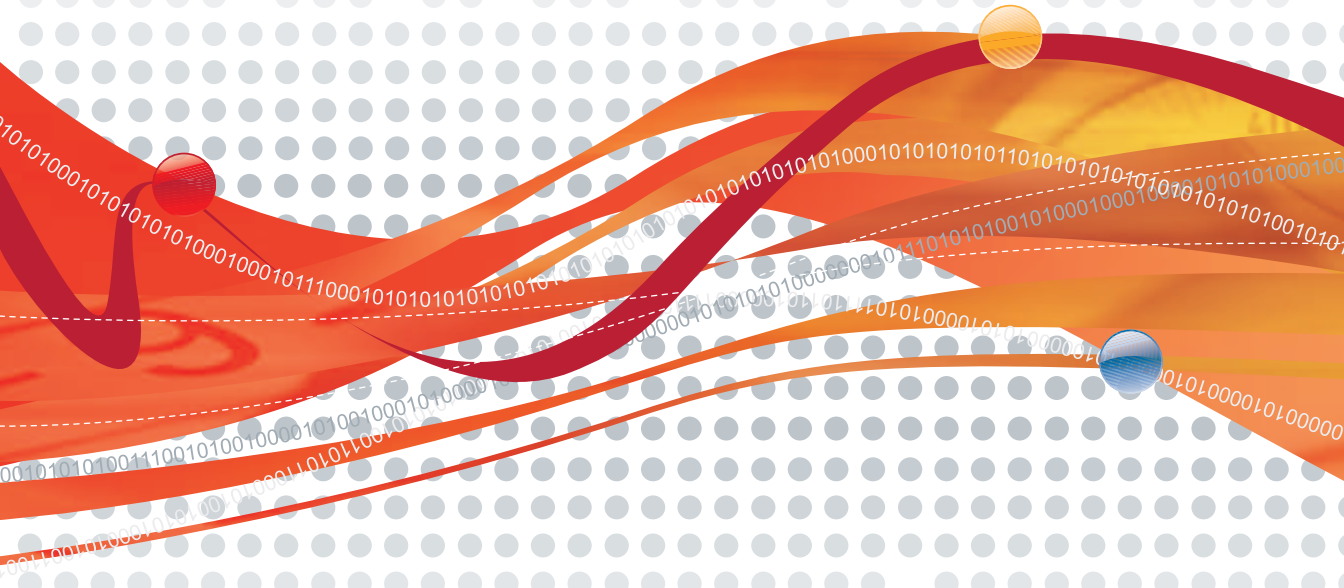
TREND MICRO

OfficeScan™ Client/Server Edition 8

for Enterprise and Medium Business

Installation and Deployment Guide



Endpoint Security

Document Part No. OSEM83054/70130

Release Date: May 2007, updated December 2007

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

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

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

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

Please evaluate this documentation on the following site:

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

Contents

Appendix A: Sample Deployment

Index

Chapter 1

Planning Server Installation

Topics in this chapter:

Installation Requirements

The following are the requirements for the OfficeScan server and Web console.

OfficeScan Server Requirements

TABLE 1-1. OfficeScan server requirements

Resource	Requirement
Operating System	• Microsoft™ Windows™ 2000 Server with Service Pack 3 or 4 • Microsoft Windows 2000 Advanced Server with Service Pack 3 or 4 • Microsoft Windows Server 2003 32-bit Edition with or without Service Pack 1 or 2 • Microsoft Windows Server 2003 64-bit Edition with or without Service Pack 1 or 2 • Microsoft Windows Server 2003 R2 32-bit Edition with or without Service Pack 1 or 2 • Microsoft Windows Server 2003 R2 64-bit Edition with or without Service Pack 1 or 2 • Microsoft Windows Storage Server 2003 32-bit Edition • Microsoft Windows Storage Server 2003 64-bit Edition • Microsoft Cluster Server 2000 • Microsoft Cluster Server 2003
Hardware	• 800MHz Intel™ Pentium™ processor or equivalent • 512MB of RAM • 1GB of disk space • Network Interface Card (NIC) • Monitor that supports 800 x 600 resolution at 256 colors or higher
Web server	• Microsoft Internet Information Server (IIS) on Windows 2000: version 5.0 (Service Pack 3 or 4) on Windows Server 2003: version 6.0 • Apache™ Web server 2.0 or later (for Windows 2000/Server 2003 only)

TABLE 1-1. OfficeScan server requirements

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

Note: If you plan to install the Cisco™ Trust Agent (CTA) on the same computer as the OfficeScan server, do not install OfficeScan server on Windows Server 2003 x64 Edition. See the *Administrator's Guide* for more information on CTA requirements.

Web Console Requirements

TABLE 1-2. Web console requirements

Resource	Requirement
Hardware	• 300MHz Intel Pentium processor or equivalent • 128MB of RAM • 30MB of available disk space • Monitor that supports 800 x 600 resolution at 256 colors or higher
Browser	Microsoft Internet Explorer™ 5.5 Service Pack 1 or later

Product Versions and Keys

Full Version and Evaluation Version

Install either a full version of OfficeScan or a free, evaluation (trial) version.

- **Full version:** Includes all the product features and technical support, and provides a grace period (usually 30 days) after the license expires. If you do not renew the license after the grace period expires, you will not be

able to obtain technical support and perform component update. The scan engines will still scan computers using out-of-date components. These out-of-date components may not be able to protect you completely from the latest security risks. You can renew the license before or after it expires by purchasing a maintenance renewal.

- **Evaluation (Trial) version:** Includes all the product features. You can upgrade an evaluation version to a full version at any time. If not upgraded at the end of the evaluation period, OfficeScan disables component update, scanning, and all client features.

Note: Both versions require a different type of Activation Code. Register your product if you do not have an Activation Code.

The Registration Key and Activation Codes

During installation, OfficeScan prompts you to enter the Activation Codes for the Antivirus, Damage Cleanup Services™ (optional) and Web Threat Protection services.

If you do not have the Activation Code(s), use the Registration Key that came with your product to register on the Trend Micro Web site and receive the Activation Code(s). The OfficeScan master installer automatically redirects you to the Trend Micro Web site:

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

If you do not have either the Registration Key or Activation Code, contact your Trend Micro sales representative (see *Contacting Trend Micro* on page 6-1).

Note: For questions about registration, refer to http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326.

