that masquerades as a harmless application. Trojans do not replicate like viruses but can just be as destructive. Traditional antivirus solutions can detect and remove most viruses but are often unable to detect Trojans, especially those that are already running on the system.

DCS detects and removes live Trojans and repairs system files that were modified by Trojans. It kills Trojan processes and deletes files that they have dropped.

The OfficeScan server executes DCS on the client when you do the following:

- Run Cleanup Now from the Web console
- Run Scan Now from the Web console and OfficeScan finds a Trojan
- Enable a manual, scheduled, or real-time scan and OfficeScan finds a Trojan
- Enable a scheduled clean
- Run DCS from OfficeScan client on a client computer

Because DCS is automatically executed, you do not need to configure it to help ensure that clients are protected against Trojans. Users are not even aware when it is executed because it runs in the background (when the client is running). However,


DCS may sometimes require the user to restart the computer to complete the process of removing a Trojan from the computer.

If clients have been infected, you can run Cleanup Now from the OfficeScan server Web console to run Damage Cleanup Services on your clients remotely.

## Running Cleanup Now

If clients have been infected, you can run Cleanup Now on your clients remotely.

### To run Cleanup Now:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which you want to run Cleanup Now by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon . You can also search for clients by selected criteria, such as computer name, IP address, virus pattern file version, etc. You can also change the client tree view.
3. On the sidebar, click **Cleanup Now**. The **Cleanup Now** screen appears, displaying the clients or domain members you selected.
4. Under **Computer**, click the clients on which you want to run Cleanup Now, and then click **Start Notification**. The server sends a request to the client to run Cleanup Now using the latest damage cleanup template that OfficeScan server received from TrendLabs.

Click **Select Un-notified Computers** to select all clients that have not yet been notified.

To search for a specific computer, type all or part of its name in the Computer Name field.

If you want to stop notifications to clients that have not yet started Cleanup Now, do the following:

### To stop notifications:

1. Select the clients that you no longer want to run Cleanup Now.
2. Click **Stop Notification**. Clients that have not yet started Cleanup Now will skip the request. However, this will not affect clients that are already running Cleanup Now.



# Configuring Enterprise Client Firewall

This chapter describes how to configure Enterprise Client Firewall settings to help protect your clients from hacker attacks and network viruses. The following topics are covered:

- *Understanding Enterprise Client Firewall* on page 7-2
- *Deploying the Firewall* on page 7-7
- *Verifying Deployment* on page 7-10
- *Configuring Enterprise Client Firewall* on page 7-11
- *Disabling the Firewall* on page 7-17

## Understanding Enterprise Client Firewall

The following steps are necessary to successfully deploy and use Enterprise Client Firewall:

1. **Create a policy** – the policy allow you to select a security level that blocks or allows all client traffic 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 client 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 a profile** – the profile allows you to choose a policy (which includes exceptions) to associate with the profile, specify which clients receive the profile, and set client privileges that allow or restrict users from modifying firewall settings
4. **Select profiles and deploy them to clients** – select which profiles you want to use and deploy them to the clients specified in the profile.

---

**Tip:** Trend Micro recommends uninstalling other software-based firewalls on OfficeScan clients before deploying and enabling Enterprise Client Firewall. Multiple vendor firewall installations on the same computer may produce unexpected results.

For the latest information regarding third-party firewall compatibility issues, see Knowledge Base Solution ID 20473. It is available at the following Web site:  
<http://kb.trendmicro.com/solutions/search/main/search/solutionDetail.asp?solutionId=20437>

---

## Understanding policies, exceptions, and profiles

Enterprise Client Firewall uses policies, exceptions, and profiles to organize and customize methods for protecting clients on the network.

### Policies

Policies are comprised of the following:

- **Security level** – a general setting that blocks or allows all in coming and/or all out going traffic
- **Enterprise Client Firewall settings**– enable or disable Enterprise Client Firewall, the Intrusion Detection System, and an alert message
- **An exception list** – a list of configurable exceptions to block or allow various types of network traffic

## Exceptions

Exceptions are comprised of 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.

Exception settings include both actions and criteria:

### Exception Actions

- **Action** – block or allow all traffic that meets the exception criteria

### Exception Criteria

If the following criteria are met, the firewall carries out the exception action:

- **Direction** – inbound or outbound network traffic to/from the client
- **Protocol** – the type of traffic: TCP, UDP, ICMP
- **Port(s)** – ports on the client computer on which to perform the action
- **Computers** – the computers on the network to which the above traffic criteria apply

### 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

OfficeScan uses profiles to specify the clients to which the associated policy applies and to set client firewall privileges. You can group, scan, and update settings



logically by OfficeScan domain or by selecting individual clients. Profiles provide flexibility by allowing you to choose the criteria that a client or group of clients must meet before applying a policy. Profiles are comprised of the following:

- **An associated policy** – each profile uses a single policy
- **Client criteria** – the policy is applied to clients that meet the following criteria:
  - **IP address** – a client that has a certain IP address, clients who fall within a range of IP addresses, or clients whose IP address belongs to a specified subnet
  - **Domain** – clients that belong to a certain OfficeScan domain
  - **Machine name** – clients with specified machine names
  - **Platform** – clients that are running either Windows Server (NT/2000/Server 2003) or Windows Workstation (NT/2000/XP)
  - **Logon Name**– clients onto which specified users have logged on
  - **Client status** – if clients are online or offline

Select any combination of client criteria to specify client machines

- **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

## Firewall defaults

Enterprise Client Firewall provides default policies, exceptions, and profiles to give you a basis for initiating your client firewall protection strategy. The defaults are meant to include common conditions that may exist on your clients, such as installations for the Cisco NAC Trust Agent and the need to access the Scan Mail for MicroSoft Exchange Web console.

Default 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

Default Policy Name	Security Level	Client settings	Exceptions	Recommended use
Communication Ports for TCM	Low	Enable firewall	Allow all incoming/outgoing TCP/UDP traffic through ports 80 and 10319	Use when clients have a Control Manager 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

Default 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 default exceptions, specify which clients to which you want the exceptions to apply.

---

Default Profile Name	Policy used	Applied to clients
All clients profile	All access	unspecified

## Enterprise Client Firewall features

Enterprise Client Firewall helps protect OfficeScan Windows NT/2000/XP/Server 2003 clients from hacker attacks and network viruses by creating a barrier between the client and the network.

### Traffic filtering

Enterprise Client Firewall filters all in coming and out going traffic, providing the ability to block certain types of traffic based on the following criteria:

- Direction (in coming or out going)
- Protocol (TCP/UDP/ICMP)
- Destination ports
- Destination computer

### Scanning for network viruses

Enterprise Client Firewall also examines each packet to determine if it is infected with a network virus (see [Network viruses](#) on page 1-4 for more information).

### Customized profiles and policies

Enterprise Client 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 Enterprise Client Firewall settings for your clients.

### Stateful inspection

Enterprise Client 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 when normal conditions are violated. Filtering decisions, therefore, are based not only on profiles and policies, but also on the context established by analyzing connections and filtering packets that have already passed through the firewall.

## Intrusion Detection System

Enterprise Client 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.

## Firewall Outbreak Monitor

Firewall Outbreak Monitor sends a customized alert message to specified recipients when log counts exceed certain thresholds, which may signal an attack.

## Client firewall privileges

Grant clients the privilege to view the Enterprise Client Firewall tab on the OfficeScan client program. The Enterprise Client Firewall tab displays the Enterprise Client Firewall settings for the client. Also grant users the privilege to enable or disable the firewall, the Intrusion Detection System, and the Enterprise Client Firewall Alert message (see [Granting Privileges to Clients](#) on page 4-43).

---

**Note:** You can install, configure, and use Trend Micro Enterprise Client Firewall on Windows XP machines that also have Internet Connection Firewall™ enabled. However, you must manage your 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, the traffic will be blocked. See the your Microsoft documentation for details on Internet Connection Firewall.

---

## Deploying the Firewall

This section provides the necessary steps for successful deployment of Enterprise Client Firewall.

### To deploy the firewall:

1. On the sidebar, click **Enterprise Client Firewall > Policy List**. The **Policy List** screen appears.
2. Select a default policy by selecting the check box next to the policy name. If you want to create a new policy, Click **Add**. The **Policy Editor** screen appears.

3. Type a name for the policy.
4. Click a **Security Level** to allow or block inbound/outbound traffic.
5. Click the **Enable Firewall** check box. You can also enable the Intrusion Detection System and/or an alert message that appears on the client if it blocks an outgoing packet.
6. Under **Exception**, select the check boxes next to the default exceptions to include in this policy.  
If you want to create new exceptions, do the following:
  - a. Click **Add**. The **Edit Exception** screen appears.
  - b. Type a name for the exception.
  - c. Next to **Action**, choose whether or not to allow or deny network traffic for this exception
  - d. Next to **Direction**, click **Inbound** or **Outbound** to select the type of traffic to which to apply the exception settings.
  - e. From the **Protocol** list, select the protocol that the network traffic you are allowing or denying uses:
    - **All**
    - **TCP/UDP (default)**
    - **TCP**
    - **UDP**
    - **ICMP**
  - f. Click one of the following to specify client ports:
    - **All ports** (default)
    - **Range:** type a range of ports
    - **Specified:** specify individual ports. Use a comma "," to separate port numbers.
  - g. Under **Computers**, select client IP addresses to include in the exception. For example, if you select **Deny all network traffic (Inbound and Outbound)** and type the IP address for single computer on the network, then any client that has this exception in its policy will not be able to send or receive data to or from that IP address.  
Click one of the following:

- **All IP addresses** (default)
  - **Single IP:** type the host name or IP address of a client. To resolve the client host name to an IP address, click **Resolve**.
  - **IP range:** type a range of IP addresses
  - **Subnet mask:** type an IP address and subnet mask
- h. Click **Save**. The **Policy Editor** screen appears with the new exception in the exception list.
7. Click the check boxes next to the exceptions you want to include in the profile.
  8. Click **Save**. The **Policy List** screen appears with the new policy you created.
  9. On the sidebar, click **Enterprise Client Firewall > Profile List**. The **Profile List** screen appears.
  10. To create a new profile, click **Add**. The **Profile Editor** screen appears.
  11. Click **Enable this profile** to allow OfficeScan server to deploy this profile to OfficeScan clients.
  12. Type a name to identify the profile and an optional description.
  13. From the list box next to **Use the following policy**, select the policy you created for this profile.
  14. Select the clients to which OfficeScan applies the policy. Select from the following criteria:
    - **IP address:** the IP address(es) of the client(s). Click one of the following:
      - **Single IP:** Type a client IP address.
      - **Range:** Type a range of IP addresses in the **From** and **To** text fields.
      - **Subnet:** Type an IP address of the subnet and the subnet mask. OfficeScan uses these to calculate the network address.
    - **Domain:** the domain name of the client(s). Click **Go to client console** to select clients from the domain tree.
    - **Machine name:** the name of the client(s). Click **Go to client console** to select clients from the domain tree.
    - **Platform:** the operating system of the client(s). Select from the following:
      - Windows Server (NT/2000/Server 2003)
      - Windows Workstation (NT/2000/XP)

- **Logon Name:** the ID(s) of the users logged on as client(s). If typing multiple entries, insert a comma "," between IDs.
  - **Client status:** if the OfficeScan Client application is online or offline. Click one of the following:
    - Online
    - Offline
15. Under **User Privilege**, select from among the following options:
- **Allow user to change security level:** clients can change the Enterprise Client Firewall policy security level
  - **Allow user to edit traffic exception list:** clients can edit a configurable list of exceptions to allow specified types of traffic
16. Click **Save**. The **Profile List** screen appears.
17. Click **Deploy to clients** to deploy the profile, which includes the associated policy and its exception list.

## Verifying Deployment

To verify that you successfully deployed Enterprise Client Firewall to selected clients, view the client in the OfficeScan domain tree.

### To verify the deployment:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domain to which the client belongs.
3. Select **Firewall view** from the **Client tree view** list.
4. Ensure that a green check mark exists in the **Firewall** column of the client tree. If you enabled the **Intrusion Detection System** for that client, ensure that a green check mark also exists in the **IDS** column.
5. Verify that the correct firewall policy was applied to the client. The policy appears under the **Acting Policy** column. in the client tree.

# Configuring Enterprise Client Firewall

This section explains how to configure firewall settings after deployment. For more detailed explanations of the various fields and selections, see [Deploying the Firewall](#) on page 7-7.

## Configuring policies

The Enterprise Client Firewall policy list provides a summary of all policies. Manage the policy list from this screen. Also edit the template for Enterprise Client Firewall exceptions.

### To edit a policy:

1. On the sidebar, click **Enterprise Client Firewall > Policy List**. The **Policy List** screen appears.
2. To create a new policy, click **Add**.  
To edit an existing policy, select the check box next to the corresponding policy to edit and click **Edit**.
3. Type a name for the policy.
4. Click a **Security Level** to allow or block inbound/outbound traffic:
  - **High:** blocks all in coming and out going traffic except any traffic allowed in the exception list
  - **Medium:** blocks all in coming traffic and allows all out going traffic except any traffic allowed and blocked in the exception list
  - **Low:** allows all in coming and out going traffic except any traffic blocked in the exception list
5. Click the check boxes next to the Enterprise Client Firewall functions to enable:
  - **Enable Firewall**
  - **Enable Intrusion Detection System**
  - **Enable Alert Message:** the Client Alert Message for Enterprise Client Firewall appears when the firewall blocks an out going packet (see [Modifying Client Alert Messages](#) on page 5-2 for information on changing the Enterprise Client Firewall alert message)
6. Under **Exception**, select the check boxes next to the Enterprise Client Firewall exceptions to include in this policy.



7. Click **Save** to save the policy.

## Configuring exceptions

The Enterprise Client Firewall exception list contains entries you can configure to allow or block different kinds of network traffic based on client computer port number(s) and IP address(es). Exceptions are applied to policies. After creating an exception, edit the policies to which the exception applies.

Decide which type of exception you want to use. There are two types of exceptions:

- **Restrictive** – these exceptions block only specified types of network traffic and are applied to policies that allow all network traffic. An example use of a restrictive exception is blocking client ports that are commonly vulnerable to attack, such as a ports that Trojans often use (see the OfficeScan help for information on Trojan ports).
- **Permissive** – these exceptions allow only specified types of network traffic and are applied 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 (see the OfficeScan help for information on the Trusted port).

### To add an entry:

1. On the sidebar, click **Enterprise Client Firewall > Policy List**. The **Policy List** screen appears.
2. Click **Edit exception template**. The **Exception List** screen appears showing a list of existing exceptions.
3. Click **Add**.
4. Type a name for the exception.
5. Next to **Action**, click one of the following:
  - **Allow all network traffic**
  - **Deny all network traffic**
6. Next to **Direction**, select **Inbound** or **Outbound** to select the type of traffic to which to apply the exception settings.
7. Select the type of network protocol from the **Protocol** list:

- **All**
  - **TCP/UDP (default)**
  - **TCP**
  - **UDP**
  - **ICMP**
8. Click one of the following to specify client ports:
- **All ports** (default)
  - **Range:** type a range of ports
  - **Specified:** specify individual ports. Use a comma "," to separate port numbers.
9. Under **Computers**, select client IP addresses to include in the exception. For example, if you select **Deny all network traffic (Inbound and Outbound)** and type the IP address for single computer on the network, then any client that has this exception in its policy will not be able to send or receive data to or from that IP address.
- Click one of the following:
- **All IP addresses** (default)
  - **Single IP:** type the host name or IP address of a client. To resolve the client host name to an IP address, click **Resolve**.
  - **IP range:** type a range of IP addresses
  - **Subnet mask:** type an IP address and subnet mask
10. Click **Save**.

**To delete an entry:**

1. On the sidebar, click **Enterprise Client Firewall > Policy List**. The **Policy List** screen appears.
2. Click **Edit exception template**. The **Exception List** screen appears showing a list of existing exceptions.
3. Select the check box(es) next to the exception(s) to delete.
4. Click **Delete**. OfficeScan removes the exception(s) from the list.

**To change the order of exceptions in the list:**

1. On the sidebar, click **Enterprise Client Firewall > Policy List**. The **Policy List** screen appears.

2. Click **Edit exception template**. The **Exception List** screen appears showing a list of existing exceptions.
3. Select the check box next to the exception to move.
4. Click **Move up** or **Move down**. The ID number of the exception changes to reflect the new position.

**To save the exception list settings:**

Click one of the following save options:

- **Save as template:** save the exception list with current entries. Existing policies that use exceptions you modified are not updated, but the template will be automatically applied to policies you create in the future.
- **Save and apply to all existing policies:** save the exception list with current entries. Existing policies that use exceptions you modified are updated, and the template will be automatically applied to policies you create in the future.

## Configuring profiles

The **Enterprise Client Firewall Profile List** provides a summary of all profiles, including profile name, the policy each profile uses, and the current profile status. Manage the profile list from this screen. Also select profiles and deploy them to OfficeScan clients to update their Enterprise Client Firewall settings.

OfficeScan applies Enterprise Client Firewall profiles to clients in the order in which the profiles appear in the list. For example, if a client matches the first profile, OfficeScan applies the actions configured for that profile to the client. The other profiles which are also configured for that client are ignored.

---

**Tip:** Put the most exclusive policies at the top of the list. For example, put policies you create for a single client at the top, followed by those for a range of clients, a network domain, and finally all clients.

---

**To add or edit a profile:**

1. On the sidebar, click **Enterprise Client Firewall > Profile List**. The **Profile List** screen appears.
2. To create a new profile, click **Add**.

To edit an existing profile, select the check box next to the corresponding profile to edit and click **Edit**.

3. Click **Enable this profile** to allow OfficeScan server to deploy this profile to OfficeScan clients.
4. Type a name to identify the profile and an optional description.
5. From the list box next to **Use the following policy**, select an existing policy for this profile to use.
6. Select the clients to which OfficeScan applies the policy by using the following:
  - **IP address:** the IP address(es) of the client(s). Click one of the following:
    - **Single IP:** Type a client IP address.
    - **Range:** Type a range of IP addresses in the **From** and **To** text fields.
    - **Subnet:** Type an IP address of the subnet and the subnet mask.  
OfficeScan uses these to calculate the network address.
  - **Domain:** the domain name of the client(s). Click **Go to client console** to select clients from the domain tree.
  - **Machine name:** the name of the client(s). Click **Go to client console** to select clients from the domain tree.
  - **Platform:** the operating system of the client(s). Select from the following:
    - Windows Server (NT/2000/Server 2003)
    - Windows Workstation (NT/2000/XP)
  - **Logon Name:** the ID(s) of the users logged on as client(s). If typing multiple entries, insert a comma "," between IDs.
  - **Client status:** if the OfficeScan Client application is online or offline. Click one of the following:
    - Online
    - Offline
7. Under **User Privilege**, select from among the following options:
  - **Allow user to change security level:** clients can change the Enterprise Client Firewall policy security level
  - **Allow user to edit traffic exception list:** clients can edit a configurable list of exceptions to allow specified types of traffic
8. Click **Save**.

**To change the order of profiles in the list:**

1. On the sidebar, click **Enterprise Client Firewall > Profile List**. The **Profile List** screen appears.
2. Select the check box next to the profile to move.
3. Click **Move up** or **Move down**.

