

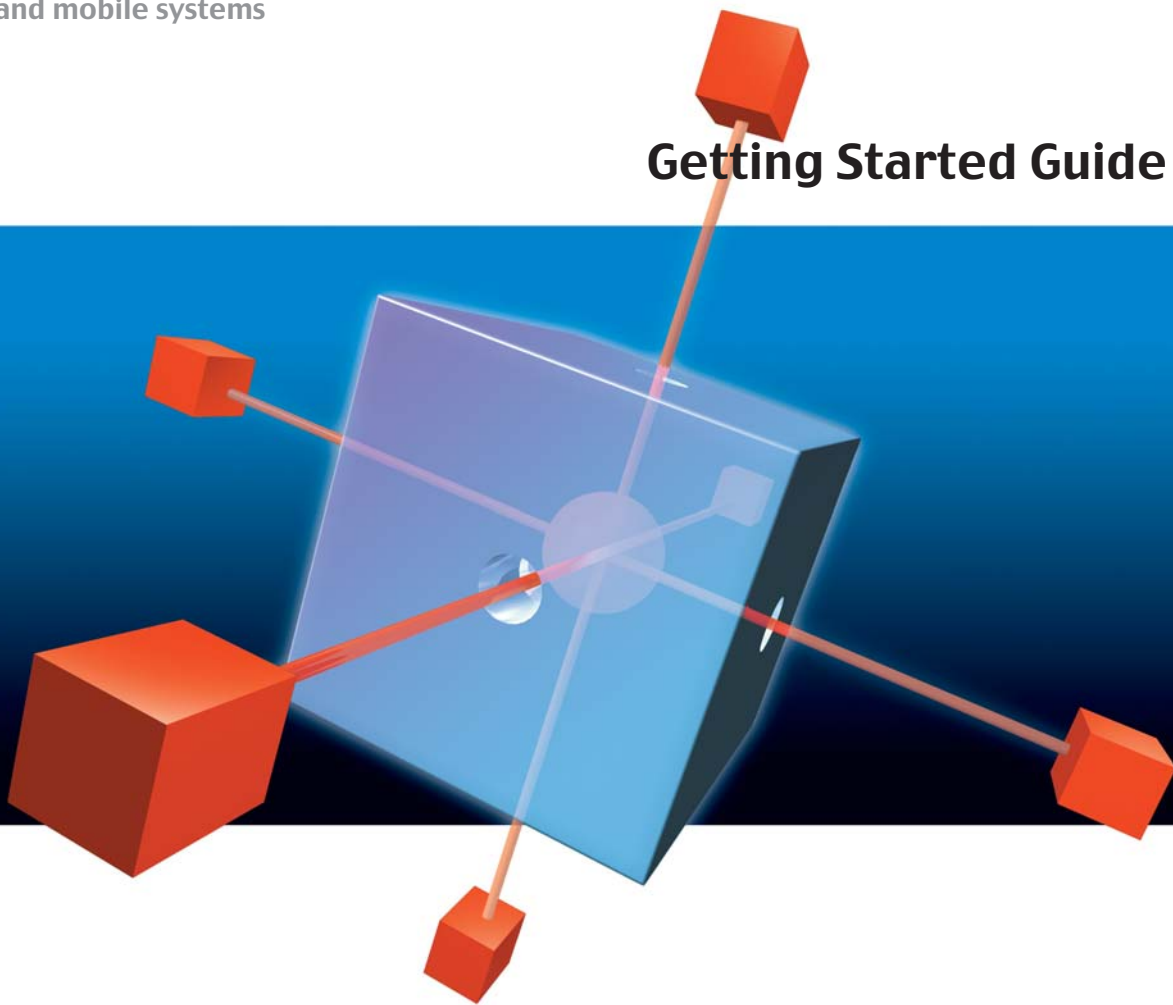
TREND MICRO™

# OfficeScan™

## Corporate Edition

Centrally managed virus protection for business desktop  
and mobile systems

### Getting Started 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 Getting Started Guide, which are available from the Trend Micro Update Center:

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

Select this product, then select the latest documents from User Guides.

NOTE: A license to Trend Micro antivirus software includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at the then-current Maintenance fees of Trend Micro to have the right to continue receiving these services.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

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

Trend Micro, OfficeScan, Control Manager, ServerProtect, TrendLabs, and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in certain jurisdictions.

This product includes software developed by the Apache Software Foundation ([www.apache.org/](http://www.apache.org/)). Copyright © 2003 The Apache Software Foundation. All rights reserved.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright © 1997-2003 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. OSEM51353/30109

Release Date: February 2003

Protected by U.S. Patent No. 5,951,698

The Getting Started 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 on the Trend Micro Web site.

At Trend Micro, we are always seeking to improve our 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 at the following site:

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

# Contents

## Chapter 1: Introducing OfficeScan Corporate Edition

What is OfficeScan Corporate Edition? .....	1-2
How does OfficeScan work? .....	1-2
Understanding the OfficeScan architecture .....	1-4
Compatibility with Control Manager .....	1-9
What you can do with OfficeScan .....	1-10
Enforce antivirus policies .....	1-10
Perform virus scans from one location .....	1-10
Quarantine infected files .....	1-10
Update your protection .....	1-11
Analyze your network's protection against viruses .....	1-11
Manage OfficeScan domains and clients .....	1-11
Control outbreaks on the network .....	1-11
Protect your PDAs from viruses .....	1-12
Getting started with OfficeScan .....	1-12
Phase 1 summary .....	1-13
Phase 2 summary .....	1-13
Phase 3 summary .....	1-14

## Chapter 2: Installing the Server

Planning for deployment .....	2-2
Planning for optimal client-server ratio .....	2-2
Planning for network traffic .....	2-4
Determining if you need to install a dedicated server .....	2-5
Conducting a pilot deployment .....	2-6
Choosing a pilot site .....	2-6
Creating a rollback plan .....	2-7
Deploying the pilot .....	2-7
Evaluating the pilot deployment .....	2-7
Minimum system requirements .....	2-7
Minimum system requirements for the Web console .....	2-7
Preparing for server installation .....	2-8
Where to run the setup program .....	2-8

Required protocols .....	2-9
Required rights .....	2-9
Required restarts .....	2-9
Required information .....	2-9
Shared directories .....	2-10
Windows licenses .....	2-10
TCP port for HTTP communication .....	2-10
Running master setup .....	2-11
Verifying a successful installation .....	2-14
Upgrading from a previous version .....	2-14
Upgrading HTTP-based OfficeScan .....	2-15
Upgrading file-based OfficeScan .....	2-16
Verifying the upgrade .....	2-19
Removing the server .....	2-20

## **Chapter 3: Rolling Out Clients**

Choosing a client installation method .....	3-2
Minimum system requirements .....	3-3
Windows Me/98/95 clients .....	3-3
Windows 2000/NT clients .....	3-3
Windows XP clients .....	3-4
Preparing for installation .....	3-4
Installing the client from an internal Web page .....	3-4
Installing the client with Login Script Setup .....	3-5
Windows 2000/NT scripts .....	3-7
Installing the client with Client Packager .....	3-9
Sending the package using the email function .....	3-12
Installing the client with Windows NT Remote Install .....	3-13
Installing the client from a disk image .....	3-14
Installing the client with NT Remote Install utility .....	3-15
Installing the client with NT Client Installer .....	3-17
Installing the client using Microsoft SMS .....	3-18
Verifying a successful installation .....	3-21
Using Vulnerability Scanner to verify the client installation .....	3-21
Testing the client installation .....	3-23
Removing the client .....	3-24
Removing the client using Uninstall Now .....	3-25

Removing the client using its uninstallation program .....	3-25
--	------

## **Chapter 4: Configuring OfficeScan**

Opening the Web console .....	4-2
Getting around the Web console .....	4-3
Other links on the console .....	4-8
Understanding the domain tree .....	4-9
Working with domains .....	4-11
Keeping your protection current .....	4-13
Updating the server .....	4-13
Updating clients .....	4-15
Setting up notifications .....	4-22
Configuring standard alerts .....	4-22
Configuring outbreak alerts .....	4-25
Configuring the scan settings .....	4-27
Default antivirus settings .....	4-28
Configuring real-time scan .....	4-29
Configuring manual scan .....	4-31
Configuring scheduled scan .....	4-33
Excluding files and folders from scanning .....	4-35
Running Scan Now .....	4-36
Granting privileges to clients .....	4-37
Registering OfficeScan .....	4-38

## **Chapter 5: Troubleshooting and Contacting Technical Support**

Troubleshooting installation issues .....	5-2
Server installation .....	5-2
Client installation .....	5-3
Contacting technical support .....	5-4
Before contacting technical support .....	5-4
Requesting for basic technical support .....	5-4

## **Appendix A: Using Manual Outbreak Prevention**

Blocking shared folders .....	A-2
Blocking ports .....	A-3
Denying write access to files and folders .....	A-5
Configuring client notification for outbreaks .....	A-7

Restoring network settings to normal .....	A-8
--	-----

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

Introducing Control Manager .....	B-2
What is Outbreak Prevention Service? .....	B-2
What you can do with Control Manager .....	B-2
What is a Control Manager agent? .....	B-4
Requirements for installing the agent .....	B-4
Required information for agent installation .....	B-4
Installing the agent .....	B-5
Managing OfficeScan using Control Manager .....	B-7
Status .....	B-8
Configuration .....	B-9
Tasks .....	B-9
Logs .....	B-10
Viewing summary reports for OfficeScan .....	B-11
Modifying the polling interval of the agent .....	B-15
Removing the agent .....	B-16

## **Appendix C: Setting Up Check Point SecureClient with OfficeScan**

Overview of Check Point Firewall architecture and configuration ...	C-2
Integrating with OfficeScan .....	C-2
Configuring Check Point for use with OfficeScan .....	C-4
Installing SecureClient support on the OfficeScan client .....	C-6

# Introducing OfficeScan Corporate Edition

This chapter introduces Trend Micro™ OfficeScan™ Corporate Edition and describes how it helps protect Microsoft™ Windows™ computers from viruses. It also discusses the benefits of using OfficeScan and provides a summary of tasks that you need to perform to deploy OfficeScan.

The topics discussed in this chapter include:

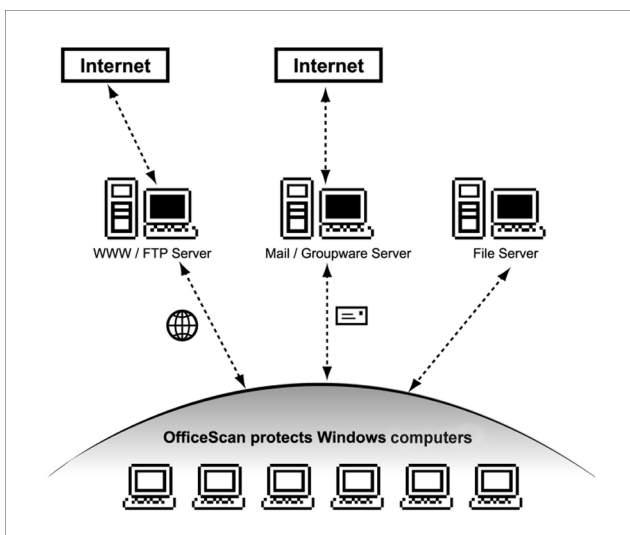
- What is OfficeScan Corporate Edition?
- How does OfficeScan work?
- What you can do with OfficeScan
- Getting started with OfficeScan



## What is OfficeScan Corporate Edition?

Trend Micro OfficeScan Corporate Edition is a centrally managed antivirus solution for desktop and notebook computers. OfficeScan helps protect your organization's Windows XP/2000/NT and Windows Me/98/95 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. You configure, monitor, and update these clients via the server's management console.



**FIGURE 1-1. OfficeScan protects desktop and notebook computers**

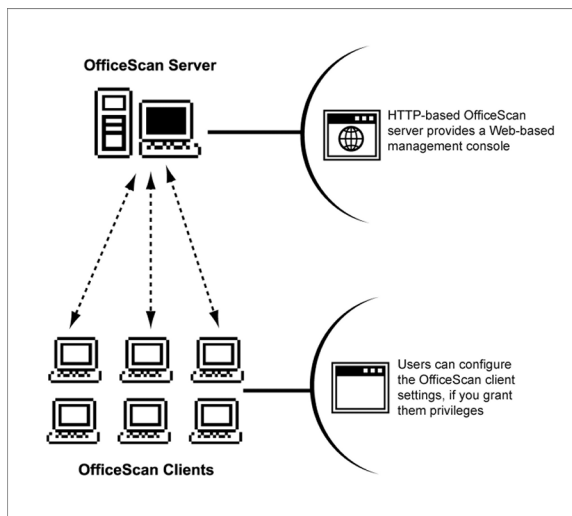
## How does OfficeScan work?

The server-based, centralized deployment and management features of OfficeScan give you tools to manage and enforce antivirus policies for an entire organization, and to react quickly to virus emergencies from nearly anywhere using its Web console.

The OfficeScan client program is installed on Windows XP/2000/NT and Windows Me/98/95 computers. It scans for viruses and performs real-time reporting of all virus incidents to the server, allowing you to view virus activities on each client from the Web console.

With the Web console, you are free to determine what action to take based on the situation. You can:

- Reconfigure the antivirus settings
- Initiate an enterprise-wide update of the pattern, scan engine, and program on clients
- Scan desktop and notebook computers for viruses from the management console



**FIGURE 1-2. How OfficeScan works**

## Understanding the OfficeScan architecture

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

- The server, which hosts the management console and downloads updates from the Trend Micro update server
- The client, which protects Windows XP/2000/NT and Windows Me/98/95 computers from viruses, Trojans, and other malicious programs
- The management console, which you use to configure and manage the clients from one location

### OfficeScan server

The OfficeScan server is the central repository for all client configurations, virus logs, and client software and updates. It can be installed on a Windows NT Server or Windows 2000 Server/Advanced Server.

The server performs two important functions:

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

There are two versions of the OfficeScan server:

- HTTP-based
- File-based

---

**Note:** This version of OfficeScan only supports the HTTP-based server.

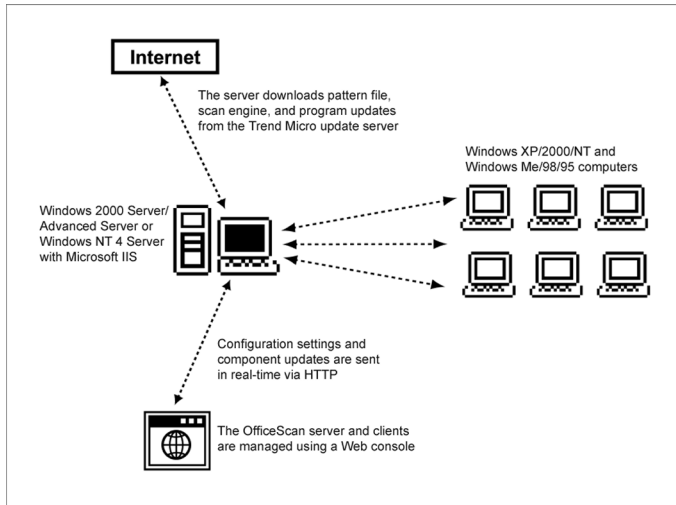
---

### HTTP-based server

The HTTP-based server is installed on a Windows NT 4.0 Server or Windows 2000 Server/Advanced Server with Internet Information Server™ (IIS) 4.0 or later. The HTTP-based server is capable of providing real-time, bidirectional communication between the server and clients.

If you install an HTTP-based server, you manage the clients from a Web browser-based management console, which you can access from virtually anywhere on the network.

As the name indicates, an HTTP-based server communicates with the client (and vice versa) via HyperText Transfer Protocol (HTTP). An 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.



**FIGURE 1-3. How an HTTP-based server works**

## OfficeScan client

You can 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. It 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.

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

---

**Note:** If you have clients in low-bandwidth remote offices reporting to the server in the main office, Trend Micro recommends installing Remote Agent on these clients. Remote Agent minimizes bandwidth usage by allowing a single client to download updates from the Trend Micro update server and share these updates with other clients. For more information on Remote Agent, see the *OfficeScan Deployment Guide* or the *Remote Agent Configuration Guide*.

---










OfficeScan clients are generally classified into two categories:


- Normal clients
- Roaming clients

### Normal clients

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

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

Icon	Description	Real-time scan	Manual and scheduled scans
	Normal client	Enabled	Enabled
	Pattern file is outdated	Enabled	Enabled
	Scan Now, manual scan, or scheduled scan is running	Enabled	Enabled
	Real-time scan is disabled	Disabled	Enabled
	Real-time scan is disabled and the pattern file is outdated	Disabled	Enabled
	Real-time Scan Service is not running	Disabled	Disabled
	Real-time Scan Service is not running and the pattern file is outdated	Disabled	Disabled
	Disconnected from the server	Enabled	Enabled
	Disconnected from the server and the pattern file is outdated	Enabled	Enabled

Icon	Description	Real-time scan	Manual and scheduled scans
	Disconnected from the server and real-time scan is disabled	Disabled	Enabled

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

## Roaming clients

Roaming clients are computers with the OfficeScan client installed that do not always maintain a constant network connection with the server, such as notebook computers. These clients continue to provide antivirus protection, but have delays in sending their status to the server.





You can assign roaming privileges to clients that are disconnected from the OfficeScan server for an extended period of time. Roaming clients do not accept commands/requests from the server, except when you select the **Force notification to all clients, including roaming clients** check box on the **Client Update** screens (Manual Deployment and Automated Deployment).



Roaming clients get updated only on three occasions:

- When the client user performs an Update Now
- When you set an automated update deployment and select **Force notification to all clients, including roaming clients** on the **Automated Deployment** screen
- When you select the **Check the OfficeScan server for updates** check box on the **Advanced Settings** screen and grant clients the privilege to enable scheduled update

For more information on how to update clients, see [Updating clients](#) on page 4-15.

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 the roaming client.

Icon	Description	Real-time scan	Manual and scheduled scans
	Roaming client	Enabled	Enabled
	Real-time scan is disabled	Disabled	Enabled
	Pattern file is outdated	Enabled	Enabled
	Real-time scan is disabled and the pattern file is outdated	Disabled	Enabled

Icon	Description	Real-time scan	Manual and scheduled scans
	Real-time Scan Service is not running	Disabled	Disabled
	Real-time Scan Service is not running and the pattern file is outdated	Disabled	Disabled

**TABLE 1-2. Icons that appear on the roaming client**

## About Damage Cleanup Services

OfficeScan also protects 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. Unlike viruses, Trojans do not replicate but can just be as destructive. An application that claims to rid a computer of viruses when it actually introduces viruses onto it is an example of a notorious Trojan. Traditional antivirus solutions can detect and remove viruses but not 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.

In OfficeScan, DCS is automatically executed on the client on three occasions:

- Whenever users run manual scan on the client
- Whenever you perform Scan Now on the client from the management console
- Whenever a hot fix is deployed to the client

Because DCS is automatically executed, you do not need to configure it to 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.