Installation Considerations

Take the following factors into consideration when planning to install the OfficeScan server:

Location of the OfficeScan Server

OfficeScan can accommodate a variety of network environments. For example, you can position a firewall between the OfficeScan server and its clients, or position both the server and all clients behind a single network firewall. If there is a firewall between the server and its clients, configure the firewall to allow traffic between the client and server listening ports (see *OfficeScan Ports* on page 1-11 for more information).

Note: For information on resolving potential problems you may encounter when managing OfficeScan clients on a network that uses Network Address Translation, see the *Administrator's Guide* and the OfficeScan server online help).

Remote Installation

Remote installation allows you to launch the installation on one computer but install OfficeScan to another computer. If you perform remote installation, the Setup program will analyze if the target computer meets the requirements for server installation.

To ensure that installation can proceed:

- Ensure that you have administrator rights to the target computer.
- Take note of the computer's host name and logon credentials (user name and password).
- Make sure the computer meets the OfficeScan server system requirements. Refer to *Installation Requirements* on page 1-1 for more information.
- If using Microsoft IIS server as the Web server, make sure the version is 5.0 or higher. If you choose to use Apache Web server, Setup will automatically install this server if not present on the target computer.

Server Performance

Enterprise networks require servers with higher specifications than those required for small and medium-sized businesses. Ideally, the OfficeScan server computer would have at least 2GHz dual processors and over 1GB of memory.

The number of networked computer clients that a single OfficeScan server can manage depends on several factors, such as available server resources and your network topology. Contact your Trend Micro representative for help in determining the number of clients your server can manage.

OfficeScan servers with 2GHz dual processor and 2GB of RAM can usually manage 3000 to 5000 clients.

Dedicated Server

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

- How much CPU load will the computer handle?
- What other functions does the computer perform?

If the target computer has other uses (for example, a computer that functions as an application server), Trend Micro recommends choosing a computer that does not run critical or resource-intensive applications.

Unsupported Client Platforms

OfficeScan no longer supports Windows 95, 98, Me, NT and IA64 architecture. If you plan to upgrade to this version of OfficeScan and clients run these operating systems:

- Do not upgrade all OfficeScan servers to this OfficeScan version.
- Designate an un-upgraded OfficeScan server to manage these clients.
- Before upgrading, open the Web console and move the clients to the designated server. In OfficeScan 7.3, you can access the Move Clients screen by clicking **Clients > Move**.

If you already upgraded OfficeScan but did not move unsupported clients to an un-upgraded server, see *Using Client Mover for Legacy Platforms* on page 2-21 for instructions.

Number of Domains

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

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

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

Number of Clients

If your networked computers run different Windows operating systems, check the number of computers running a specific Windows version. Use this information to decide which client deployment method will work best in your environment.

Number of clients a single OfficeScan server can manage:

- OfficeScan server with 2GHz dual processor with 2GB of RAM: 3000 to 5000
- OfficeScan server with 3GHz dual processor with 4GB of RAM: 5000 to 8000

Network Traffic

When planning for deployment, consider the network traffic that OfficeScan generates. The server generates traffic when it does the following:

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

The client generates traffic when it does the following:

- Starts up
- Updates components manually or based on a schedule
- Updates settings and installs a hot fix
- Switches between roaming mode and normal mode

Network traffic during component updates

OfficeScan generates significant network traffic when it updates a component. To reduce network traffic generated during component updates, OfficeScan performs component duplication. Instead of downloading an updated full pattern file, OfficeScan only downloads the "incremental" patterns (smaller versions of the full pattern file) and merges them with the old pattern file after the download.

Clients updated regularly only download the incremental pattern, which is approximately 500KB to 900KB. Otherwise, they may have to download the full pattern file, which is more than 20MB.

Trend Micro releases new pattern files regularly. However, Trend Micro releases a new pattern file as soon as the detection routine of a damaging and actively circulating virus/malware is available.

Update Agents and network traffic

If there are "low-bandwidth or "heavy traffic" sections of your network between clients and the OfficeScan server, you can designate selected OfficeScan clients as update source for other clients. This helps distribute the burden of deploying components to all clients.

For example, if you have a remote office with 20 or more computers, designate an Update Agent to replicate updates from the OfficeScan server and act as a Local Distribution point for other client computers on the local LAN. See the *Administrator's Guide* for more information on update agents.

Trend Micro Control Manager and network traffic

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

Use Control Manager to manage several OfficeScan servers from a single location. A Control Manager server with fast, reliable Internet connection can download components from the Trend Micro ActiveUpdate server and deploy the components to one or more OfficeScan servers with unreliable or no Internet connection.

See the *Administrator's Guide* for more information on Control Manager.

Placement of the Program Files

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

The default client installation path is C:\Program Files\Trend Micro\OfficeScan Client.

Third Party Antivirus Applications

Trend Micro highly recommends removing third party antivirus and anti-spyware applications from the computer on which you will install OfficeScan server because these applications may prevent successful OfficeScan server installation or affect its performance.

Note: OfficeScan cannot uninstall the server component of any third-party antivirus product, but can uninstall the client component (see *Migrating from Third-party Antivirus Applications* on page 4-17 for details).

Required Installation Information

The master installer prompts you for the following information during installation:

- **Proxy server details:** If a proxy server handles Internet traffic on your network, specify proxy server information the OfficeScan server will use when downloading the latest components from the Trend Micro ActiveUpdate server.
- **Console password:** Prevent unauthorized access to the OfficeScan Web console by specifying a password.
- **Client software installation path:** Specify the location where the master installer will copy the OfficeScan program files.

OfficeScan Ports

OfficeScan uses two types of ports:

- **Server listening port (HTTP port):** The port used for the OfficeScan server Web console. By default, OfficeScan uses one of the following:
  - **IIS server default Web site:** The same port number as your HTTP server's TCP port
  - **IIS server virtual Web site:** 8080 (HTTP) and 4343 (HTTPS)
  - **Apache server:** 8080
- **Client listening port:** A randomly generated port number through which the client receives commands from the server.

You can modify the server listening port during installation or on the OfficeScan server Web console after installation. You cannot modify the client listening port.

WARNING! *Many hacker and virus/malware attacks delivered over HTTP use ports 80 and/or 8080 because most organizations use these port numbers as the default Transmission Control Protocol (TCP) ports for HTTP communications. Trend Micro recommends using other port numbers if you currently use the default port numbers.*

Other Installation Notes

Computer Restart not Required

OfficeScan server installation does not require a computer restart. After completing the installation, immediately configure the server and install clients to networked computers. If using an IIS Web server, the Setup program automatically stops and restarts the IIS service during Web server installation.