**To deploy profiles to clients:**

1. On the sidebar, click **Enterprise Client Firewall > Profile List**. The **Profile List** screen appears.
2. Select the check box(es) next to the profile(s) to deploy.
3. To overwrite the current security level and the exception list of the client(s), select the **Overwrite client security level/exception list** check box.

---

**Note:** If you gave clients the privilege to modify firewall settings, users may have modified their security level and/or exception list (see See [Granting Privileges to Clients](#) on page 4-43).

Selecting the **Overwrite client security level/exception list** check box ensures that the security level and exception list you configured for the policy will be applied to all selected clients.

---

4. Click **Deploy to clients**.

---

**Note:** When you click Deploy to clients, OfficeScan deploys all profiles on the Profile List to the clients that match the criteria set in the profile(s).

---

## Configuring Firewall Outbreak Monitor

An excessive number of log entries may signal the possibility of a virus outbreak. Enable Enterprise Client Firewall Outbreak Monitor to have OfficeScan declare a firewall outbreak alert if log counts exceed certain thresholds. Also enable and configure an alert message to have OfficeScan automatically notify relevant parties of the potential outbreak.

**To enable Firewall Outbreak Monitor:**

1. On the sidebar, click **Enterprise Client Firewall > Firewall Outbreak Monitor**.
2. Select the **Enable Firewall Outbreak Monitor** check box.
3. Under **Alert Criteria for Firewall Outbreak Monitor**, configure the threshold of log records at which an alert is triggered for the following types of logs:
  - **IDS logs**
  - **Enterprise Client Firewall logs**
  - **Network virus logs**
4. Type the number of hours within which OfficeScan must detect the specified number of log records.
5. To enable and configure an optional alert message do the following:
  - a. Select the **Send a notification via email if alert criteria are met** check box.
  - b. Under **Alert Message Settings**, type the following:
    - **SMTP:** the Simple Mail Transfer Protocol (SMTP) mail server host name or IP address
    - **Port Number:** the port number of the SMTP server (default 25)
    - **To:** the recipient email addresses. Type a semicolon ";" to separate addresses.
    - **From:** the sender name or email address (default is "OfficeScan")
    - **Subject:** type a subject (default is "Firewall Outbreak Monitor Alert")
    - **Message:** type a message (default message includes the alerts triggered and the total log counts in the number of hours specified above)
6. Click **Save**.

## Disabling the Firewall

To disable Enterprise Client Firewall on client machines from the OfficeScan Web console, create a new policy that does not enable the firewall and apply the policy to clients.

**To disable the firewall:**

1. On the sidebar, click **Enterprise Client Firewall > Policy List**. The **Policy List** screen appears.
2. To create a new policy, click **Add**.
3. Type a name for the policy.
4. Clear the **Enable Firewall** check box.
5. Click **Save** to save the policy.
6. On the sidebar, click **Enterprise Client Firewall > Profile List**. The **Profile List** screen appears.
7. To create a new profile, click **Add**.
8. Click **Enable this profile** to allow OfficeScan server to deploy this profile to OfficeScan clients.
9. Type a name to identify the profile and an optional description.
10. From the list box next to **Use the following policy**, select the policy you created.
11. Select the clients on which you want to disable the firewall.
12. Click **Save**.
13. Click **Deploy to Clients** to deploy the profile, which disables the firewall.

# Viewing and Interpreting Logs

This chapter describes how to use OfficeScan logs to monitor your system and analyze your protection.

The topics discussed in this chapter include:

- *Viewing and Interpreting Logs* on page 8-2
- *Viewing virus logs* on page 8-2
- *Deleting virus logs* on page 8-3
- *Viewing server update logs* on page 8-4
- *Viewing client update logs* on page 8-4
- *Viewing system event logs* on page 8-5
- *Viewing verify connection logs* on page 8-6
- *Viewing Enterprise Client Firewall logs* on page 8-6



## Viewing and Interpreting Logs

OfficeScan keeps comprehensive logs about virus incidents, events, and updates. Use these logs to assess your organization's virus protection policies and to identify clients that are at a higher risk of infection. Also use these logs to check client-server connection and verify that updates were deployed successfully.

---

**Note:** Use spreadsheet applications, such as Microsoft Excel, to view CSV log files.

---

OfficeScan maintains the following logs:

- Virus Logs
- Client Update Logs
- Server Update Logs
- System Event Logs
- Verify Connection Logs
- Enterprise Client Firewall Logs

### Viewing virus logs

OfficeScan records log entries for viruses detected on your clients. Virus logs include the following information:

- **Date and time:** the time OfficeScan created the log entry
- **Computer name:** the name of the OfficeScan client
- **Virus name:** the virus(es) OfficeScan detected
- **Infection source:** the client from where the virus originated
- **Infected file:** file(s) that the virus(es) infected
- **Scan type:** the type of scan OfficeScan performed when it detected the virus (Manual, Real-time, Scheduled)
- **Scan result:** what OfficeScan did after the scan

**To view virus logs:**

1. On the sidebar, click **Logs > Virus Logs**. The **Clients** screen appears.

2. Click domain or client icons in the tree to view corresponding virus logs. To select all domains and clients, click the root icon.
3. On the sidebar, click **OfficeScan clients**. The **View Virus Logs** screen appears.
4. Under **Time**, click **Select a time period** and make a selection from the list or click **Specify a range** and enter a range of dates.
5. Under **Scan Types**, select the types of logs to display by selecting the corresponding check boxes.
6. Under **Sort by**, click an option to specify how to classify the logs. The options are:
  - Date and time
  - Computer name
  - Virus name
  - Scan type
  - Scan result
7. To view the log, click **View logs**.
8. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

## Deleting virus logs

To conserve disk space on the server, delete virus logs manually.

### To delete virus logs:

1. On the sidebar, click **Logs > Virus Logs**. The **Clients** screen appears.
2. Click domain or client icons in the tree to view corresponding virus logs. To select all domains and clients, click the root icon.
3. On the sidebar, click **Delete Logs**. The **Delete Logs** screen appears.
4. Under **Select log types**, select the types of logs (based on the type of scan that OfficeScan performed) to delete.
5. Under **Deletion**, specify the logs to delete. The options are:
  - **Delete all log content in the selected log types**
  - **Delete logs older than { } days**

If you click **Delete logs older than { } days**, type a value for the number of days. For example, if you type '20', OfficeScan deletes logs that you created 20 days ago and earlier.

6. Click **Apply** to delete the logs.

## Viewing server update logs

OfficeScan keeps logs for server updates. This helps you keep track of the server's update history and the update methods used.

### To view server update logs:

1. Click **Logs > Update Logs > Server Update** on the sidebar. The **Server Update Logs** screen appears, showing the following information:
  - Time and date of update
  - Result of the update
  - Update component
  - Update method
2. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

## Viewing client update logs

OfficeScan also provides client update logs. Use these logs to verify update deployment.

### To view client update logs:

1. Click **Logs > Update Logs > Client Update** on the sidebar. The **Client Update Logs** screen appears, showing the following information:
  - Date and time of update
  - Update components
  - Progress
  - Details
2. Select the number of results to view on each page from the **Display results per page** list.

3. Click on the column headings **Time/Date** or **Update Components** to sort the table.

**To view how many clients were updated for a particular update deployment:**

1. Click **View** under the **Progress** column. The **Client Update Progress** screen appears.
2. From this screen, view the number of clients updated for every 15-minute interval and the total number of clients updated.

**To view which clients were updated for a particular update deployment:**

1. Click **View** under the **Detail** column. The **Client Update Detail** screen appears, showing the names of clients that OfficeScan updated and the update details.
2. Sort the table by clicking on column headings: **Computer name**, **Notification sent**, **Notification received**, **Update completed**, or **Update Source**.
3. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

## Viewing system event logs

OfficeScan also records events related to the server program, such as shutdown and startup. Use these logs to verify that the server is running smoothly and that the services necessary for OfficeScan to work on your network are running.

**To view system event logs:**

1. Click **Logs > System Event Logs** on the sidebar. The **System Event Logs** screen appears, showing recent events on the server.
2. Select the number of results to view on each page from the **Display results per page** list.
3. Sort the table by clicking on column headings: **Time/Date** or **Computer Name**, or **Event Description**.
4. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

## Viewing verify connection logs

OfficeScan keeps Verify Connection logs to allow you to determine the connection status between the server and clients.


### To view Verify Connection logs:

1. Click **Logs > Verify Connection Logs** on the sidebar. The **Verify Connection Log** screen appears, showing log time/dates, clients' computer names, domains, IP addresses, and connection status.
2. Select the number of results you want to view on each page from the **Display results per page** list.
3. You can sort the table by clicking on column headings: **Time/Date**, **Computer Name**, **Domain**, **IP Address**, or **Status**.
4. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. A confirmation screen appears.
  - Click **Open** to view the file in your spreadsheet application without saving it.
  - Click **Save** and then specify the location to which you want to save the CSV file.
5. Click **Save**.

## Viewing Enterprise Client Firewall logs

OfficeScan clients that have Enterprise Client Firewall enabled store firewall events in a log on the client computer. View these logs to analyze how Enterprise Client Firewall is protecting your clients from attacks. To view the latest client Enterprise Client Firewall logs, you must first notify clients to send their logs to the OfficeScan server.

### To notify clients to send Enterprise Client Firewall logs to the OfficeScan server:

1. Click **Logs > Firewall Logs** on the sidebar. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to send Enterprise Client Firewall Logs by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon . You can also search for clients by selected criteria, such as computer name, IP address, virus pattern file version, etc. You can also change the client tree view.

3. On the sidebar click **Client Notification**. The **Client Notification for Firewall Logs** screen appears.
4. Click **Apply**.

**To view Enterprise Client Firewall logs:**

1. Click **Logs > Firewall Logs > View Logs** on the sidebar. The **Enterprise Client Firewall Logs** screen appears, showing the following information:
  - Time and date of the log entry
  - The computer that logged the entry
  - The remote host
  - The local host
  - The protocol
  - A description of the log entry
  - The destination port
  - Details of the log entry
2. Select the number of results you want to view on each page from the **Display results per page** list.
3. You can sort the table by clicking on any of the column headings.
4. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. A confirmation screen appears.
  - Click **Open** to view the file in your spreadsheet application without saving it.
  - Click **Save** and then specify the location to which you want to save the CSV file.

## Managing Logs

Manage logs by performing scheduled log maintenance to keep their size from occupying too much space on your hard disk. You can configure OfficeScan to automatically delete the logs based on a schedule.

**To perform scheduled log maintenance:**

1. On the sidebar, click **Logs > Log Maintenance**. The **Log Maintenance** screen appears.

2. Select the **Enable Scheduled Deletion of Logs** check box to perform scheduled maintenance.
3. Under **Log type(s) to delete**, select the log types to delete automatically. The options are:
4. Under **Log entry deletion criteria**, specify which logs to delete. The options are:
  - **Delete all log content in the selected log types**
  - **Delete logs older than { } days**

If you click **Delete logs older than { } days**, type a value in the text box.

5. Under **Schedule**, specify a frequency when to perform scheduled log maintenance:
  - **Days**
  - **Weekly, every { }**
  - **Monthly, on day { }**

If you click **Weekly**, select a day from the list.

If you click **Monthly**, select a date from the list.

Regardless of the frequency you set, specify when to perform scheduled log maintenance in **Start time**.

6. Click **Save** to save your settings.

# Troubleshooting and Technical Support

This chapter describes how to troubleshoot problems that may arise with OfficeScan.

In this chapter, you will learn about potential issues regarding the following:

- *Client-server Communication* on page 9-2
- *Incorrect Number of Clients on the Web Console* on page 9-2
- *Incorrect Client Status on the Web Console* on page 9-2
- *Incorrect Component Versions* on page 9-3
- *Unsuccessful Installation from Web page or Remote Install* on page 9-4
- *Client Icon Does Not Appear on Web Console After Installation* on page 9-5
- *Issues During Migration from Third-party Antivirus Software* on page 9-6

Contact information

- *Contacting Trend Micro* on page 9-10
- *Contacting Technical Support* on page 9-11
- *The Trend Micro Knowledge Base* on page 9-12
- *About TrendLabsSM* on page 9-13



## Client-server Communication

This section explains some key points about OfficeScan client-server communication. Understanding the client-server communication will help you more quickly troubleshoot problems and take advantage of the Web console's central management capabilities.

The actual status and the displayed status are not synchronized primarily because the server database records do not match with the values in the client registry.

## Incorrect Number of Clients on the Web Console

You may see that the number of clients reflected on the Web console is incorrect.

This happens if you retain client records in the database after client program removal. For example, if client-server communication is lost while removing the client, the server does not receive notification about the client removal. The server retains client information in the database and still shows the client icon on the console. When you reinstall the client, the server creates a new record in the database and displays a new icon on the console.

This error can occur in steps 4 and 5 of the client-server communication flow (see [Client-server Communication](#) on page 9-2).


Use the Verify Connection feature to check for duplicate client records. See [Verifying Client-Server Connection](#) on page 4-26 for more information.

## Incorrect Client Status on the Web Console

You may see that OfficeScan does not synchronize the actual client status and the client status on the console. This happens if the client is unable to launch the client program or if, at startup, the client loses connection to the server before it could report its status.

This error can occur in steps 4 and 5 of the client-server communication flow (see [Client-server Communication](#) on page 9-2).

**To resolve this, try the following:**

- Use the OfficeScan Verify Connection feature of the server to check if client-server communication exists. See [Verifying Client-Server Connection](#) on page 4-26 for more information. If the server can communicate with the client, it will display the client status as **Online**.
- Check if the client computer is off or if the client program has been unloaded, removed, or stopped. These conditions will cause the server to display the client status as **Off**. If there was an error during any of these processes, it is possible that the client was not able to inform the server that it is shutting down or that it is being unloaded, removed, or stopped. As a result, the server did not know to change the status of the client from **On** to **Off**. On the client, check if the OfficeScan icon appears as . If it does, the client has switched to roaming mode.

---

**Note:** If this does not help you find the real cause of the issue, use ActiveSupport to collect `Ofcdebug.log` from both the server and client. Then contact Trend Micro technical support. See the OfficeScan client help for information on running Active Support.

---

## Incorrect Component Versions

OfficeScan may incorrectly display the version number of the client components. This happens when the client is unable to write its status information to the registry and send this information to the server.

For example, you updated the pattern file of a client from 411 to version 413. However, after updating, the console still shows 411. It is possible that you updated the client but the client was unable to write its updated information to the registry.

**To resolve the incorrect display problem, try the following:**

- Use ping or telnet to verify that the client is on the network
- Use the OfficeScan Verify Connection feature of the server to check if client-server communication exists. If the server can communicate with the client, it will display the client status as **Online** (see [Verifying Client-Server Connection](#) on page 4-26).

- If you have limited bandwidth, check for connection timeouts between the server and the client
- If you are using a proxy server for client-server communication, check that the proxy settings are correct
- Open a Web browser on the client, type `http://{Server name}:{Server port}/officeScan/cgi/cgionstart.exe` in the address text box, and then press ENTER. (If using SSL, type `http://{Server name}:{Server port}/officeScan/cgi/cgionstart.exe`). If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client. In this case, please contact Trend Micro support.
- Check if the user has local administrator rights to the client computer to write to the registry. OfficeScan writes client information, including the version of the pattern file, scan engine, and program, to the registry.
- Check if the user modified files or registry values but forgot to restart the `Tmlisten.exe` service on the client for Windows NT/2000XP/Server 2003 or `Pccwin97.exe` on the client for Windows 95/98/Me/98 SE.

---

**Note:** If this does not help you find the real cause of the issue, use ActiveSupport to collect `Ofcdebug.log` from both the server and client. Then contact Trend Micro technical support. See the OfficeScan client help for information on running Active Support.

---

## Unsuccessful Installation from Web page or Remote Install

**If users report that they cannot install from the internal Web page or if installation with Remote Install is unsuccessful, try the following:**

- Verify that client-server communication exists by using ping and telnet
- Verify that you have administrator privileges to the target computer where you want to install the client
- Check if TCP/IP on the client is enabled and properly configured
- Check if the target computer meets the minimum system requirements

- Check if any file has been locked
- If you have limited bandwidth, check if it causes connection timeout between the server and the client
- If you are using a proxy server for client-server communication, check if the proxy settings are configured correctly
- Open a Web browser on the client, type `http://{Server name}:{server port} /officeScan/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client.

## Client Icon Does Not Appear on Web Console After Installation

You may discover that the client icon does not appear on the console after you install the client. This happens when the client is unable to send its status to the server.

### To resolve this, do the following:

- Verify that client-server communication exists by using ping and telnet
- If you have limited bandwidth, check if it causes connection timeout between the server and the client
- Check if the \PCCSRV folder on the server has shared privileges and if all users have been granted full control privileges
- Verify the OfficeScan server proxy settings to ensure they are correct
- Open a Web browser on the client, type `http://{OfficeScan_Server_Name}:{port number}/officeScan/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client.

---

**Note:** If this does not help you find the real cause of the issue, use ActiveSupport to collect `Ofcdebug.log` from both the server and client. Then contact Trend

Micro technical support. See the OfficeScan client help for information on running Active Support.

---

## Issues During Migration from Third-party Antivirus Software

This section discusses some issues you may encounter when migrating from third-party antivirus software.

### Client migration

The setup program for the OfficeScan client utilizes the third-party software's uninstallation program to automatically remove it from your users' system and replace it with the OfficeScan client. If automatic uninstallation is unsuccessful, users get the following message:

```
Uninstallation failed.
```

There are several possible causes for this error:

- The third-party software's version number or product key is inconsistent
- The third-party software's uninstallation program is not working
- Certain files for the third-party software are either missing or corrupted
- The registry key for the third-party software cannot be cleaned
- The third-party software has no uninstallation program

There are also several possible solutions for this error:

- Manually remove the third-party software
- Stop the service for the third-party software
- Unload the service or process for the third-party software

#### **To manually remove the third-party software:**

- If the third-party software is registered to the Add/Remove Programs
  - a. Open the Control Panel.
  - b. Double-click **Add/Remove Programs**.

- c. Select the third-party software from the list of installed programs.
  - d. Click **Remove**.
- If the third-party software is not registered to the Add/Remove Programs
  - a. Open the Windows registry.
  - b. Go to  
`HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Uninstall.`
  - c. Locate the third-party software and run the uninstall string value.
  - d. If the third-party software's setup program is in MSI format:
    - Locate the product number
    - Verify the product number
    - Run the uninstall string

---

**Note:** Some product uninstallation keys are in the Product Key folder.

---

#### **To modify the service for the third-party software**

1. Restart the computer in safe mode.
2. Modify the service startup from automatic to manual.
3. Restart the system again.
4. Manually remove the third-party software.

#### **To unload the service or process for the third-party software**

---

**WARNING!** *This procedure may cause undesirable effects to your computer if performed incorrectly. Trend Micro highly recommends backing up your system first.*

---

1. Unload the service for the third-party software.
2. Open the Windows registry, then locate and delete the product key.
3. Locate and delete the run or run service key.

Verify that the service registry key in

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services has been removed.

## Client Connection Time-out Occurs Frequently

If you have deployed a large number of clients to the network, it is possible that you may encounter frequent connection time-outs between the client and server. This issue is caused by a restriction on the maximum number of simultaneous TCP/IP connections between hosts set by Microsoft Windows.