## Management console

The management 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 computers' antivirus settings. You can use to the management console to:

- Deploy the client 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, and SNMP Trap
- Control outbreaks by configuring and enabling Manual Outbreak Prevention

A Web browser-based management console, or Web console, is installed when you install the HTTP-based version of the OfficeScan server. The Web console uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

You can open the Web console from any computer on the network that has the required Web browser and communication protocols.

## Compatibility with Control Manager

Trend Micro Control Manager™ is a centralized network administration tool that works like a command center to reduce the impact of virus attacks. Control Manager provides a comprehensive view of the entire network, identifying how Trend Micro products and services can be deployed to create effective, targeted antivirus strategies.

You can monitor virus activities on the network and the performance of most Trend Micro products using the Control Manager Web-based administration console. During an attack, the Control Manager console functions as a centralized "command post" to monitor the outbreak progress, implement containment strategies, and deploy newly downloaded pattern files as soon as they become available.

OfficeScan is fully compatible with Trend Micro Control Manager. Use Control Manager with OfficeScan to simplify the task of managing antivirus protection throughout the network.

For more information on managing OfficeScan with Control Manager, refer to [\*Using Control Manager with OfficeScan\*](#) starting on page B-1.



## What you can do with OfficeScan

You can perform key administrative tasks using the OfficeScan management console. You can:

- Enforce antivirus policies
- Perform virus scans from one location
- Quarantine infected files
- Update your protection
- Analyze your network's protection against viruses
- Manage OfficeScan domains and clients
- Control outbreaks on the network
- Protect your PDAs from viruses

### Enforce antivirus policies

OfficeScan provides three types of scans: real-time scan, scheduled scan, and manual scan. You can enforce your organization's antivirus policies throughout the network by configuring the three types of scans based on these policies. You can specify the types of files to scan and the action to take when a virus is found.

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

### Perform virus scans from one location

Use the Web console to perform Scan Now (manual scan) on all clients. You can also use the Web console to configure scheduled scans to run during off-peak hours when network traffic is low.

### Quarantine infected files

You can control live viruses and infected files by specifying a quarantine folder for all viruses detected on the network and configuring OfficeScan to automatically move infected files to the quarantine folder. In case you encounter files infected with

new viruses that OfficeScan cannot clean, you can send these files to Trend Micro for analysis.

## **Update your protection**

New viruses are written and released via different media everyday, especially the Internet. To ensure that you stay protected against the latest threats, you must periodically update the OfficeScan components, including the pattern file, scan engine, and program. New virus patterns files are usually released by Trend Micro on a weekly basis.

## **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 computers that are vulnerable to infection.

You can also use these as a basis for designing and redesigning your network's protection. You can identify computers that are at a higher risk of infection and change the antivirus settings accordingly for these computers.

## **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 2000/NT domain. There can be several OfficeScan domains in one Windows 2000/NT domain.

You can group clients into domains to simultaneously apply the same configuration to all domain members, making clients easier to manage.

## **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, you can enable Manual Outbreak Prevention to prevent viruses from spreading.

By blocking shared folders and vulnerable ports and denying write access to files on clients, Manual Outbreak Prevention allows you to prevent the outbreak from overwhelming the network. After you enable Manual Outbreak Prevention, download the latest pattern file (if any), and then perform Scan Now on all clients to remove any existing virus.

## 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, refer to the *OfficeScan for Wireless Quick Start Guide* and online help. A shortcut to the Quick Start Guide is created in the Trend Micro Wireless Protection Manager program group when you install Wireless Protection Manager. 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.

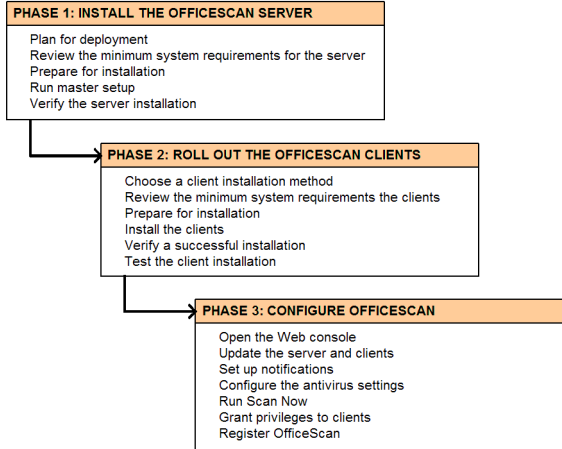
---

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

---

## Getting started with OfficeScan

This guide groups getting started tasks into phases. Each phase has corresponding sections in that discuss in detail the tasks that you need to perform.



**FIGURE 1-4. Getting started tasks are grouped into three phases**

## Phase 1 summary

During phase 1, you set up the server on the network by completing the following tasks:

- Plan for deployment by gathering information about your environment and clients
- Review the minimum system requirements for the server
- Prepare for installation
- Run master setup to install the server
- Verify the server installation

For more information, refer to *Installing the Server* starting on page 2-1.

## Phase 2 summary

During phase 2, you roll out the clients by completing the following tasks:

- Choose a client installation method that is suitable for your environment
- Review the minimum system requirements for the clients
- Prepare for installation

- Roll out the clients using the chosen installation method
- Verify the client installation
- Test the client installation

For more information, refer to *Rolling Out Clients* starting on page 3-1.

## Phase 3 summary

During phase 3, you use the Web console to perform basic scan and configuration tasks to ensure all clients are protected. You complete this phase by performing the following tasks:

- Open the Web console
- Update the server and clients
- Set up notifications
- Configure the antivirus settings
- Run Scan Now
- Grant privileges to clients
- Register OfficeScan

For more information, refer to *Configuring OfficeScan* starting on page 4-1.

# Installing the Server

This chapter describes how to plan for deployment and prepare for server installation. It also provides step-by-step instructions for installing the OfficeScan server and verifying the installation.

The topics discussed in this chapter include:

- Planning for installation
- Minimum system requirements
- Preparing for server installation
- Running master setup
- Verifying a successful installation
- Upgrading from a previous version
- Removing the server

## Planning for deployment

Deployment is the process of strategically distributing OfficeScan to your network environment to facilitate management and to provide optimal protection against viruses.

Installing and deploying an enterprise-wide, client-server application like OfficeScan to a heterogeneous environment (and even to a homogenous one) requires careful planning and assessment before running the installation program.

Following are basic tasks that you can perform to plan for installation:

- Plan for an optimal client-server ratio
- Plan for network traffic
- Determine if you need to install a dedicated server

---

**Note:** This guide only provides an overview of deployment planning. For more information on planning for deployment, refer to the *OfficeScan Corporate Edition Deployment Guide*.

---

## Planning for optimal client-server ratio

To ensure optimal performance of OfficeScan on the network, plan for the ratio of the servers and clients. Having an optimal client-server ratio enhances the performance of both the server and clients, allows updates to be deployed faster, and makes configuration and management of OfficeScan on the network a lot easier.

### Client-server ratio on a LAN

The most critical factor in determining how many clients a single server can manage on a local network is client startup time. Client startup time affects the performance of the server and the number of clients it can manage. On startup, clients connect to the server to report their status and check for configuration changes and available updates. In most organizations, CPU utilization on the server is highest in the morning, when clients are started.

If all client computers in your organization are started at the same time or if the startup intervals are very short, you can use the table below as a guide in determining how many servers you will need to install.

**Note:** The information presented in Table 2-1 is based on an internal lab test conducted at Trend Micro and should only be used as a reference. You may get a different set of results, depending on your network environment.

Number of Clients	Server Configuration				
	CPU	RAM	Hard Disk	Network Bandwidth	Operating System
100 or less	166MHz Intel Pentium™ processor	128MB	IDE	10Mbps	Windows 2000 Server/Advanced Server with SP1/SP2/SP3 or Windows NT 4.0 with SP5, IIS 4.0, NTFS
1000 or less	Dual 266MHz Intel Pentium II processors	512MB	SCSI	100Mbps	Windows 2000 Server/Advanced Server with SP1/SP2/SP3 or Windows NT 4.0 with SP5, IIS 4.0, NTFS
3000 or less	Quad 350MHz Intel Pentium II processors or dual 700Mhz Intel Pentium III processors	1GB	SCSI 3 with RAID 5 disk mirroring (80MB/sec disk I/O)	100Mbps	Windows 2000 Server/Advanced Server with SP1/SP2/SP3 or Windows NT 4.0 with SP5, IIS 4.0, NTFS

**TABLE 2-1. Sample server configurations and the number of clients each configuration can manage**

If computers in your organization have staggered startup times (for example, if users work in different shifts), the server may be able to manage more clients.

The performance of the server is also determined by the rate at which data can be accessed from its hard drive. Using high-speed SCSI or RAID drives result in better performance and is recommended. Adding more CPU power and RAM can also help improve performance. Given a high-speed drive and more memory and processing power, the server may be able to handle more clients.

**Client-server ratio across the WAN**

When deploying OfficeScan across the WAN, the server in the main office may have to manage some clients in remote offices. If you have clients in a remote office that



report to the server in the main office over the WAN, the factors that you need to consider are:

- The diversity of the network bandwidth in your WAN environment
- The normal startup time of clients

Having a diversified network bandwidth in your WAN environment can be beneficial to OfficeScan. If you have clients both on the LAN and across the WAN reporting to the same server, client reporting is staggered naturally: the server prioritizes the clients with the faster connection, which, in almost all cases, are the clients on the LAN.

The startup time of clients also affects the deployment of updates. During startup, clients connect to the server to report their status and check for configuration changes and available updates. In most organizations, CPU utilization on the server is highest in the morning, when the clients are started. If all clients connect to the server simultaneously, the performance of the server may be affected.

If clients are located in several remote offices with different time zones or if users have diversified working hours, the possibility of all these clients starting up at the same time is quite remote. Therefore, the server may be able to handle more clients across the WAN than it can on the LAN.

Refer to the information in Table 2-1 to help you plan for an optimal client-server ratio in your WAN environment.

---

**Note:** Although installing more servers allows you to update clients faster, it also increases the overall effort required to manage them.

---

## Planning for network traffic

When planning for deployment, you need to 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 on the following occasions:

- When it connects to the Trend Micro update server to check for and download updated pattern files, scan engines, hot fixes, and programs

- When it notifies clients to download updated pattern files, scan engines, hot fixes, and programs
- When it notifies clients about configuration changes

The client, on the other hand, generates traffic on the following occasions:

- When it is started
- When the user performs an Update Now
- When it performs a scheduled update
- When it switches from roaming mode to normal mode

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

Significant network traffic is only generated when there is an updated version of the pattern file, scan engine, or program. The scan engine and program are not updated very often; generally, these are only updated when a new version of OfficeScan is released. Pattern files, on the other hand, are updated regularly to ensure that clients stay protected against the latest virus threats.

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 discovered “in the wild” or is actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available, usually within a few hours.

## **Determining if you need to install a dedicated server**

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

- How much CPU load is carried by the server?
- 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.

## **OfficeScan and Control Manager on the same machine**

Both OfficeScan and Control Manager use IIS to communicate with clients and agents, respectively.

There is no conflict between these two applications, but since both of them are using IIS resources, Trend Micro recommends installing Control Manager on another machine to reduce the performance stress on the server.

## **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 for feedback to determine how features work and the level of support you will likely need after full deployment.

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

Here are some tasks you can perform to conduct a pilot deployment:

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

## **Choosing a pilot site**

Choose a pilot site that matches, more or less, your production environment. Try to simulate, as closely as possible, the type of topology that would serve as an adequate representation of your production environment.

## Creating a rollback plan

You should create a disaster recovery or rollback plan, in case there are some difficulties with the installation or upgrade.

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

## Deploying the pilot

Deploy OfficeScan to the pilot site and evaluate which client installation methods are most suitable for your environment.

## Evaluating the pilot deployment

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

## Minimum system requirements

To install the OfficeScan server, you need the following:

- 233MHz Intel™ Pentium™ II processor or equivalent
- Microsoft™ Windows™ NT 4.0 Server with SP5 or later, Windows 2000 Server, or Windows 2000 Advanced Server
- 64MB of free RAM
- 300MB of free disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft™ Internet Explorer 4.0 or later
- Microsoft™ Internet Information Server (IIS) 4.0 or later

## Minimum system requirements for the Web console

The Web console is automatically installed when you install the HTTP-based server. However, if you plan to open the Web console using other computers on the network, these computers must have the following:

- 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
- Microsoft Internet Explorer 5.0 or later
- Java Virtual Machine (JVM)

## 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
- Shared directories
- Windows licenses
- TCP port for HTTP communication

## Where to run the setup program

You can run the setup program on any computer running:

- Windows XP Professional or Home Edition
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Professional
- Windows NT 4 Server
- Windows NT 4 Workstation

## 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 server. After completing the installation, you can immediately configure the server, and then proceed to rolling out clients.

If you are installing an HTTP-based server, Setup will automatically stop and restart the IIS service. Make sure that you do not install the server on a computer that is running applications that might lock IIS, which will cause installation to fail. Due to the resource demands, Trend Micro does not recommend installing OfficeScan to a server that is also running Trend Micro Control Manager.

## Required information

Have the following information ready before starting the installation:

- **Serial number.** If you type a valid serial number on the **User Information** screen, Setup will install the full version. Leaving the serial number text box blank will install a 30-day trial version. You can later convert the 30-day trial version to the full version by purchasing an OfficeScan license and typing the serial number on the **Welcome** screen of the Web console.
- **Proxy information.** If Internet traffic on the network is handled via a proxy server, you must type the proxy server information and your user name and password to be able to download the latest virus pattern, scan engine and program from the Trend Micro update server. Alternatively, you can leave the proxy information blank, and then configure it on the OfficeScan console after you install the server.

- **Console password.** To prevent unauthorized access to the OfficeScan Web console, you need to specify a password which will be required of anyone who tries to open the console.
- **Custom client virus alert message (optional).** When the OfficeScan client detects a virus on a computer during real-time scan, a virus alert message appears. You can customize the message that is displayed on the clients.
- **Client software installation path (optional).** You can configure the client installation path where OfficeScan files will be copied to during client setup. On the **Client Installation Path** screen, you can also enable network scan for mapped drives and shared folders and add manual scan to the Windows shortcut menu on clients.
- **Windows shortcut entries (optional).** You can customize the names of the program shortcuts that the OfficeScan setup program will create on the Windows **Start** menu.

## Shared directories

Before installing the server, you must share a directory on the target server (with write privileges) where you want the program files to be installed. The setup program will prompt for this shared folder during master setup.

If you plan to use Login Script Setup to install the clients, you must share the target Windows NT or Windows 2000 directory as `admin$`.

## Windows licenses

Make sure your organization has sufficient Windows 2000/Windows NT 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, you have to reinstall the OfficeScan server to ensure successful client-server communication.

## Running master setup

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

You can run Setup on either the target server or on a Windows computer on the network. For a list of Windows computers where you can run Setup, refer to [Where to run the setup program](#) on page 2-8.

---

**WARNING!** *Remember to close any running application before installing the server. If you install while there are other applications running, the installation process may take longer to complete.*

---

### To install the HTTP-based server

1. In Windows Explorer, open the folder that contains the setup files and double-click **Setup** (setup.exe). The **Welcome** screen appears.
2. Click **Next**. The **Software License Agreement** screen appears.
3. Read the agreement carefully, then click **Yes** to agree to all the terms.

The **Select Target Server** screen appears.

4. Browse for the target server in the list of servers. You can also type the name of the target server in **Find a server** and click **Search**.

Once you locate the target server, double-click it to display its shared directories. Select the target directory, then click **Next**.

The **User Information** screen appears.



5. Type your name, the name of your organization, and your serial number in the text boxes provided.

If you do not provide a serial number at this time, a 30-day trial version of OfficeScan (which you can later upgrade to the full version) will be installed on the server.

Click **Next**. The **Server Information** screen appears.

6. Specify how clients will identify the server by clicking either **Domain name** or **IP address**.

- If you clicked **Domain name**, verify that the target server's domain name is correct. You can also use the server's fully qualified domain name (FQDN) if necessary to ensure successful client-server communication.
- If you clicked **IP address**, verify that the target server's IP address is correct. Clicking **IP address** is not recommended if the server's IP address is subject to change (as in a DHCP environment).

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.

7. Verify that the port number shown on-screen is correct. OfficeScan uses the same TCP port number that your HTTP server is using. Setup automatically retrieves this port number and displays it on this screen.

Make sure your HTTP port number and the port number displayed on-screen are the same. This will be the port number on the server through which clients will connect.

Click **Next** to continue. The **Proxy Settings** screen appears.

8. 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 have provided on-screen is correct. This information will be used by the server to connect to the Trend Micro update server and download updated components, such as pattern files and scan engines.

Click **Next** to continue. The **Management Console Password Setting** screen appears.

9. Type your password and confirm that password in the text boxes. This helps prevent unauthorized users from accessing the management console and modifying the settings or removing the clients.

Click **Next**. The **Client Virus Alert Message** screen appears.

10. Accept the default client virus alert message or customize it. The virus alert message is displayed on clients whenever a virus is detected. Click **Next**. The **Client Installation Path** screen appears.

The client installation path is where the client setup program will place program files during client installation. The default client installation path is `$Program Files\Trend Micro\OfficeScan Client`.

11. Accept the default client installation path or change it as necessary.

Three other options are available on this screen:

- **Enable network scan for mapped drives and shared folders** - select if you want the clients to run real-time scan whenever they access shared folders on the network
- **Add manual scan to the Windows shortcut menu on clients** - select if you want to create a shortcut to the manual scan function on the Windows shortcut menu
- **Port number** - modify as necessary. This is a randomly generated port number on clients through which the server will communicate. In OfficeScan 5.02 and earlier versions, the server uses a fixed port number — port 12345.

---

**WARNING!** *You cannot modify this port number once you finish with Setup. To determine the port number on the client that is used for communication with the server, check the value for **Client communication port** on any domain tree screen. If the server is behind a firewall, you must open this port number for clients outside the firewall to successfully connect to the server.*

---

Click **Next** to continue. The **Select Program Folder** screen appears.

12. Accept the default folder name, **Trend Micro OfficeScan Corporate Edition-{Server Name}**, or specify a new one. Setup will create shortcuts and a program group for OfficeScan on the Windows **Start** menu.

Click **Next** to continue.

Setup starts installing OfficeScan on the target server. The screen shows the progress of the installation.

When installation is complete, the **OfficeScan Directory Sharing** screen appears, informing you that Setup has created a shared directory in the folder you shared for OfficeScan.

13. Click **Next**. The **Setup Complete** screen appears.

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

14. Click **Finish** to close the setup program.

## Verifying a successful installation

After completing the installation, check if the OfficeScan server was properly installed.