WARNING! *Installing the Web server on a computer running IIS-locking applications may prevent successful installation. See your IIS documentation for more information.*

Other OfficeScan Programs

You can enable the OfficeScan firewall and install Policy Server for Cisco NAC during or after OfficeScan server installation.

Tip: Trend Micro highly recommends installing OfficeScan during non-peak hours to minimize the effect on your network.

Client Settings

You can preserve client settings when you upgrade to this version of OfficeScan and use them if you reinstall the OfficeScan server. See *Restoring Settings after Rollback or Reinstallation* on page 2-24 for instructions.

Apache Web Server

You can install Apache Web server when you install the OfficeScan server. By default, the administrator account is the only account created on the Apache Web server. Trend Micro recommends creating another account from which to run the Web server to prevent compromising the OfficeScan server if a hacker takes control of the Apache Web server.

Refer to http://www.apache.org for the latest information on Apache Web server upgrades, patches, and security issues.

Planning a Pilot Deployment

Before performing a full-scale deployment, Trend Micro recommends conducting a pilot deployment in a controlled environment. A pilot deployment provides an opportunity to determine how features work and the level of support you may need after full deployment. It also gives your installation team a chance to rehearse and refine the deployment process, and test if your deployment plan meets your organization's antivirus and anti-spyware initiative.

For a sample OfficeScan deployment, see *Sample Deployment* on page A-1.

Choosing a Pilot Site

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

Creating a Rollback Plan

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

This process should take into account local corporate policies and technical specifics.

Deploying Your Pilot

Check the deployment method suitable for your particular environment. See *Installing and Upgrading the OfficeScan Server* on page 2-1 for details.

Evaluating Your Pilot Deployment

Create a list of successes and failures encountered throughout the pilot process. Identify potential pitfalls and plan accordingly. Include this pilot evaluation plan in the overall product deployment plan.

Known Compatibility Issues

This section explains compatibility issues if you install OfficeScan server on the same computer with certain third-party applications. Refer to the documentation of third-party applications installed on the same computer on which you will install OfficeScan server.

Microsoft Small Business Server

Write down the server port used by ISA before installing OfficeScan on a computer running Microsoft Small Business Server™ that is also running Microsoft Internet Security Acceleration server (ISA). By default, both the OfficeScan server and ISA use port 8080.

Choose another server listening port when installing OfficeScan server.

Microsoft Lockdown Tools and URLScan

If you use the Microsoft IIS Lockdown Tool or URLScan, the lockdown of OfficeScan configuration (.ini), data (.dat), dynamic link library (.dll), and executable (.exe) files may block OfficeScan client and server communication.

To prevent URLScan from interfering with client-server communication, stop the World Wide Web Publishing service on the OfficeScan server, modify the URLScan configuration file to allow the file types specified above, and restart the service. See your lockdown tool documentation for additional information.

Microsoft Exchange Server

If you choose to install the OfficeScan client during server installation, OfficeScan needs access to all files the client will scan. Since Microsoft Exchange Server queues messages in local directories, these directories need to be excluded from scanning to allow the Exchange Server to process email messages.

OfficeScan automatically excludes all Microsoft Exchange 2000/2003 directories from scanning. This setting is set in the Web console (**Networked Computers > Global Client Settings > Virus/Malware Scan Settings**).

For Microsoft Exchange 2007, refer to http://technet.microsoft.com/en-us/library/bb332342.aspx for scan exclusion details.

Trend Micro™ ScanMail™ for Microsoft Exchange can protect your Exchange server from viruses/malware and other potential threats. See the Trend Micro Web site (http://www.trendmicro.com) or your sales contact for information about ScanMail for Microsoft Exchange.

SQL Server

You can scan SQL Server databases. However, this may decrease the performance of applications that access the databases. Trend Micro recommends excluding SQL Server databases and their backup folders from Real-time Scan. If you need to scan a database, perform a Manual Scan during off-peak hours to minimize the impact of the scan.

Internet Connection Firewall (ICF)

Windows Server 2003 provides a built-in firewall called Internet Connection Firewall (ICF). Trend Micro highly recommends removing any third-party firewall applications if you enable the OfficeScan firewall. However, if you want to run ICF or any other third-party firewall, add the OfficeScan listening ports to the firewall exception list (see *OfficeScan Ports* on page 1-11 for information on listening ports and see your firewall documentation for details on how to configure exception lists).

Chapter 2

Installing and Upgrading the OfficeScan Server

Installation/Upgrade scenarios:

> **Note:** For more information on the differences between the full and evaluation versions, see *Product Versions and Keys* on page 1-3.

Recommended post-installation tasks:

- *Using Client Mover for Legacy Platforms* on page 2-21

  Note: Perform this task only if you have clients running unsupported platforms, which include Windows 95, 98, Me, NT and IA64 architecture.

- *Restoring Settings after Rollback or Reinstallation* on page 2-24
- *Registering OfficeScan to Control Manager* on page 2-26

  Note: Control Manager registration only applies to newly installed OfficeScan servers.

- *Installing Plug-in Manager* on page 2-26

Other task:

- *Uninstalling the Server* on page 2-27

Installing or Upgrading the OfficeScan Server

You can perform fresh installation or upgrade a previous OfficeScan version either locally or remotely. This version of OfficeScan supports upgrade from versions 7.3, 7.0, 6.5 and 5.58 but not from Trend Micro Client/Server Suite or Client/Server/Messaging Suite.

You can preserve your client settings when you reinstall or upgrade to this version of OfficeScan. See *Restoring Settings after Rollback or Reinstallation* on page 2-24 for more information.

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

Below is a list of the installation screens (arranged sequentially) and tasks for installing or upgrading OfficeScan locally or remotely. For screen-specific information and instructions, click **Help** in the applicable Setup screens.