**To prevent this behavior, do one of the following:**

- Increase the port range used for anonymous ports.
  - a. Open the Windows Registry Editor (Regedit.exe).
  - b. Locate the following path in the registry:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
  - c. Click **Edit > New > DWord value**.
  - d. Type **MaxUserPort** in the **Name** column.
  - e. Click **Edit > Modify**.
  - f. Under **Base**, click **Decimal**.
  - g. Type a value in the **Value Data** field. The default value is 5000. Trend Micro recommends using a value higher than the total number of OfficeScan clients installed on your network. The acceptable range of values is 1 to 65534.
- Decrease the default TCP timeout value.
  - a. Open the Windows Registry Editor (Regedit.exe).
  - b. Locate the following path key in the registry:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
  - c. Click **Edit > New > DWord value**.
  - d. Type **TcpTimedWaitDelay** in the **Name** column.

- e. Click **Edit > Modify**.
- f. Under **Base**, click **Decimal**.
- g. Type a value in the **Value Data** field. The default value is 240. Trend Micro recommends using a value lower than the default. The acceptable range of values is 30 to 300.

---

**Note:** More information about the registry keys MaxUserPort and TcpTimedWaitDelay can be found by performing a search of the Microsoft knowledge base at:  
<http://support.microsoft.com/>

---



## Contacting Trend Micro

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

<http://www.trendmicro.com/en/about/contact/overview.htm>

---

**Note:** The information on this Web site is subject to change without notice.

---

## The Trend Micro Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

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

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of threats expected to trigger in the current week, and describes the 10 most prevalent threats around the globe for the current week
- View a Virus Map of the top 10 threats around the globe
- Consult the Virus Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
  - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other threats
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security threat terminology
- Download comprehensive industry white papers

- Subscribe to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Web masters
- Read about TrendLabs<sup>SM</sup>, Trend Micro's global antivirus research and support center

## Known Issues

Known issues are features in OfficeScan software that may temporarily require a work around. Known issues are typically documented in the Readme document you received with your product. Readme's for Trend Micro products can also be found in the Trend Micro Update Center:

<http://www.trendmicro.com/download/>

Known issues can be found in the technical support Knowledge Base:

<http://kb.trendmicro.com/solutions/>

Trend Micro recommends that you always check the Readme text for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

## Contacting Technical Support

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

You can contact Trend Micro via fax, phone, and email, or visit us at:

<http://www.trendmicro.com>

## Speeding Up Your Support Call

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

- Microsoft Windows and Service Pack versions

- Microsoft Exchange server and Microsoft Exchange Service Pack versions
- Number of mailboxes
- Network type
- Computer brand, model, and any additional hardware connected to your machine
- Amount of memory and free hard disk space on your machine
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

## The Trend Micro Knowledge Base

Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in Knowledge Base are product FAQs, important tips, preventive antivirus advice, and regional contact information for support and sales.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

<http://kb.trendmicro.com/solutions/>

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

## Sending Suspicious Files to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

<http://subwiz.trendmicro.com/SubWiz>

Click **Submit a suspicious file/undetected virus**. You are prompted to supply the following information:

- **Email** – Your email address where you would like to receive a response from the antivirus team.
- **Product** – The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Number of Infected Seats** – The number of users in your organization that are infected.
- **Upload File** – Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word “virus” as the password—then select the protected zip file in the **Upload File** field.
- **Description** – Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will “dissect” the file to identify and characterize any threats it may contain and return the cleaned file to you, usually within 48 hours.

---

**Note:** Submissions made via the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

---

When you click **Next**, an acknowledgement screen displays. This screen also displays a case number for the problem you submitted. Make note of the case number for tracking purposes.

If you prefer to communicate by email message, send a query to the following address:

[virusresponse@trendmicro.com](mailto:virusresponse@trendmicro.com)

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAY, or 877-873-6328

## About TrendLabs<sup>SM</sup>

TrendLabs is Trend Micro’s global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The “virus doctors” at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Irvine, CA, to mitigate virus outbreaks and provide urgent support.

TrendLabs’ modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

## Using OfficeScan Tools

OfficeScan includes a set of tools that can help you easily accomplish various OfficeScan tasks, including server configuration and client management.

These tools are classified into two categories:

- **Administrative tools** – developed to help configure the server and manage clients (see *Administrative Tools* on page A-2)
- **Client tools** – developed to help enhance the performance of the client program (see *Client Tools* on page A-10)

Refer to Table 1-1 for a complete list of tools included in this version of OfficeScan

**Note:** Some tools available in previous versions of OfficeScan are not available in this version. If you require these tools, contact technical support. See *Integrated Tools* on page A-15 for a list of tools whose functions have been integrated into this version of OfficeScan.

Administrative Tools	Client Tools
Database Backup	Client Packager
Login Script Setup	Image Setup Utility
Vulnerability Scanner	Restore Encrypted Files
Server Tuner	Client Mover I
	Touch Tool

**TABLE 1-1. OfficeScan tools**

**Note:** You cannot run these tools from the OfficeScan Web console.

## Administrative Tools

This section contains information about the following OfficeScan administrative tools:

- Database backup
- Login Script Setup
- Vulnerability Scanner
- Server Tuner


## Database backup

The database on the server contains all OfficeScan settings, including scan settings and privileges. Backing up the OfficeScan database is a routine task that Trend Micro recommends you perform. If the server database becomes corrupted, you can easily restore it if you have a stored copy of the database.

Database Backup requires the following files:

- Main file: `DBBackup.exe`
- Required DLL file: `svcmgr.dll`

### To back up a database:

1. On the server, open Windows Explorer and go to the `\PCCSRV\Admin\Utility\DBBackup` folder of OfficeScan.
2. Double-click `DBBackup.exe` to start Database Backup. The tool's icon appears in the Windows system tray.
3. Right-click the Database Backup icon in the system tray. A pop-up menu appears.
4. Click **DB Backup Settings**. The Database Backup console appears.
5. In **Backup path**, click  to browse for the folder where you want to store the backup. Trend Micro recommends creating the backup folder on another drive or folder other than the OfficeScan folder.

---

**Note:** You cannot store the backup on mapped drives. Use the local drives on the computer you are running Database Backup.

---

6. Under **Backup Schedule**, select a frequency with which Database Backup will run:
  - **No Action** - select if you do not want to back up the database
  - **Daily** - select to back up the database daily. Select a time when Database Backup will run from the **Time** lists. Use the first list box to specify the hour and the second to specify the minute. Database Backup uses the 24-hour format. For example, to back up the database at 8:35 pm, select 20 in the first list box and then select 35 in the second list box.



- **Weekly** - select to back up the database once every week. Select the day and time when to Database Backup will run from the **Day of the week** box and **Time** lists, respectively.
- **Monthly** - select to back up the database once every month. Select the date and time when to Database Backup will run from the **Day of the month** box and **Time** lists, respectively.

7. Click **Apply** to save your settings.

## Login Script Setup

With Login Script Setup, you can automate the installation of the OfficeScan client to unprotected computers when they log on to the network. Login Script Setup adds a program called autopcc.exe to the server login script. The program `autopcc.exe` performs the following functions:

- Determines the operating system of the unprotected computer and installs the appropriate version of the OfficeScan client
- Updates the virus pattern file and program files

For instructions on installing clients, see [Installing with Login Script Setup](#) on page 3-23.

## Vulnerability Scanner

Use Vulnerability Scanner to detect installed antivirus solutions and to search for unprotected computers on your network. To determine if computers are protected, Vulnerability Scanner pings ports that are normally used by antivirus solutions. Vulnerability Scanner can perform the following functions:

- Perform a DHCP scan to monitor the network for DHCP requests so that when computers first log on to the network, Vulnerability Scan can determine their status
- Ping computers on your network to check their status and retrieve their computer names, platform versions, and descriptions
- Determine the antivirus solutions installed on the network. It can detect Trend Micro products (including OfficeScan, ServerProtect for Windows NT and Linux, ScanMail for Microsoft Exchange, InterScan Messaging Security Suite, and PortalProtect) and third-party antivirus solutions (including Norton AntiVirus Corporate Edition v7.5 and v7.6, and McAfee VirusScan ePolicy Orchestrator).

- Display the server name and the version of the pattern file, scan engine and program for OfficeScan and ServerProtect for Windows NT
- Send scan results via email
- Run in silent mode (command prompt mode)
- Install OfficeScan client remotely on computers running Windows NT/2000/XP/(Professional only)/Server 2003

You can also automate Vulnerability Scanner by creating scheduled tasks. For information on how to automate Vulnerability Scanner, see the TMVS online help.

To run Vulnerability Scanner on a computer other than the server, copy the TMVS folder from the \PCCSRV\Admin\Utility folder of the server to the computer.

---

**Note:** You can use Vulnerability Scanner on machines running Windows 2000 or Server 2003; however, the machines cannot be running Terminal Server.

You cannot install OfficeScan clients with Vulnerability Scanner if an OfficeScan server installation is present on the same machine.

---

#### To configure Vulnerability Scanner:

1. In the drive where you installed OfficeScan server, open the following directories: **OfficeScan > PCCSRV > Admin > Utility > TMVS**. Double-click **TMVS.exe**. The Vulnerability Scanner console appears.
2. Click **Settings**. The **Settings** screen appears.
3. Under **Product Query**, select the products that you want to check for on your network.  
If you have Trend Micro InterScan and Norton AntiVirus Corporate Edition installed on your network, click **Settings** next to the product name to verify the port number that Vulnerability Scanner will check.
4. Under **Description Retrieval Settings**, click the retrieval method that you want to use. Normal retrieval is more accurate, but it takes longer to complete.  
If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting the **Retrieve computer descriptions when available** check box.

5. To automatically send the results to yourself or other administrators, under **Alert Settings** select the **Email results to the system administrator** check box, and then, click **Configure** to specify your email settings.
  - In **To**, type the email address of the recipient.
  - In **From**, type your email address. This will let the recipient know who sent the message, if you are not only sending it to yourself.
  - In **SMTP server**, type the address of your SMTP server. For example, you can type smtp.company.com. The SMTP server information is required.
  - In **Subject**, type a new subject for the message or accept the default subject.Click **OK** to save your settings.
6. To display an alert on unprotected computers, select the **Display alert on unprotected computers** check box. Then, click **Customize** to set the alert message. The **Alert Message** screen appears. You can type a new alert message or accept the default message. Click **OK**.
7. To save the results as a comma-separated value (CSV) data file, select the **Automatically save the results to a CSV file** check box. By default, CSV data files are saved to the TMVS folder. If you want to change the default CSV folder, click **Browse**. The **Browse for folder** screen appears. Browse for a target folder on your computer or on the network and then click **OK**.
8. You can enable Vulnerability Scanner to ping computers on the network to get their status. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout** text boxes.
9. To remotely install OfficeScan Client and send a log to the server, type the OfficeScan server name and port number. If you want to automatically remotely install OfficeScan client, select the **Auto-install OfficeScan Client for unprotected computer** check box.
10. Click **Install Account** to configure the account. The **Account Information** screen appears. Type user name and password that permits installation. Click **OK**.
11. If you want to send log to server, select the **Report log to OfficeScan server** check box.

12. Click **OK** to save your settings. The **Trend Micro Vulnerability Scanner** console appears.

**To run a manual vulnerability scan on a range of IP addresses:**

1. Under **IP Range to Check**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers. Note that the Vulnerability Scanner only supports class B IP addresses.
2. Click **Start** to begin checking the computers on your network. The results are displayed in the **Results** table.

---

**Note:** You can also run Vulnerability Scanner at the command prompt. For more information, see the Vulnerability Scanner online help.

---

**To run Vulnerability Scanner on computers requesting IP addresses from a DHCP server:**

1. Click the **DHCP Scan** tab in the **Results** box. The **DHCP Start** button appears.
2. Click **DHCP Start**. Vulnerability scanner begins listening for DHCP requests and performing vulnerability checks on computers as they log on to the network.

**To create scheduled tasks**

1. Under **Scheduled Tasks**, click **Add/Edit**. The **Scheduled Task** screen appears.
2. Under **Task Name**, type a name for the task you are creating.
3. Under **IP Address Range**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers.
4. Under **Task Schedule**, click a frequency for the task you are creating. You can set the task to run **Daily**, **Weekly**, or **Monthly**. If you click **Weekly**, you must select a day from the list. If you click **Monthly**, you must select a date from the list.
5. In the **Start time** lists, type or select the time when the task will run. Use the 24-hour clock format.
6. Under **Settings**, click **Use current settings** if you want to use your existing settings, or click **Modify settings**.

If you click **Modify settings**, click **Settings** to change the configuration. For information on how to configure your settings, refer to steps 4 and 5 in the "To configure Vulnerability Scanner:" procedure.

7. Click **OK** to save your settings. The task you have created appears under **Scheduled Tasks**.

## Other settings

To configure the following settings you need to modify `TMVS.ini`:

- **Debug** – enable or disable the debug log
- **EchoNum** – set the number of computers that Vulnerability Scanner will simultaneously ping
- **ThreadNumManual** – set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software
- **ThreadNumSchedule** – set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running scheduled tasks
- **ThreadNumSilent** – set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running the tool at the command prompt

### To modify these settings:

1. Open the `TMVS` folder and locate the `TMVS.ini` file.
2. Open `TMVS.ini` using Notepad or any text editor.
3. To enable the debug log, change the value from `Debug=0` to `Debug=1`.
4. To set the number of computers that Vulnerability Scanner will simultaneously ping, change the value for `EchoNum`. Specify a value between 1 and 64.  
For example, type `EchoNum=60` if you want Vulnerability Scanner to ping 60 computers at the same time.
5. To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software, change the value for `ThreadNumManual`. Specify a value between 8 and 64.  
For example, type `ThreadNumManual=60` to simultaneously check 60 computers for antivirus software.

6. To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running scheduled tasks, change the value for `ThreadNumSchedule`. Specify a value between 8 and 64.

For example, type `ThreadNumSchedule=60` to simultaneously check 60 computers for antivirus software whenever Vulnerability Scanner runs a scheduled task.

7. To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running the tool at the command prompt, change the value for `ThreadNumSilent`. Specify a value between 8 and 64.

For example, type `ThreadNumSilent=60` to simultaneously check 60 computers for antivirus software whenever you run Vulnerability Scanner at the command prompt.

8. Save `TMVS.ini`.

## Server Tuner

Use Server Tuner to optimize the performance of your server.

---

**Note:** You can only use this tool in OfficeScan 3.54 and later versions.

---

Server Tuner requires the following file:

- Main file: `SvrTune.exe`

### To run Server Tuner:

1. On the server, open Windows Explorer and go to the `\PCCSRV\Admin\Utility\SvrTune` folder of OfficeScan.
2. Double-click `SvrTune.exe` to start Server Tuner. The **Server Tuner** console opens.
3. Under **Download**, modify the following settings based on your network traffic:
  - **Timeout for**
  - **Timeout for update**
  - **Retry count**

- **Retry interval**
- 4. Under **Buffer**, modify the following settings based on your network traffic:
  - **Event Buffer:** used in reporting client status
  - **Log Buffer:** used in reporting detected viruses
- 5. Under **Network Traffic Control**, modify the following settings based on your network traffic:
  - **Normal hours**
  - **Off-peak hours**
  - **Peak hours**

---

**Note:** If the number of clients reporting to your server is large, you may want to increase the buffer size. A higher buffer size, however, means higher memory utilization on the server.

---

## Client Tools

This section contains information about the following OfficeScan client tools:

- Client Packager
- Image Setup Utility
- Restore Encrypted Files
- Client Mover I
- Touch Tool

### Client Packager

Client Packager is a tool that can compress setup and update files into a self-extracting file to simplify delivery via email, CD-ROM, or similar media. It also includes an email function that can access your Microsoft Outlook address book and allow you to send the self-extracting file from within the tool's console.

To run Client Packager, double-click the file. OfficeScan clients that are installed using Client Packager report to the server where the setup package was created.

For instructions on how to use Client Packager, *Installing with Client Packager* on page 3-25.

## Image Setup Utility

Disk imaging technology allows you to create an image of an OfficeScan client and make clones of it to other computers on your network.

Each client installation needs to a Globally Unique Identifier (GUID), so that the server can identify your clients individually. Use an OfficeScan program called `imgsetup.exe` to create a different GUID for each clone.

Image Setup Utility helps you use hard drive imaging technology to deploy the OfficeScan client software.

For instructions on how to use Image Setup Utility, see *Installing from a client disk image* on page 3-29.

## Restore Encrypted Files

Whenever OfficeScan detects an infected file, it encrypts this file and stores it in the `Suspect` folder of the client, normally in `C:\Program Files\Trend Micro\OfficeScan Client\SUSPECT`. The infected file is encrypted to prevent users from opening it and spreading the virus to other files on the computer.

However, there may be some situations when you have to open the file even if you know it is infected. For example, an important document has been infected and you need to retrieve the information from the document, you will need to decrypt the infected file to retrieve your information.

You can use Restore Encrypted Files to decrypt infected files from which you want to open.

---

**Note:** To prevent OfficeScan from detecting the virus again when you use Restore Encrypted Files, exclude the folder to which you decrypt the file from Real-time Scan.

---

---

**WARNING!** Decrypting an infected file may spread the virus to other files.

---



Restore Encrypted Files requires the following files:

- Main file: `VSEncode.exe`
- Required DLL file: `Vsapi32.dll`

**To decrypt files in the Suspect folder:**

1. On the client where you want to decrypt an infected file, open Windows Explorer and go to the `\PCCSRV\Admin\Utility\VSEncrypt` folder of OfficeScan.
2. Copy the entire `VSEncrypt` folder to the client computer.

---

**Note:** Do not copy the `VSEncrypt` folder to the OfficeScan folder. The `Vsapi32.dll` file of Restore Encrypted Files will conflict with the original `Vsapi32.dll`.

---

3. Open a command prompt and go to the location where you copied the `VSEncrypt` folder.
4. Run Restore Encrypted Files using the following parameters:
  - `no` parameter: encrypt files in the Suspect folder
  - `-d`: decrypt files in the Suspect folder
  - `-debug`: create debug log and output in the root folder of the client
  - `/o`: overwrite encrypted or decrypted file if it already exists
  - `/f: {filename}`: encrypt or decrypt a single file
  - `/nr`: do not restore original file name

For example, you can type `VSEncode [-d] [-debug]` to decrypt files in the Suspect folder and create a debug log. When you decrypt or encrypt a file, the decrypted or encrypted file is created in the same folder.

---

**Note:** You may not be able to encrypt or decrypt files that are locked.

---

Restore Encrypted Files provides the following logs:

- `VSEncrypt.log` - contains the encryption or decryption details. This file is created automatically in the root system drive (normally, on the C: drive).

- `VSEncDbg.log` - contains the debug details. This file is created automatically in the root folder if you run `VSEncode.exe` with the `-debug` parameter.

### To encrypt or decrypt files in other locations:

1. Create a text file and then type the full path of the files you want to encrypt or decrypt.

For example, if you want to encrypt or decrypt files in `C:\My Documents\Reports`, type `C:\My Documents\Reports\*. *` in the text file. Then save the text file with an INI or TXT extension, for example, you can save it as `ForEncryption.ini` on the `C:` drive.