### To verify the installation

- Check if the OfficeScan program shortcuts were created on the Windows **Start** menu of the computer you used to run master setup
- Check if OfficeScan is in the **Add/Remove Programs** list of the OfficeScan server's Control Panel
- Check if you can successfully log on to the Web console

## Upgrading from a previous version

The procedures for upgrading from a previous version of OfficeScan depend on the type of server you have.

If you have an HTTP-based server, refer to [Upgrading HTTP-based OfficeScan](#) on page 2-15.

If you have a file-based server, refer to *Upgrading file-based OfficeScan* on page 2-16.

## Upgrading HTTP-based OfficeScan

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

1. Back up `ofcscan.ini` and the database
2. Upgrade the server using master upgrade

Client upgrade should be automated if you configured OfficeScan to automatically deploy updates to the clients whenever the server gets an update. However, if automatic upgrade fails, there are several alternative methods you can use to ensure that clients get the latest program version of OfficeScan.

To learn more about these alternative methods, refer to the *OfficeScan Corporate Edition Deployment Guide*. This guide also contains detailed information on upgrading and migrating to OfficeScan.

### Backing up ofcscan.ini and the database

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

#### To back up ofcscan.ini and the database

1. In Windows Explorer, go to the server's OfficeScan folder.
2. Go to the `\PCCSRV` folder and copy `ofcscan.ini` to another location (for example, to different directory on the same server, to another computer, or to a removable drive).
3. Go to the `\PCCSRV\HTTPDB` folder and copy the contents to another location (for example, to different directory on the same server, to another computer, or to a removable drive).

### Upgrading the server using master upgrade

Master upgrade refers to running Setup to install a newer version of OfficeScan on the existing server. The upgrade procedure is very similar to master setup. The only

difference is that you select the existing OfficeScan server when you specify the server on which to install OfficeScan.

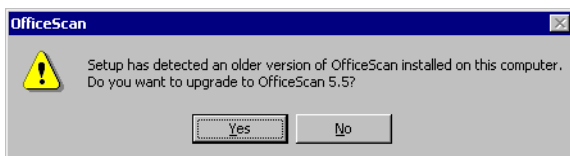
You need not share a new folder; simply select the existing OfficeScan folder and Setup will do the rest.

---

**Note:** You cannot change the type of OfficeScan server by running master upgrade. For example, you cannot upgrade a file-based server to an HTTP-based server.

---

If you specified an update schedule on the **Scheduled Server Update** screen of the Web console and selected **Server and client programs** under **Components to Update**, the clients will be upgraded automatically when the scheduled update runs.



**FIGURE 2-1. Verify that want to upgrade to a newer version of OfficeScan**

To learn about other methods that you can use to upgrade the HTTP-based OfficeScan server, refer to the *OfficeScan Corporate Edition Deployment Guide*.

## Upgrading file-based OfficeScan

This version of OfficeScan does not support the file-based server and clients. If you are currently using file-based OfficeScan, Trend Micro highly recommends upgrading to HTTP-based OfficeScan.

The HTTP-based version of OfficeScan provides real-time, bidirectional communication between the server and clients. It also includes a Web console that you can access virtually from any Windows computer on the network.

Upgrading from file-based to HTTP-based OfficeScan is a four-step process:

1. Remove all file-based clients

2. Verify that file-based clients are completely removed
3. Remove the file-based server
4. Install the HTTP-based server and clients

## Removing file-based clients

The first step in upgrading to HTTP-based OfficeScan is to remove all file-based clients. You can remove all file-based clients by modifying a file called `AUTOPCC.INI`. This file is executed whenever clients log on to the server using login script.

### To modify autopcc.ini

1. On the file-based OfficeScan server, go to the `\PCCSRV\Autopcc.cfg` folder.
2. Using a text editor (for example, Notepad), open `AUTOPCC.INI`.
3. Look for the section called `[INSTALL]`.
4. Under `[INSTALL]`, change the value for `Uninstall` from 0 to 1.
5. Save the file.

The next time clients report to the file-based server, they will get the updated `AUTOPCC.INI` and remove OfficeScan from their host computers.

## Verifying that file-based clients have been removed

After modifying `AUTOPCC.INI`, verify that all clients have been removed. Do this by logging on to the OfficeScan Windows console and checking if clients still appear in the domain tree.

## Removing the file-based server

Once clients are completely removed, you can remove the file-based server. There are two ways to remove the file-based server:

- By clicking the **Uninstall OfficeScan** shortcut on the **Programs** menu
- By using the **Add/Remove Programs** feature of Windows

**To remove the file-based server using the Uninstall OfficeScan shortcut on the Programs menu**

1. On the computer you used to install the OfficeScan server, click the **Start** menu, and then click **Programs > {Trend Micro OfficeScan Corporate Edition} > Uninstall OfficeScan**.

A confirmation window appears.

2. Click **Yes**. The **OfficeScan Master Uninstaller** screen appears. Master Uninstaller connects to the server and prompts you for the Master Password (password you use to open the management console).
3. Type the Master Password in text box, and then click **OK**. Master Uninstaller proceeds with removing the server.

When Master Uninstaller completely removes the server, the message "OfficeScan uninstallation finished. Please press OK to continue" appears.

4. Click **OK** to close Master Uninstaller.

**To remove the file-based server using the Add/Remove Program feature of Windows**

1. On the computer you used to install the OfficeScan server, click the **Start** menu, and then click **Settings > Control Panel**.

The Control Panel window appears.

2. Double-click **Add/Remove Programs**.

The Add/Remove Programs window appears, displaying all currently installed programs.

3. Click **Trend Micro OfficeScan Corporate Edition**, and then click **Change/Remove**.

A confirmation window appears.

4. Click **Yes**. The **OfficeScan Master Uninstaller** screen appears. Master Uninstaller connects to the server and prompts you for the Master Password (password you use to open the management console).
5. Type the Master Password in text box, and then click **OK**. Master Uninstaller proceeds with removing the server.  
  
When Master Uninstaller completely removes the server, the message "OfficeScan uninstallation finished. Please press OK to continue" appears.
6. Click **OK** to close Master Uninstaller.

## Installing the HTTP-based server and clients

After removing the file-based server and clients, you can perform a fresh install of the HTTP-based server and clients.

For information on how to plan for deployment, see [Planning for deployment](#) on page 2-2.

For information on how to perform a fresh install of the HTTP-based server, see [Running master setup](#) on page 2-11.

For information on how to install clients, see [Rolling Out Clients](#) starting on page 3-1.

## 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 the *Using the tools* topic of the OfficeScan online help.



## Removing the server

OfficeScan includes several automated tools to help you remove the server and client software from the network. The key thing to remember, however, is to 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 > {OfficeScan program group} > Uninstall OfficeScan**.

A confirmation screen appears.

2. Click **Yes**. Master Uninstaller, the server uninstallation program, is started. Master Uninstaller prompts you for the administrator's password.
3. Type the administrator's password in the text box and click **OK**. Master Uninstaller starts removing the server files.

When the OfficeScan server is completely removed, the message "OfficeScan uninstallation finished" appears.

4. Click **OK** to close the uninstallation program.

# Rolling Out Clients

OfficeScan provides multiple ways of installing the client to Windows computers on the network. This chapter describes the different client installation methods to help you decide which ones are most suitable for your environment. It also discusses how to prepare for client installation and provides step-by-step instructions for rolling out clients, verifying the installation, and testing the client installation.

The topics discussed in this chapter include:

- Choosing a client installation method
- Minimum system requirements
- Preparing for client installation
- Installing clients
- Verifying a successful installation
- Testing the client installation
- Removing the client

## Choosing a client installation method

OfficeScan provides several methods to install the client. You can choose one or a combination of these installation methods that you consider suitable for your environment. To use any of these methods, you must have local administrator rights to the target computers.

You can install the clients:

- From an internal Web page
- Using Login Script Setup
- Using Client Packager
- Using Windows NT Remote Install (from the Web console)
- From a client disk image
- Using NT Remote Install utility
- Using NT Client Installer
- Using Microsoft™ SMS

For a comparison of the different client installation methods, see Table 3-1.

	Web page	Login Script Setup	Client Packager	Windows NT Remote Install	Client image setup	NT Remote Install utility	NT Client Installer	Microsoft SMS
Suitable for deployment across slow links	Yes	No	Yes	No	Yes	No	No	No
Suitable for centralized administration and management	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Requires client user intervention	Yes	No	Yes	No	No	No	No	Yes
Requires IT resource	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Suitable for mass deployment	No	Yes	Yes	No	Yes	Yes	Yes	Yes
Delivery mechanism	HTTP	UNC	Email, CD-ROM, or similar media	UNC	Physical delivery	UNC	UNC	UNC

	Web page	Login Script Setup	Client Packager	Windows NT Remote Install	Client image setup	NT Remote Install utility	NT Client Installer	Microsoft SMS
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	Low, if scheduled

**TABLE 3-1. A comparison of the various client installation methods**

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

---

**WARNING!** *Remember to close any running application before installing the client. If you install while there are other applications running, the installation process may take longer to complete.*

---

## Minimum system requirements

The OfficeScan client has a slightly different set of requirements for Windows Me/98/95, Windows 2000/NT, and Windows XP.

### Windows Me/98/95 clients

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

- 133MHz Intel™ Pentium™ processor or equivalent
- Microsoft Windows 95/95 OSR2/98/98 SE/Me
- 20MB of free RAM
- 80MB of free disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft Internet Explorer 4.0 or later

### Windows 2000/NT clients

To install the client to Windows 2000/NT computers, they must have the following:

- 150MHz Intel Pentium processor or equivalent
- Microsoft Windows NT 4.0 workstation with SP5 or later, or Windows 2000 Professional
- 20MB of free RAM
- 80MB of free disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft Internet Explorer 4.0 or later

## Windows XP clients

To install the client to Windows XP computers, they must have the following:

- 233MHz Intel Pentium processor or equivalent
- Microsoft Windows XP Professional or Home Edition
- 20MB of free RAM
- 80MB of free disk space
- Monitor that supports 800 x 600 resolution at 256 colors

## Preparing for installation

You can identify which desktop and notebook computers on the network are not protected against viruses by running Trend Micro Vulnerability Scanner. This tool checks computers on the network for installed antivirus software 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 the topic *Using the tools* in the OfficeScan online help.

## Installing the client from an internal Web page

If you installed an HTTP-based server on a Windows NT 4.0 Server or Windows 2000 Server/Advanced Server with IIS 4.0 or later, users can install the client from the internal Web page that was created during master setup.

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


Users must have Microsoft Internet Explorer 4.0 or later to successfully download the client setup files. You can send an email message to users with the following client installation instructions.

### To install from the internal Web page

1. Open an Internet Explorer window and type  
`http://{Server_Name}/Officescan/clientinstall` in the address bar  
 (where {Server\_Name} is the computer name or IP address of the OfficeScan server).

The **OfficeScan Client Installation** screen appears.

2. Click **Install Now** to start installing the 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 the client with Login Script Setup

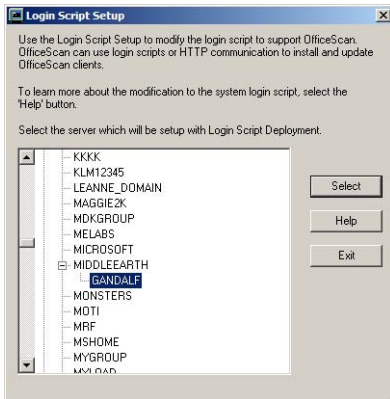
Using Login Script Setup, you can automate the installation of the client to unprotected computers when they log on to the network. Login Script Setup adds a program called `autopcc.exe` to the server login script. `Autopcc.exe` performs the following functions:

- 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

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

1. On the computer you used to run master setup, click **Programs > {Trend Micro OfficeScan Corporate Edition} > Login Script Setup** from the Windows **Start** menu.

The Login Script Setup console loads, displaying a tree that shows all domains on the network.



**FIGURE 3-1. Search for the target Windows 2000/NT Server**

2. Search for the Windows 2000/NT Server whose login script you want to modify, click it, and then click **Select**.

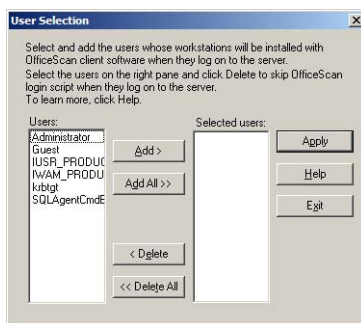
Login Script Setup prompts for a user name and password.



**FIGURE 3-2. Type your user name and password**

3. Type your user name and password. Make sure you have administrator rights to the target servers. Click **OK** to continue.

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



**FIGURE 3-3. Select the user profiles whose login scripts you want to modify**

- To modify the login script of a single or multiple user profiles, click them from the **Users** list, and then click **Add**.
  - To modify the login script of all users, click **Add All**.
  - To exclude a user profile that you have previously selected, click the name from the **Selected users** list, and then click **Delete**.
  - To reset your choices, click **Remove All**.
4. Click **Apply** when all target user profiles are in the **Selected users** list.  
A message appears, informing you that you have modified the server login script successfully.
  5. Click **OK**. Login Script Setup utility returns to its initial screen.
    - To modify the login script 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.

## Windows 2000/NT scripts

If you already have an existing login script, a command that executes `autopcc.exe` will be appended to it. Otherwise, a batch file called `ofcscan.bat` (which contains the command to run `autopcc.exe`) will be created.



The following is appended at the end of the login script:

```
\\{Server_name}\ofcscan\autopcc
```

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 (normally, 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\SYSTEMVOL\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
```

## Installing the client with Client Packager

Client Packager is an OfficeScan 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 setup package, all they have to do is double-click the file to run the setup program. OfficeScan clients that are installed using the Client Packager report to the server where the setup package was created.

This tool is especially useful when deploying client setup or update files to clients in low-bandwidth remote offices.

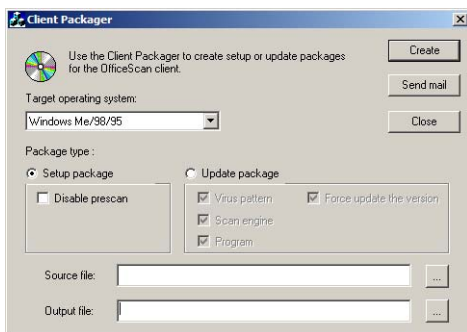
---

**Note:** To run Client Packager on the server, it must have Outlook Express installed. Running Client Packager requires `MAPI32.DLL`, which is provided by Outlook Express. You must also have write permission to `ClnExtor.ini`. Otherwise, clients may not inherit the OfficeScan settings you specify.

---

### To create a setup package with Client Packager

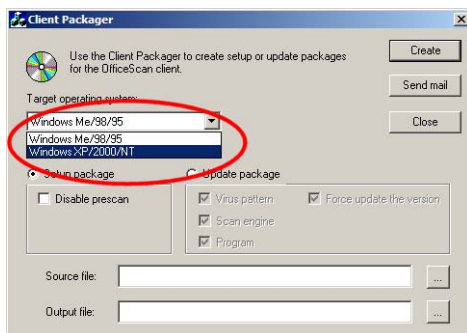
1. On the OfficeScan server, open Windows Explorer.
2. Browse to `\PCCSRV\Admin\Utility\ClnPack` folder of OfficeScan.
3. Double-click `ClnPack.exe` to run the tool. The Client Packager console opens.



**FIGURE 3-4. The Client Packager console opens**

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

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



**FIGURE 3-5. Select the operating system of the target computers**

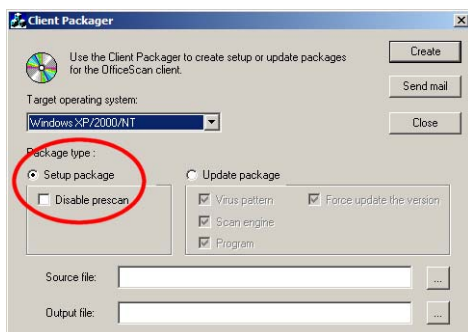
5. Under **Package create options**, click **Setup package**.

If you want to disable the normal file scanning that OfficeScan performs before starting setup, make sure the **Disable prescan before setup** check box is selected.

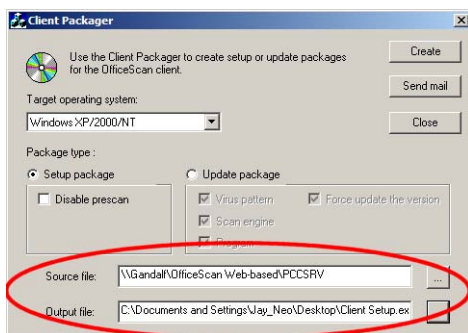
---

**Note:** If you want to create an update package, click **Update package** instead of **Setup package**. An update package can contain virus pattern files, scan engines, or program updates.

---



6. In **Source file**, click . The **Open** dialog box appears.
7. Browse for the `ofcscan.ini` file. This file is normally located in the `\PCCSRV` folder of the OfficeScan server.
8. Click `ofcscan.ini`, and then click **Open**. The Client Packager console appears again.
9. In **Output file**, click . The **Save As** dialog box appears.
10. Browse to the location where you want to create the setup package.
11. In the **File name** text box, type a file name for the client setup package (for example, `ClientSetup.exe`), and then click **Save**. The Client Packager console appears again.



**FIGURE 3-6.** Specify the location of the `ofcscan.ini` file and where you want to create the client setup package

12. Click **Create** to start building the client setup package. When Client Packager finishes creating the package, the message "Package created successfully" appears.

To verify that the package has been created successfully, check the output directory you specified.

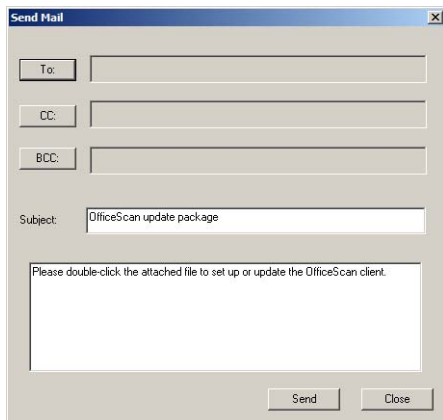
13. Send the setup package to users via email, or copy it to a CD or similar media and distribute among users.

## Sending the package using the email function

You need to have Microsoft Outlook installed to use the Client Packager email function.

### To send the package using the console

1. Click **Send mail**. The **Send mail** screen opens with the default subject and message.



**FIGURE 3-7. The Send mail screen opens with the default subject and message**

2. Click **To** to specify the recipients of the package. Client Packager opens your Microsoft Outlook address book.

Click **CC** or **BCC** if you want to send copies to other recipients in your organization.

3. Edit the default subject and message as necessary.
4. Click **Send**.

---

**Note:** If Client Packager is unable to find your Microsoft Outlook address book, an error occurs when you click **Send mail**, **To**, **CC**, or **BCC**.

---

## Installing the client with Windows NT Remote Install

You can remotely install the client to Windows XP/2000/NT computers that are connected to the network, and you can install to multiple computers at the same time without having to physically go to each computer.

To use Windows NT Remote Install, you need to have administrator rights to the target computers.

### To install with Windows NT Remote Install

1. On any computer on the network, open Internet Explorer.
2. Type `http://{Server_name}/OfficeScan` (where {Server\_name} is the computer name or IP address of the OfficeScan server) in the address bar.

The **Welcome** screen of the Web console appears.

3. Type the administrator's password, and then click **Enter** to open the Web console.
4. On the sidebar, click **Client Administration > NT Remote Install**.

The **NT Remote Install** screen appears. The **Domains and computers** list displays all Windows 2000/NT domains on the network. To display computers under a domain, double-click the domain name.

5. In the **Domains and computers** list, select a client, and then click **Add Client**.

Windows NT Remote Install prompts for a user name and password to the target computer. Make sure you have administrator rights to the target computer.

6. Type your user name and password, and then click **Log in**. The target computer appears in the **Selected computers** list.
7. Repeat steps 5 and 6 until the **Selected computers** list displays all the Windows XP/2000/NT computers to which you want to install the client.
8. Click **Apply** when you are ready to install the client to the target computers.

A confirmation screen appears.

9. Click **Yes** to confirm that you want to install the OfficeScan client to the target computers. A progress window is displayed as the program files are copied to each target computer.

When OfficeScan completes the installation to a target computer, the computer name disappears from the **Selected computers** list and appears in the **Domains and computers** list with a red check mark.

When all target computers appear with red check marks in the **Domains and computers** list, you have completed client installation via Windows NT Remote Install.

---

**Note:** If you are installing to multiple computers, any unsuccessful installation will be recorded in the log file, but it will not postpone the other installations. You do not have to supervise the installation once you click **OK**.

---

## Installing the client from a disk image

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

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

### 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` 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 the disk imaging software.
6. Restart the clone. `Imgsetup.exe` will automatically start and create a new GUID. The client will report this new GUID to this server and the server will create a new record for the new client.

---

**Note:** 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 client.

---

## Installing the client with NT Remote Install utility

Using the NT Remote Install utility, you can also remotely install the client to Windows XP/2000/NT computers. This utility is useful if you have already identified the target computers and want to immediately install the client. Since you already know the target computers, the tool no longer needs to search the network for unprotected Windows XP/2000/NT computers, saving you time and effort.

### To install with NT Remote Install utility

1. Write down the computer names or IP addresses of the Windows XP/2000/NT computers on which you want to install the client.
2. On the server, go to the `\PCCSRV\Admin\Utility\NTBRInst` folder of OfficeScan.
3. Copy `NTBRinst.exe` and `NTBRinst.ini` to `\PCCSRV\Admin`.
4. Using a text editor such as Notepad, open `NTBRinst.ini`.
5. Search for the string `[INI_SERVER_SECTION]`, and then specify the UNC path to the server. For example:

```
[INI_SERVER_SECTION]
# Server master path
```



```
Master_Path=\\Server_name\OfficeScan\PCCSRV\
```

Where:

- `Server_name` is the computer name or IP address of the OfficeScan server
- `OfficeScan` is the name of the OfficeScan folder

6. Search for the string `# Server mode`, and then specify 0 if the server is HTTP-based, or 1 if file-based. For example:

```
# Server mode  
  
# 0 - file base, 1 - http base  
  
Server_Mode=1
```

Where `Server_Mode=1` means you have an HTTP-based server.

7. Search for the string `[INI_CLIENT_SECTION]`, and then specify the number of target computers. For example:

```
[INI_CLIENT_SECTION]  
  
# Number of NT workstation clients  
  
Client_Num=3
```

Where `Client_Num=3` means you are installing to 3 Windows XP/2000/NT computers.

8. Search for the string `# Domain name and computer name of NT workstation clients`, and then specify the domain names and computer names (or IP addresses) of the target computers. For example:

```
# Domain name and computer name of NT workstation clients  
  
# domain_name\machine_name  
  
Client1=Company\Computer1  
  
Client2=Company\Computer2  
  
Client3=Company\100.4.13.75
```

Where:

- `Company` is the domain name
- `Computer1`, `Computer2`, and `100.4.13.75` are the computer names and IP address of the target computers.

9. Save `NTBRinst.ini`.
10. Open a command prompt and go to `\PCCSRV\Admin`.
11. Run `NTBRinst.exe` using the following syntax:

```
NTBRInst User_name Password
```

Where `User_name` and `Password` are the user name and password you use to log in to these computers. Make sure you have administrator rights to the target computers.

The NT Remote Install utility installs the client to the target computers.

## Installing the client with NT Client Installer

Use the NT Client Installer utility to search for unprotected Windows XP/2000/NT computers on the network and install the OfficeScan client. The NT Client Installer is suitable for deploying the client to large networks.

### To install with NT Client Installer

1. On the OfficeScan server, open Windows Explorer and browse to the `\PCCSRV\Admin\Utility\CNIC` folder of OfficeScan.
2. Copy the contents of the folder to the `\PCCSRV\Admin` folder.
3. Go to the `\PCCSRV\Web\Cgi` folder and copy `Tmnotify.dll` to the `\PCCSRV\Admin` folder.
4. Go to the `\PCCSRV\Admin` folder and double-click `Cnic.exe`. The NT Client Installer console opens.
5. Click **Select server**, and then browse for the database file (`Dbcidata.dbf`) on the server. This file is in the `\PCCSRV\HTTPDB\Data` folder of OfficeScan.
6. Select `Dbcidata.dbf`, and then click **Open**.
7. Specify the domains that you want to check for unprotected Windows XP/2000/NT computers by selecting the corresponding check boxes.

If there is a specific IP address range that you want to check for unprotected clients, click **Set IP Range**, and then type the IP address range.

8. Click **Check and Install** to search for unprotected Windows XP/2000/NT computers and automatically install the client on them.

The **Select OfficeScan Version** screen appears.

9. Click **HTTP-based OfficeScan**, and then click **OK**.

The **Enter Administrator Information** screen appears.

10. Type your user name and password in the text boxes. The account must have domain administrator privileges.

11. Click **OK**.

NT Client Installer checks for unprotected Windows XP/2000/NT computers in the selected domains. When it finds an unprotected computer, it will automatically install the client.

After NT Client Installer completes checking for unprotected computers and installing the clients, the console displays the results, including:

- The number of computers that were checked
- The number of unprotected computers that were found
- The number of successful client installations
- The number of unsuccessful client installations

## 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:

- Create the setup package
- Distribute or “advertise” the package to the target computers

---

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

---

### To create the setup package

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 XP/2000/NT client is in \PCCSRV\PCCNT\Disk1\setup.pdf. The PDF for the Windows Me/98/95 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 XP/2000/NT client, it will show “OfficeScan Client NT/2K/XP setup”. If you selected the PDF for the Windows Me/98/95 client, it will show “OfficeScan Client 95/98/ME setup”.

8. Click **Next**. The **Source Files** screen appears.
9. Click **Always obtain files from a directory source**, and then click **Next**.

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

10. 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 XP/2000/NT, click **All Windows NT Systems**.
- If you created a client setup package for Windows 95 only, click **All Windows 95 Systems**.
- If you created a client setup package for Windows 98 only, click **All Windows 98 Systems**.
- If you created a client setup package for both Windows 98 and Windows 95, click **All Windows 98 Systems** and **All Windows 95 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 and spin 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 and spin boxes.

16. Click **Next**. The **Assign Program** screen appears.
17. Click **No. Do not 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.

## Verifying a successful installation

You can check if there are still desktop and notebook computers on the network that are not protected against viruses by running Trend Micro Vulnerability Scanner. This tool checks computers on the network for installed antivirus software based on an IP address range you specify.

## Using Vulnerability Scanner to verify the client installation

Use Vulnerability Scanner to detect installed antivirus solutions and to search for unprotected computers on the network. This tool pings ports that are normally used by antivirus solutions to determine if computers are protected.

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/NT 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.

---

**WARNING!** *You cannot run Vulnerability Scanner on computers running Windows XP/Me/98/95.*

---

### To verify client installation using Vulnerability Scanner

1. Open the TMVS folder, and then double-click `TMVS.exe`. The Vulnerability Scanner console appears.
2. Click **Settings**. The **Settings** screen appears.
3. Under **Product Query**, select the **OfficeScan Corporate Edition** check box.
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. 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, 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. If you want 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.
7. Type a new alert message in the text box or accept the default message, and then click **OK**.

8. If you want 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.

9. Browse for a target folder on your computer or on the network, and then click **OK**.
10. 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.
11. Click **OK**. The Vulnerability Scanner console appears.
12. In **IP Range to Check**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers.
13. Click **Start** to begin checking the computers on the network.

Vulnerability Scanner checks the network and displays the results in the **Results** table. Verify that all desktop and notebook computers running Windows XP/2000/NT and Windows Me/98/95 have the client installed.

If Vulnerability Scanner finds any unprotected desktop and notebook computers, install the client on them using your preferred client installation method.

## Testing the client installation

After installing the client, you may test it to verify that the antivirus function is working properly and to see how virus detection and notifications actually work.

The European Institute for Computer Antivirus Research (EICAR) has developed a test script that can be used to test antivirus software. This script is an inert text file whose binary pattern is included in the virus pattern file of most antivirus vendors.

The EICAR test script is not a virus and does not contain any program code. Trend Micro does not recommend using real viruses to test your antivirus installation.

### To test the client installation using the EICAR test script

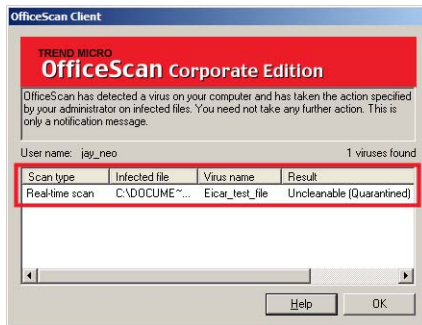
1. Make sure that real-time scan is enabled on the client.



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. On the **File** menu, click **Save As**. The **Save As** dialog box appears.
4. In **File name**, type `eicar.com`, and then click **Save**. Real-time scan detects the test script and displays the screen shown in Figure 3-8.



**FIGURE 3-8. Real-time scan detects the EICAR test script**

You can also download the EICAR test script from the following URLs:

[www.trendmicro.com/vinfo/testfiles/](http://www.trendmicro.com/vinfo/testfiles/)

[www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)

If you are downloading the EICAR test script, disable any antivirus software running on the computer before downloading. Otherwise, it will detect the EICAR test script as a virus and stop the download.

## Removing the client

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

- Remove the client using Uninstall Now
- Remove the client using its uninstallation program

## Removing the client using Uninstall Now


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

---

**WARNING!** *Removing the OfficeScan client may expose your computer to virus threats.*

---

### To remove the client using Uninstall Now

1. On the sidebar, click **Client Administration**. The domain tree for Client Administration 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 Now**. The **Uninstall Now** screen appears.
4. Under **Computer**, select the clients that you want to remove, and then click **Start Notification**. The server sends a request to the client to run the client uninstallation program.

### To stop notifications

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

- Select the clients that you no longer want to remove.
- 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 will not be affected.

## Removing the client using its uninstallation program

If you granted users the privilege to remove the client program, you can instruct them to run the client uninstallation program.

### **To run the client uninstallation program**

1. On the Windows **Start** menu, click **All 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.

When uninstallation is complete, the message "Uninstallation is complete" appears. If you are using Windows XP, you need to restart your computer to complete the uninstallation.

# Configuring OfficeScan

This chapter discusses the essential configuration tasks that you need to perform to get OfficeScan up and running on the network.

The topics discussed in this chapter include:

- Opening the Web console
- Getting around the Web console
- Keeping your protection current
- Configuring the antivirus settings
- Running Scan Now
- Granting privileges to clients
- Registering OfficeScan

## Opening the Web console

The Web console is installed when you install the HTTP-based version of the OfficeScan server. This version of the management console 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://{server name}/officescan` in the address bar.
2. Press ENTER. The browser displays the **Welcome** screen of OfficeScan.



**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 Web console.

---

**Note:** The **Welcome** screen of the Web console contains a text box where you can type your serial number to upgrade a 30-day trial version of OfficeScan to the full version. It also has a link that users can click to install the client on their desktop and notebook computers.

---

## Getting around the Web console

The Web console is divided into two main parts: the sidebar and the main frame. The sidebar groups tasks that you perform into sections (except for the Toolbox section). **Set Privileges** and **Scan Now**, for example, are tasks that you can run under **Client Administration**.

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 which you use to perform the task.

The sidebar contains the following sections:

- Manual Outbreak Prevention
- Client Administration
- Server Administration
- Update & Upgrade
- Logs
- Toolbox
- Registration

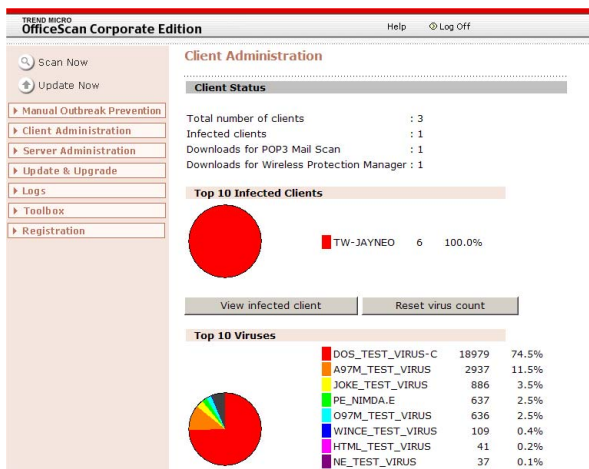


FIGURE 4-2. The Web console, displaying the Client Administration screen

The sidebar also contains shortcuts to **Scan Now** and **Update 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 updated pattern file, scan engine, and program.

## Manual Outbreak Prevention

Activate Now	Enable Manual Outbreak Prevention to control an outbreak that may be developing on the network.  For more information, see <a href="#">Using Manual Outbreak Prevention</a> starting on page A-1.
Restore to Normal	Disable Manual Outbreak Prevention and restore network settings to normal after an outbreak is contained.  For more information, see <a href="#">Restoring network settings to normal</a> on page A-8.

## Client Administration

Set Scan Options	Configure the real-time scan, manual scan, scheduled scan, and file exclusion settings
Set Privileges	Grant users privileges to modify individual scan settings, update components, and remove or unload the client
Scan Now	Perform a manual scan on selected clients from the Web console
Uninstall Now	Remove the client program from the Web console
View Status	View client information, including its privileges and the versions of its program, pattern file, and scan engine

NT Remote Install	Install the client software to Windows XP/2000/NT computers remotely using the Web console. You can install to multiple computers at the same time without having to physically go to each computer.
Verify Connection	Check the connection status of the clients manually or automatically
Advanced 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

## **Server Administration**

Set Password	Change the password to the Web console periodically to prevent unauthorized users from modifying the settings or removing the clients
Standard Alert	Send alerts to yourself or other administrators in your organization whenever OfficeScan detects a virus on any client
Outbreak Alert	Send alerts to yourself or other administrators in your organization whenever the outbreak criteria you have defined is met
Client Alert Message	Modify the message that is displayed on the clients whenever a virus is detected



Intranet Proxy	Type the proxy server information if client-server communication is handled by a proxy server on the intranet
Web Server	Update the settings whenever the Web server settings are modified
Inactive Clients	Automatically remove inactive clients to ensure that the domain tree displays active clients only
Quarantine Manager	Set the capacity of the quarantine folder and the maximum file size for every infected file that can be stored in it

## Update & Upgrade

Server Update	<p>Update the components on the server manually or automatically</p> <p>For more information, see <a href="#">Updating the server</a> on page 4-13.</p>
Client Update	<p>Update the clients manually or automate the deployment of updates</p> <p>For more information, see <a href="#">Updating clients</a> on page 4-15.</p>
Rollback	Revert the pattern file or scan engine to the previous version if you encounter problems after deploying it
Internet Proxy	Configure your proxy settings to download updates from the Trend Micro update server

## Logs

Virus Logs	View a list of viruses that have infected clients on the network, with details about the infection.
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.
Update Logs	View update details for both the server and clients. Use these logs to keep track of the server's update history and to verify that updates were successfully deployed to clients.
Verify Connection Logs	View Verify Connection logs to determine the connection status between the server and clients.
Log Maintenance	To conserve disk space on the server, set a schedule when logs will be deleted.

## Toolbox

Administrative Tools	View information on tools that can help you manage the server and clients
Client Tools	View information on tools that can help the OfficeScan client adapt to different enterprise environments

## Registration

Register OfficeScan to receive technical support, and pattern and program updates for one year

## 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.

### Links at the upper right corner

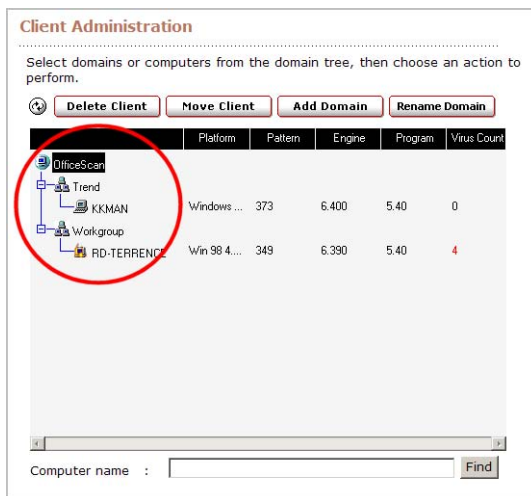
Help	Click to open the online help system
Log Off	Click to end your session. Logging off the Web console prevents unauthorized users from modifying the settings or removing the clients.

### Links below the main frame

Help	Click to open the online help system
Support	Click to display the Trend Micro support Web page, where you can submit questions and find answers to common questions about Trend Micro products
Security Info	Click to display the Trend Micro Security Information page, where you can read about the latest virus threats
About	Click to display the About screen, which contains an overview of the product and tells you how to check the version of the components

## Understanding the domain tree

The domain tree is displayed in the main frame when you click any function from the Manual Outbreak Prevention, Client Administration, and Logs groups. It is a Java-based tree that displays OfficeScan domains and clients on the network.



**FIGURE 4-3. The domain tree for Client Administration**

Most of the functions in the Manual Outbreak Prevention, Client Administration, and Logs groups require you to select a domain or client in the domain tree before performing an action.

For an explanation of the icons on the Web console, see [Understanding the domain tree icons](#) on page 4-10.

## How domains are created

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


For example, if your network currently has a domain called 'YourCompany' with three computers named 'Sith', 'Jedi', and 'Maul', when you install OfficeScan on these

three computers, OfficeScan will automatically create a domain called 'YourCompany' and populate this domain with these three computers.


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

## Selecting domains and clients from the tree

You can select domains or clients to simultaneously apply settings.

- To select a single domain or client, click the domain or client name. The domain or client name will be highlighted.
- To select multiple, adjacent domains or clients, click the first domain or client in the range, hold down the SHIFT key, and then click the last domain or client in the range. All the domains or clients between the two mouse clicks will be selected.
- To select a range of non-adjacent domains or clients, click the first domain or client in the range. Hold down the CTRL key and then click the domains or clients that you want to select. All domains or clients that you click will be selected.
- To select all clients that report to the server, click the root icon .

## Refreshing the tree

To refresh the domain tree, click the refresh button .

## Understanding the domain tree icons

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



OfficeScan domain, double-click to display clients that belong to this domain



Normal client



Offline client, either it is turned off or it cannot establish communication with the server



Infected client



Roaming client



Normal client in Manual Outbreak Prevention mode



Infected client in Manual Outbreak Prevention mode

## Working with domains

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

For ease of management, you can group clients based on the departments to which they belong or the functions they perform. You can 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 2000/NT domain. There can be several OfficeScan domains in one Windows 2000/NT domain.


By default, OfficeScan creates domains based on existing Windows 2000/NT domains and refers to each client according to its computer name. You can delete or rename the domains that OfficeScan has created for you, or you can create a new domain. You can even transfer clients from one domain to another.

### To add a domain

1. On the sidebar, click **Client Administration**. The domain tree for Client Administration appears.
2. Click **Add Domain** in the main frame. A dialog box appears.
3. Type a name for the domain you are adding, and then click **OK**. The new domain appears in the domain tree.

### To delete a domain

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

2. In the domain tree, double-click the domain that you want to delete. The clients that belong to the domain are displayed.
3. Move the clients to other domains. You can do this by dragging and dropping the clients to other domains.
4. When the domain is empty, click the refresh button . The domain is deleted.  
You can also leave the domain empty to delete it. OfficeScan automatically removes empty domains.

#### To rename a domain

1. On the sidebar, click **Client Administration**. The domain tree for Client Administration appears.
2. Click the domain that you want to rename, and then click **Rename Domain**. A dialog box appears.
3. Type a new name for the domain, and then click **OK**. The domain is renamed in the domain tree.

#### To move a client

1. On the sidebar, click **Client Administration**. The domain tree for Client Administration appears.
2. Select the client that you want to move, and then click **Move Client**. A list box appears.
3. From the list, select the domain where you want to move the client, and then click **OK**. The client appears under the domain you have selected.

Another way is to drag and drop the client to the domain where you want to move it.

## Keeping your protection current

To ensure that clients stay protected against the latest virus threats, you need to regularly update the OfficeScan components, including the virus pattern file, scan engine, and program. Updating the components is one of the key administrative tasks that you should regularly perform after installation.

Trend Micro recommends updating the components at least once every week. The easiest way to ensure that components are updated regularly is to configure scheduled updates to run every week.

## Updating the server

You update components by configuring the server to download pattern file, scan engine, or program updates from the Trend Micro update server. After the server downloads any available updates, it deploys these to the clients based on the deployment schedule you specified on the **Automated Deployment** screen under **Client Update**.

The scan engine and program are not updated very often; generally, these are only updated when a new version of OfficeScan is released. Pattern files, on the other hand, are updated every week to ensure that clients are protected from new virus threats.

OfficeScan provides two methods of updating the server. You can:

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

## Configuring scheduled updates for the server

You can configure the server to regularly check the Trend Micro update server and automatically download any available update. Because clients normally get updates from the server, automating server update is an easy and effective way of ensuring that your protection against viruses is always up-to-date.

### To update the server based on a schedule

1. On the sidebar, click **Update & Upgrade > Server Update > Scheduled Update**. The **Scheduled Server Update** screen appears.



2. Under **Enable Scheduled Server Update**, select the **Enable scheduled update of the OfficeScan server** check box.
3. Under **Update schedule**, specify a schedule when to perform scheduled update.
  - **Hourly** - click to perform scheduled update every hour
  - **Daily** - click to perform scheduled update every day
  - **Weekly** - click to perform scheduled update once a week. You must select a day from the list.
  - **Monthly** - click to perform scheduled update once a month. You must select a date from the list.

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

4. If you want the server to continue retrying a failed update attempt, select the **Retry 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.

5. Under **Components to Update**, select the components that you want to download from the Trend Micro update server.
6. Click **Apply** to save your settings.

## Updating the server manually

You can 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 **Update & Upgrade > Server Update > Manual Update**. The **Manual Server Update** screen appears, showing the current components, their version numbers, and the dates when they were last updated.
2. Click **Update**. The server checks the Trend Micro update server for updated components. If there are available updates, these will be displayed on the

**Available Updates From Trend Micro** screen, with the component names and version numbers.

3. Select the check boxes for the components you want to update.
4. Click **Update Now**. The server downloads the updated components. The download progress is shown on the **Manual Update** screen.

---

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

---

To check if you have specified a download schedule, click **Update & Upgrade > Client Update > Automated Deployment** on the sidebar.

---

**Note:** If you use a proxy server to connect to the Internet, make sure your proxy settings are properly configured to download updates successfully. For information on how to configure proxy settings, refer to the topic *Setting the Internet proxy* in the online help.

---

## Updating clients

To ensure that clients stay protected from the latest virus threats, you need to regularly update their components. The clients get updates from the server, which, in turn, downloads updates from the Trend Micro update server.

Before updating the clients, verify that the server has the latest components, including the pattern file, scan engine, and program. For information on how to update the server, refer to *Updating the server* on page 4-13.

The scan engine and program are not updated very often; generally, these are only updated when a new version of OfficeScan is released. Pattern files, on the other hand, are updated every week to ensure that clients are protected from new virus threats.

OfficeScan provides you four methods of updating clients. You can:

- Update the clients using Automated Deployment
- Update the clients using Manual Deployment

- Enable Scheduled Updates
- Use Update Now on the client

Except for using Update Now on the client, these methods can update the following components on the client:

- Pattern file
- Scan engine
- Program
- Hot fix
- Configuration settings, including privilege settings, advanced settings, scan settings, and Manual Outbreak Prevention settings

## Updating clients using Automated 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 Automated Deployment

1. On the sidebar, click **Update & Upgrade > Client Update > Automated Deployment**. The **Automated Deployment** screen appears.
2. Under **Target Clients**, specify which clients to update automatically by clicking either **All online clients** or **Selected client(s)**.
  - If you clicked **Selected client(s)**, do the following:
    - i. Click **Select** to choose the clients to update. The **Selected Clients** screen appears.
    - ii. In the **Domain** list, click all the domains or clients that you want to update automatically.
    - iii. When all domains or clients are selected, click **Add Client**. The selected domains or clients appears in the **Target** list on the right.
    - iv. Click **Back**. The **Automated Deployment** screen appears again.

3. If you want to update all online clients including roaming clients with functional connections to the server, select the **Force notification to all clients, including roaming clients** check box.
4. Under **Deployment Schedule**, specify when to deploy the updates. You can select either or both **Deploy immediately (including hot fix)** and **Deploy to clients (excluding roaming clients) when they are restarted** check boxes.

---

**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.

---

5. Click **Apply** to save your settings.

## Updating clients using Manual Deployment

You can update clients manually by pushing updated components on the server to the clients using Manual Deployment.

### To update clients using Manual Deployment

1. On the sidebar, click **Update & Upgrade > Client Update > Manual Deployment**. The **Manual Deployment** screen appears.
2. If you want to update all online clients, including roaming clients with functional connections to the server, select the **Force notification to all clients, including roaming clients** check box.
3. Click **Notify** to select clients to update manually. The **Clients to Update Manually** screen appears.
4. Select the clients that you want to update by clicking the client name in the domain tree.
  - 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. All clients between the two mouse clicks will be selected.
  - To select a range of non-adjacent clients, click the first client in the range, hold down the CTRL key, and then click the clients that you want to select. All clients that you clicked will be selected.


- If the clients that you want to update do not appear in the domain tree, type the name of a client in the **Computer name** text box, and then click **Find**. Once the server finds the client, it will appear in the domain tree.
5. When you have selected all clients that you want to update, click **Start Notification**. The server starts notifying each client to download the updates. The **Status** and **Error** columns will show if the notification has been received and if the update was successful, respectively.