TABLE 2-1. Installation screens and tasks

Screens/Tasks	Fresh Installation (Local)	Fresh Installation (Remote)	Upgrade (Local)	Upgrade (Remote)
Welcome	✓	✓	✓	✓
License Agreement *Task:* Agree to the license agreement.	✓	✓	✓	✓
Installation Destination *Task:* Select whether to install locally or remotely.	✓	✓	✓	✓
Prescan *Task:* Decide whether to scan the target computer before installation. If performing prescan: • Local installation: Scanning occurs when you click **Next**. • Remote installation: Scanning occurs during the actual installation.	✓	✓	✓	✓
Setup Status (Computer Analysis)	✓		✓	

TABLE 2-1. Installation screens and tasks

Screens/Tasks	Fresh Installation (Local)	Fresh Installation (Remote)	Upgrade (Local)	Upgrade (Remote)
Installation Path This screen displays if you perform remote fresh installation and upgrade. However, settings you specify here apply only to remote fresh installation. For remote upgrade, OfficeScan will use the previous version's settings. *Task:* Use the default installation path or specify a new one.	✔	✔		✔
Proxy Server Settings This screen displays if you perform remote fresh installation and upgrade. However, settings you specify here apply only to remote fresh installation. For remote upgrade, OfficeScan will use the previous version's settings. *Task:* Specify proxy server settings if you use a proxy server for client-server communication. Otherwise, skip this step.	✔	✔		✔
Web Server Settings This screen displays if you perform remote fresh installation and upgrade. However, settings you specify here apply only to remote fresh installation. For remote upgrade, OfficeScan will use the previous version's settings. This screen also displays if you upgrade from OfficeScan 5.58 locally. *Task:* Choose whether to use an IIS or Apache Web server and then configure HTTP port and SSL settings.	✔	✔	✔	✔

TABLE 2-1. Installation screens and tasks

Screens/Tasks	Fresh Installation (Local)	Fresh Installation (Remote)	Upgrade (Local)	Upgrade (Remote)
Computer Identification This screen displays if you perform remote fresh installation and upgrade. However, settings you specify here apply only to remote fresh installation. For remote upgrade, OfficeScan will use the previous version's settings. *Task:* Determine whether OfficeScan clients will identify the server computer by its domain name or IP address.	✔	✔		✔
Registration *Task:* Register OfficeScan using the Registration Key that came with your product and then obtain the Activation Codes. If you already registered and received the Activation Codes, skip this step.	✔	✔	✔	✔
Activation *Task:* Enter the Activation Codes of the product services.	✔	✔	✔	✔
Remote installation destination *Task:* Specify the target computer to which you will install OfficeScan.		✔		✔
Remote installation computer analysis *Tasks:* • Click **Analyze** so Setup can determine whether the target computer meets the installation requirements. • To save the selected computers to a text file, click **Export**.		✔		✔

TABLE 2-1. Installation screens and tasks

Screens/Tasks	Fresh Installation (Local)	Fresh Installation (Remote)	Upgrade (Local)	Upgrade (Remote)
Install Other OfficeScan Programs • If the OfficeScan client exists on the target computer, the installer upgrades the client automatically after server installation. • If Trend Micro ServerProtect™ exists on the computer, uninstall it before installing the OfficeScan client. • Cisco NAC programs are unavailable if you do not activate the Antivirus service. • You can skip installing the OfficeScan client and Cisco NAC programs and install them after server installation. For OfficeScan client installation, refer to *Installing and Upgrading the OfficeScan Client on page 4-1*. For CTA installation, open the Web console and go to **Cisco NAC > Agent Deployment**. For Policy Server installation, run the installer from your OfficeScan installation package. • Refer to the Administrator's Guide for more information about Cisco NAC. **Tasks:** • Select the programs to install. • If installing Cisco Trust Agent (CTA), specify the location of the agent certificate file (if the certificate is available to you; if not, contact your Trend Micro representative).	✔	✔	✔	✔

TABLE 2-1. Installation screens and tasks

Screens/Tasks	Fresh Installation (Local)	Fresh Installation (Remote)	Upgrade (Local)	Upgrade (Remote)
Cisco Trust Agent Installation/Upgrade • If you perform fresh installation, this screen displays only if you choose to install Cisco Trust Agent in the previous screen. Select the CTA package to install to clients. • If you upgrade, this screen displays only if you have previously installed CTA. Choose whether to upgrade CTA to the current version (2.1). If upgrading, select the CTA upgrade package. • If you did not select to install CTA during server installation, you can still install it using the Web console.				
Cisco Trust Agent License *Task:* Agree to the license agreement.				
World Virus Tracking *Task:* Decide whether to join the Trend Micro World Virus Tracking program.				
Administrator Account Password *Task:* Specify passwords to perform the following: • Access the Web console • Unload and uninstall the OfficeScan client				

TABLE 2-1. Installation screens and tasks

Screens/Tasks	Fresh Installation (Local)	Fresh Installation (Remote)	Upgrade (Local)	Upgrade (Remote)
Client Installation Path *Task:* Accept the default client installation settings or specify a different • Client installation path • Port number the OfficeScan server will use to communicate with clients • Client security level	✔	✔		
Enable Firewall This screen displays only if you activate the Antivirus service.	✔	✔	✔	✔
Enable Assessment Mode This screen displays only if you activate the Web Threat Protection service.	✔	✔	✔	✔
Program Folder Shortcut *Task:* Accept the default folder name or specify a new one. You can also select an existing folder to which Setup will add program shortcuts.	✔			
Installation Information *Tasks:* • Check if installation information is correct. • Click **Back** to modify settings.	✔	✔	✔	✔
OfficeScan Server Installation	✔	✔	✔	✔

TABLE 2-1. Installation screens and tasks

Screens/Tasks	Fresh Installation (Local)	Fresh Installation (Remote)	Upgrade (Local)	Upgrade (Remote)
Policy Server Installation This screen displays if you chose to install Policy Server for Cisco NAC. The succeeding Policy Server installation screens that display include: • Welcome • License Agreement • Installation Destination • Web Server Selection • Web Server Settings • Policy Server Console Password • ACS Server Authentication Password • Policy Server Installation • Installation Complete				
OfficeScan Server Installation Complete *Tasks:* • View the readme file. • Open the Web console to start configuring OfficeScan settings. See *Updating OfficeScan Components* on page 2-20 for more information.				

Performing Silent Installation

Install multiple OfficeScan servers silently if the servers will use identical installation settings. Silent installation involves two procedures:

1. Create a response file by running the Setup wizard and recording the installation settings to an .iss file. All servers installed silently using the response file will use the settings.

   Important:

   - The Setup wizard only shows screens for local installation (fresh installation or upgrade). See *Installing or Upgrading the OfficeScan Server* on page 2-2 for the relevant screens that will display.
   - If you plan to upgrade OfficeScan servers to this version, make sure to create the response file from a computer with an OfficeScan server installed. Similarly, if you plan to perform fresh installation, create a response file from a computer without an OfficeScan server installed.

2. Run Setup from a command prompt and point Setup to the location of the response file to use for silent installation. You can use the silent installation process to upgrade an OfficeScan server from an earlier version. The process is similar to fresh installation.

To record the server Setup configuration to a response file:

Note: This procedure does not install OfficeScan. It only records the server Setup configuration to a response file.