2. At a command prompt, run Restore Encrypted Files by typing `VSEncode.exe -d -i {location of the INI or TXT file}`, where {location of the INI or TXT file} is the path of the INI or TXT file you created (for example, `C:\ForEncryption.ini`).

## Client Mover I

If you have more than one OfficeScan server on the network, you can use the Client Mover tool to transfer clients from one OfficeScan server to another. This is especially useful after adding a new OfficeScan server to the network when you want to transfer existing OfficeScan clients to the new server.

---

**Note:** The two servers must be of the same language version.

---

### To use Client Mover I:

1. On the OfficeScan server, go to the following directory:

```
\PCCSRV\Admin\Utility\IpXfer
```

2. Copy the `IpXfer.exe` file to the client that you want to transfer.
3. On the client, open a command prompt and then go to the folder where you copied the file.
4. Run Client Mover using the following syntax:

```
IpXfer.exe -s <server_name> -p <server_listening_port> -m 1  
-c <client_listening_port>
```

where:

<server\_name> = the server name of the destination OfficeScan server (the server to which the client will transfer)

<server\_listening\_port> = the listening (Trusted) port of the destination OfficeScan server. To view the listening port on the OfficeScan Web console, click **Administration > Web server** in the sidebar.

1 = the HTTP-based server (you must use the number "1" after "-m")

<client\_listening\_port> = the port number of the client machine

5. To confirm the client now reports to the other server, do the following:
  - a. On the client machine, right click on the OfficeScan client program icon in the system tray.
  - b. Select **OfficeScan Main**.
  - c. Click **Help** in the menu and select **About**.
  - d. Verify the OfficeScan server that the client reports to under **Communication information, Server name/port**.

## Touch Tool

The Touch Tool synchronizes the time stamp of one file with the time stamp of another file or with the system time of the computer. If you unsuccessfully attempt to deploy a hot fix (an update or patch that Trend Micro releases) on the OfficeScan server, use the Touch Tool to change the time stamp of the hot fix. This causes OfficeScan to interpret the hot fix file as new, which makes the server attempt to automatically deploy the hot fix again.

### To run the Touch Tool:

1. On the OfficeScan server, go to the following directory:  
`\PCCSRV\Admin\Utility\Touch`
2. Copy the `TMTouch.exe` file to the folder where the file you want to change is located. If synchronizing the file time stamp with the time stamp of another file, put both files in the same location with the Touch tool.
3. Open a command prompt and go to the location of the Touch Tool.

4. Type the following:

```
TmTouch.exe <destination_filename> <source_filename>
```

where:

<destination\_filename> = the name of the file (the hot fix, for example) whose time stamp you want to change

<source\_filename> = the name of the file whose time stamp you want to replicate

If you do not specify a source filename, the tool sets the destination file time stamp to the system time of the computer.

---

**Note:** You can use the wildcard character "\*" in the destination file name field, but not the source file name field.

---

5. To verify the time stamp changed, type `dir` in the command prompt or right click the file in Windows explorer and select **Properties**.

## Integrated Tools

The functionality of the following tools, which were included in previous versions of OfficeScan, have been integrated into this version:.

Tool	Function	Integration
Client Mover II	Client Mover II transferred online HTTP-based clients from one HTTP-based OfficeScan server to another. Unlike Client Mover I, which is run from the command line interface, Client Mover II included a Windows console.	You can now move clients to other OfficeScan servers through the OfficeScan server Web console (see <a href="#">Working with OfficeScan domains</a> on page 4-12 for detailed instructions).
Database Packer	Database Packer compressed the OfficeScan database and organized information to decrease the size of the database and increase efficiency when performing queries.	OfficeScan now automatically compresses and reorganizes the database to optimize performance.

Tool	Function	Integration
Icon Cleaner	Icon Cleaner removed duplicate client records in the OfficeScan database.	<p>If a client user uninstalls the OfficeScan program, the client machine notifies the OfficeScan server, which automatically removes the client from the client domain tree.</p> <p>You can verify client-server connection to update the status of clients on the network (see <a href="#">Verifying Client-Server Connection</a> on page 4-26).</p>
Network Scan Switch	Network Scan Switch allowed you to enable and disable the client's ability to scan mapped network drives and folders.	You can now enable scanning for mapped drives and shared network folders when configuring client scan settings (see <a href="#">Configuring the Scan Settings</a> on page 4-31 for detailed instructions).
Register Shell	Register Shell allowed you to add a Manual Scan shortcut on the client machine's Windows shortcut menu.	You can now add a Manual Scan shortcut to the client machine's Windows shortcut menu from the OfficeScan server Web console on the <b>Global Client Settings</b> screen. On the sidebar, click <b>Clients &gt; Global Client Settings</b> (see the online help for detailed instructions).
Remote Agent	Remote Agent allowed clients to obtain the latest update components directly from the Trend Micro ActiveUpdate server, instead of only from the OfficeScan server. Updating directly from the ActiveUpdate server was necessary when client machines were unable to communicate with the OfficeScan server.	<p>When clients are not able to communicate with the OfficeScan server (for example, if they are not connected to your network), you can allow them to receive component updates from other sources by specifying them as Update Agents.</p> <p>Specify a list of update sources on the Update Source screen and allow Update Agents to receive updates from these sources on the Update Agent screen. Next, use Client Packager to create and deploy a package to the clients (see <a href="#">Using Update Agent</a> on page 4-17, <a href="#">Updating OfficeScan</a> on page 4-13, and <a href="#">Installing with Client Packager</a> on page 3-25).</p>
GUID Changer	GUID changer assigned new Globally Unique Identifiers (GUIDs) to clients. If you used imaging tools other than Image Setup Utility to create a client disk image, you had to assign a new GUID to each client that was installed from the disk image.	You must now use the Image Setup Utility to create an image of an OfficeScan client and make clones of it. A new GUID is created for each clone (see <a href="#">Image Setup Utility</a> on page A-11).

# Using Control Manager™ with OfficeScan

This appendix introduces Trend Micro Control Manager and describes how it can help simplify the administration of Trend Micro antivirus and content security solutions in your organization. It also provides instructions on how to install the agent for OfficeScan and how to access the OfficeScan server from the Control Manager management console.

The topics discussed in this appendix include:

- *Introducing Control Manager* on page B-2
- *What You Can do with Control Manager and OfficeScan* on page B-2
- *What is a Control Manager Agent?* on page B-3
- *Requirements for Installing the Agent* on page B-3
- *Obtaining the Public Encryption Key* on page B-4
- *Installing the Control Manager Agent* on page B-4
- *Accessing OfficeScan with Control Manager* on page B-7
- *Removing the Agent* on page B-7

## Introducing 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 antivirus and content security 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 update components throughout the network, helping ensure that protection is consistent and up-to-date. Update components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

## What You Can do with Control Manager and OfficeScan

Control Manager builds on the centralized management concept Trend Micro pioneered with Trend Virus Control System (Trend VCS). If you are currently running Trend VCS, you can purchase an upgrade to obtain all the new benefits of Control Manager. For more information on upgrading your management server from Trend VCS to Control Manager, see the *Control Manager Getting Started Guide*.

Using Control Manager, you can accomplish the following:

- Configure, monitor, and maintain most Trend Micro software, including OfficeScan, from a single console, regardless of location or platform
- Simplify the implementation of a your organization's antivirus security policies
- Delegate tasks and determine access control based on a hierarchical structure. You can assign different operators separate access to individual branches of the hierarchy
- Respond to outbreaks quickly using Outbreak Prevention Service

## What is a Control Manager Agent?

A Control Manager agent is an application installed on a computer with a Trend Micro product installation. The agent allows Control Manager to manage the product. It receives commands from the Control Manager server, applies them to the managed product, and collects logs to send to Control Manager.

## Requirements for Installing the Agent

The requirements for installing the agent are the same as those for installing the OfficeScan server.

---

**Note:** You cannot install the Control Manager agent on Microsoft Windows .NET™ Server.

---

For information on the minimum system requirements for the OfficeScan server, see [System requirements](#) on page 3-19.

## Required Information for Agent Installation

You will need the following information before deploying the agent:

- The fully qualified domain name (FQDN) or IP address of the Control Manager server
- Administrator privileges to the server where you want to install the agent
- A Control Manager User ID with Administrator, Power User, or Operator privileges. It is very important to maintain this account. If the Control Manager User ID is deleted, the agent will not be able to re-register with the Control Manager server.
- The location of the public encryption key of the Control Manager server with which you will register the agents



## Obtaining the Public Encryption Key

All products that Control Manager manages are required to have a public encryption key to register and establish communications with the Control Manager server. Obtain the public encryption key with the Control Manager management console.

### To obtain the public encryption key:

1. On any computer on the network, open a Web browser and type `http://{Control Manager Server Name}/ControlManager`, where {Control Manager Server Name} is the computer name or IP address of the Control Manager server.

The **Welcome** screen of the Control Manager management console appears.

2. Type a user ID and password.
3. Click **Products**.
4. Click **Add/Remove Product Agents**.
5. Right-click the **Public encryption key**, then click **Save As**.
6. Save the public encryption key `E2EPublic.dat` to a location that is accessible to the OfficeScan server where the agent will be installed.

## Installing the Control Manager Agent

After obtaining the public encryption key and storing it on the OfficeScan server, install the agent.

The following agent install methods are available:

- **The OfficeScan server master installer** – install the agent at the same time you install the OfficeScan server (see *Installing OfficeScan Server* on page 3-2)
- **The Control Manager Agent setup program** – use the remote install tool available from the Control Manager management console and on the OfficeScan Standard CD at the following location:

`output/CMAgent/ControlMangerAgent Setup.exe`

### To install the agent:

1. Do one of the following:

- If installing with the OfficeScan master installer, when the **Select Components** screen appears, select the **Install Control Manager agent** check box. Later, the Control Manager agent installation screen appears.
  - If installing the Control Manager agent from the included CD, double click the `Setup.exe` file located in the `Programs\OfficeScan\cmagent` folder. The installer window appears.
2. Type an existing ID for the Control Manager server. Trend Micro recommends using the root user ID.
  3. Confirm the name of the OfficeScan server in the **Entity Name** field.
  4. Click **Next**.

If the installer does not detect any Control Manager installation (including Control Manager server or Control Manager agent) on the computer, the **Setup Message Routing Path** screen appears.

If the installer detects a Control Manager installation on the computer, a prompt appears asking you if you want to reconfigure the settings for the upgrade to the current version of Control Manager agent.

    - Click **No** to keep the original settings and complete the upgrade.
    - Click **Yes** to modify the settings. The **Setup Message Routing Path** screen appears.
- 
- Note:** When upgrading to the current version of Control Manager agent, you cannot modify the Control Manager account name associated with the agent. The installer preserves the account name used with the previous installation.
- 
5. Specify a path for the incoming messages from the Control Manager server:
    - **Any host** – click to have the agent accept incoming messages from any host on the network.
    - **IP port forwarding** – click if incoming messages from the Control Manager server pass through a firewall or network device that uses port forwarding and type the device IP address, the port number the device listens at, and the port number to which it forwards messages.
    - **Proxy server** – click if incoming messages route through a proxy server and click **Proxy Server Configuration** to configure the proxy server settings. The **Proxy Configuration** screen appears.

- a. Type the name of the proxy server, the port number it uses, and the type of protocol it supports (HTTP or SOCKS 4/5).
  - b. If the proxy server requires log on credentials, click the **Authentication required** text box and type the user name and password.
  - c. Click **OK** to return to the **Setup Message Routing Path** screen.
  - d. Specify the route for outgoing messages:
    - **Route direct to server** – click if outgoing messages, which include commands, route directly to the Control Manager server
    - **Proxy server** – click if outgoing messages route through a proxy server and click **Proxy Server Configuration** to configure the proxy server settings. The **Proxy Configuration** screen appears.
  - i. Type the name of the proxy server, the port number it uses, and the type of protocol it supports (HTTP or SOCKS 4/5).
  - ii. If the proxy server requires log on credentials, click the **Authentication required** text box and type the user name and password.
  - iii. Click **OK** to return to the **Setup Message Routing Path** screen.
6. Click **Next**. The **Register with Control Manager** screen appears.
  7. Click **Import** to select the public encryption key `E2EPublic.dat` you obtained from the Control Manager server (see *Obtaining the Public Encryption Key* on page B-4).
  8. Select the public encryption key and click **Open**. The Control Manager information appears under **Server Information**.
  9. Click **Next**. When the installation is complete, a notification message appears.
  10. Click **OK**.

## Accessing OfficeScan with Control Manager

The Control Manager agent for OfficeScan accepts commands from the Control Manager server and instructs OfficeScan to carry out actions. For example, when you click **Tasks > Deploy engines** on the Control Manager console, the agent instructs OfficeScan to deploy the latest scan engine.

### To open the Control Manager console:

1. On any computer on the network, open a Web browser and type `http://{Control Manager server name}/ControlManager`, where `{Control Manager server name}` can be the computer name or IP address of the Control Manager server.

The **Welcome** screen of the Control Manager console appears.

2. Click **Products**.
3. In the **Product Directory**, click the OfficeScan server to manage. The following tabs are displayed:
  - **Product Status** – view OfficeScan server information, such as the server name, the version numbers of components, the operating system used on the server machine, and Control Manager agent details
  - **Configuration** – access the OfficeScan Web console
  - **Tasks** – deploy the scan engine, virus pattern file, and damage cleanup template, enable Real-time Scan, and perform Scan Now
  - **Logs** – view Control Manager event and security logs

## Removing the Agent

You can easily remove the Trend Micro Control Manager agent for OfficeScan using the **Add/Remove Programs** function of Windows.

### To remove the agent:

1. On the server where the agent is installed, click the **Start** menu and click **Settings > Control Panel > Add/Remove Programs**. The **Add/Remove Programs** window appears. Click **Trend Micro Control Manager Agent for OfficeScan**, and then click **Change/Remove**. A confirmation screen appears.

2. Click **Yes**. Windows removes the agent from the server. When the agent is completely removed, click **OK**.

---

**Note:** Removing the OfficeScan server automatically removes the Control Manager agent for OfficeScan.

---

# Policy Server for Cisco™ NAC Primer

This appendix serves as a primer for Cisco Network Admission Control (NAC). It provides fundamental information on Cisco NAC technology. Read this appendix to become familiar with the concepts and terminology associated with Cisco NAC before installing and configuring the various Cisco NAC components.

Topics discussed in this appendix include:

- *Introduction to Trend Micro Policy Server for Cisco NAC* on page C-2
- *Understanding Components and Terms* on page C-2
- *Cisco NAC Architecture* on page C-4
- *The Client Validation Sequence* on page C-5
- *Understanding the Policy Server* on page C-7
- *Understanding Certificates* on page C-14
- *Policy Server system requirements* on page C-16

## Introduction to Trend Micro Policy Server for 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 instructing client computers to update their OfficeScan client components, enable Real-time Scan, and perform Scan Now and Cleanup Now. It also includes the ability to 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, you also have the option to 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](http://www.cisco.com/go/nac).

---

## Understanding 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:

- **Cisco Trust Agent (CTA)** – an installation on a client that allows it to communicate with other Cisco NAC components
- **OfficeScan client** – a client 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 routers, see [Accepted Cisco router models](#) on page C-18.

- **Cisco Secure Access Control Server (ACS)** – a server that receives OfficeScan client antivirus data from the client via 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.

---

**Note:** The ACS server has configuration options outside of the scope of the Trend Micro implementation of Policy Server for Cisco NAC. For example, it is capable of performing other actions on the client, such as preventing network access. See your Cisco Secure Access Control Server documentation for more information.

---

- **Policy Server** – a computer that receives and evaluates OfficeScan client antivirus data. After performing the evaluation, the Policy Server determines what actions the OfficeScan client should carry out. It then passes this information back to the client.
- **OfficeScan server** – the OfficeScan server reports the current virus pattern file and scan engine versions to the Policy Server, which uses this information to perform the evaluation of the OfficeScan client

## Terms

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

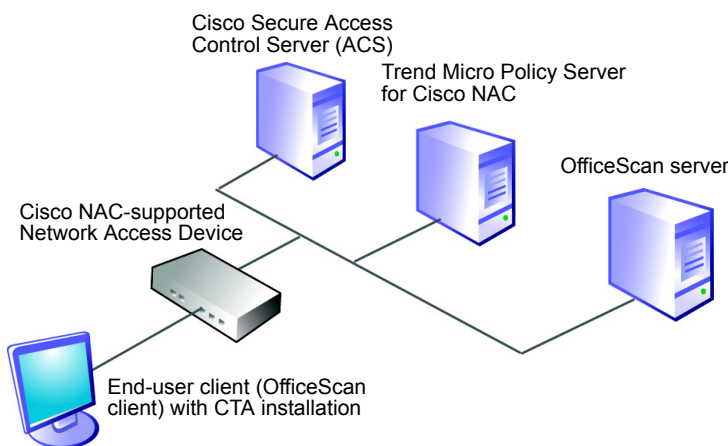
- **Security posture** – the presence and currency of antivirus software on a client. In this implementation, security posture refers to whether or not the OfficeScan client program is installed on clients, the status of certain OfficeScan client settings, and how up-to-date the versions of the scan engine and virus pattern file are.
- **Posture token** – information the Policy Server creates after OfficeScan client validation, including instructions that tell 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 [Understanding Policy Server policies and rules](#) on page C-8 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 [Understanding Policy Server policies and rules](#) on page C-8 for detailed information).

## Cisco NAC Architecture

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



**FIGURE C-1 Basic Cisco NAC architecture**

The OfficeScan client in Figure C-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 located 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.

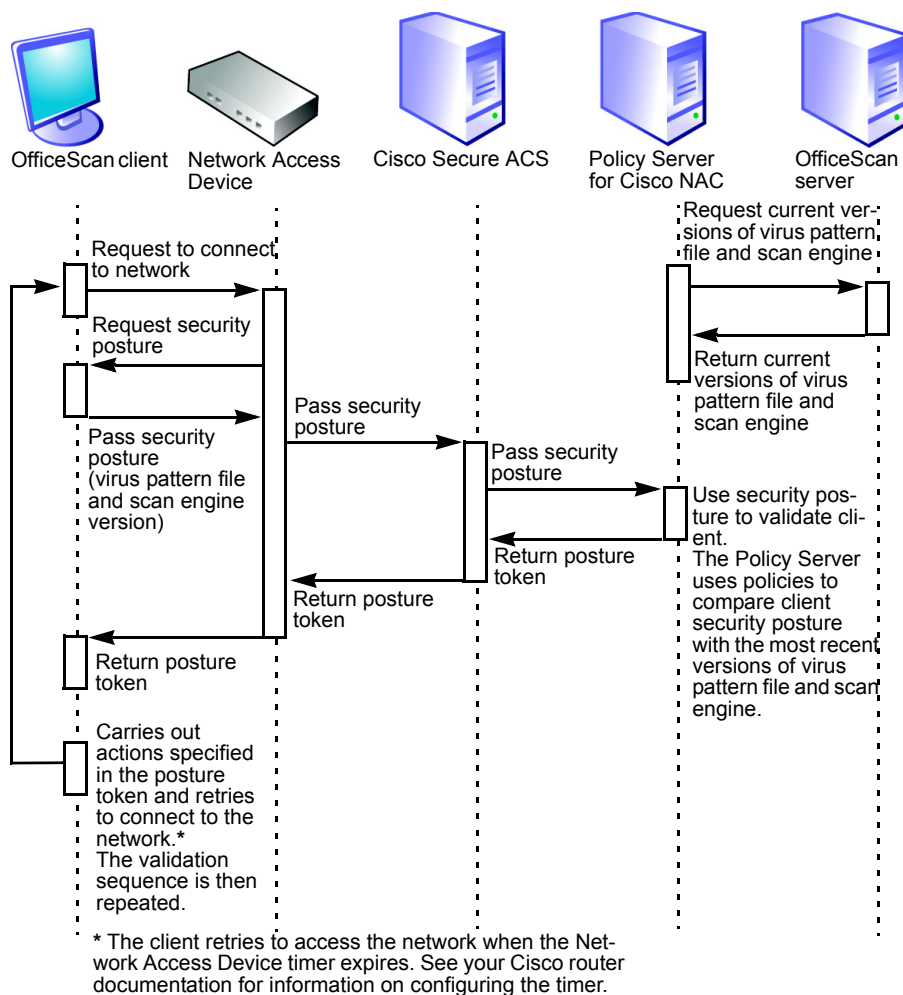
---

## 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 C-2 illustrates the sequence of events that occurs when an OfficeScan client attempts to access the network. The Cisco Network Access Device starts the validation sequence by requesting the security posture of the client, and then passes this data on to the ACS server. The ACS server passes the security posture to the Policy Server, which performs the evaluation.