## Updating clients using Scheduled Update


Scheduled Update lets clients check the server for updates based on the schedule you specify. Enabling Scheduled Update is a two-step process:

- Grant clients the privilege to enable Scheduled Update
- Configure the Scheduled Update settings

### To grant clients Scheduled Update privileges

1. On the sidebar, click **Client Administration**. The domain tree for Client Administration appears.
2. Click the domains or clients to which you want 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 **Set Privileges**. The **Set Privileges** screen appears.
4. Under **Update**, select the **Enable scheduled update** check box.
5. Click **Apply** to grant the privilege to the selected domains or clients.

---

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

---

### To configure the Scheduled Update settings

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


2. On the sidebar, click **Advanced Settings**. The **Advanced Settings** screen appears.
3. Under **Scheduled Update Settings**, select the **Check the OfficeScan server for updates** check box.  
  
Then, specify a schedule by clicking an option. If you clicked **Every { } hour(s)**, you must specify the frequency by selecting values from the **hour(s)** and **minute(s)** list boxes.
4. Click **Apply**.

Scheduled Update is now enabled. The clients you selected will check the server for updates based on the schedule you specified.


## Updating clients using Update Now

You can instruct users to update the client components by performing Update Now on the client. Performing Update Now downloads updated components from the OfficeScan server. 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 update server

1. On the sidebar, click **Client Administration**. The domain tree for Client Administration appears.
2. Click the domains or clients to which you want 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 **Set Privileges**. The **Set Privileges** screen appears.
4. Under **Update**, select the **Download from the Trend Micro update server** check box.
5. Click **Apply** to grant the privilege to the selected domains or clients.

---

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

---

**To perform Update Now on the client**

1. Right-click the OfficeScan icon in the system tray. The OfficeScan shortcut menu appears.
2. Click **Update Now**. The **Update Now Settings** screen appears.
3. In the **Domain name/IP address** list, choose an update source.
  - If you want to download from the OfficeScan server, verify that the domain name/FQDN or IP address of the server is correct.
  - If you want to download from the Trend Micro update server and you have been granted this privilege, click the **Domain name/IP address** arrow, and then click the address of the Trend Micro update server. The default address is:

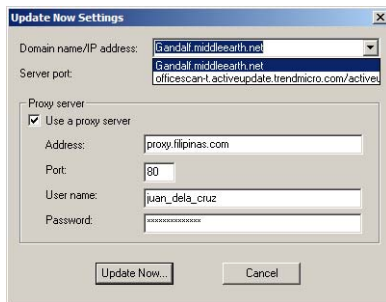
officescan-t.activeupdate.trendmicro.com/activeupdate

---

**Note:** If you are downloading directly from the Trend Micro update server, you can only update the pattern file and scan engine.

---

4. In **Server port**, verify that the server port number, which the client uses to communicate with it, is correct. The default port number is port 80, which is also normally used as the HTTP port.



**FIGURE 4-4.** Choose an update source by clicking the **Domain name/IP address** arrow, and then specify the server port

5. If a proxy server has been set up to handle client-server communication on the network, select the **Use a proxy server** check box.

6. Type the proxy server address and port number in the text boxes. If the proxy server requires a user name and a password, type your user name and password.
7. Click **Update Now**. The client connects to the selected update source to check for updates. If updates are available, the client automatically downloads these.

## Verifying a successful update

You can check the Client Update Logs to verify that an update has been successfully deployed.

### To view the Client Update Logs

1. On the sidebar of the Web console, click **Logs > Update Logs > Client Update**. The **Client Update Logs** screen appears.
2. If you want 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.
3. If you want to view the details of a particular update, click **View** under the **Details** column. The **Client Update Details** screen appears, displaying the following information:
  - The computer name of each client that was updated
  - The date and time when the server sent the update notification to the client
  - The date and time when the client received the update notification from the server
  - The date and time when the update was completed



## Setting up notifications

The latest Internet-aware viruses, if left unchecked, can spread quickly throughout your organization and overwhelm network resources. You should set up notifications for OfficeScan to inform you about detected viruses or any outbreak that may be developing on the network.

You can configure OfficeScan to send two types of alerts:

- Standard alerts
- Outbreak alerts

## Configuring standard alerts

You can send alerts to yourself or other administrators in your organization whenever OfficeScan detects a virus on any client. Standard alerts keep you informed about virus activities on the network.

To ensure that recipients get the alerts, OfficeScan provides you with multiple ways of sending alerts. You can send standard alerts by way of:

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

### To send alerts via email

1. On the sidebar, click **Server Administration > Standard Alert > Email Notification**. The **Standard Alert** screen appears.
2. Select the **Enable email notification** check box.
3. Type the name of the SMTP server and its port number.
4. In **To**, type the email address where you want to send the alert. If you are sending to multiple email addresses, separate the addresses with commas.
5. In **From**, type your name or email address. This will let the alert recipients know where the alert came from.

6. Edit the subject of the message, if necessary. The default subject is 'Standard Alert'.
7. Type your message in the **Message** text box.

To provide more information with the alert, the following information is included in the message by default:

  - Computer name
  - User name
  - Domain name
  - File path of the infected file
  - Virus name
  - Date and time of detection
  - Scan action and result
8. Click **Apply** to save your settings.

#### **To send alerts via pager**

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

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

1. On the sidebar, click **Server Administration > Standard Alert > NT Event Log**. The **Standard Alert** screen appears.
2. Select the **Enable notification via NT Event Log** check box.
3. Type your message in the **Message** text box.

To provide more information with the alert, the following information is included in the message by default:

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

4. Click **Apply** to save your settings.

#### **To send alerts via SNMP Trap**

1. On the sidebar, click **Server Administration > Standard Alert > SNMP Trap**. The **Standard Alert** screen appears.
2. Select the **Enable notification via SNMP Trap** check box.
3. Type the IP address you use for SNMP trap notifications and the community name.
4. Type your message in the **Message** text box.

To provide more information with the alert, the following information is included in the message by default:

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

5. Click **Apply** to save your 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 will constitute an outbreak.

Responding to an outbreak is very critical. Unless corrective action is taken, an outbreak can spread quickly throughout and beyond the network.

To help you respond to outbreaks that may be developing on the network, you can send outbreak alerts to yourself or other administrators in your organization whenever the outbreak criteria you have defined is met.

Major outbreaks can quickly overwhelm a network. Trend Micro recommends setting the time period to be relatively short (between 1 to 5 hours) to be able to respond to an outbreak when it is just starting.

When you get an outbreak alert, you can use Manual Outbreak Prevention to control the outbreak on the network. For more information on Manual Outbreak Prevention, see [Using Manual Outbreak Prevention](#) on page A-1.

OfficeScan provides you with multiple ways of sending alerts. You can send outbreak alerts by way of:

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

### To send alerts via email

1. On the sidebar, click **Server Administration > Outbreak Alert > Email Notification**. The **Outbreak Alert** 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 will constitute an outbreak.
4. Type the name of the SMTP server and its port number.
5. In **To**, type the email address to which you want to send the alert. If you are sending to multiple email addresses, separate the addresses with commas.

6. In **From**, type your name or email address. This will let the recipients know where the alert came from.
7. Edit the message subject, if necessary. The default subject is 'Outbreak Alert'.
8. Type your message in the **Message** text box.

To provide more information with the alert, the following information is included in the message by default:

  - Client/domain name
  - Path of the infected file
  - Virus name
  - Action taken
  - Date and time of outbreak
9. Click **Apply** to save your settings.

#### **To send alerts via pager**

1. On the sidebar, click **Server Administration > Outbreak Alert > Pager Notification**. The **Outbreak Alert** 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 will constitute an outbreak.
4. Type the pager number to which you want to send the alert message.
5. Select the COM (communications) port to which the modem is connected.
6. Type your message in the **Message** text box.
7. Click **Apply** to save your settings.

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

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

**To send alerts via SNMP trap**

1. On the sidebar, click **Server Administration > Outbreak Alert > SNMP Trap**. The **Outbreak Alert** 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 will constitute an outbreak.
4. Type the IP address you use for SNMP trap notifications and the community name.
5. Type your message in the **Message** text box.
6. Click **Apply** to save your settings.

## Configuring the scan settings

OfficeScan provides three types of scans: real-time scan, scheduled scan, and manual scan. You can enforce your organization's antivirus policies throughout the network by configuring the three types of scans based on these policies. You can 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, shown in Table 4-1, also provide adequate level of protection for most environments.

You can also 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 4-35.

## Default antivirus settings

The table below displays the scan settings that clients will inherit if you deploy the client program without modifying the default settings of OfficeScan.

	File types to scan	Scan target	Action on infected files	Action on uncleanable files	Quarantine directory
Manual Scan	Use IntelliScan	Boot area, compressed files	Auto clean	Quarantine	http://server_name
Real-time Scan	Files with specified extensions only	Compressed files	Auto clean	Quarantine	http://server_name
Scheduled Scan	Use IntelliScan	Boot area, compressed files	Auto clean	Quarantine	http://server_name
Scan Now (from the Web console)	Use IntelliScan	Memory, boot area, compressed files	Auto clean	Quarantine	http://server_name

**TABLE 4-1. Default scan settings of OfficeScan**

## About IntelliScan

IntelliScan is a new method of identifying files to scan that is more efficient than the standard **Scan all files** option. 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 brings you 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.

## About 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. For this reason, Trend Micro came up with ActiveAction.

ActiveAction is a set of pre-configured scan actions for viruses and other types of malware. 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 brings you 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 customizing the scan actions.
- Updateable scan actions — Virus writers constantly change the way viruses attack computers. To ensure that clients are protected against the latest threats and the latest methods of virus attacks, ActiveAction settings are updated in every new pattern file.

## Configuring real-time scan

You can set OfficeScan to scan a file in real-time whenever it is opened or saved. If no virus is detected, the user can proceed with opening or saving the file. If a virus is detected, OfficeScan displays an alert message, showing the name of the infected file and the virus name.

The speed of real-time scanning depends on its settings. You can speed up 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 **Client Administration**. The domain tree for Client Administration appears.
2. Click the domains or clients to which you want 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 **Set Scan Options > Real-time Scan**. The **Real-time Scan Settings** screen appears. If you are configuring these settings for the first time, the **Default Real-time Scan Settings** screen appears.
4. Under **Enable real-time scan**, select the **Enable real-time scan** check box.



5. Under **Scan Target**, specify the files to scan by selecting the check boxes and clicking the options.
- **Scan floppy drives at shutdown** - select to run real-time scan on floppy drives every time the client is shut down
  - **Scan boot area** - select to scan the boot sector of the hard disk on the client. This setting is not applicable to Windows XP/2000/NT clients.
  - **Scan compressed files** - select to scan compressed files that are saved or opened on the client. In the **Up to { } compression layers** list, select the maximum number of compression layers that you want to scan.
  - **Scan all files** - click to scan all files that the client opens or saves
  - **Use IntelliScan - all essential file types** - click if you want to use IntelliScan
  - **Scan files with the following extensions** - click if you want to manually specify the files to scan based on their extensions

You can add or delete extensions from the default set of extensions. The default extensions include: .BIN, .COM, .DOC, .DOT, .DRV, .EXE, .SYS, .XLS, .XLA, .XLT, .VBS, .JS, .HTM, .HTML, .CLA, .CLASS, .SCR, .MDB, .PPT, .DLL, .OCX, .OVL, .POT, .SHS, .PIF, .HLP, .HTA, .MPP, .MPT, .MSG, .OFT, .PPS, .RTF, .VSD, .VST, .EML, .NWS, and .ASP.

---

**Tip:** You can also use ? and \* as wildcards when specifying extensions. For example, if you want to scan all files with extensions starting with D, you can type .D? or .D\*. OfficeScan will scan all files with extensions starting with D, including .DOC, .DOT, and .DAT.

---


6. Under **Scan Action**, specify how to handle viruses when detected.
- **Use ActiveAction - recommended actions by file type** - click if you want to use ActiveAction
  - **Specify scan action** - click if you want to manually specify how to handle viruses when detected
  - In the **Action on infected files** list, select the action to perform on infected files. You can click **Pass**, **Delete**, **Rename**, **Quarantine**, and **Auto clean**. The recommended scan action is **Auto clean**. If you select **Auto clean**, you must specify an alternative action, in case the file cannot be cleaned, in the **Action on uncleanable files** list.

Cleaning a file may sometimes damage it. Trend Micro recommends backing up the file before cleaning it. To save a copy of the file before it is cleaned, select the **Back up files before cleaning** check box.

- In the **Action on uncleanable files** list, select an alternative action, in case the file cannot be cleaned.
- In **Quarantine directory**, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path where you want to store the infected files.

7. Click **Apply** to save your real-time scan settings.

---


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

---

## Configuring manual scan

Also called Scan Now, manual scan occurs momentarily after being invoked and completely scans all files you have 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 **Client Administration**. The domain tree for Client Administration appears.
2. Click the domains or clients to which you want 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 **Set Scan Options > Manual Scan**. The **Manual Scan Settings** screen appears.
4. Under **Scan Target**, specify the files to scan by selecting the check boxes and clicking the options.
  - **Scan memory** - select to scan the Random Access Memory (RAM) of the client. This setting is not applicable to Windows XP/2000/NT clients.
  - **Scan boot area** - select to scan the boot sector of the hard disk on the client

- **Scan compressed files** - select to scan compressed files that are stored on the client. In the **Up to { } compression layers** list, select the maximum number of compression layers that you want to scan.
- **Scan all files** - click to scan all files that the client opens or saves
- **Use IntelliScan - all essential file types** - click if you want to use IntelliScan
- **Scan files with the following extensions** - click if you want to manually specify the files to scan based on their extensions
- **Scan files with the following extensions** - click if you want to manually specify the files to scan based on their extensions

You can add or delete extensions from the default set of extensions. The default extensions include: .BIN, .COM, .DOC, .DOT, .DRV, .EXE, .SYS, .XLS, .XLA, .XLT, .VBS, .JS, .HTM, .HTML, .CLA, .CLASS, .SCR, .MDB, .PPT, .DLL, .OCX, .OVL, .POT, .SHS, .PIF, .HLP, .HTA, .MPP, .MPT, .MSG, .OFT, .PPS, .RTF, .VSD, .VST, .EML, .NWS, and .ASP.


5. Under **Scan Action**, specify how to handle viruses when detected.

- **Use ActiveAction - recommended actions by file type** - click if you want to use ActiveAction
- **Specify scan action** - click if you want to manually specify how to handle viruses when detected
  - In the **Action on infected files** list, select the action to perform on infected files. You can click **Pass**, **Delete**, **Rename**, **Quarantine**, and **Auto clean**. The recommended scan action is Auto clean. If you select **Auto clean**, you must specify an alternative action, in case the file cannot be cleaned, in the **Action on uncleanable files** list.

Cleaning a file may sometimes damage it. Trend Micro recommends backing up the file before cleaning it. To save a copy of the file before it is cleaned, select the **Back up files before cleaning** check box.
  - In the **Action on uncleanable files** list, select an alternative action, in case the file cannot be cleaned.
  - In **Quarantine directory**, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path where you want to store infected files.

6. Click **Apply** 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 clients** will appear beside **Apply**. If you want all existing and future clients to have these manual scan settings, click **Apply to all clients**.

---

## 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 **Client Administration**. The domain tree for Client Administration appears.
2. Click the domains or clients to which you want 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 **Set Scan Options > Scheduled Scan**. The **Scheduled Scan Settings** screen appears.
4. Under **Enable scheduled scan**, select the **Enable scheduled scan** check box.
5. Under **Scanning schedule**, specify a schedule when to perform scheduled scan.
  - **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 when to perform schedule 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.
  - **Scan memory** - select to scan the Random Access Memory (RAM) of the client. This setting is not applicable to Windows XP/2000/NT clients.


- **Scan boot area** - select to scan the boot sector of the hard disk on the client.
- **Scan compressed files** - select to scan compressed files that are stored on the client. In the **Up to { } compression layers** list, select the maximum number of compression layers that you want to scan.
- **Scan all files** - click to scan all files that the client opens or saves.
- **Use IntelliScan - all essential file types** - click if you want to use IntelliScan
- **Scan files with the following extensions** - click if you want to manually specify the files to scan based on their extensions.

You can add or delete extensions from the default set of extensions. The default extensions include: .BIN, .COM, .DOC, .DOT, .DRV, .EXE, .SYS, .XLS, .XLA, .XLT, .VBS, .JS, .HTM, .HTML, .CLA, .CLASS, .SCR, .MDB, .PPT, .DLL, .OCX, .OVL, .POT, .SHS, .PIF, .HLP, .HTA, .MPP, .MPT, .MSG, .OFT, .PPS, .RTF, .VSD, .VST, .EML, .NWS, and .ASP.

7. Under **Scan Action**, specify how to handle viruses when detected.
    - **Use ActiveAction - recommended actions by file type** - click if you want to use ActiveAction
    - **Specify scan action** - click if you want to manually specify how to handle viruses when detected
      - In the **Action on infected files** list, select the action to perform on infected files. You can click **Pass**, **Delete**, **Rename**, **Quarantine**, and **Auto clean**. The recommended scan action is **Auto clean**. If you select **Auto clean**, you must specify an alternative action (in case the file cannot be cleaned) in the **Action on uncleanable files** list.
- Cleaning a file may sometimes damage it. Trend Micro recommends backing up the file before cleaning it. To save a copy of the file before it is cleaned, select the **Back up files before cleaning** check box.
- In the **Action on uncleanable files** list, select an alternative action, in case the file cannot be cleaned.
  - In **Quarantine directory**, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path where you want to store the infected files.

8. Click **Apply** to save your scheduled scan settings.

---


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

---

## Excluding files and folders from scanning

To speed up scanning and 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 **Client Administration**. The domain tree for Client Administration appears.
2. Select the domains or clients on which you want 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 **Set Scan Options > File Exclusion**. The **File and Folder Exclusion Settings** screen appears.
4. In the text boxes, type the file or folder names that you want to exclude from scanning.

File names must be written as `filename.ext`. For example, you can type `policies.doc`.

Folder names must be written as `{Drive letter}:\{folder name}`. For example, you can type `C:\Windows`.

---

**WARNING!** *Do not use wildcards when typing file and folder names that you want to exclude from scanning. File and folder exclusion does not support wildcards.*

---

5. If you want to apply this setting to all future clients that will belong to the domain you selected, click **Apply**.

If you want to apply this setting to all existing and future clients that belong and will belong to the domain you selected, click **Apply to all clients**.

If you selected a client or clients, not domains, in Step 2, only **Apply** will appear. Click **Apply** to save you settings.

---


**Note:** The files and folders you specify in the exclusion list will apply to all types of scans (manual scan, real-time scan, scheduled scan, and Scan Now).

---

## Running Scan Now

You can 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 that you suspect to be infected.

### To run Scan Now

1. On the sidebar, click **Client Administration**. The domain tree for Client Administration appears.
2. Click the domains or clients on which you want 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 you have selected or the members of the domain you have selected.
4. Under **Computer**, select the clients on which you want to run Scan Now, and then click **Start Notification**. The server sends a request to the client to run Scan Now.

### To stop Scan Now

If you want to stop Scan Now on clients that are currently running it, do the following:

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

### To stop notifications

If you want to stop notifications to clients that have not yet started Scan Now, do the following:

1. Select the clients that 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 types 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 can grant users privileges to modify individual scan settings, update components, and remove or unload the client. You still retain control over OfficeScan on the network, even if you grant users privileges. Granting users privileges is simply a way of sharing control over individual client settings.

However, if you want 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 **Client Administration**. The domain tree for Client Administration appears.
2. Click the domains or clients to which you want 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 **Set Privileges**. The **Privileges** screen appears.
4. Select the privileges that you want to grant users. You can configure four areas:



- **Configuration** — Select the check boxes for the scan configuration privileges that you want to grant to users
- **Update** — Select the check boxes for the update privileges that you want to grant to users. You can allow users to **Enable Scheduled Update** and **Download from the Trend Micro update server**.


---

**Note:** Scheduled update can update the pattern file, scan engine, program, and hot fix. Downloading from the Trend Micro update server can only update the pattern file and scan engine. If you grant clients the privilege to **Enable Scheduled Update**, make sure you select the **Check the OfficeScan server for updates** check box on the **Advanced Settings** screen.

---

- **Uninstallation** — If you want to allow users to remove the client without requiring a password, click **Allow the client user to uninstall OfficeScan**. If you only want users with the uninstall password to be able to remove the client, click **Do not allow the client user to uninstall OfficeScan**, and then type an uninstall password in the text box.
  - **Unloading** — If you want to allow users to unload (or turn off) the client without requiring a password, click **Allow the client user to unload OfficeScan**. If you only want users with the unload password to be able to turn off the client, click **Do not allow the client user to unload OfficeScan**, and then type an unload password in the text box.
5. Click **Apply** to grant the privileges you have set to the selected domains or clients.

---

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

---

## Registering OfficeScan

Trend Micro provides technical support, virus pattern downloads, and program updates to all registered users for one year, after which you must purchase renewal maintenance.

**To register OfficeScan**

1. Open the Web console.
2. On the sidebar, click **Registration**. The **Online Registration** page of the Trend Micro Web site appears.
3. Type the required information in the text boxes. You may also provide the optional information.
4. Click **Submit**.

You can also type the following address in a Web browser to open the **Online Registration** page:

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

# Troubleshooting and Contacting Technical Support

This chapter provides solutions to common issues that you may encounter while installing the server and clients. It also points you to resources where you can find answers to your questions about OfficeScan and contains information on how to contact Trend Micro technical support.

The topics discussed in this chapter include:

- Troubleshooting installation issues
- Contacting technical support

## Troubleshooting installation issues

This section discusses some issues during:

- Server installation
- Client installation

### Server installation

This section discusses some issues that you may encounter when installing the server.

#### Server name without special characters

During master setup, if you select a server that has a space in its name, you may get this error message:

```
Please specify a server name that does not have special characters.
```

Resolve this issue by changing the computer name and removing the space. For example, if the server name is `TREND MICRO`, change it to `TRENDMICRO`. Then try installing OfficeScan again.

#### Insufficient memory during master setup

If you encounter the error message, "Insufficient memory available to run Setup", close all applications to make more memory available, and then run Setup again.

If this error occurs when there is sufficient memory available, run Setup at the command prompt with the following syntax:

```
setup -IZ1 -Z1
```

This makes the setup program to skip memory checking.

## Client installation

This section discusses some issues that you may encounter when installing the client.

### Client installation using Windows NT Remote Install fails

If Windows NT Remote Install does not accept the default user name and password, try typing the user name and password using the following syntax:

```
domain name\user name
```

### Login Script Setup error

If you are using Login Script Setup to install the client, you may get the following error message:

```
Error - Failed to logon. Please make sure the selected server  
<Server Name> is a Windows NT server, and enter the correct user  
name and password.
```

To correct this error, use an account that has domain administrator privileges.

### Windows XP/2000/NT computers are not displayed on the Windows NT Remote Install screen

Some Windows XP/2000/NT computers may not appear on the **Windows NT Remote Install** screen even if they are online. These computers and the server may be on the same subnet and the communication can be verified by using 'ping'.

To correct this problem, enable the file and print sharing in the Network Connection properties so that these computers can be visible on the network. Then try performing Windows NT Remote Install again.

### Client installation using the internal Web page is unsuccessful

If users cannot install the client from the internal Web page, their browser's Internet Options settings may be incorrect.

**To correct this error, instruct users to do the following:**

1. Open Internet Explorer.

2. Click **Tools > Internet Options**.
3. Click the **Connections** tab, and then click **LAN Settings**.
4. Verify that the **Bypass proxy server for local addresses** check box is not selected.
5. Click **OK** to save your changes and exit.
6. Try installing the client again from the internal Web page.

## Contacting technical support

If you cannot find an answer to a problem, the basic technical support team of Trend Micro will help you find the solution.

You must register OfficeScan to be eligible for support. For information on how to register OfficeScan, see [Registering OfficeScan](#) on page 4-38.

## Before contacting technical support

Before contacting technical support, here are two things you can do to quickly find the answer to a problem:

- Check the documentation — the Getting Started Guide and online help provide comprehensive information about OfficeScan. Search both documents to see if they contain the answer you are looking for.
- Search Trend Micro Knowledge Base — Trend Micro Knowledge Base contains comprehensive information about all Trend Micro products. Questions that were previously answered are also posted and a list of frequently asked questions is also available.

To search Knowledge Base, visit

[kb.trendmicro.com/solutions/solutionSearch.asp](http://kb.trendmicro.com/solutions/solutionSearch.asp).

## Requesting for basic technical support

A license to Trend Micro antivirus software includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one

year. Thereafter, you must renew Maintenance on an annual basis at the then-current Maintenance fees to have the right to continue receiving these services.

You can send an email message to the highly trained basic technical support staff of Trend Micro or you can visit the Trend Micro Support Web site.

- Email: [support@trendmicro.com](mailto:support@trendmicro.com)
- Web site: [kb.trendmicro.com/solutions/](http://kb.trendmicro.com/solutions/)

To speed up the resolution of a problem, you can provide the Trend Micro support staff with the following information:

- Product serial number
- Version numbers of the program, scan engine, and pattern file
- Operating system and version
- Type of Internet connection
- Exact text of the error message, if any
- Steps to reproduce the problem

# Using Manual Outbreak Prevention

OfficeScan helps you control outbreaks on the network with Manual Outbreak Prevention. This appendix explains how to use Manual Outbreak Prevention to block shared folders, block ports, and deny write access to files and folders.

The topics discussed in this appendix include:


- Blocking shared folders
- Blocking ports
- Denying write access to files and folders
- Configuring client notification for outbreaks




## Blocking shared folders

During virus outbreaks, you can block shared folders on the network to prevent viruses from spreading through the shared folders. Viruses like NIMDA gain access to computers through shared folders.

### To block shared folders

1. On the sidebar, click **Manual Outbreak Prevention**. The domain tree for Manual Outbreak Prevention appears.
2. Select the domains or clients on which you want to enable Manual 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 **Activate Now**. The **Manual Outbreak Prevention** 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 Manual Outbreak Prevention is enabled. You can click:
  - **Read access only**
  - **No read and write access**
7. Click **Save**.
8. Click **Back** to return to the **Manual Outbreak Prevention** screen.
9. Click **Activate Now** to enable Manual Outbreak Prevention on the selected domains or clients. A confirmation screen appears.
10. Click **OK**. The **Manual Outbreak Prevention** screen appears, showing the current outbreak prevention settings.

To verify that Manual Outbreak Prevention has been enabled, check if the client icons in the domains you selected appear as .

---


**WARNING!** *Enable Manual Outbreak Prevention only when there is a virus outbreak. Take special care in configuring the Manual Outbreak Prevention settings. Incorrect configuration can cause network problems.*

---

## Blocking ports

During virus outbreaks, you can block vulnerable ports that viruses and Trojans might use to gain access to clients.

### To block ports

1. On the sidebar, click **Manual Outbreak Prevention**. The domain tree for Manual Outbreak Prevention appears.
2. Select the domains or clients on which you want to enable Manual 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 **Activate Now**. The **Manual Outbreak Prevention** screen appears.
4. Under **Outbreak Prevention Settings**, select **Block ports**.
5. To configure the port blocking settings, click **Settings**. The **Port Blocking** screen appears.
6. If you want to block the trusted ports, which the server and client use for communication, select **Block trusted ports**.
7. To add ports to block, click **Add ports**. The **Port Blocking Settings** screen appears.
8. Under **Ports to Block**, specify which ports you want to block. You can click:
  - **Block all ports (including ICMP)** — click if you want to block all ports, including the Internet Control Message Protocol (ICMP). ICMP is an extension of Internet Protocol (IP), and it supports packets containing error, control, and informational messages.

---

**Note:** Clicking **Block all ports (including ICMP)** will block all ports except the trusted ports. If you also want to block the trusted ports, select the **Block trusted ports** check box on the **Port Blocking** screen.

---

- **Block specified ports** — click if you want to specify the ports to block. You can specify:
  - **Commonly used ports** — click if you want to block port numbers that are normally used for popular Internet services; for example, Port 80 for Web (HTTP), Port 25 for Send Email (SMTP). If you click **Commonly used ports**, you must select at least one port number for the port blocking settings to be saved.
  - **All Trojan ports** — click if you want to block all ports that are known to be vulnerable to Trojan attacks. To learn more about these Trojan ports, see the topic *What are Trojan ports?* in the OfficeScan online help.
  - **A port number or port range between 1 and 65535** — click if you want 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 that you want to block in the text box. Separate entries with commas.

In **Protocol**, select the communication method that you want to block from the drop-down list. You can select Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or both.

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


- **Ping protocol** — click if you only want to block ICMP packets, such as ping.

---

**Note:** Specify ports from one category (for example, **Commonly used ports** or **All Trojan ports**), then click **Save**. To specify ports from other categories, click **Add ports** again on the **Port Blocking** screen.

---

9. Click **Save**. 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 **Manual Outbreak Prevention** screen.
12. Click **Activate Now** to enable Manual Outbreak Prevention on the selected domains or clients. A confirmation screen appears.
13. Click **OK**. The **Manual Outbreak Prevention** screen appears, showing the current outbreak prevention settings.

To verify that Manual Outbreak Prevention has been enabled, check if the client icons in the domains you selected appear as .

---

**WARNING!** *Enable Manual Outbreak Prevention only when there is a virus outbreak. Take special care in configuring the Manual Outbreak Prevention settings. Incorrect configuration can cause network problems.*

---

## Denying write access to files and folders

Some viruses are programmed to modify or delete files and folders on their host computers. You can configure OfficeScan to prevent viruses from modifying or deleting files and folders on clients during a virus outbreak.



---

**Note:** Deny write settings can only be applied to clients running Windows XP, 2000, and NT.

---

### To deny write access to files and folder

1. On the sidebar, click **Manual Outbreak Prevention**. The domain tree for Manual Outbreak Prevention appears.

2. Select the domains or clients on which you want to enable Manual 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 **Activate Now**. The **Manual Outbreak Prevention** screen appears.
4. Under **Outbreak Prevention Settings**, select the **Deny write files and folders** check box.
5. To configure the shared folder blocking settings, click **Settings**. The **Deny Write Settings** screen appears.
6. If you want to protect specific directories and file name extensions, type the path of the directory to protect in **Directory path**. For example, you can type `C:\Windows\System32`. Make sure you type the absolute path, not the virtual path, for the directory. If you are typing multiple paths, separate entries with semicolons (;).
7. When you finish typing the directory path you want to protect, click . The path you have typed appears under **Protected directories**. Before continuing, make sure all the directories that you want to protect appear under **Protected directories**.


---


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

---

8. Specify which files in the **Protected directories** list will be protected based on their extensions. You can click:


- **All extensions in the protected directories**
- **Specified extensions**

If you click **Specified extensions**, select the extensions you want to protect from **Extensions list** and click  to add them to the **Protected extensions** list.

If you want to specify an extension that is not in the list, type this in the text box, and then click  to add it to the **Protected extensions** list. If you are typing multiple extensions, separate entries with semicolons (;).

If you want to protect specific files, type the full file names under **File Names to Protect**.

- 
9. Click **Save** to save your settings. A confirmation screen appears.
  10. Click **OK**. The **Deny Write Settings** screen shows the message, "Your settings have been updated."
  11. Click **Back** to return to the **Manual Outbreak Prevention** screen.
  12. Click **Activate Now** to enable Manual Outbreak Prevention on the selected domains or clients. A confirmation screen appears.
  13. Click **OK**. The **Manual Outbreak Prevention** screen appears, showing the current outbreak prevention settings.

To verify that Manual Outbreak Prevention has been enabled, check if the client icons in the domains you selected appear as .

---

**WARNING!** *Enable Manual Outbreak Prevention only when there is a virus outbreak. Take special care in configuring the Manual Outbreak Prevention settings. Incorrect configuration can cause network problems.*

---

## Configuring client notification for outbreaks

Enabling Manual Outbreak Prevention can prevent users from gaining access to network resources. To inform users that Manual Outbreak Prevention has been enabled, you can display outbreak notifications on clients.


### To display outbreak notifications on clients


1. On the **Manual Outbreak Prevention** screen, select the **When Manual Outbreak Prevention is enabled, display the following message on the client** check box.
2. Accept the default message or create a new one by typing your message in the text box.
3. Click **Activate Now** to save your settings.

## Restoring network settings to normal

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

### To restore network settings to normal

1. On the sidebar, click **Manual Outbreak Prevention**. The domain tree for Manual Outbreak Prevention appears.
2. Select the domains or clients on which you want to disable Manual 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 to Normal**. The **Manual Outbreak Prevention** screen appears.
4. If you want to inform users that the outbreak is over, make sure the **When Manual Outbreak Prevention is disabled, display the following message on the client** check box is selected. You can accept the default message or create a new one by typing your message in the text box.
5. Click **Restore to Normal**. A confirmation screen appears.
6. Click **OK**. The **Manual Outbreak Prevention** screen displays a message, informing you that Manual Outbreak Prevention has been disabled on the selected domains and computers.

To verify that Manual Outbreak Prevention has been disabled, check if the client icons in the domains you selected no longer appear as .

---

**Note:** If you do not restore network settings manually, these will be restored when the number of hours specified in **Automatically restore network settings to normal after { } hours** on the **Manual Outbreak Prevention** screen is reached.

---

# 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 manage OfficeScan using Control Manager.

The topics discussed in this appendix include:

- Introducing Control Manager
- What is Outbreak Prevention Service?
- What you can do with Control Manager
- Requirements for installing the agent
- Required information for agent installation
- Installing the agent
- Managing OfficeScan using Control Manager
- Modifying the polling interval of the agent
- Removing the agent



## Introducing Control Manager

Trend Micro Control Manager delivers powerful centralized management of antivirus and content security strategies deployed throughout a network. With single point-of-contact administration, monitoring, and deployment, Control Manager helps organizations manage antivirus and content security strategies more effectively.

With Control Manager, you can remotely configure groups of servers to perform the same tasks and use the same configuration settings. If you have a large network, Control Manager can greatly reduce the time you spend in configuring servers.

## What is Outbreak Prevention Service?

Outbreak Prevention Service (OPS) is a Trend Micro service that you can avail of using Control Manager. OPS allows you to take proactive steps against new virus threats before the necessary virus pattern file update becomes available. By bridging the gap between threat notification and virus pattern delivery, you can quickly contain virus outbreaks, minimize system damage, and prevent undue downtime.

OPS provides you with outbreak prevention policies — product setting recommendations designed to secure the network during outbreaks. Control Manager applies and manages these policies on products using Outbreak Commander.

Outbreak Commander applies policies in four stages:

- Prevention — threat information delivery and deployment of precautionary content security policies (anti-spam rules)
- Notification — notifications are automatically sent to the relevant individuals and Control Manager User Groups
- Scanning — real-time scanning on antivirus products is enabled
- Updates — an abbreviated update schedule is implemented for the duration of the policy. This ensures that you get the updated pattern files and scan engines as soon as they become available.

## What you can do with Control Manager

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 Trend Micro Control Manager Getting Started Guide.

Using Control Manager, you can:

- Configure, monitor, and maintain most Trend Micro software installed on the network from a single console, regardless of location or platform
- Simplify the implementation of a corporate virus and content security policy
- 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 Commander, which provides proactive attack protection service. Outbreak Commander blocks malicious code by file name or specific file details, while new pattern files that can detect and clean the new threat are being developed.

Control Manager uses a new communications infrastructure called the Trend Micro Management Infrastructure (TMI) that is built on the Secure Socket Layer (SSL) protocol. TMI protects communication between the Control Manager server and managed product with a combination of encryption and authentication.

Communicators handle communication between the agents on the product-machine and the Control Manager server. Agents can share a Communicator, so only one needs to be installed on the product-server.

## What is a Control Manager agent?

A Control Manager agent is an application installed on a product-server that allows Control Manager to manage the product. It receives commands from the Control Manager server, and then applies them to the managed product. It also collects logs from the product and sends them to Control Manager.

If you are upgrading from Trend VCS, you are probably already familiar with the term. It should be noted, however, that unlike the original Trend VCS server, the Control Manager agent does not communicate with the Control Manager server directly. Instead, it interfaces with a component called the Communicator.

Control Manager agents serve two primary purposes:

- To receive command inputs from the Control Manager server and apply them to the managed product
- To collect logs from the product, and report them to the Control Manager server

## Requirements for installing the agent

The requirements for installing the agent are the same as those for installing the OfficeScan server. You can install the Control Manager agent on any server where you can install OfficeScan.

---

**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 [Minimum system requirements](#) on page 2-7.

## 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

## Installing the agent

Installing the Control Manager agent is a two-step process:

- Obtain the public encryption key
- Install the agent

---

**Note:** The setup files for the Control Manager agent for OfficeScan are in the `/OfficeScan/cmagent` folder of the Trend Micro Enterprise CD.

---

### 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}` can be the computer name or IP address of the Control Manager server.

The **Welcome** screen of the Control Manager console appears.

2. Type a user ID and password.  
The Control Manager console appears.
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 to a location that is accessible to the server where the agent will be installed.

### To install the agent

1. Log on to the target server using an administrator account.
2. Click `Setup.exe` to start the installation process. The **Control Manager agent setup** screen appears.

3. On the **Welcome** screen, click **Next**. The **License Agreement** screen appears.
4. Read the License Agreement carefully, and then click **Yes** to accept the terms.
5. In **User ID**, type a user name with Administrator, Power User, or Operator rights to the Control Manager server. Be sure to maintain this account. If the account you use here is deleted, either deliberately or accidentally, you will no longer be able to manage the agent.

---

**Note:** When installing the agent, Trend Micro recommends using the Root account.

---

6. When the **Message Routing Path Configuration** screen appears, set the path for inbound and outbound messages.

Inbound messages can be received using any of the following methods:

- **Any host** - accept message from any source
- **IP Port forwarding** - type the IP address and port number that have been mapped for Control Manager communication
- **Proxy server** - select **Proxy Server Communication** to specify the proxy server IP address, port number, and type (HTTP or SOCKS4). If the proxy server requires, select **Authentication required**, and then type the user name and password.

Outbound messages can be sent either directly or through a proxy server. Select one, and then click **Next**.

7. To set up secure communications with the Control Manager server, click **Import**. Locate the public encryption key, `E2EPublic.dat`, of the Control Manager server to which you are registering the agent.
8. Follow the installation prompts to complete the installation.

To verify that the Control Manager agent installation was successful, open the Control Manager console and navigate to the entity you created.

---

## Managing OfficeScan using Control Manager

The Control Manager agent for OfficeScan accepts commands from the Control Manager server and instructs OfficeScan to perform them. For example, when you click **Tasks > Deploy scan engine** 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. Under **Product Directory**, click **OfficeScan Corporate Edition**. The following tabs are displayed:
  - **Status**
  - **Configuration**
  - **Tasks**
  - **Logs**

Status	Configuration	Tasks	Logs									
<b>Product Information</b>												
Product:	OfficeScan Corporate Edition											
Product version:	5.5 Build: 1076											
Product language:	English (en)											
Agent version:	2.5.1217											
Registered with Control Manager:	2003/01/09 上午 10:56:10											
Status:	Running since 2003/01/09 上午 10:56:11											
Spam rule version:	n/a											
Spam rule information:	n/a											
Virus pattern version:	431 LastUpdateTime: 2003/01/08 上午 11:41:58											
Scan engine version:	<table><tr><th>EngineType</th><th>EngineVersion</th><th>LastUpdateTime</th></tr><tr><td>NTKD</td><td>6.510</td><td>2003/01/08 上午 11:20:36</td></tr><tr><td>VxD</td><td>6.510</td><td>2003/01/08 上午 11:20:36</td></tr></table>			EngineType	EngineVersion	LastUpdateTime	NTKD	6.510	2003/01/08 上午 11:20:36	VxD	6.510	2003/01/08 上午 11:20:36
EngineType	EngineVersion	LastUpdateTime										
NTKD	6.510	2003/01/08 上午 11:20:36										
VxD	6.510	2003/01/08 上午 11:20:36										
<b>Operating System Information</b>												
Name:	Microsoft Windows NT											
Version:	5.0 (Build 2195)											
Service Pack:	Service Pack 3 (3.0)											
Language:	Traditional Chinese (zh_TW)											
<b>Agent Environment Information</b>												
Domain name:	client.tw.trendnet.org											
Host name:	TW-CHENGWEILIN1											
IP address:	10.1.116.103											
MAC address:	00-04-76-DC-84-63											

**FIGURE 2-1. The OfficeScan screen, as displayed on the Control Manager console**

To learn more about how to use these tabs, refer to the following sections.

## Status

The **Status** tab, which is displayed by default, contains the following information:

- Product Information
  - Product name and product version
  - Registered with Control Manager
  - Status
  - Spam rule version and information
  - Virus pattern version
  - Scan engine version
- Operating System Information - displays information about the operating system, such as the version, service pack, and language

- 
- **Networking Information** - displays network information such as the domain name, host name, IP address, and MAC address

## Configuration

The **Configuration** tab allows you to load the OfficeScan Web console on the Control Manager console.

---

**Note:** If you are using Internet Explorer 6.0 or later, you may have to configure your browser settings to accept cookies to successfully load the Web console.

---

### To load the OfficeScan Web console

1. Under **Product Directory** on the sidebar, select the OfficeScan server whose Web console you want to load.
2. Click the **Configuration** tab. The **Configuration** screen appears.
3. In **Select a product**, make sure **OfficeScan Corporate Edition** is selected.
4. In **Select a configuration**, make sure **Configure OfficeScan Corporate Edition** is selected.
5. Click **Next**. The Web console loads on the Control Manager console.

## Tasks

The **Tasks** tab allows you to start tasks remotely for individual OfficeScan servers. It contains the following options:

- **Start Scan Now** (or **Stop Scan Now**)
- **Start Real-time Scan** (or **Stop Real-time Scan**)
- **Deploy virus pattern/spam rule**
- **Deploy scan engine**
- **Deploy program files**

### To start a task

1. Select the task.
2. In **Supported products**, select the OfficeScan version.



3. Click **Next**.

## Logs

By default, the agent checks the OfficeScan server for new logs every minute. Whenever the agent detects a new log on the OfficeScan server, it automatically sends this to the Control Manager server.

Use the **Logs** tab on the Control Manager console to view these logs. You can view Event Logs and Security Logs.

### To view Event Logs

1. Click **Event Logs**.
2. In **Severity**, select the type of logs to view. You can select **Critical**, **Warning**, **Information**, **Error**, and **Unknown**.
3. In **Incident**, select the type of event that you want to view. You can select **All events**, **Virus outbreak**, **Module update**, **Service ON**, **Service OFF**, or **Security Violation**.
4. In **Product**, select **OfficeScan Corporate Edition**.
5. In **Start date**, select a start date for logs you want to view.
6. In **End date**, select an end date for logs you want to view.
7. In **Sort logs by**, select a classification by which the logs will be generated. You can select **Event date/time**, **Computer name**, **Product**, **Event**, or **Severity**.
8. In **Sort orders**, select the order by which the logs will be displayed. You can select **Ascending** or **Descending**.
9. Click **View Logs**. The **Query Result (Event Logs)** screen appears, showing the available log information for the date range you specified.

To save the log as a comma-separated value (CSV) date file, click **Save Logs as CSV**. Control Manager saves the log as a CSV data file.

### To view Security Logs

1. Click **Security Logs**.
2. Select the type of Security Log by clicking **Query** next to the log type. You can query any of the following:

- 
- All virus log incidents
  - Content security violations
  - Viruses found in download traffic (HTTP, FTP)
  - Viruses found in email
  - Viruses found in files
  - Web security violations (applies to other Trend Micro products)

The **Security Logs (Query)** screen appears.

3. Select the log period and sorting order.
4. Click **View Logs** to view the logs you selected. The **Query Result (Event Logs)** screen appears, showing the available log information for the date range you specified.

To save the log as a comma-separated value (CSV) data file, click **Save Logs as CSV**. Control Manager saves the log as a CSV data file.

## Viewing summary reports for OfficeScan

Using Control Manager, you can generate summary reports for OfficeScan. You can use these reports to analyze your network's protection.

### To generate a summary report

1. On the Control Manager console, click **Reports**. The **Reports** screen appears.
2. On the sidebar, click **Create Report Profile**. The **Create Report Profile** screen appears, displaying **Contents** as the active tab.

**Create Report Profile**  
Use one of the report templates below to create a new report.

1 Contents 2 Targets 3 Frequency 4 Recipients 5 Summary

**Contents**

**Name this report**  
12/02 Desktop Antivirus Sum

**Enter report title**  
Desktop Antivirus Summary

**Describe this report**

**Select report template**  
(7) Top 10 Security Violation Report  
(8) Deployment Rate  
(9) Virus Infection Channel v.s Product  
(10) Web Security Violations Report  
(11) Desktop Antivirus Protection Summary  
(12) Consolidated Report

**Select output format**  
RTF

Next >>

**FIGURE 2-2. The Create New Report tab, where you define the type of report to generate**

3. Fill in the boxes for the following:
  - Name this report - type a name for the report. This will help you distinguish the report from other reports you may generate.
  - Enter report title - type a report title
  - Describe this report - type a description for the report
4. Under **Select report template**, click **(11) Desktop Antivirus Protection Summary**.
5. Under **Select output format**, choose a format that will be used to display the report. You can choose **RTF**, **PDF**, **ActiveX**, or **Crystal Report Format**.
6. Click **Next**. The **Targets** tab becomes active.




**FIGURE 2-3. The Targets tab, where you select the product for which you want to generate the log**

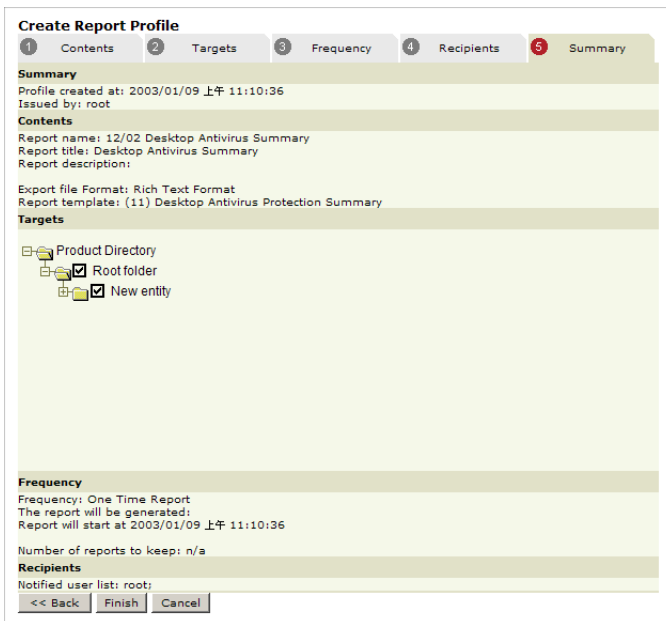
7. In the **Product Directory** tree, select the check boxes for the OfficeScan servers.
8. Click **Next**. The **Frequency** tab becomes active.
9. Under **Frequency**, specify the frequency when the log will be generated. You can click **One time only**, **Every day**, **Every week/2 weeks**, or **Every month**.
  - If you click **One time only**, specify the date range that will be covered in the report by selecting dates from the **From** and **To** boxes.
  - If you click **Every week/2 weeks**, select from the list the day of the week when the report will be generated.
  - If you click **Every month**, select from the list when to generate the report. You can select **first day of the month**, **15th day of the month**, or **end of the month**.
10. Under **Specify when to start generating this report**, click either **Immediately (One time report only)/After today** or **Start at**.  
If you click **Start at**, select the date and time from the list.
11. Under **Log maintenance**, select the **Number of reports to keep** check box if you want to automatically delete old logs, and then select a number from the list.

---

**Note:** If you clicked **One time only** under **Frequency**, the **Number of reports to keep** check box will be grayed out.

---

12. Click **Next**. The **Recipients** tab becomes active. On this tab, select the users to whom you want to send the report via email.
13. Select users from the left list, and then click  to add them to the right list. The right list displays users who will receive the report via email.
14. When all the intended recipients appear in the right list, click **Next**. The **Summary** tab becomes active, displaying a summary of the report you are generating.



**Create Report Profile**

1 Contents 2 Targets 3 Frequency 4 Recipients 5 Summary

**Summary**

Profile created at: 2003/01/09 上午 11:10:36  
 Issued by: root

**Contents**

Report name: 12/02 Desktop Antivirus Summary  
 Report title: Desktop Antivirus Summary  
 Report description:  
 Export file Format: Rich Text Format  
 Report template: (11) Desktop Antivirus Protection Summary

**Targets**

☐ Product Directory  
☒ Root folder  
☒ New entity

**Frequency**

Frequency: One Time Report  
 The report will be generated:  
 Report will start at 2003/01/09 上午 11:10:36

Number of reports to keep: n/a

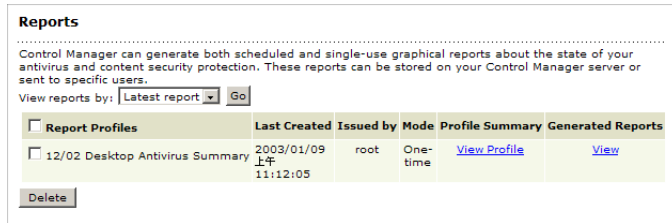
**Recipients**

Notified user list: root:

<< Back Finish Cancel

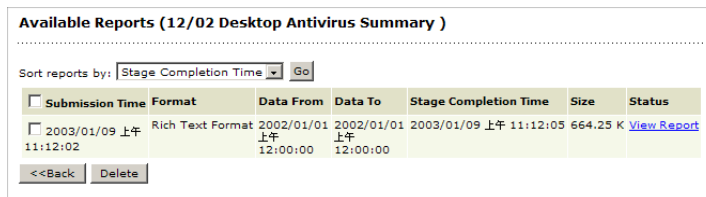
**FIGURE 2-4. A summary of the report settings is displayed**

15. Click **Finish**. The **Reports** screen appears, displaying the name of the report you are generating.



**FIGURE 2-5.** The Report screen displays the names of the reports you are generating

16. Under **Generated Reports**, click **View**. The **Available Reports** screen appears.



**FIGURE 2-6.** The Available Reports screen displays the format of the report you are generating and the time the report generation was completed

17. Under **Status**, click **View Report** to display the report. By this time, the recipients you specified on the **Recipients** tab should have already received the summary report.

## Modifying the polling interval of the agent

The Control Manager agent sends logs to the Control Manager server every three minutes. You can change the interval to send the logs in the registry.

### To modify the polling interval

1. On the server where the agent is installed, open a command prompt, type `regedit`, and press ENTER. The **Registry Editor** console appears.

2. Go to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\TrendMicro\AgentCommon\LogInterval. The registry information for the agent appears in the right pane.
3. In **Log Interval**, modify the value. The default value is 180 seconds. The minimum value is 60 and the maximum is 3600. If you type a value outside this range, OfficeScan will reset it to the default value.

## 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**. The **Control Panel** window appears.
2. Double-click **Add/Remove Programs**. The **Add/Remove Programs** window appears.
3. Click **Trend Micro Control Manager Agent for OfficeScan**, and then click **Remove**. A confirmation screen appears.
4. Click **Yes**. Windows removes the agent from the server. When the agent is completely removed, click **Close**.

---

**Note:** Removing the OfficeScan server automatically removes the Control Manager agent for OfficeScan.

---

# Setting Up Check Point SecureClient with OfficeScan

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).

This appendix includes the following information:

- Overview of Check Point Firewall architecture and configuration
- Integrating with OfficeScan
- Configuring Check Point for use with OfficeScan



## Overview of Check Point Firewall architecture and configuration

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, in turn, 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, refer to [Configuring Check Point for use with OfficeScan](#) on page C-4.

## Integrating with OfficeScan

OfficeScan client periodically passes the pattern file number and scan engine number to SecureClient for verification. SecureClient then compares these values with values in the client `local.scv` file. The `local.scv` file would look like the following if you open it in a text editor such as Wordpad™:

```
(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:** Pattern file and scan engine version numbers in the SCV file are not updated automatically by Check Point. Whenever the scan engine or pattern file is updated, 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.

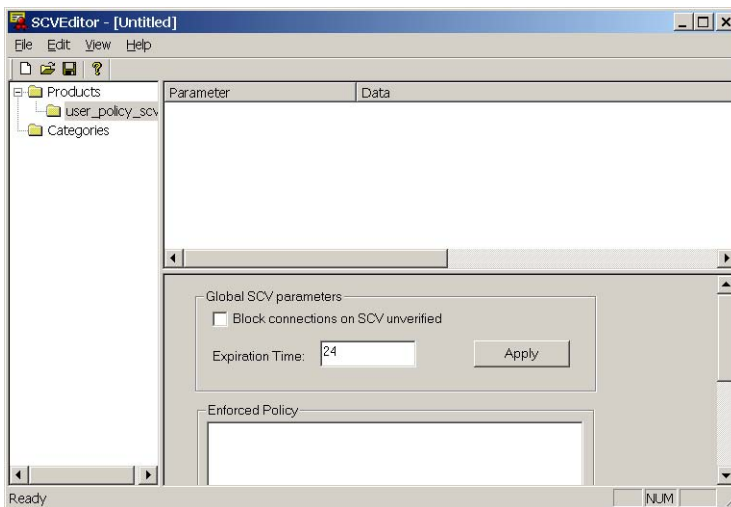
---

## Configuring Check Point for use with 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.



**FIGURE C-1. The SCV Editor**

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.

---

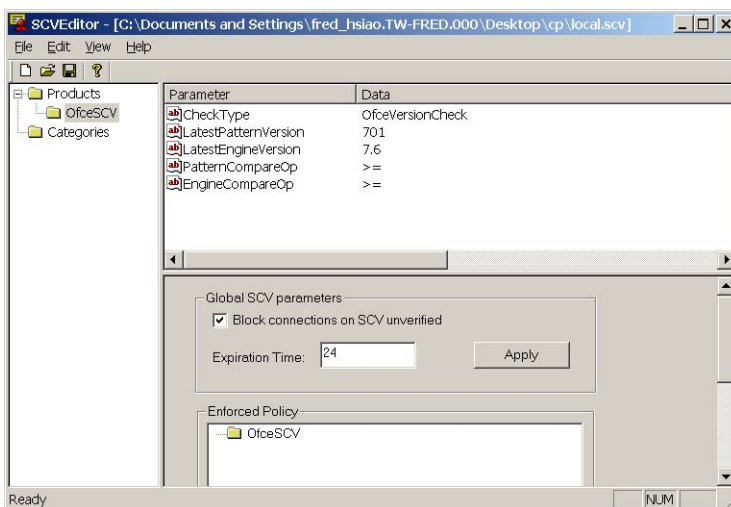
5. Now add five parameters. To add a parameter, click **Edit > Parameters > Add**, and then type a **Name** and **Value** in the corresponding boxes. Table C-1 lists the parameter names and values. Parameter names and values are case-sensitive, and must be typed in the order given in Table C-1.

Name	Value
CheckType	OfceVersionCheck
LatestPatternVersion	{current pattern file number}
LatestEngineVersion	{current scan engine number}
PatternCompareOp	>=
EngineCompareOp	>=

**TABLE C-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 C-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**.




**FIGURE C-2. The completed Secure Configuration Verification file is ready to be saved**

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**.

---

# Index

## Numerics

30-day trial version 2-12

## A

About screen 4-8  
Activate Now 4-4  
ActiveAction 4-28  
ActiveX 1-2  
adding a domain 4-11  
Administrative Tools 4-7  
Advanced Client Settings 4-5  
alerts  
    setting up 4-22  
antivirus policy  
    enforcing 1-10  
antivirus settings  
    default 4-28  
architecture 1-4  
Automated Deployment 4-16  
automated updates  
    client 4-16  
autopcc.exe. *See* Login Script Setup

## B

blocking ports A-3  
blocking shared folders A-2

## C

choosing  
    client installation method 3-2  
    pilot site 2-6  
client  
    automating updates 4-16  
    disconnected 1-6  
    granting privileges  
        client privileges 4-37  
    installation methods 3-2  
    installation path 2-10  
    network traffic 2-5  
    preparing for installation 3-4  
    ratio with server 2-2  
    removing 3-24

    removing using Uninstall Now 3-25  
    requirements for Win 2000/NT computers 3-3  
    requirements for Win Me/98/95 computers 3-3  
    requirements for Win XP computers 3-4  
    system requirements 3-3  
    updating 4-15  
    updating manually 4-17  
    virus alert 2-10  
Client Administration 4-4  
Client Alert Message 4-5  
client events 1-5  
client icons 5-4  
client installation  
    choosing a method 3-2  
    from a disk image 3-14–3-15  
    from the internal Web page 3-4–3-5  
    preparing for 3-4  
    testing with the EICAR test script 3-23  
    using Microsoft SMS 3-18–3-21  
    verifying 3-21  
    with Client Packager 3-9–3-13  
    with Login Script Setup 3-5–3-8  
    with NT Client Installer 3-17–3-18  
    with NT Remote Install utility 3-15–3-17  
    with Windows NT Remote Install 3-13–3-14  
client installation path 2-10  
Client Packager 3-9  
    using the email function 3-12  
Client Tools 4-7  
Client Update 4-6  
clients 1-5  
    classifications 1-6  
    managing 1-11  
    normal 1-6  
    roaming 1-7  
client-server ratio 2-2  
    across the WAN 2-3  
    on a LAN 2-2  
ClnPack.exe. *See* Client Packager  
conducting a pilot 2-6  
configuration settings 4-16  
configuring 4-22, 4-25  
configuring outbreak notifications A-7  
console 2-10  
contacting technical support 5-4

- Control Manager 1-9
  - agent B-4
  - capabilities B-2
  - installing the agent B-5
  - introduction B-2
  - Outbreak Prevention Service B-2
  - public encryption key B-5
  - viewing summary reports for OfficeScan B-11
- Control Manager agent B-4
  - installation B-5
  - modifying the polling interval B-15
  - removing B-16
  - required information B-4
  - requirements B-4
- controlling
  - virus outbreak 1-11

## D

- Damage Cleanup Services 1-8
- Damage Cleanup Services. *See* DCS
- DCS 1-8
- DCS *See* Damage Cleanup Services
- dedicated server 2-5
- default antivirus settings 4-28
- deleting a domain 4-11
- denying write access to files and folders A-5
- deployment
  - definition 2-2
  - evaluating the pilot 2-7
  - pilot 2-6–2-7
  - planning 2-2
- deployment planning 2-2
- domain
  - adding 4-11
  - creating 4-9
  - deleting 4-11
  - moving clients from 4-12
  - renaming 4-12
  - selecting from 4-10
  - working with 4-11
- domain name 2-12, 4-20
- domain tree 4-9
  - icons 4-10
  - refreshing 4-10
  - selecting from 4-10

- domains
  - managing 1-11

## E

- EICAR test script 3-23
- events 1-5
- exclusion list 4-35

## F

- file-based server 1-5
- FQDN 2-12, 4-20
- full pattern file 2-5
- fully qualified domain name 2-12

## G

- getting started tasks 1-12
- granting privileges to clients 4-37
- GUID 3-14

## H

- hacker attacks 2-10
- Help 4-8
- HTTP communication 2-10
- HTTP server 2-12
- HTTP. *See* HyperText Transfer Protocol
- HTTP-based server 1-4
- HyperText Transfer Protocol 1-5

## I

- IIS 1-4
- Image Setup 3-14
- imgsetup.exe 3-15
- Inactive Clients 4-6
- incremental update 2-5
- infected files
  - sending to the quarantine folder 1-10
- installation issues 5-2
- installing
  - clients 3-4–3-21
  - Control Manager agent B-5
  - server 2-1
- IntelliScan 4-28
- Internet Information Server. *See* IIS
- Internet Proxy 4-6
- Intranet Proxy 4-6



---

## J

Java applet 1-2

## L

LAN

- client-server ratio 2-2

local.scv C-2

Log Maintenance 4-7

Log Off 4-8

Login Script Setup 3-5

login scripts

- Windows 2000/NT servers 3-7

Logs 4-7

## M

macro virus 1-2

management console

- functions 1-8

- Web console 1-9

managing

- domains and clients 1-11

Manual Deployment 4-17

Manual Outbreak Prevention 4-4, A-1

- blocking ports A-3

- configuring outbreak notifications A-7

- denying write access to files and folders A-5

- restoring network settings to normal A-8

- shared folder blocking A-2

manual scan 4-31

manual update

- clients 4-17

- server 4-14

Master Password 2-18

master setup 2-10

- client installation path 2-10

- proxy information 2-9

- required information 2-9

- required protocols 2-9

- required restarts 2-9

- required rights 2-9

- serial number 2-9

- shared directory 2-10

- starting 2-11

- virus alert message 2-10

- where to run 2-8

- Windows licenses 2-10

- Windows shortcuts 2-10

Master Uninstaller 2-18

master upgrade 2-15–2-16

methods

- client installation 3-2

Microsoft SMS 3-18

moving clients from a domain 4-12

## N

network traffic

- pattern updates 2-5

- planning for 2-4

- server 2-4–2-5

normal clients 1-6

notifications

- setting up 4-22

NT Client Installer 3-17

NT Remote Install 4-5

NT Remote Install utility 3-15

NTBRinst.exe. *See* NT Remote Install utility

## O

OfficeScan

- and Control Manager on the same server 2-6

- architecture 1-4

- capabilities 1-10

- client 1-5

- compatibility with Control Manager 1-9

- configuring 4-1

- domain 4-9

- getting started 1-12

- integrating with SecureClient C-2

- introducing 1-1

- management console 1-4, 1-8

- managing with Control Manager B-7

- registering 4-8, 4-38

- server 1-4

- summary reports B-11

- tasks 1-12

- three-tier application 1-4

OfficeScan for Wireless 1-12

OPS B-2

outbreak

- controlling 1-11

- using Manual Outbreak Prevention A-1
- Outbreak Alert 4-5
- outbreak alert 4-25
  - email 4-25
  - pager 4-26
  - SNMP Trap 4-27
  - Windows NT Event Log 4-26
- Outbreak Prevention Service. *See* OPS

## P

- package description file. *See* PDF
- password 2-10
- pattern file
  - compressed 2-5
  - extracted 2-5
  - full 2-5
  - incremental update 2-5
- pattern updates
  - network traffic 2-5
- PDF 3-19
- performing scans 1-10
- pilot deployment 2-6
- pilot site
  - choosing 2-6
- planning
  - client-server ratio 2-2
  - deployment 2-2
  - network traffic 2-4
- planning for deployment 2-2
- Policy Servers C-2
- preparing for
  - client installation 3-4
  - server installation 2-8
- protection
  - analyzing using logs 1-11
  - keeping current 4-13
  - updating 1-11
- protocols 2-9
- proxy 2-9
- public encryption key B-5

## Q

- Quarantine Manager 4-6

## R

- real-time scan 4-29

- registering OfficeScan 4-8, 4-38
- Registration 4-8
- registration benefits 4-38
- removing
  - client 3-24
  - Control Manager agent B-16
  - server 2-20
- renaming a domain 4-12
- required protocols 2-9
- required restarts 2-9
- required rights 2-9
- requirements
  - client 3-3
  - server 2-7
  - Web console 2-7
- Restore to Normal 4-4
- restoring network settings to normal A-8
- roaming clients 1-7
  - privileges 1-7
  - updating 1-7
- Rollback 4-6
- rollback plan 2-7

## S

- Scan Now 4-4
  - running 4-36
- scan options 4-27
  - default 4-28
- scan settings
  - configuring 4-27
  - default 4-28
  - excluding files and folders 4-35
  - manual scan 4-31
  - real-time scan 4-29
  - scheduled scan 4-33
- scanning
  - excluding files and folders 4-35
  - from one location 1-10
  - Scan Now 4-36
- scheduled scan 4-33
- Scheduled Update 4-18
- scheduled updates
  - server 4-13
- SCV Editor C-2
- Secure Configuration Verification. *See* SCV

---

- SecureClient C-2
  - integrating with OfficeScan C-2
  - Policy Servers C-2
  - SCV Editor C-2
- Security Info 4-8
- serial number 2-9
- server
  - configuring scheduled updates 4-13
  - dedicated 2-5
  - file-based 1-5
  - HTTP-based 1-4
  - installing 2-1
  - network traffic 2-4
  - preparing for installation 2-8
  - ratio with clients 2-2
  - removing 2-20
  - system requirements 2-7
  - updating 4-13
  - updating manually 4-14
- Server Administration 4-5
- server installation 2-1
  - preparing 2-8
  - verifying 2-14
- Server Update 4-6
- Set Password 4-5
- Set Privileges 4-4
- Set Scan Options 4-4
- setting client privileges 4-37
- setting up
  - notifications 4-22
- shared directory 2-10
- Standard Alert 4-5
- standard alert 4-22
  - email 4-22
  - pager 4-23
  - SNMP Trap 4-24
  - Windows NT Event Log 4-23
- Support 4-8
- System Event Logs 4-7
- system requirements
  - Web console 2-7
  - Win 2000/NT client 3-3
  - Win Me/98/95 client 3-3
  - Win XP client 3-4

## T

- TCP 2-10
- TCP port 2-10, 2-12
- TCP/IP 1-5, 2-9
- technical support 5-4
  - before contacting 5-4
  - requesting for 5-4
- testing
  - with EICAR test script 3-23
- three-tier application 1-4
- Toolbox 4-7
- Transmission Control Protocol. *See* TCP
- Trend Micro
  - Knowledge Base 5-4
  - Support 5-5
- trial version 2-12
- Trojan 1-8
- troubleshooting 5-2

## U

- understanding architecture 1-4
- Uninstall Now 3-25, 4-4
- uninstalling
  - client 3-24
  - Control Manager agent B-16
  - server 2-20
- update
  - verifying 4-21
- Update & Upgrade 4-6
- Update Logs 4-7
- Update Now 1-7, 4-19
- updating
  - clients 4-15
  - OfficeScan 4-13
  - roaming clients 1-7
  - server 4-13
  - using Update Now. *See* Update Now
- updating clients 4-15
  - using Automated Deployment 4-16
  - using Manual Deployment 4-17
  - using Scheduled Update 4-18
  - using Update Now 4-19
- updating the server 4-13
  - using Manual Server Update 4-14
  - using scheduled update 4-13

upgrading

file-based OfficeScan 2-16

## **V**

Verify Connection 4-5

Verify Connection Logs 4-7

verifying

client installation 3-21

server installation 2-14

verifying updates 4-21

View Status 4-4

Virtual Private Network. *See* VPN

virus alert message 2-10

Virus Logs 4-7

virus outbreak

controlling 1-11

virus scanning 1-10

VPN C-6

Vulnerability Scanner 2-19, 3-4

## **W**

WAN

client-server ratio 2-3

Web console 1-9

Client Administration 4-4

domain tree 4-9

getting around 4-3

Logs 4-7

Manual Outbreak Prevention 4-4

opening 4-2

other links 4-8

Registration 4-8

Server Administration 4-5

system requirements 2-7

Toolbox 4-7

Update & Upgrade 4-6

Web Server 4-6

Windows licenses 2-10

Windows NT Remote Install 3-13

Windows shortcuts 2-10

Wireless Protection Manager 1-12