---

1. Open a command prompt and type the directory of the OfficeScan Setup.exe file. For example, "CD C:\OfficeScan installer".
2. Enter setup.exe -r. The -r switch commands the program to record the installation details to a response file.
3. In the Setup wizard, follow the installation steps. After completing these steps, check the response file (setup.iss) in %windir%.

To run silent installation:

1. Copy the installation package (includes all installation files and folders, and the setup.exe file) and setup.iss to the target computer.
2. In the target computer, open a command prompt and type the directory of the setup.exe file.
3. Type setup.exe -s -f1{path}setup.iss -f2{path}setup.log.

   For example: C:\setup.exe -s -f1C:\setup.iss -f2C:\setup.log

   Where:

   - **-s:** Commands the Setup program to perform silent installation
   - **-f1{path}setup.iss:** Location of the response file. If the path contains spaces, enclose the path with quotes ("). For example, -f1"C:\osce script\setup.iss".
   - **-f2{path}setup.log:** Location of the log file that Setup will create after installation. If the path contains spaces, enclose the path with quotes ("). For example, -f2"C:\osce log\setup.log".
4. Press **Enter**. Setup.exe silently installs the server to the computer.
5. To determine if installation is successful, check the OfficeScan program shortcuts on the target computer. If the shortcuts are not available, retry the installation.

Upgrading from an Evaluation Version

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

To upgrade from an evaluation version:

1. Open the OfficeScan Web console.
2. Click **Administration** > **Product License**. The Product License screen appears.

3. If you have an Activation Code, type it in the **New Activation Code** field and click **Activate**.

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

Upgrading from Control Manager

You can upgrade multiple OfficeScan servers that a Trend Micro Control Manager server manages.

Supported versions

The following OfficeScan server versions can be upgraded to version 8.0 using Control Manager 2.5, 3.0 or 3.5:

- 5.58 with Control Manager Agent 2.51
- 7.0 with Control Manager Agent 2.53
- 7.3 with Control Manager Agent 2.55

Note: Although you can use Control Manager 2.5 or 3.0 to upgrade OfficeScan servers, Control Manager 3.5 patch 2 or later is required to manage the upgraded OfficeScan servers. After upgrading the OfficeScan servers, make sure to upgrade Control Manager to 3.5 patch 2 or later.

Before upgrading, prepare the following:

- The Control Manager server
- The OfficeScan servers to upgrade (Please make sure the server computers are up and running during the upgrade.)
- The installation package for this OfficeScan version
- A valid Activation Code
- An encryption tool, such as SecurePass™
- The **UpgradeEncryptOSCESrvAgent.zip** file

Note: To obtain this file, contact your Trend Micro representative or visit http://solutionfile.trendmicro.com/SolutionFile/24290/en/UpgradeEncryptOSCESrvAgent.zip.

To upgrade OfficeScan from Control Manager:

1. Copy all the OfficeScan Setup files and folders from your installation package to a temporary folder in the OfficeScan 5.58 or 7.x server computer. Assume that the temporary folder name is "OSCE8".
2. On the computer with the encryption tool, create and encrypt a file containing all the OfficeScan 5.58 or 7.x servers.
   a. Create a file named pass.csv and then enter the host names and administrator accounts (user names and passwords) of the OfficeScan server computers. You can include OfficeScan 5.58 and 7.x servers in the list.

      For example:

      computer01,administrator,password01

      computer02,administrator,password02

      computer03,administrator,password03

   b. Open a command prompt and go to the directory of the encryption tool.

   c. Enter the encryption tool name followed by the /e or /d command, and then by the location and file name of pass.csv. The /e command encrypts the file; the /d command decrypts the file.

      Sample usage:

      - If securepass.exe (the encryption tool name) and pass.csv are on the same directory:

        securepass.exe /e pass.csv

      - If the files are on different directories:

        securepass.exe /e C:\temp\pass.csv

   d. Copy pass.csv to the folder created in step 1.

3. Create a response file on the OfficeScan 5.58 or 7.x server computer.

   Note: Enter a valid full version or evaluation version Activation Code when creating the response file. If you enter an evaluation version Activation Code, remember to change it after the upgrade.

   a. Open a command prompt and go to the temporary folder created in step 1.

   b. Type **setup -r** and press the **Enter** key.

   c. In the Setup wizard that opens, follow the local upgrade steps. See *Installing or Upgrading the OfficeScan Server* on page 2-2 for the upgrade screens that will display. After completing these steps, check the response file (setup.iss) in the temporary folder.

      Note: This procedure does not install OfficeScan; it only records the server Setup configuration to a response file.

   d. Rename setup.iss to:

      - setup558.iss if upgrading from OfficeScan 5.58
      - setup700.iss if upgrading from OfficeScan 7.x

4. Archive the folder created in step 1 using a tool such as WinZip. If we use the sample temporary folder name in step 1 (OSCE8), the archive file name should be OSCE8.zip.

a. Take note of the archive file size in bytes (NOT the size on disk). You will need this information when you modify the server.ini file in the Control Manager server computer. To check the file size, right-click the archive file and click **Properties**.

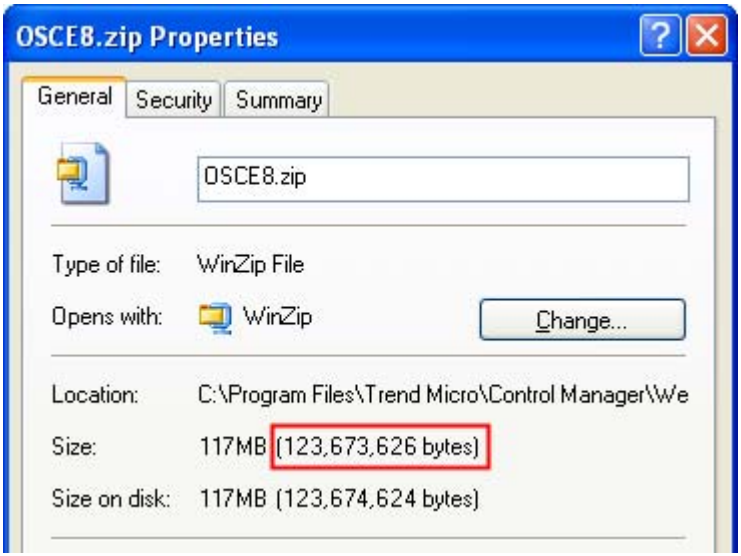


FIGURE 2-1. File size of a sample archive file

b. Copy the archive file to the Control Manager server computer, on the following folder: \WebUI\download\activeupdate\Product.