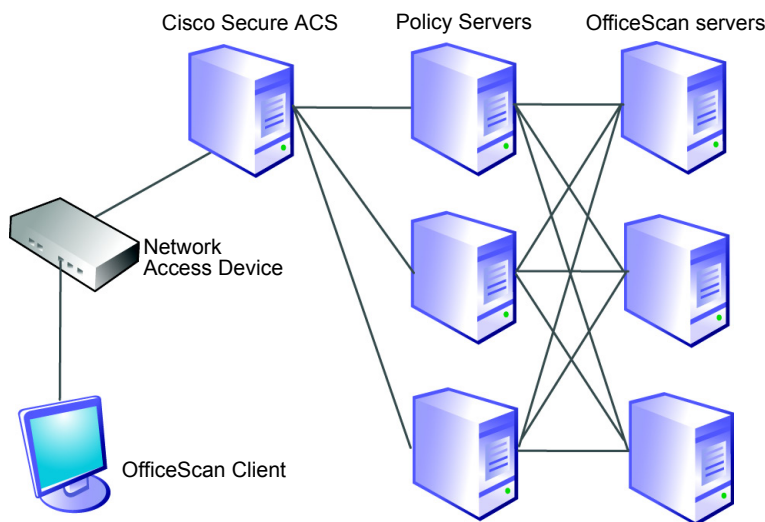
In a separate process, the Policy Server periodically polls the OfficeScan server for pattern file and scan engine information to keep its data current. It then uses a policy you configure to perform a comparison of this information with the client security posture data. Following that, the Policy Server creates a posture token, and passes it back to the OfficeScan client. Finally, the client performs the actions configured in the posture token.

**FIGURE C-2 Network access validation sequence**

## Understanding the Policy Server

The Policy Server is responsible for evaluating the OfficeScan client's security posture and for creating the posture token. It performs the evaluation by comparing the security posture with the latest versions of the virus pattern file and 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 via 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 and to act as a backup if a Policy Server becomes inoperable. If multiple OfficeScan servers are installed 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 that is registered to all the Policy Servers. Figure C-3 illustrates the relationship of multiple OfficeScan servers and Policy Servers.



**FIGURE C-3 Multiple Policy Server/OfficeScan server relationship**

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

## Understanding Policy Server policies and rules

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

*Rules* are comprised of 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 *Instructing the Policy Server and the OfficeScan client to carry out actions* on page C-9).

*Policies* are comprised of one or more rules. Assign one policy to each registered OfficeScan server on your network for both Outbreak mode and normal mode (see *Using Outbreak Prevention* on page 6-2 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 *Instructing the Policy Server and the OfficeScan client to carry out actions* on page C-9).

---

**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 *Creating OfficeScan domains* on page 4-9).

---

## Rule composition

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

### Security posture criteria

Rules are comprised of the following security posture criteria:

- Client Real-time Scan status – if Real-time Scan is enabled or disabled
- Client scan engine version currency – if the scan engine is up-to-date

- Client virus pattern file status – how up-to-date the virus pattern file is. The Policy Server determines this by checking one of the following:
  - if the virus pattern file is a certain number of versions older than the Policy Server version
  - if the virus pattern file was released a certain number of days prior to the validation

## Default responses for rules

Responses are used to 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 conforms to your security policies
- **Checkup** – the client needs to update its antivirus components
- **Quarantine** – the client is at high risk of being infected
- **Infected** – the client is infected or has at risk of infection
- **Unknown** – any other condition

---

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

---

## Instructing the Policy Server and the OfficeScan client to carry out 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 *Using the client validation logs* on page D-26 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 OfficeScan client scans all files when they are opened or saved (see *Configuring Real-time Scan* on page 4-34 for more information)

- Update all OfficeScan components (see *Updating OfficeScan* on page 4-13 for more information)
- Scan the client after Real-time Scan is enabled or after an update
  - If the above is selected, automatically run Damage Cleanup Services (Cleanup Now) with the option of automatically performing Scan Now

---

**Note:** Enable Real-time Scan on clients to automatically perform Scan Now.

---

- Display a notification message to the client user

## Default rules

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

### Rule Name: Healthy

#### Matching criteria:

Real-time Scan status enabled

Scan engine and virus pattern file up-to-date

#### Response if criteria matched:

Healthy

#### Server action:

none

#### Client action:

none

### Rule Name: Checkup

#### Matching criteria:

Client virus pattern status is at least one version older than the version on the OfficeScan server with which the client is registered

#### Response if criteria matched:

Checksum

**Server action:**

Create entry in client validation log

**Client action:**

Update components

Perform automatic Cleanup Now on the client after Real-time Scan is enabled or after an update

Display notification message to the client user

---

**Tip:** If you use this rule, Trend Micro recommends using automatic deployment. This helps ensure that clients receive the latest virus pattern file immediately after the OfficeScan server downloads new components (see [Updating clients using Automatic Deployment](#) on page 4-21).

---

**Rule Name: Quarantine**

**Matching criteria:**

Virus pattern file is at least five versions older than the pattern file on the OfficeScan server with which the client is registered

**Response if criteria matched:**

Quarantine

**Server action:**

Create entry in client validation log

**Client action:**

Update components

Perform automatic Cleanup Now and Scan Now on the client after Real-time Scan is enabled or after an update

Display notification message to the client user



**Rule Name: Not protected****Matching criteria:**

Real-time Scan status disabled

**Response if criteria matched:** Infected

**Server action:**

Create entry in client validation log

**Client action:**

Enable client Real-time Scan

Display notification message to the client user

## Policy composition

Policies are comprised 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 rules, and remove existing rules 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 C-9 for the list of responses).

### Instructing the Policy Server and OfficeScan client to carry out actions

OfficeScan client and the Policy Server can carry out the same set of actions for policies as they do for rules. However, the actions are performed only when client security posture does not match any rules in the policy (see *Instructing the Policy*

*Server and the OfficeScan client to carry out actions* on page C-9 for a list of the actions).

## 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:

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 automatic Cleanup Now and Scan Now on the client after Real-time Scan is enabled or update is performed

Display notification message to the client user

## Understanding Synchronization

Regularly synchronize the Policy Server with registered OfficeScan servers to keep the Policy Server versions of the virus pattern file, scan engine, and server outbreak status (normal mode or Outbreak mode) up-to-date with the those on the OfficeScan server. Use the following methods to perform synchronization:

- Manually – perform synchronization at any time on the Summary screen (see *Viewing summary information for a Policy Server* on page D-18)
- By schedule – set a schedule to have OfficeScan perform synchronization (see *Configuring scheduled synchronization* on page D-29)

## Understanding Certificates

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

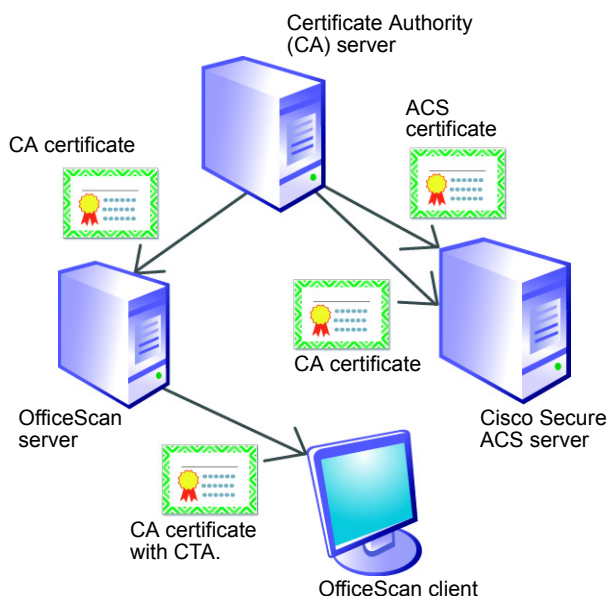
- **ACS certificate** – establishes trusted communication between the ACS server and the Certificate Authority (CA) server. The Certificate Authority server signs the ACS certificate before you save it on the ACS server.
- **CA certificate** – authenticates OfficeScan clients with the Cisco ACS server. The OfficeScan server deploys the CA certificate to both the ACS server and to OfficeScan clients (included with the Cisco Trust Agent package).
- **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.

---

**Tip:** The Policy Server SSL certificate is optional. However, Trend Micro recommends using to encrypt the data sent between the Policy Server and ACS server.

---

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



**FIGURE C-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). You can then install the ACS certificate on the ACS server. The process is described as *Enrolling the Cisco Secure ACS server* on page D-3.
2. Next, you can export a CA certificate from the CA server and install it on the ACS server. See *Exporting and Installing the CA Certificate* on page D-7 for detailed instructions.
3. Following that, save a copy of the same CA certificate on the OfficeScan server.
4. The OfficeScan server deploys the CA certificate to clients with the CTA. See *Deploying the Cisco Trust Agent* on page D-11 for detailed instructions.

## Understanding 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 have already enabled machine authentication for Cisco Secure ACS using Windows Active Directory, which you can configure to automatically produce an end user client certificate when a new computer is added in active directory. For instructions, see Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows.

For users of networks that have 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 CTA setup (which is done during OfficeScan installation) or from the OfficeScan Web Console. OfficeScan distributes the certificate when it deploys the Cisco Trust Agent to clients (see *Deploying the Cisco Trust Agent* on page D-11).

---

**Note:** If you have 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 prepare the certificate (see *Enrolling the Cisco Secure ACS server* on page D-3).

## Policy Server system requirements

The following are minimum requirements to install the Policy Server and the Cisco Trust Agent (CTA).

### Operating system

- Microsoft™ Windows™ NT series (Service Pack 6a)
- Windows 2000 Series (Service Pack 2)
- Windows XP (Professional Edition only, Service Pack 1)
- Windows Server 2003

## Hardware

- 300MHz Intel Pentium™ II processor or equivalent
- 128MB of RAM
- 300MB of disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft Internet Explorer 5.5 or later

## Web server

- Microsoft Internet Information Server (IIS)
  - on Windows NT: version 4.0
  - on Windows 2000: version 5.0
  - on Windows XP: version 5.1
  - on Windows Server 2003: version 6.0
- Apache Web server 2.0 or later (for Windows 2000/XP/Server 2003 only)

## Minimum system requirements for the Web console

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

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

## Cisco Trust Agent (CTA) requirements

The Cisco Trust Agent can be installed only on clients running Windows NT/2000/XP.

### CTA on Windows NT/2000

- 150MHz Intel Pentium processor or equivalent

- Microsoft Windows NT 4.0 with SP6a or later, Windows 2000 Server/Advanced Server with SP2 or later, Windows 2000 Pro with SP 2 or later
- Windows Installer 2.0
- 64MB of RAM
- 80MB of available hard disk space

### **CTA on Windows XP**

- 300MHz Intel Pentium processor or equivalent
- Microsoft Windows XP Home or Professional Edition with SP1
- 128MB of RAM
- 80MB of available hard disk space

## **Accepted Cisco router models**

The following Cisco router models can be used with Policy Server for Cisco NAC.

---

**Note:** This list is subject to change. Contact Cisco Systems Inc. for an updated list or see [www.cisco.com/go/nac](http://www.cisco.com/go/nac).

---

- 831 (16MB flash memory)
- 1701 (16MB flash memory)
- 1711 (16MB flash memory)
- 1712 (16MB flash memory)
- 1721 (16MB flash memory)
- 1751 (16MB flash memory)
- 1751-V (16MB flash memory)
- 1760 (16MB flash memory)
- 2600XM (32MB flash memory)
- 2691 (32MB flash memory)
- 3640/3640A (32MB flash memory)
- 3660-ENT Series (32MB flash memory)
- 3725 (32MB flash memory)

- 3745 (32MB flash memory)
- 7200 (32MB flash memory)





## Deploying Policy Server Cisco NAC

This appendix describes how to install and configure the Policy Server for Cisco Network Admission Control (NAC). It also includes information on deploying the Cisco Trust Agent (CTA) and creating and deploying digital certificates used between the various Cisco NAC components.

Topics discussed in this appendix include:

- *Policy Server for NAC Deployment Overview* on page D-2
- *Enrolling the Cisco Secure ACS server* on page D-3
- *Exporting and Installing the CA Certificate* on page D-7
- *Preparing the Policy Server SSL Certificate* on page D-9
- *Deploying the Cisco Trust Agent* on page D-11
- *Installing the Policy Server for Cisco NAC* on page D-13
- *Configuring the ACS Server* on page D-15
- *Configuring the Policy Server for Cisco NAC* on page D-16

---

**Note:** This appendix 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, refer to 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 *Installing OfficeScan Server* on page 3-2).
2. **Install OfficeScan clients** – install the OfficeScan client program on all clients whose antivirus protection you want Policy Server to evaluate (see *Installing OfficeScan Clients* on page 3-19).
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 *Enrolling the Cisco Secure ACS server* on page D-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 *Exporting and Installing the CA Certificate* on page D-7).
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 *Deploying the Cisco Trust Agent* on page D-11).
6. **Install the Policy Server for Cisco NAC** – install the Policy Server for Cisco NAC to handle requests from the ACS server (see *Installing the Policy Server for Cisco NAC* on page D-13).
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 *Installing the Policy Server for Cisco NAC* on page D-13).

8. **Configure the ACS server** – configure the ACS server to forward posture validation requests to the Policy Server (see *Configuring the ACS Server* on page D-15).
9. **Configure the Policy Server for NAC** – create and modify rules and policies to enforce your organization's security strategy for OfficeScan clients (see *Configuring the Policy Server for Cisco NAC* on page D-16).

---

**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 appendix, verify that the Network Access Device(s) on your network are able to support Cisco NAC (see *Accepted Cisco router models* on page C-18). 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.

---

## Enrolling the Cisco Secure ACS server

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 intended 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.

**To enroll the Cisco Secure ACS server with a Windows Certificate Authority server:**

1. Generate a certificate signing request at the Cisco Secure ACS server.
  - a. In the navigation bar of the ACS Web console, click **System Configuration**.
  - b. Click **ACS Certificate Setup**.
  - c. Click **Generate Certificate Signing Request**. Cisco Secure ACS displays the **Generate new request** table on the **Generate Certificate Signing Request** screen.

- d. In the **Certificate subject** text box, type **cn=** followed by the name that you would like to use as subject name in this ACS certificate, for example, `cn=ACSTrend`.
  - e. In the **Private key file** text box, type the full directory path and name of the file in which the private key is saved, for example, `c:\privateKeyFile.pem`.
  - f. In the **Private key password** text box, type a new password that will serve as the private key password, and retype it in the **Retype private key password** box.
  - g. From the **Key length** list, select the length of the key to be used. The choices for Key length are 512 or 1024 (default) bits.
  - h. From the **Digest to sign with** list, select the digest (or hashing algorithm). The choices for Digest to sign with are MD2, MD5, SHA, and SHA1 (default).
  - i. Click **Submit**. Cisco Secure ACS displays a certificate signing request (CSR) in the display area, on the right, under a banner that displays the following message:

“Now your certificate signing request is ready. You can copy and paste it into any certification authority enrollment tool.”
2. Use a certificate authority enrollment tool, such as Windows 2000 Server Certification Authority, to sign the certificate:
- a. Verify that Certificate Services Web Enrollment Support is installed on the Windows 2000 Server you are using to service certificate requests.
  - b. Type the following: `http://{CA_Server}/certsrv/`, where `{CA_Server}` is the web address of the Windows 2000 Server you are using to service certificate requests. The Microsoft Certificate Services **Welcome** screen appears.
  - c. Click **Request a Certificate** and click **Next >**. The **Choose Request Type** screen appears.
  - d. Click **Advanced request** and click **Next >**. The **Advanced Certificate Requests** screen appears.

- e. Click **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file** and click **Next**. The **Submit a Saved Request** screen appears.
  - f. If the CA server is installed on a machine with Active Directory, select **Web Server** next to **Certificate Template**.
  - g. Copy the CSR from the Cisco Secure ACS screen and paste it into the **Saved Request** box.
  - h. Click **Submit** >. The Certificate Server stores the request.
3. Issue the certificate request from the CA server:

---

**Note:** If your CA server is configured to automatically issue certificates upon request, skip to part d in the next step.

---

- a. On the CA server that processed the request, click **Start > Run**. The **Run** screen opens.
  - b. Type **mmc** in the **Open** box. A new Web console screen opens.
  - c. Click **Console > Add/Remove Snap-in**. the **Add/Remove Snap-in** screen appears.
  - d. Click **Add**. The **Add Standalone Snap-in** screen opens
  - e. Click **Certification Authority** and click **Add**. The **Certification Authority** 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 **Certification Authority > {local certification authority}/Pending Requests**, where {local certification authority} is the name you assigned the Certificate Authority server during installation.
  - j. Right-click the request and click **Issue**.
4. Download the CA certificate from the Microsoft Certificate Services Web page.

- a. Reopen the Microsoft Certificate Services Web page from the ACS server (see Step b on page D-4).
  - b. Click **Check on pending certificate**.
  - c. Click the certificate request and click **Next**.
  - d. Click **DER encoded** then click **Download CA certificate**. The file download screen opens with a security warning.
  - e. Click **Save**.
  - f. Save the certificate to a location on the ACS server's local hard drive
5. Install the signed certificate on the ACS server.
  - a. Open the Cisco Secure ACS management console.
  - a. In the navigation bar, click **System Configuration**.
  - b. Click **ACS Certificate Setup**.
  - c. Click **Install ACS Certificate**. Cisco Secure ACS displays the **Install ACS Certificate** screen.
  - d. Select **Read certificate from file**, and then type the full directory path and filename of the certificate file in the **Certificate file** text box.
  - e. In the **Private key file** text box, type the full directory path and name of the file that contains the private key.
  - f. In the **Private key password** text box, type the private key password.

---

**Note:** This is the value you entered in **Private key password** on the **Generate Certificate Signing Request** page (see *Enrolling the Cisco Secure ACS server* on page D-3).