5. Copy the UpgradeEncryptOSCESrvAgent.zip file also to the following folder on the Control Manager server computer: \WebUI\download\activeupdate\Product.

6. Take note of the file size in bytes of the UpgradeEncryptOSCESrvAgent.zip file.

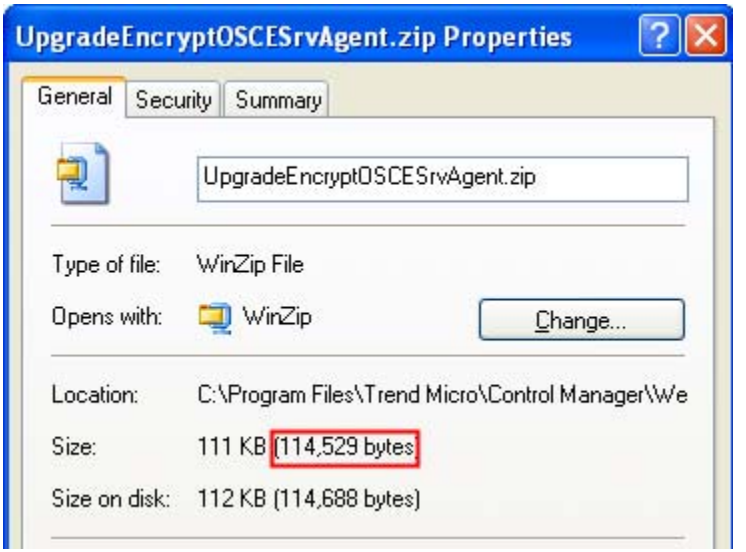


FIGURE 2-2. File size of the UpgradeEncryptOSCESrvAgent.zip file (sample only, please do not copy)

7. In the Control Manager server computer, open the **server.ini** file in the folder \WebUI\download\activeupdate.
8. Modify the following in the server.ini file:

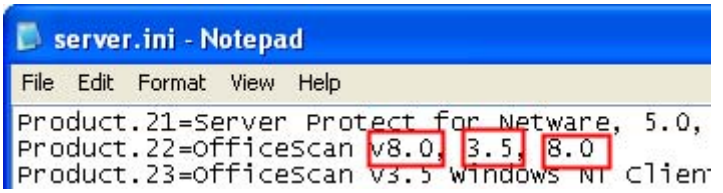


FIGURE 2-3. Variables in the server.ini file

Where:

- **v8.0** is the version of the OfficeScan installation package
- **3.5** is the minimum supported version
- **8.0** is the maximum supported version

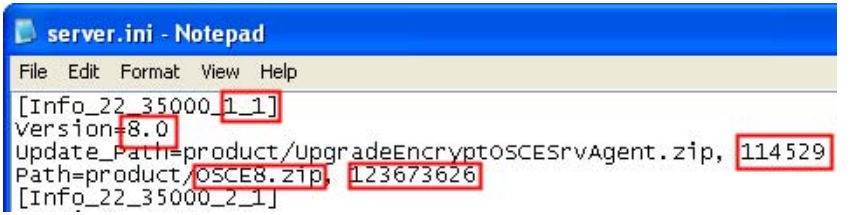


FIGURE 2-4. Variables in the server.ini file

Where:

- **1_1** is the English language version of OfficeScan

Note: The Japanese language version is 1_4.

- **8.0** is the version of the OfficeScan installation package
- **114529** is the file size (in bytes) of UpgradeEncryptOSCESrvAgent.zip

Note: This value is only a sample. Please obtain the actual file size.

- **OSCE8.zip** is the archive file name

Note: This is the sample file name created in step 4. Please use the actual file name of your archive file.

- **123673626** is the file size (in bytes) of OSCE.zip

Note: This value is only a sample. Please obtain the actual file size.

9. Open the Control Manager console and go to **Products > Tasks > Deploy program files**.

   The appropriate OfficeScan servers managed by Control Manager start to upgrade. For example, if you create the archive file from an OfficeScan 5.58 server computer, only OfficeScan 5.58 servers listed in pass.csv and included in the Product Directory entity will upgrade. If you have OfficeScan 7.x servers, repeat steps 1 to 9.

10. Control Manager 3.5 patch 2 or later is required to manage OfficeScan 8.0 servers. If you used Control Manager 2.5 or 3.0 to upgrade OfficeScan servers to version 8.0, upgrade Control Manager to version 3.5 patch 2 or later. Refer to the Control Manager documentation for upgrade instructions.

Post-installation Tasks

Trend Micro recommends performing the following post-installation tasks:

- *Verifying the Server Installation or Upgrade* on page 2-19
- *Updating OfficeScan Components* on page 2-20
- *Checking Default Settings* on page 2-20
- *Using Client Mover for Legacy Platforms* on page 2-21

Note: Perform this task only if you have clients running unsupported platforms, which include Windows 95, 98, Me, NT and IA64 architecture.

- *Restoring Settings after Rollback or Reinstallation* on page 2-24

- *Registering OfficeScan to Control Manager* on page 2-26

Note: Control Manager registration only applies to newly installed OfficeScan servers.

- *Installing Plug-in Manager* on page 2-26

Verifying the Server Installation or Upgrade

After completing the installation or upgrade, verify the following:

- OfficeScan program shortcuts on the Windows **Start** menu
- List of currently installed programs in the Add/Remove Programs screen, which should include "Trend Micro OfficeScan Server"
- Web console connection:
  - http://{OfficeScan server name}:{port number}/OfficeScan
  - *or if using SSL*: https://{OfficeScan server name}:{port number}/OfficeScan

  Where {OfficeScan server name} is the name or IP address of the OfficeScan server.
- OfficeScan services included in Windows services:
  - OfficeScan Master Service (should be running)
  - Trend Micro Policy Server for Cisco NAC (if installed)
- Running OfficeScan processes:
  - OfcService.exe
  - DBServer.exe
- Installation log: OFCMAS.LOG in %windir%
- Registry keys: HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan
- Program folder: {Installation Drive and folder}\Trend Micro\OfficeScan

Updating OfficeScan Components

After installation or upgrade, update the server immediately with the latest OfficeScan components.

Note: This section shows you how to perform manual update. For information on scheduled update and update configurations, see the OfficeScan server online help.

To update the OfficeScan server:

1. Open the OfficeScan Web console.
2. On the main menu, click **Updates** > **Server** > **Manual Update**. The Manual Update screen appears, showing the current components, their version numbers, and the most recent update dates.
3. Select the components to update.
4. Click **Update**. The server checks the update server for updated components. The update progress and status display.

Checking Default Settings

OfficeScan installs with default settings. If these settings do not conform to your security requirements, modify and then save the settings on the Web console before installing OfficeScan clients. Refer to the online help and Administrator's Guide for details on the settings available on the Web console.

Scan settings

OfficeScan provides several types of scans to protect your clients from security risks. You can modify the scan settings from the Web console by going to **Networked Computers > Client Management > Settings > {Scan Type}**.

- **Real-time Scan:** OfficeScan scans files in real time. If OfficeScan detects no security risk, users can proceed to open or save the file. If OfficeScan detects a security risk, it displays a notification message, showing the name of the file and the specific security risk.

- **Manual Scan:** Manual Scan for virus/malware starts immediately after a user launches it in the client console. The length of the scan depends on the number of files to scan and the client computer's hardware resources. The scan time and coverage for spyware/grayware depends on the scan method you or client users (with Manual Scan configuration privilege) specify. You can select the scan method to use in the Manual Scan Settings page in the Web console.
- **Scheduled Scan:** Scheduled Scan has similar scan behavior as Manual Scan. The only difference is that Scheduled Scan runs automatically on the scheduled date and time. Use Scheduled Scan to automate routine scans on the client and improve scan management efficiency.
- **Scan Now:** Scan Now and Manual Scan are the same type of scan. The only difference is that you initiate Scan Now remotely using the Web console, while users run Manual Scan locally on their client computers.

Global client settings

OfficeScan provides several types of settings that apply to all clients registered to the server or to all clients with a certain privilege. You can modify global client settings from the Web console by going to **Networked Computers > Global Client Settings**.

Client privileges

Default client privileges include displaying the **Mail Scan** and **Toolbox** tabs on the client console. Modify default client privileges from the Web console by going to **Networked Computers > Client Management > Settings > Privileges and Other Settings**.

Using Client Mover for Legacy Platforms

This version of OfficeScan no longer supports Windows 95, 98, Me, NT and IA64 architecture. If you have clients running these platforms and you upgraded to this version of OfficeScan:

- The OfficeScan server stops managing the unsupported clients. The clients' status becomes "Disconnected".

- The OfficeScan server saves the clients' information to the **unsupCln.txt** file on the OfficeScan installation folder. The typical file path is C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\unsupCln.txt.
- Ensure you have an earlier version of the OfficeScan server that will manage unsupported clients.
- In the upgraded OfficeScan server computer, run a tool called Client Mover for Legacy Platforms to move clients to the earlier OfficeScan server version. The tool notifies clients that a different OfficeScan server will manage them. Clients that receive the notification will register to that server. The tool can also verify if client movement succeeds.

To move clients to an earlier version of the OfficeScan server:

1. Run the Client Mover for Legacy Platforms (clientmover.exe) on the computer with the upgraded OfficeScan server. You can access this tool from the OfficeScan installation folder, typically: C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Admin\Utility\ClientMover.
2. In the command window, type the command using the following format: ClientMover [/P:ExportDataPath] [/S:ServerIP:port] [/N]

   For example:

   ClientMover /P:"C:\Program Files\TrendMicro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:1.2.3.4:21112 /N

   Where:

   /P: The path and file name of the file (unsupCln.txt) containing client information. The typical path is: C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\unsupCln.txt.

   /S: The IP address and port number of the previous version of OfficeScan server that will manage the clients

   /N: A command that notifies and then moves the clients to the previous version of the OfficeScan server; use in conjunction with the /V command

3. Use the /V command to verify if the tool moved the clients.

   For example:

   ClientMover /P:"C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\ unsupcln.txt" /S:1.2.3.4:21112 /V

   Where:

   /V: A command that verifies if the tool successfully moved the clients. This command compares the IP addresses of the upgraded OfficeScan server and the earlier version. If the IP addresses are the same, the tool was unable to move the clients.

4. To check the result:

   a. Access the resulting log in C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\. The log file name is in the following format: unsupcln.txt.log.{date_time}

      For example: unsupcln.txt.log.20061201_162502

   b. Also in the same folder, verify if OfficeScan updated and backed up the unsupcln.txt file. The backup file name is unsupcln.txt.bak.

   The following is a sample entry in the updated unsupcln.txt file:

   ```
   ----------------------------------------------------------------------------------------------------
   f50bb480-5abf-11db-ab38-000c292c4a67    1518338314    21112    0
   ----------------------------------------------------------------------------------------------------
   ```

   Where:

   Client's GUID: f50bb480-5abf-11db-ab38-000c292c4a67

   Client's IP address: 1518338314 (Dec) = 0x5A80010A (Hex)

   0A.01.80.5A (Hex) = 10.1.128.90 (Dec)

   Client's communication port: 21112

Result: 0, or any of the following:

0 = Notification completed

1 = Client notification successful

2 = Client notification unsuccessful

3 = Verification successful

4 = Verification unsuccessful

The following is a sample entry in the unsupcln.txt.log.{date_time} file:

```
----------------------------------------------------------------------------------------------
f50bb480-5abf-11db-ab38-000c292c4a67     10.1.128.90:21112
Unable to send the notification. Please check the network or client status.
----------------------------------------------------------------------------------------------
```

Where:

Client's GUID: f50bb480-5abf-11db-ab38-000c292c4a67

Client's IP address and communication port: 10.1.128.90:21112

Result: Unable to send the notification. Please check the network or client status.

5. Use the /F command to force the notification or verification without checking the current client status.

Restoring Settings after Rollback or Reinstallation

You can save a copy of the OfficeScan database and important configuration files to roll back your OfficeScan program. You may want to do this if you experience problems and want to reinstall OfficeScan, or if you want to revert to a previous configuration.

To restore program settings after rollback or reinstallation:

1. Back up the OfficeScan server database to a location outside of the OfficeScan program directory.

Perform database backup through the OfficeScan Web console (**Administration > Database Backup**). See the *Administrator's Guide* or the OfficeScan server online help for instructions.