---

- g. Click **Submit**.
6. Restart the ACS server:
  - a. Click **System Configuration > Service Control**.
  - b. Click **Restart**.

## Exporting and Installing the CA Certificate

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. Later, when you create the CTA agent deployment package, the CA certificate is included (see *Understanding the CA certificate* on page C-16 and *Deploying the Cisco Trust Agent* on page D-11).

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 intended for users running a Windows Certification Authority server to manage certificates on the network. Refer to your vendor documentation if you are using 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 that 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 machine where OfficeScan server is installed so you can deploy it to the client with the CTA (see *Deploying the Cisco Trust Agent* on page D-11 for more information).

---

**Note:** Store the certificate on a local drive; mapped drives are not acceptable.

---

## Preparing the Policy Server SSL Certificate

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 is running on 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 is running on Apache 2.0:**
  - a. Obtain the certificate file `server.cert`. 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 located 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 located 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.

## Deploying the Cisco Trust Agent

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 [Exporting and Installing the CA Certificate](#) on page D-7).

---

**Note:** Install Windows Installer 2.0 for NT 4.0 on clients 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, click **Agent Deployment** in the menu. The client tree appears.
  - If you haven't yet distributed certificates to clients, do the following:
    - i. Click **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 [Exporting and Installing the CA Certificate](#) on page D-7.
    - 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 **Agent Deployment** in the sidebar. The **Agent Install/Uninstall** screen appears.
5. Click **Install/upgrade Cisco Trust Agent** and then click **Save**. The **Set Install CTA** page appears.

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 deployment request when the client comes online.

---

If you already prepared a CA certificate before installing the OfficeScan server, the option exists to deploy the CTA agent during OfficeScan server installation with the master installer.

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

1. During OfficeScan server installation, the **Components Selection** screen of the OfficeScan server master installer displays. For instructions on using the OfficeScan server master installer, refer to *Using master installer to install OfficeScan server* on page 3-6.
2. Select the **Enable Agent Deployment for Cisco NAC** check box.
3. 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**. A file browser appears.
    - ii. Select the prepared certificate file from the file browser and click **OK**. For instructions on preparing a certificate file, refer to *Exporting and Installing the CA Certificate* on page D-7.
    - iii. Click **Next** >.
4. Continue with OfficeScan server master installation.

## Verifying Cisco Trust Agent installation

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.

## Installing the Policy Server for Cisco NAC

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 machine)

---

**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, the installer automatically installs Apache version 2.0.48. If the computer contains a more recent version of Apache, the installer does not perform any installation.

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

---

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

1. Log on the machine 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 package.
4. Follow the installation instructions.

It is also possible to install the Policy Server to the same machine as the OfficeScan server.

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

1. During OfficeScan server installation, the **Components Selection** screen of the OfficeScan server master installer displays. For instructions on using the OfficeScan server master installer, refer to *Installing OfficeScan Server* on page 3-2 and the installer help.
2. Select the **Install Policy Server for Cisco NAC** check box.
3. Click **Next >**.
4. Continue with OfficeScan server master installation.

5. 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.
6. Read the agreement and click **Yes** to continue. The **Choose Destination Location** screen appears.
7. Modify the default destination location if necessary by clicking **Browse...** and selecting a new destination for the Policy Server installation.
8. Click **Next>**. The **Web Server** screen appears.
9. Choose the Web server for the Policy Server:
  - **IIS server:** click to install on an existing IIS Web server installation
  - **Apache 2.0 server:** click to install on an Apache 2.0 Web server.
10. Click **Next>**. The **Web Server Configuration** screen appears.
11. 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 installed on the same machine and 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 enabling Secured Socket Layer (SSL) security. Select the Enable SSL check box. Type the number of years to keep the SSL certificate valid (the default is 3 years) and type an SSL port number. 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://{PolicyServer_Server_Name}:{port number} or  
https://{PolicyServer_Server_Name}:{port number} (if you enable  
SSL)
```

12. Click **Next**. The **Setup Complete** screen appears.
13. You have completed installing Policy Server. Click **Finish**.  
The OfficeScan server master installer will continue.

---

**Note:** If upgrading from a previous version of OfficeScan, the master installer upgrades to OfficeScan 6.5 and also installs Policy Server (if you specify to install it).

---

## Configuring the ACS Server

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.

---

**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 Trend Micro's Policy Server for Cisco NAC implementation and are not in this document. See your ACS documentation for details on configuring other ACS functions.

---

### To configure the ACS server for use with the Trend Micro Policy Server for Cisco NAC:

1. Open the Cisco Secure ACS management console.
2. Click **External User Databases > Database Configuration > Network Admission Control**.
3. In **External User Database Configuration**, click **Configure**. The **Network Admission Control Expected Host Configuration** screen appears.
4. In **Credential Validation Policies**, click **External Policies**. The **Select External Policies** screen appears.
5. Click **New External Policy**. The **External Policy Configuration** screen appears.



6. Type a **Name** and **Description** for the external Policy Server.
7. Select the **Primary Server Configuration** check box, and type the following URL of the Policy Server in the URL field:  

```
https://{Policy_Server_IP}:{Port_Number}/antibody/cgi-bin/PostureRequest.dll?PostureRequest
```

For example:

```
https://192.168.16.134:4343/antibody/cgi-bin/PostureRequest.dll?PostureRequest
```
8. Type the user name and password that you specified for **ACS login** during Policy Server installation in the **Username** and **Password** fields, respectively.
9. Select the Policy Server SSL certificate that you prepared. For more information on the certificate, see *Preparing the Policy Server SSL Certificate* on page D-9.
10. In **Forwarding Credential Types**, select **Trend:AV** from the **Available Credentials** list and click ->. **Trend:AV** appears in the **Selected Credentials** list.
11. Click **Submit**. The **Select External Policies** screen appears with the name of the Policy Server listed in the **Available Policies** list.
12. Click the name of the external Policy Server on the **Available Policies** list and click ->. The Policy Server appears in the **Selected Policies** list.
13. Click **Submit**. The name of your external policy appears in the **Credential Validation Policies** table.

## Configuring the Policy Server for Cisco NAC

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 via the **Policy Servers** menu item in the OfficeScan Web console.

This section describes the following aspects of Policy Server configuration:

- *Adding and removing Policy Servers* starting on page D-17 describes how to manage Policy Servers on the OfficeScan Web console
- *Viewing summary information for a Policy Server* starting on page D-18 shows you how to get an overview of Policy Servers on your network

- *Adding or editing OfficeScan servers* starting on page D-20 is the first step in configuring Policy Servers
- *Configuring rules* starting on page D-22 shows you how to create and edit rules that comprise policies
- *Configuring policies* starting on page D-24 shows you how to create and edit policies that ultimately determine how Policy Server measures client security posture
- *Using the client validation logs* starting on page D-26 gives an overview of how to use logs to understand the security posture status of clients on your network
- *Performing administrative tasks* starting on page D-28 describes how to change the Policy Server password and set a schedule for synchronization

## Adding and removing Policy Servers

The first step in configuring Policy Servers is adding the installed Policy Servers to the OfficeScan server. This allows you to open the Policy Server Web console from the OfficeScan Web console. The **Policy Servers** screen shows all the Policy Servers currently installed on your network. Add or delete Policy Servers from this screen.

### To add a Policy Server:

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for 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 management console.
5. Click **Add**.

### To delete a Policy Server:

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for 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.

---

## Viewing 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 with 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 with 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 sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for 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 that registered OfficeScan servers can use
  - **Rule(s):** the Policy Server rules that comprise policies

If you want multiple Policy Servers on your network to have the same settings, including the same rules and policies, export settings from one server and import them into the others.

---

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

---

**To export Policy Server configuration settings:**

1. On the sidebar, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for 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 **Export**.
4. Click **Save** and select a destination.

---

**Note:** The Policy Server configuration settings are saved as a binary file with a .dat extension.

---

**To import Policy Server configuration settings:**

1. On the sidebar, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for 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 **Import**. The **Summary - Import Configurations** screen appears.
4. Click **Browse** and select the location to import the configuration file from.
5. Click **Import**. The settings in the file display.
6. Click **Save**.

The **Client Validation Logs** table provides a link to the current validation log, which is saved as a .CSV file.

**To view the current validation log:**

- Click **View current validation log**. The log opens in the default spreadsheet application for .CSV files on your computer.

The **Registered OfficeScan servers** table displays a read-only list of the IP addresses of registered OfficeScan servers on your network, the date last synchronized, the current virus pattern file version and last update date, and the current scan engine version.

**To synchronize the Policy Server with registered OfficeScan servers:**

- 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 of the registered OfficeScan servers
  - Synchronization Result:** if the synchronization was successful
  - Last Synchronized:** the date of the last successful synchronization

For more information on synchronization, see [Understanding Synchronization](#) on page C-14.

## Adding or editing OfficeScan servers

Register the Policy Server with at least one OfficeScan server so the Policy Server can obtain virus pattern file and scan engine version information (see Figure C-2 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 on the **OfficeScan servers** screen.

**To add or edit an OfficeScan server:**

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for all Policy Servers.
2. Click the server name of the Policy Server whose details you want to view. The **Summary** screen for that server appears. Choose one of the following methods to access the **Add OfficeScan server** screen:

- On the **Summary** screen, click the link that represents the number of Registered OfficeScan server(s).
- On the sidebar, click **Configurations > OfficeScan servers**.

The **OfficeScan Servers** screen appears.

3. To add a server:

- Click **Add**. The **Add OfficeScan Server** screen appears.

To edit the details of an existing server:

- Click the name of an OfficeScan server to edit. The **Update OfficeScan Server** screen appears.

4. Next to **OfficeScan server address**, type the IP address, server name, or Fully Qualified Domain Name (FQDN) of the server you want to add.
5. Next to **HTTP port number**, type the number of the port the OfficeScan server uses for HTTP communication.

---

**Note:** Type the same HTTP server port you configured during installation of the OfficeScan server (the default is 8080). This is NOT the port used for HTTPS communication (if using SSL). To view the port number from the OfficeScan Web console, click **Administration > Web Server** in the sidebar.

---

If editing the details of an existing OfficeScan server, the name of the server appears next to **OfficeScan server name**. If adding a new server, **n/a** appears.

6. Under **Policy Information**, select the policies to use when the network is normal or when outbreak mode is in effect.
7. Configure proxy settings if a proxy server is between the OfficeScan server and the Policy Server:
  - a. Select the **Enable HTTP proxy** check box.
  - b. Type the IP address and port number of the proxy server.

If the proxy server uses authentication, click the **Authentication** check box and type the user name and password required to access the server.
8. Click **Save**.

## Configuring 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 C-8 for detailed information on rules).

### Adding or editing a rule

#### To add or edit a rule:

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for all Policy Servers.
2. Click the server name of the Policy Server whose details you want to view. The **Summary** screen for that server appears. Choose one of the following methods to access the **Rules** screen:
  - On the **Summary** screen, click the link that represents the number of **Rules**.
  - On the sidebar, click **Configurations > Rules**. The **Rules** screen appears.
3. To add a new rule:
  - Click **Add**. The **New Rule** screen appears.To edit an existing rule:
  - Click the name of the rule. The **Edit Rule** screen for that rule appears.
4. Next to **Rule name** and **Description**, type a name to represent the policy and an optional description.
5. Under **Matching criteria**, select criteria that the OfficeScan clients must match to return a response. Policy Server returns a response when all of the selected criteria matches. If the criteria is not matched, Policy Server returns the response you configure in the policy to which this rule is applied.
  - To trigger a response based on the status of Real-time scan, select the check box next to **Client Real-time scan is** and click **Enabled** or **Disabled**.
  - To trigger a response based on the status of Real-time scan, select the check box next to **Client scan engine is** and click **Up-to-date** or **Not-up-to-date**.
  - To trigger a response based on the status of the virus pattern file, select the check box next to **Client virus pattern status** and click one of the following:

- **By version:** the version of the OfficeScan client virus pattern file is at most or at least { } versions older than the version of the virus pattern file on the OfficeScan server  
Select **at most** or **at least** and the number of versions from the lists
  - **By pattern release date:** the release date of the OfficeScan client virus pattern file is at most or at least { } days older than the release date of the virus pattern file on the OfficeScan server  
Select **at most** or **at least** and the number of days from the lists
6. Next to **Return response**, select a response for OfficeScan to return if the client security posture matches all the items in **Matching criteria** (see *Default responses for rules* on page C-9 for additional information on responses):
- **Healthy**
  - **Checkup**
  - **Infected**
  - **Quarantine**
  - **Unknown**

---

**Note:** You cannot add or delete items from the **Default response** list.

---

7. Under **Server-side actions**, select the **Log this incident if all criteria matched** check box to have the Policy Server log this incident.
8. Under **Client-side actions**, select from among the following options for OfficeScan clients if all policy criteria are matched (see *Instructing the Policy Server and the OfficeScan client to carry out actions* on page C-9 for explanations of these actions):
- **Enable client Real-time scan**
  - **Update components**
  - **Scan after Real-time scan is enabled or after an update**
    - **Perform Cleanup Now and Scan Now**
    - **Perform Cleanup Now**
  - **Display notification message on client computer** (modify the message as needed)



9. Click **Save**.

## Configuring policies

After configuring new rules or ensuring that the default rules are suitable for your security enforcement needs, configure policies to that registered OfficeScan servers can use (see *Policy composition* on page C-12 for detailed information on policies).

### Adding or editing a policy

Add a new Cisco NAC policy or edit an existing policy to determine which rules are enforced and to take action on clients in the event that client security posture does not match any rules.

#### To add a new policy:

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for all Policy Servers.
2. Click the server name of the Policy Server whose details you want to view. The **Summary** screen for that server appears. Choose one of the following methods to access the **Policies** screen:
  - On the **Summary** screen, click the link that represents the number of **Policies**.
  - On the sidebar, click **Configurations > Policies**.

The **Policies** screen appears.

3. To add a policy:
  - Click **Add**. The **New Policy** screen appears.





To edit a policy:

- Click on a policy name. The **Edit Policy** screen for that policy appears.
4. Next to **Policy name** and **Description**, type a name to represent the policy and an optional description.
  5. Under **Rules**, select which existing rules will compose this policy. Existing rules appear in the **Rules available** column. Rules are enforced in the order that they appear in the **Rules in use** column.

---

**Note:** If the criteria of a rule are not matched, the Policy Server continues to the next rule.

---

- To move rules between the **Rules Available** and **Rules in use** columns, click a rule and then click either  or .
  - To change the order of the rules in use, click the rule and then click either  or .
6. Under **Default Response**, select a response for the Policy Server to return if none of the rules returns a response:
- **Healthy**
  - **Checkup**
  - **Infected**
  - **Quarantine**
  - **Unknown**

---

**Note:** You cannot add or delete items from the **Default response** list.

---

7. Under **Server-side actions**, select the **Log this incident if all criteria matched** check box to have the Policy Server log this incident (see *Using the client validation logs* on page D-26 for more information).
8. Under **Client-side actions**, select from among the following actions OfficeScan will take for OfficeScan clients if all policy criteria are matched (see *Instructing the Policy Server and the OfficeScan client to carry out actions* on page C-9 for explanations of these actions):
- **Enable client Real-time scan**
  - **Update components**
  - **Scan after Real-time scan is enabled or manual update is performed**
    - **Perform Cleanup Now and Scan Now**
    - **Perform Cleanup Now**
  - **Display notification message on client desktop**
9. Click **Save**.

---

**Note:** Only one policy can be associated with an OfficeScan server at one time. You can assign one policy when the network is in normal mode and another when the network is in Outbreak mode (see *Adding or editing OfficeScan servers* on page D-20 and *Using Outbreak Prevention* on page 6-2 for more information).

---

## Using the 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 C-5).

---

**Note:** To be able to view client validation logs, enable Policy Server to log client validations when adding or editing a new rule/policy by selecting the check box under **Server-side actions** (see *Adding or editing a rule* on page D-22 and *Adding or editing a policy* on page D-24).

---

## Viewing client validation logs

The Policy Server saves client validation logs as .CSV files. Open the log files in a spreadsheet application.

### To view and save client validation logs:

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for all Policy Servers.
2. Click the server name of the Policy Server whose details you want to view.
3. On the sidebar, click **Logs > View Client Validation Logs**. The **View Client Validation Logs** screen appears showing a list of logs sorted in ascending order by date.
4. To view a log, click a date entry.

## Configuring client log maintenance

The Policy Server archives client validation logs when they reach a size you specify. Policy Server deletes archived client validation logs after a specified number accumulates. Specify the way that the Policy Server maintains client validation logs.

### To configure log maintenance:

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for all Policy Servers.
2. Click the server name of the Policy Server whose details you want to view.
3. On the sidebar, click **Logs > Log Maintenance**. The **Log Maintenance** screen appears.
4. Next to **Log format**, click the type of format you want the Policy Server to record:
  - **Simple:**
    - Time of the validation
    - Client IP address
    - Validation result
  - **Detailed:**
    - Time of the validation
    - Client IP address
    - Validation result
    - Client Real-time scan service status
    - Client scan engine version
    - Client virus pattern version
    - Client virus pattern release date
    - OfficeScan server location
    - Policy matched
    - Rule matched
    - Server scan engine version
    - Server virus pattern version

- Server virus pattern release date
- 5. Type the maximum size (between 1 and 1024 Mb) for each log. The Policy Server creates a new log file when the maximum size is reached.
- 6. Type the number of log files (between 2 and 30) for the Policy Server to maintain.
- 7. Click **Save**.

## Performing administrative tasks

Perform the following administrative tasks on the Policy Server:

- Change password – change the password configured when adding the Policy Server (see *Adding and removing Policy Servers* on page D-17)
- Configure a synchronization schedule – set a schedule to synchronize registered OfficeScan servers with the Policy Server

## Changing passwords

Password authentication is required to log on to the Policy Server. Use the **Change Password** screen to change passwords.

### To change the Policy Server password:

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for all Policy Servers.
2. Click the server name of the Policy Server whose details you want to view.
3. On the sidebar, click **Administration > Change Password**. The **Change Password** screen appears.
4. Type the existing password created while configuring the Policy Server.
5. Type the new password.
6. Type the new password again to confirm.
7. Click **Save**.

## Configuring scheduled synchronization

The Policy Server needs to periodically obtain the version of the virus pattern file and 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 [Understanding Synchronization](#) on page C-14 for more information).

---

**Note:** You can manually synchronize the Policy Server at any time on the **Summary** screen (see [Viewing summary information for a Policy Server](#) on page D-18).

---

### To set a schedule for synchronizing the servers:

1. On the sidebar of the OfficeScan Web console, click **Cisco NAC > Policy Servers**. The **Policy Servers** screen appears displaying a list of server names (IP addresses or Fully Qualified Domain Names) for all Policy Servers.
2. Click the server name of the Policy Server whose details you want to view.
3. On the sidebar, click **Administration > Scheduled Synchronization**. The **Scheduled Synchronization** screen appears.
4. Type the number of minutes (between 3 and 1440 minutes) to set the time interval for the scheduled synchronization.
5. Click **Save**.



## Configuring OfficeScan with Add-ons and Third-party Software

This appendix describes how to install and use Windows Protection Manager to help manage your OfficeScan for Wireless files and Check Point™ SecureClient™ to verify the security configuration of your clients.

Topics discussed in this appendix include:

- *About Wireless Protection Manager* on page E-2
- *Installing Wireless Protection Manager* on page E-3
- *Using Wireless Protection Manager* on page E-5
- *Overview of Check Point Firewall Architecture and Configuration* on page E-9
- *Configuring Check Point for OfficeScan* on page E-11
- *Installing SecureClient Support on the OfficeScan Client* on page E-12



## About Wireless Protection Manager

As personal digital assistants (PDAs) and other handheld computing devices increase the number of ways for communicating with other devices, the chances of becoming infected also increase. These days, it is common for PDAs to feature Internet connectivity.

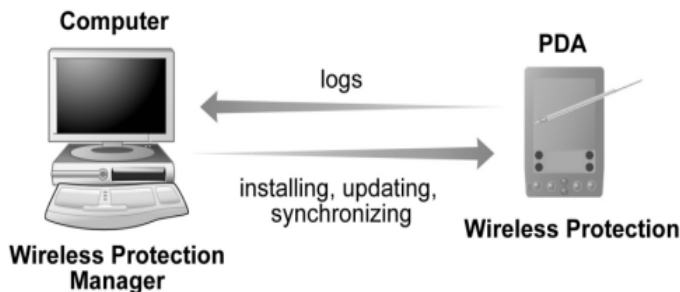
---

**Note:** In this manual, the term "PDA" is used to describe personal digital assistants and other handheld computing devices.

---

OfficeScan for Wireless provides portable, easy-to-use virus protection for wireless devices to defend against potential threats. Malicious code or other threats specifically designed for portable platforms can enter your Palm, Pocket PC, or EPOC device during beaming, synchronization, or Internet access.

You need to install Wireless Protection Manager on your desktop or laptop PC to help manage OfficeScan for Wireless files that are installed, synchronized, or updated on your PDA device. It also receives information in the form of logs from the PDA devices.



**FIGURE E-1 Relationship between Wireless Protection Manager on your computer and wireless protection on your PDA**

---

**Note:** Wireless Protection Manager does not provide any virus protection for your desktop or laptop PC.

---

## PDA system requirements

Your PDA requires the following to run Trend Micro OfficeScan for Wireless.

### Palm

- Palm™ OS 3.x or 4.x
- 2MB of memory
- 100KB of available memory for program installation
- Desktop computer must have Palm Desktop™ 3.1 or above and HotSync™ applications

### Pocket PC

- Windows CE 3.0
- 16MB of RAM
- 1MB of available memory for program installation
- Desktop computer must have Microsoft ActiveSync™ 3.1 or above application

### EPOC

- Psion Revo™ or Revo™ Plus
- 8MB of RAM
- 200KB of available memory for program installation
- Desktop computer must have PsiWin 2.3.2 application

## Installing Wireless Protection Manager

You need to install the following to provide virus protection on your PDA.

- Wireless Protection Manager on your computer
- OfficeScan for Wireless on your PDA

Before you install Wireless Protection Manager, make sure you have already installed your synchronization software (for example, Palm Desktop) and your PDA is firmly and correctly seated in its cradle.

**To install Wireless Protection Manager:**

1. In the system tray, right-click the OfficeScan Client icon, and then click **OfficeScan Main**. The OfficeScan client window appears.
2. Under the **Toolbox** tab, click **Install/Upgrade Wireless Protection**. A message box appears. Click **Yes** to install. The setup wizard appears.
3. Click **Next**. The **License Agreement** screen appears.
4. Click **I accept the terms in the license agreement**, and then click **Next**. You must agree to continue installation. The **Customer Information** screen appears.
5. Make sure the information is correct, and then click **Next**. The **Destination Folder** screen appears. You can choose where to install Wireless Protection Manager or use the default location. To change the location click **Change**, and then browse to the desired location.
6. Click **Next**. Select the check box of the platform of your PDA, depending on the synchronization software you have already installed (for example, Palm Desktop).
7. Click **Next**, and then click **Install**.
8. Click **Finish**.

After you have chosen the synchronization software platform and installed Wireless Protection Manager on your computer, OfficeScan for Wireless is automatically installed on your PDA.

---

**Note:** For Palm OS-based PDAs, the next time you perform a HotSync, OfficeScan for Wireless is installed on your PDA. In addition, after installing OfficeScan for Wireless, you need to manually close and re-open HotSync Manager. Reloading HotSync Manager is needed to successfully obtain virus logs from Palm OS-based devices.

---

## Using Wireless Protection Manager

Use Wireless Protection Manager to update your pattern file and scan engine on PDAs. You can specify the download location to get the update components, set proxy settings, and synchronize files between the main program and the files on your PDA.

### Opening Wireless Protection Manager

After you have installed Wireless Protection Manager, you need to open it to access the functions.

**To open Wireless Protection Manager:**

### Updating OfficeScan for Wireless

To protect your PDA against the latest threats, you need to update your scan engine and virus pattern files. Although all components can be updated, new pattern files are released on at least a weekly basis. Updating your pattern file provides you with the most up-to-date protection and lets OfficeScan for Wireless scan for the latest viruses or other malicious programs.

Trend Micro recommends regular updates to your virus pattern file to maintain a high-level of virus protection.

In addition, as new viruses are discovered and existing ones evolve, it becomes necessary to update certain program files and add new functionality to the scan engine. Updating your scan engine ensures OfficeScan for Wireless can act on the new instructions in the virus pattern to detect and remove viruses.

Updating your wireless protection involves the following steps:

1. Manually downloading the files from either the Trend Micro ActiveUpdate Server or another specified source
2. Synchronizing the files with your PDA

## Downloading update components

You need to download the update components from the Trend Micro ActiveUpdate Server or another specified update source. These components include the virus pattern file, scan engine, and other program files.

To ensure you have the latest Trend Micro virus protection technology, you need to keep your files updated.

### To download update components:

1. Open Wireless Protection Manager.
2. Click the **Manual Update** tab.
3. Under **Component Download Source**, confirm the update source is correct. If not, do one of the following:
  - Click **Trend Micro ActiveUpdate Server** to download from Trend Micro
4. Click **Other source** to download from another specified location.
5. Click **Update Now**.

## Enabling and configuring proxy settings

If you use a proxy server on your network, you need to type the IP address and port number of this proxy server. You may also need to supply the appropriate logon credentials.

### To enable and configure proxy settings:

1. Open Wireless Protection Manager.
2. On the menu bar, click **Option > Proxy Settings**. The **Proxy Settings** window appears.
3. Under **Proxy server**, select the **Use a proxy server...** check box.
4. In **Host name**, type the IP address or name of the proxy server (for example, proxy.yourcompany.com).
5. In **Port**, type the port number of the proxy server (for example, 80).
6. In **Protocol**, click the protocol your proxy server uses (**HTTP** or **SOCKS**).

7. Under **Authentication**, in **User name** and **Password**, type your proxy server logon credentials.
8. Click **OK**.

## Synchronizing with Your PDA

To make sure the latest update components are on your PDA, you need to synchronize the updated files on your computer with your PDA.

Before manually synchronizing through Wireless Protection Manager, please do the following:

- Make sure your PDA is firmly and correctly seated in its the cradle
- Close any antivirus software running on your PDA

---

**Note:** This function currently only works with PDAs running on Pocket PC and EPOC platforms. For Palm-based PDAs, you need to manually synchronize using the Palm HotSync function.

---

### To synchronize with your PDA:

1. Open Wireless Protection Manager.
2. Click the **Manual Synchronize** tab.
3. Click **Synchronize**.

## Working with logs

All virus events are recorded as log entries. Log entries contain useful information about virus events that have occurred including the type of virus scan, the date and time the virus was detected, the file and virus name, and the performed action.

### Viewing logs

If you have detected a virus, view virus logs stored on Wireless Protection Manager to get more information. Before you view logs, remember to synchronize Wireless Protection Manager with your PDA to make sure you are viewing the most updated logs.

**To view logs:**

1. Open Wireless Protection Manager.
2. Click the **Virus Log** tab.
3. Under **Select log range**, select the PDA type check box for the log you want to view.
4. Do the following:
  - To view all logs, in the **Log for** list select **All dates**.
  - To view logs within a specific date range, in the **Log for** list select **Specified date range**, and choose the date range.
5. Click **View Log**.

## Managing logs on your PDA

The virus log stores information about viruses detected during previous scans and the actions taken against them.

To view the log, tap **Log** on the main screen of your PDA.

The **Virus Scan Log** screen displays information about detected viruses as well as the size of the log in bytes. Tap **Back** to return to the main screen.

To delete the log entries, tap **Clear Log**. A message box appears to confirm log deletion. Tap **Yes** to remove log entries, or **No** to abort the operation.

## Deleting logs

Delete Wireless Protection Manager log entries if the information they provide is no longer useful. If the number of logs is taking up too much disk space, you may also want to delete log entries for certain dates.

**To delete logs:**

1. Open Wireless Protection Manager.
2. Click the **Virus Log** tab.
3. Under **Delete logs manually**, in the **Delete logs before** list, select a date.
4. Click **Delete Log**. A confirmation message appears. Click **Yes** to delete all logs before and including the date you selected.

## Overview of Check Point Firewall Architecture and Configuration

OfficeScan installations can be fully integrated 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](http://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 [Configuring Check Point for OfficeScan](#) on page E-11.

## Integrating with OfficeScan

OfficeScan client periodically passes the virus pattern file number and 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 will be blocked. These values are modified 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.

---

## Configuring Check Point for OfficeScan

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](http://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 E-1 lists the parameter names and values. Parameter names and values are case-sensitive, and must be typed in the order given in Table E-1

Name	Value
CheckType	OfceVersionCheck
LatestPatternVersion	{current pattern file number}
LatestEngineVersion	{current scan engine number}
LatestPatternDate	{current pattern file release date}
PatternCompareOp	>=
EngineCompareOp	>=
PatternMismatchMessage	
EngineMismatchMessage	


**TABLE E-1. SCV file parameter names and values**

Type the most current pattern file number and scan engine number in place of the text in curly braces in Table E-1. You can view the latest virus pattern and scan engine versions for clients by clicking **Update & Upgrade** on the sidebar 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.

## Installing SecureClient Support on the OfficeScan Client

If you have users that connect to the office network via 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**.



## Glossary of Terms

The following is a list of terms in this document:

Term	Description
<b>Access Control Server (ACS)</b>	Passes authentication requests from the Network Access Device to the Policy Server in order to validate end-user client security posture. The ACS server also passes the posture token from the Policy Server to the Network Access Device. The ACS server can also be configured to carry out actions on the end-user client via the Network Access Device.
<b>ACS certificate</b>	Used to establish trusted communication between the ACS server and the Certificate Authority (CA) server. The Certificate Authority server signs the ACS certificate, and it is saved on the ACS server.
<b>ActiveX malicious code</b>	A type of virus that resides in Web pages that execute ActiveX controls.
<b>Additional Threats</b>	Files and programs, other than viruses, that can negatively affect the performance of the computers on your network. These include spyware, adware, dialers, joke programs, hacking tools, remote access tools, password cracking applications, and others. The OfficeScan scan engine scans for Additional Threats (including adware, spyware, keyloggers, and dialers) as well as viruses.
<b>Adware</b>	Similar to spyware, adware gathers user data, such as Web surfing preferences, that could be used for advertising purposes.

Term	Description
<b>Authentication, Authorization, and Accounting (AAA)</b>	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.
<b>Boot sector viruses</b>	A type of virus that infects the boot sector of a partition or a disk.
<b>CA certificate</b>	Used for authentication of end-user clients with the Cisco ACS server. The CA certificate is deployed to both the ACS server and to clients (packaged with the Cisco Trust Agent by the OfficeScan server).
<b>Certificate Authority (CA)</b>	An authority on a network that distributes digital certificates for the purposes of performing authentication and securing connections between computers and/or servers.
<b>Cisco Trust Agent (CTA)</b>	Installed on end-user client computers to allow communication of security posture to Cisco Network Access Devices. The agent can be deployed to OfficeScan clients from the OfficeScan Web console.
<b>Client validation</b>	The process of having a Cisco NAC Policy Server evaluate an OfficeScan client's security posture and sending a posture token back to the client.
<b>COM and EXE file infectors</b>	A type of virus that masquerades as an application by using a .exe or .com file extension.
<b>Control Manager Agent</b>	Installed on OfficeScan server to register with the Control Manager server. This allows administration of OfficeScan through the Control Manager management console.
<b>Dialers</b>	Software that changes client Internet settings and can force the client to dial pre-configured phone numbers through a modem.
<b>Digital Certificates</b>	An attachment that is 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.
<b>Dynamic Host Control Protocol (DHCP)</b>	A device, such as a computer or switch, must have an IP address to be connected 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.
<b>Dynamic IP Address (DIP)</b>	A Dynamic IP address is an IP address that is assigned by a DHCP server. The MAC address of a computer will remain the same, however, the computer may be assigned a new IP address by the DHCP server depending on availability.

<b>Term</b>	<b>Description</b>
<b>File Transfer Protocol (FTP)</b>	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.
<b>Hacking tools</b>	Tools used to help hackers enter computers, often through empty ports.
<b>Hyper Text Transfer Protocol (HTTP)</b>	HTTP is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet.
<b>HTML, VBScript, or JavaScript viruses</b>	Viruses that reside in Web pages and are downloaded through a browser.
<b>HTTPS</b>	Hypertext Transfer Protocol using Secure Socket Layer (SSL).
<b>Internet Control Message Protocol (ICMP)</b>	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 must be 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.
<b>Internet Protocol (IP)</b>	"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)
<b>Intrusion Detection System (IDS)</b>	Intrusion Detection Systems are commonly part of firewalls. An IDS can help identify patterns in network packets that may indicate an attack on the client.
<b>Java malicious code</b>	Operating system-independent virus code written or embedded in Java.
<b>Joke program</b>	Software that causes a computer to behave abnormally, such as forcing the screen to shake.
<b>Keylogger</b>	A program that captures and stores a history of keystrokes and mouse clicks, potentially without the user's knowledge.
<b>Macro viruses</b>	A type of virus encoded in an application macro and often included in a document.
<b>Network Access Device</b>	Network access servers, firewalls, routers, switches, or wireless access points that support Cisco NAC functionality.



Term	Description
<b>Network virus</b>	Viruses that 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 computers, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure.
<b>Password cracking applications</b>	Software that can help hackers decipher user names and passwords.
<b>Phish sites</b>	A Web site that lures users into providing personal details, such as credit card information. Links to phish sites are often sent in bogus email messages disguised as legitimate messages from well-known businesses.
<b>Ping</b>	A utility that sends an ICMP echo request to an IP address and waits for a response. The Ping utility can determine if the machine with the specified IP address is online or not.
<b>Policy Server</b>	The server responsible for the determination of the posture token of end-user clients by periodically uploading current antivirus pattern file and scan engine version information from the OfficeScan servers on the network. Install Policy Server from the OfficeScan master installer or from the Enterprise CD.
<b>Policy Server policy</b>	Comprised of rules, policies are used by the Policy Server to measure end-user client security posture. One policy is assigned to each registered OfficeScan server on the network.
<b>Policy Server rule</b>	Rules are comprised of specific criteria that Policy Servers use to compare with OfficeScan client security posture data. If any aspect of client security posture matches the criteria you configure in a rule, the client can carry out actions you specify.
<b>Policy Server SSL certificate</b>	Used to ensure secure HTTPS communication between the Policy Server and ACS server. The Policy Server SSL certificate is automatically generated during Policy Server installation.
<b>Post Office Protocol 3 (POP3)</b>	POP3 is a standard protocol for storing and transporting email messages from a server to a client email application.
<b>Posture token</b>	The Policy Server creates the posture token after end-user 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.
<b>Remote access tools</b>	Tools used to help hackers remotely access and control a computer.
<b>Remote Authentication Dial-In User Service (RADIUS)</b>	An authentication system requiring clients to enter a user name and password. Cisco Secure ACS servers support RADIUS.

Term	Description
<b>Secure Socket Layer (SSL)</b>	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.
<b>SSL certificate</b>	A digital certificate that establishes secure HTTPS communication between the Policy Server and the ACS server.
<b>Security posture</b>	The presence and currency of antivirus software installed on an end-user client. The security posture of OfficeScan clients refers to if the OfficeScan client program is installed and how old the antivirus component versions are.
<b>Simple Mail Transport Protocol (SMTP)</b>	SMTP is a standard protocol used to transport email messages from server to server, and client to server, over the internet.
<b>SOCKS 4</b>	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.
<b>Spyware</b>	Software that installs components on a computer for the purpose of recording Web surfing habits (primarily for marketing purposes). Spyware sends this information to its author or to other interested parties when the computer is online. Spyware often downloads with items identified as 'free downloads' and does not notify the user of its existence or ask for permission to install the components. The information spyware components gather can include user keystrokes, which means that private information such as login names, passwords, and credit card numbers are vulnerable to theft.
<b>Stateful inspection firewall</b>	Stateful inspection firewalls monitor all connections to a client and remember all connection states. They can identify specific conditions in any connection, predict what actions should follow, and detect when normal conditions are violated. This significantly increases the chances that a firewall can detect an attack on a client.
<b>Telnet</b>	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.
<b>Terminal Access Controller Access Control System (TACACS+)</b>	A security protocol enabled through AAA commands used for authenticating end-user clients. Cisco ACS servers support TACACS+.
<b>Test file</b>	An inert file that acts like a real virus and is detectable by virus-scanning software. Use test files, such as the EICAR test script, to verify that your antivirus installation is scanning properly (see <a href="#">Testing the client installation with the EICAR test script</a> on page 3-37).

Term	Description
<b>Transmission Control Protocol (TCP)</b>	A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.
<b>TrendLabs</b>	TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.
<b>Trojan horses</b>	Executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter.
<b>User Datagram Protocol (UDP)</b>	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.
<b>Virus</b>	A virus is a program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes (see <a href="#">Understanding viruses</a> on page 1-4 for more detailed information).
<b>Worm</b>	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email. A worm can also be called a network virus.

# Index

## A

- Access Control Server (ACS) D-15
  - definition F-1
  - enrolling D-3
- ACS certificate D-3
  - definition F-1
- ActiveAction 1-13
- ActiveX 1-1, 1-4
  - definition F-1
- adding a domain 4-12
- Additional Threats 1-13
  - definition F-1
  - pattern file 1-5
- administrative tasks 5-1
- administrative tools 4-7, A-2
- adware 1-5, 1-14
  - definition F-1
- agents
  - Cisco Trust Agent (CTA) D-11
  - Control Manager F-2
  - Update Agent 4-17
- antivirus policy
  - enforcing 1-9
- Authentication, Authorization, and Accounting (AAA)
  - definition F-2
- automatic client migration 3-42
- Automatic Deployment 4-21
- automatic updates
  - client 4-21

## B

- blocking
  - ports 6-3
  - shared folders 6-2
- boot sector viruses 1-4
  - definition F-2

## C

- CA certificate C-16
  - definition F-2
  - exporting and installing D-7
- Certificate Authority (CA)
  - definition F-2
- certificates C-14
  - ACS D-3
  - CA C-16, D-7
  - Policy Server SSL D-9
- Cisco NAC 1-3, 4-5
- Cisco router models C-18
- Cisco Trust Agent (CTA) 1-6, D-11
  - definition F-2
  - deployment 4-5
  - system requirements for Windows NT/2000 C-17
  - system requirements for Windows XP C-18
- Cleanup Now 4-4, 6-11
- client alert messages 4-6
  - modifying 5-2
- client certificate
  - importing to the OfficeScan server 4-5
- client disk image 3-21
- client installation 3-20
  - client disk image 3-29
  - Client Packager 3-25
  - internal Web page 3-22
  - Login Script Setup 3-23
  - Microsoft System Management Server (SMS) 3-31
  - testing with the EICAR test script 3-37
  - verifying 3-35
  - vulnerability scanner 3-30
  - Windows remote install 3-28
- client installation path 3-5
- client notification for outbreaks 6-7
- Client Packager 3-20, A-10
- client tools 4-7, A-10
- Client validation
  - definition F-2
- clients 1-17

- classifications 1-17
  - disconnected 1-18
  - generating network traffic 2-4
  - granting privileges
    - client privileges 4-43
  - Image Setup Utility A-11
  - importing and exporting scan and privilege settings 4-44
  - installation path 3-5
  - installing 3-20
  - managing 1-10
  - migration 3-42
  - normal 1-18
  - privileges 4-4
  - removing 3-38
  - removing inactive 5-4
  - removing using Uninstall Now 3-38
  - roaming 1-19
  - searching for 4-10
  - security 1-3
  - Update Agent 4-17
  - update logs 8-4
  - updating 4-20
  - verifying migration 3-44
  - viewing status 4-5
  - virus alert 3-5
  - COM and EXE file infectors 1-4
    - definition F-2
  - common firewall driver 1-6
  - component license
    - activating 3-13
    - viewing information 3-13
  - components 1-5
    - rolling back 4-7, 4-25
    - updating 4-13
  - conducting a pilot deployment 3-13
  - configuring
    - ACS server D-15
    - client notification for outbreaks 6-7
    - Firewall Outbreak Monitor 7-16
    - Internet proxy settings 4-17
    - Manual Scan 4-32
    - outbreak alerts 4-29
    - outbreak notifications 6-7
    - Policy Server for Cisco NAC D-16
    - Quarantine Manager 5-5
    - Real-time Scan 4-34
    - Scan Now 4-40
    - scan settings 4-31
    - Scheduled Scan 4-36
    - standard alerts 4-27
  - Contacting Trend Micro 9-10
  - Control Manager B-2
    - accessing the OfficeScan server B-7
    - agent B-3
    - capabilities with OfficeScan B-2
    - installing the agent B-4
    - introduction B-2
    - public encryption key B-4
  - Control Manager agent
    - definition F-2
    - installation B-4
    - removing B-7
    - required information B-3
    - requirements B-3
  - controlling
    - virus outbreaks 1-10
- ## D
- Damage cleanup engine 1-5
  - Damage Cleanup Services 1-14, 4-4, 6-10–6-11
  - Damage cleanup template 1-5
  - Database Backup A-3
  - dedicated server 2-5
  - deleting a domain 4-13
  - denying write access to files and folders 6-6
  - deployment
    - Cisco Trust Agent (CTA) 4-5
    - OfficeScan methods 2-2
    - pilot 3-13
  - dialers 1-5, 1-14
    - definition F-2
  - digital certificates
    - definition F-2
  - documentation 1-20
  - domain
    - adding 4-12
    - creating 4-9
    - deleting 4-13
    - managing 1-10

- moving clients from 4-12
  - renaming 4-13
  - selecting from 4-9
  - working with 4-12
- domain tree 4-8
  - icons 4-11
  - refreshing 4-11
  - selecting from 4-9
- Dynamic Host Control Protocol (DHCP)
  - definition F-2
- Dynamic IP Address (DIP)
  - definition F-2
- E**
- EICAR
  - test file URL 3-38
  - URL 3-37
- enrolling the Cisco Secure ACS server D-3
- Enterprise Client Firewall 1-2, 4-5, 8-6
  - configuration 7-11
  - configuring Firewall Outbreak Monitor 7-16
  - default policies 7-4
  - defaults 7-4
  - deploying 7-7
  - disabling 7-17
  - features 7-6
  - Firewall Outbreak Monitor 7-7
  - Intrusion Detection System 7-7
  - logs 4-7, 8-6
  - policies, exceptions, and profiles 7-2
  - policy list 4-5
  - profile list 4-5
  - stateful inspection 7-6
  - understanding 7-2
  - verifying deployment 7-10
- European Institute for Computer Antivirus Research—see EICAR 3-37
- events 1-17
- excluding files and folders from scanning 4-39
- exporting and importing scan settings 4-4
- F**
- File Transfer Protocol (FTP)
  - definition F-3
- file-based server 1-17
- Firewall Outbreak Monitor 4-5, 7-7
  - configuring 7-16
  - full pattern file 2-5
- G**
- global client settings 4-5
- Glossary F-1
- Glossary of Security Threat Terms 9-10
- granting privileges to clients 4-43
- GUID 3-29
- H**
- hacking attacks 3-5
- Hacking tools
  - definition F-3
- hacking tools 1-14
- HTML, VBScript, or JavaScript viruses 1-4, F-3
- HTTP 1-16
  - communication 3-5
- HTTPS
  - definition F-3
- Hyper Text Transfer Protocol (HTTP) 1-16
  - definition F-3
- I**
- icons
  - domain tree 4-11
  - normal client 1-18
  - roaming client 1-19
- ICSA Certification 1-8
- Image Setup Utility A-11
- importing and exporting client scan and privilege settings 4-44
- inactive clients 4-6
  - removing 5-4
- incremental update 2-5
- infected files
  - sending to the quarantine folder 1-10
- installation and deployment 2-2
- installing
  - clients 3-20–3-34
  - Control Manager agent B-4
  - OfficeScan Clients 3-19
  - OfficeScan Server 3-2
  - Policy Server for Cisco NAC D-13
  - remote install 4-5

- IntelliScan 1-12
- internal Web page 3-20
- Internet 1-16
- Internet Control Message Protocol (ICMP)
  - definition F-3
- Internet Information Server (IIS) 1-16
- Internet Protocol (IP)
  - definition F-3
- Internet proxy
  - configuring settings 4-17
- intranet proxy 4-6
  - configuring 5-3
- Intrusion Detection System (IDS) 7-7
  - definition F-3
- ISO 9002 Certification-see TrendLabs 9-14

## **J**

- Java
  - applet 1-1
  - malicious code 1-4
    - definition F-3
- joke program 1-14
  - definition F-3

## **K**

- keylogger
  - definition F-3
- Knowledge Base 1-21, 4-8, 9-12
  - URL 1-21
- Known Issues
  - URL for Knowledge Base describing 9-11
  - URL for readme documents describing 9-11
- known issues with OfficeScan 9-11

## **L**

- local.scv E-9
- logging off 4-8
- Login Script Setup 3-20, 3-23, A-4
- logs 4-7
  - client update 8-4
  - Enterprise Client Firewall 4-7
  - maintaining 4-7
  - managing 8-7
  - Policy Server client validation D-26
  - server update 8-4
  - system event 4-7, 8-5

- update 4-7
- verify connection 4-7, 8-6
- viewing 8-2
- virus 4-7, 8-2

## **M**

- macro viruses 1-4
  - definition F-3
- management console
  - functions 1-20
- managing
  - domains and clients 1-10
- Manual Deployment 4-22
- Manual Outbreak Prevention 4-6
  - configuring outbreak notifications 6-7
- Manual Scan 4-32, 4-36
- manual update
  - client 4-22
  - server 4-16
- master installer 3-6
- master setup 3-6
  - client installation path 3-5
  - proxy information 3-5
  - required
    - protocols 3-3
    - restarts 3-4
  - required information 3-4
  - required rights 3-3
  - virus alert message 3-5
  - Windows licenses 3-5
- Microsoft SMS 3-31
- Microsoft System Management Server (SMS) 3-21
- migrating to and upgrading OfficeScan 3-40
- moving clients from a domain 4-12

## **N**

- Network Access Device (NAD)
  - definition F-3
- network traffic
  - pattern updates 2-5
  - planning for 2-4
  - server 2-4
- network virus 1-4
  - definition F-4
- network virus pattern file 1-6

- normal clients 1-18
- notifications
  - standard 4-26
- notify install
  - notifying clients to install 4-5
- O**
- OfficeScan
  - benefits and capabilities 1-12
  - client 1-17
  - domain 4-9
  - integrating with SecureClient E-9
  - management console 1-20
  - server 1-15
- OfficeScan client program 1-5
  - uninstalling 4-4
- OfficeScan for Wireless 1-11
- OfficeScan server
  - architecture 1-15
  - default settings 3-14
  - preparing for installation 3-3
  - synchronizing with Policy Server C-14
  - viewing summary information 4-4
- online help 1-20
- Outbreak alert 4-6
  - configuring 4-29
  - email 4-29
  - pager 4-30
  - SNMP Trap 4-30
  - Windows NT Event Log 4-31
- Outbreak Prevention 1-12, 6-2
  - applying 4-4
  - blocking ports 6-3
  - denying write access to files and folders 6-6
  - restoring network settings to normal 6-8
  - shared folder blocking 6-2
- outbreaks
  - controlling 1-10
- P**
- Package Description File (PDF) 3-31
- password
  - changing Policy Server D-28
  - changing Web console 5-2
  - setting 4-6
  - Web console 3-5
- Password cracking applications
  - definition F-4
- password cracking applications 1-14
- pattern file
  - compressed 2-5
  - extracted 2-5
  - full 2-5
  - incremental update 2-5
  - numbering 1-7
  - updates and network traffic 2-5
- PDA
  - protecting 1-11
- performing scans 1-10
- Phish sites
  - definition F-4
- pilot deployment 2-6, 3-13
- Ping
  - definition F-4
- planning
  - network traffic 2-4
- Policy Server 4-5
  - changing passwords D-28
  - client validation logs D-26
  - configuring D-16
  - configuring policies D-22, D-24
  - configuring synchronization D-29
  - definition F-4
  - enrolling the Cisco Secure ACS server D-3
  - policy definition F-4
  - rule definition F-4
  - SSL certificate D-9
    - definition F-4
  - supported Cisco routers C-18
  - synchronizing with OfficeScan server C-14
  - system requirements C-16
  - viewing client validation logs D-26
  - Web console system requirements C-17
- Policy Server for Cisco NAC
  - ACS certificate D-3
  - administrative tasks D-28
  - CA certificate C-16, D-7
  - certificates C-14
  - changing passwords D-28
  - Cisco Trust Agent (CTA) D-11



- client validation process C-5
- configuring ACS server D-15
- configuring policies D-24
- configuring Policy Server D-16
- configuring rules D-22
- configuring synchronization D-29
- default policies C-13
- default rules C-10
- deployment overview D-2
- enrolling the ACS server D-3
- policies and rules C-8
- policy composition C-12
- Policy Server installation D-13
- Policy Server SSL certificate D-9
- rule composition C-8
- synchronizing the Policy Server and OfficeScan Server C-14
- understanding Policy Server C-7
- viewing client validation logs D-26
- Policy Servers for SecureClient E-9
- Post Office Protocol 3 (POP3)
  - definition F-4
- product license
  - license 4-6
- Product Registration proxy 3-14
- protection
  - analyzing using logs 1-9
  - updating 1-10
- protocols 3-3
- proxy information 3-5
- public encryption key for Control Manager B-4

## Q

- Quarantine Manager 4-6, 5-5

## R

- readme file 1-21
- Real-time Scan 4-34
- Registering OfficeScan 3-6
- Remote access tools
  - definition F-4
- remote access tools 1-14
- Remote Authentication Dial-In User Service (RADIUS)
  - definition F-4

- remote install
  - installing 4-5
- removing
  - clients 3-38
  - Control Manager agent B-7
  - inactive clients 5-4
- renaming a domain 4-13
- required
  - rights 3-3
- required protocols 3-3
- required restarts 3-4
- requirements
  - Policy Server Web console C-17
  - server 3-2
  - Web console 3-3
- Restore 4-4
- Restore Encrypted Files A-11
- restoring network settings to normal 6-8
- Risk Ratings
  - Security Information Center 9-10
- roaming clients 1-19
  - privileges 1-19
  - updating 1-19
- rolling back components 4-7, 4-25
  - creating a plan 2-7

## S

- Safe Computing Guide 9-10
- scan engine 1-5, 1-7
  - events that trigger an update 1-8
  - ICSA certification 1-8
  - updating 1-8
  - URL to find current version 1-8
- Scan Now 4-4, 4-40
- scan options 4-4, 4-31
- scan settings
  - configuring 4-31
  - excluding files and folders 4-39
  - Manual Scan 4-32
  - Manual scan 4-36
  - Real-time Scan 4-34
  - Scan Now 4-40
  - Scheduled Scan 4-36
- scanning
  - excluding files and folders 4-39

- exporting and importing settings 4-4
  - from one location 1-10
  - Manual Scan 4-32
  - options 4-4
  - Real-time Scan 4-34
  - Scan Now 4-4, 4-40
  - scan settings 4-31
  - Scheduled Scan 4-36
  - Scheduled Scan 4-36
  - Scheduled Update
    - server updates 4-15
  - SCV Editor E-9
  - Secure Configuration Verification. *See* SCV
  - Secure Socket Layer (SSL) 1-15
    - definition F-5
  - secure Web console communication 1-15
  - SecureClient E-9
    - integrating with OfficeScan E-9
    - Policy Servers E-9
    - SCV Editor E-9
  - Security Information Center 9-10
    - EICAR test file 9-10
    - glossary of security threat terms 9-10
    - Risk Ratings 9-10
    - Safe Computing Guide 9-10
    - subscription service 9-11
    - TrendLabs 9-11
    - URL 9-10
    - Virus Alert 9-11
    - Virus Encyclopedia 9-10
    - Virus Map 9-10
    - Virus Primer 9-10
    - Webmaster tools 9-11
    - Weekly Virus Report 9-10
    - white papers 9-10
  - security posture
    - definition F-5
  - sending suspicious code to Trend Micro 9-12
  - server
    - administration 4-4
    - configuring automatic scheduled updates 4-15
    - dedicated 2-5
    - file-based 1-17
    - HTTP-based 1-16
    - network traffic 2-4
    - system requirements 3-2
    - update logs 8-4
    - updating 4-14
    - updating manually 4-16
    - upgrading from a previous version 3-15
    - upgrading from a trial version 3-17
  - server installation
    - verifying 3-13
  - Server Tuner A-9
  - Simple Mail Transport Protocol (SMTP)
    - definition F-5
  - single site deployment 2-4
  - SOCKS 4
    - definition F-5
  - SolutionBank-see Knowledge Base 1-21
  - spyware 1-5, 1-14
    - definition F-5
  - SSL 1-15
  - SSL certificate
    - definition F-5
  - standard alert 4-6
    - configuring 4-27
    - email 4-26–4-27
    - pager 4-28
    - SNMP Trap 4-28
  - standard notifications 4-26
  - stateful inspection firewall
    - definition F-5
  - Submission Wizard
    - URL 9-12
  - Subscription Service 9-11
  - synchronization
    - configuring Policy Server D-29
  - system event logs 4-7, 8-5
  - system requirements
    - Policy Server C-16
    - Win 2000/NT client 3-19
    - Windows 95/98/Me client 3-19
    - Windows XP/Server 2003 client 3-20
- T**
- TCP 3-5
  - TCP port 3-5
  - TCP/IP 1-16, 3-3
  - Technical support 9-1, 9-11

- Telnet
    - definition F-5
  - Terminal Access Controller Access Control System (TACACS+)
    - definition F-5
  - test file
    - definition F-5
  - testing
    - OfficeScan installation 3-37
    - with EICAR test script 3-37
  - tools 4-7
    - administrative 4-7, A-2
    - client 4-7, A-10
    - Client Mover I A-13
    - Client Packager A-10
    - Database Backup A-3
    - Image Setup Utility A-11
    - Login Script Setup A-4
    - previously supported A-15
    - Restore Encrypted Files A-11
    - Server Tuner A-9
    - Touch Tool A-14
    - Vulnerability Scanner A-4
  - Transmission Control Protocol (TCP)
    - definition F-6
  - Trend Micro
    - contact URL 9-10
    - contacting 9-10
  - Trend Micro System Cleaner-see Damage Cleanup Services 1-14
  - TrendLabs 9-11, 9-13
    - definition F-6
  - Trojan horses
    - definition F-6
  - Trojans 1-4, 6-10
    - symptoms of an attack 1-14
  - Troubleshooting 9-1
- U**
- Uninstall Now 3-38
  - uninstalling
    - client program 3-38
    - clients 4-4
    - Control Manager agent B-7
    - OfficeScan server 3-17
    - Update Agent 1-2, 4-17
    - update logs 4-7
    - Update Now 1-19, 4-23
    - update source 4-20
    - updating clients 4-7, 4-20
      - roaming clients 1-19
      - selecting client update source 4-20
    - Update Agent 4-17
      - using Automatic Deployment 4-21
      - using Manual Deployment 4-22
      - using Update Now 4-23
      - verifying 4-24
    - updating the server 4-14
      - using automatic scheduled update 4-15
      - using Manual Server Update 4-16
    - upgrading 3-15
      - from a previous version 3-15
      - from a trial version 3-17
      - verifying 3-17
  - URLs
    - Cisco NAC C-2
    - EICAR 3-37
    - EICAR test file 3-38
    - Knowledge Base 1-21, 9-12
    - Knowledge Base containing known issues 9-11
    - readme documents containing known issues 9-11
    - scan engine version 1-8
    - Security Information Center 9-10
    - Submission Wizard 9-12
    - Trend Micro 9-10
  - User Datagram Protocol (UDP)
    - definition F-6
- V**
- verify connection logs 4-7, 8-6
  - verifying
    - client migration 3-44
    - server installation 3-13
    - successful installation 3-35
    - updates 4-24
  - viewing
    - client status 4-5
    - client update logs 8-4
    - Enterprise Client Firewall logs 8-6
    - logs 8-2

- OfficeScan server summary information 4-4
- server update logs 8-4
- system event logs 8-5
- verify connection logs 8-6
- virus logs 8-2
- Virtual Private Network. *See* VPN
- virus
  - definition F-6
- virus alert message 3-5
- Virus Alert Service 9-11
- virus doctor-see TrendLabs 9-14
- Virus Encyclopedia 9-10
- virus logs 4-7, 8-2
- Virus Map 9-10
- Virus Outbreak Monitor 1-12, 4-4, 6-9
- virus pattern file 1-5–1-6
- Virus Primer 9-10
- viruses
  - "in the wild" 1-7
  - "in the zoo" 1-7
  - controlling outbreaks 1-10
  - scanning for 1-10
- VPN E-12
- Vulnerability Scanner 3-17, 3-44, A-4
  - installing with 3-21

## W

- Web console
  - domain tree 4-8
  - getting around 4-3
  - logging off 4-8
  - opening 4-2
  - other links 4-8
  - system requirements 3-3
  - updating 4-4
- Web server information
  - changing 5-4
- Webmaster Tools 9-11
- Weekly Virus Report 9-10
- White Papers 9-10
- Windows licenses 3-5
- Windows Remote Install 3-21
- Wireless Protection Manager 1-11
- World Virus Tracking Program 5-6
- worm 1-4