WARNING! *Do not use any other type of backup tool or application.*

2. Manually back up the following files and folders from the \Program Files\Trend Micro\OfficeScan\PCCSRV folder:
   - **ofcscan.ini:** Contains global client settings
   - **ous.ini:** Contains the update source table for antivirus component deployment
   - **Private folder:** Contains firewall and update source settings
   - **Web\tmOPP folder:** Contains Outbreak Prevention settings
   - **Pccnt\Common\OfcPfw.dat:** Contains firewall settings
   - **Download\OfcPfw.dat:** Contains firewall deployment settings
   - **Log folder:** Contains system events and the connection verification logs
   - **Virus folder:** Contains quarantined files
   - **HTTDB folder:** Contains the OfficeScan database
3. Uninstall OfficeScan (See *Uninstalling the Server* on page 2-27).
4. Perform fresh installation (See *Installing or Upgrading the OfficeScan Server* on page 2-2).
5. After the master installer finishes, stop the OfficeScan service on the target computer.
   a. Open the Windows Services screen (click **Start > Run** and type **services.msc**).
   b. Select **OfficeScan Master Service** from the list, right-click and then select **Stop**.
6. Copy the backup files to the \PCCSRV folder on the target computer. This overwrites the OfficeScan server database and the relevant files and folders.
7. Restart the OfficeScan service.

Registering OfficeScan to Control Manager

If you want a Control Manager server to manage newly installed OfficeScan servers, register OfficeScan to Control Manager after installation. You can do so from the OfficeScan Web console by going to **Administration > Control Manager Settings**. See the online help for the procedure.

Installing Plug-in Manager

With Plug-in Manager, you can start using plug-in programs developed outside of a product release as soon as they are available. Plug-in Manager displays the plug-in programs for both the OfficeScan server and client on the OfficeScan Web console. Install and manage the programs from the Web console, including deploying the client plug-in programs to clients.

Download and install Plug-in Manager by clicking **Plug-in Manager** on the main menu of the Web console. Follow the Setup screens to complete the installation. After successfully installing Plug-in Manager, check for available plug-in programs.

Notes:

- Plug-in Manager does not support remote installation. You must open the Web console on the OfficeScan server computer and install Plug-in Manager from there.
- Except for available disk space (Plug-in Manager requires at least 200MB), Plug-in Manager has the same system requirements as the OfficeScan server.
- The Client Plug-in Manager, which manages plug-in programs for clients, automatically installs after OfficeScan client installation or upgrade. It has the same system requirements as the client program. The only additional requirement is Microsoft XML Parser (MSXML) version 3.0 or later.

Uninstalling the Server

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

To uninstall the OfficeScan server:

1. On the OfficeScan server computer, click **Start** > **Programs** > **Trend Micro OfficeScan Server** > **Uninstall OfficeScan**.

   A confirmation screen appears.
2. Click **Yes**. The server uninstallation program prompts you for the administrator password.
3. Type the administrator password and click **OK**. The server uninstallation program starts removing the server files. A confirmation message appears.
4. Click **OK** to close the uninstallation program.

Chapter 3

Planning Client Installation

Topics in this chapter:

Installation Requirements

The following are the requirements for installing the OfficeScan client on computers running Windows 2000, XP, Server 2003, and Vista.

TABLE 3-1. Client system requirements

Resource	Requirement
Windows 2000	
Operating system	• Microsoft Windows 2000 with Service Pack 3 or 4 • Microsoft Cluster Server 2000

TABLE 3-1. Client system requirements

Resource	Requirement

Hardware	• 300MHz Intel Pentium processor or equivalent
	• RAM:
	  • 256MB minimum, 512MB recommended
	  • 512MB for Update Agents
	• 200MB of available disk space
	• Monitor that supports 800 x 600 resolution at 256 colors or higher

Others	Microsoft Internet Explorer 5.0 or later if performing Web setup
Windows XP/2003 32-bit Edition	
Operating system	• Microsoft Windows XP Professional with Service Pack 1 or 2 • Microsoft Windows Server 2003 with or without Service Pack 1 or 2 • Microsoft Windows 2003 Web Edition with or without Service Pack 1 or 2 • Microsoft Windows Server 2003 R2 with or without Service Pack 1 or 2 • Microsoft Windows Storage Server 2003 • Microsoft Cluster Server 2003

Hardware	• 300MHz Intel Pentium processor or equivalent; AMD™ x64 or Extended Memory 64 Technology (EM64T) processor architectures also supported
	• RAM:
	  • 256MB minimum, 512MB recommended
	  • 512MB for Update Agents
	• 200MB of available disk space
	• Monitor that supports 800 x 600 resolution at 256 colors

Others	Microsoft Internet Explorer 6.0 or later if performing Web setup

TABLE 3-1. Client system requirements

Resource	Requirement
Windows XP/2003 64-bit Edition	
Operating system	• Microsoft Windows XP Professional with Service Pack 1 or 2 • Microsoft Windows Server 2003 with or without Service Pack 1 or 2 • Microsoft Windows 2003 Web Edition with or without Service Pack 1 or 2 • Microsoft Windows Server 2003 R2 with or without Service Pack 1 or 2 • Microsoft Windows Storage Server 2003 • Microsoft Cluster Server 2003

Hardware	• Intel x64 processor, AMD x64 processor
	• RAM:
	  • 256MB minimum, 512MB recommended
	  • 512MB for Update Agents
	• 200MB of available disk space
	• Monitor that supports 800 x 600 resolution at 256 colors

Others	Microsoft Internet Explorer 6.0 or later if performing Web setup
Windows Vista	
Operating system	• Microsoft Windows Vista Business 32-bit Edition • Microsoft Windows Vista Enterprise 32-bit Edition • Microsoft Windows Vista Ultimate 32-bit Edition • Microsoft Windows Vista Business 64-bit Edition • Microsoft Windows Vista Enterprise 64-bit Edition • Microsoft Windows Vista Ultimate 64-bit Edition

TABLE 3-1. Client system requirements

Resource	Requirement
Hardware	• 800MHz Intel Pentium processor or equivalent; AMD x64 or Extended Memory 64 Technology (EM64T) processor architectures also supported • 1GB of RAM • 200MB of available disk space • Monitor that supports 800 x 600 resolution at 256 colors
Others	Microsoft Internet Explorer 7.0 or later if performing Web setup

Note: Disable **Simple File Sharing** on Windows XP computers so users can successfully install the OfficeScan client program (see your Windows documentation for instructions).

Update Agent Requirements

TABLE 3-2. Update Agent system requirements

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

Installation Methods

This section provides a summary of the different client installation methods to help you decide which method is most suitable for your network environment. All installation methods require local administrator rights on the target computers.

Web install page

Instruct the users in your organization to go to the Web install page and download the client Setup files (see *Installing from the Web Install Page* on page 4-2).

Login Script Setup

Automate the installation of the OfficeScan client to unprotected computers when they log on to the network (see *Installing with Login Script Setup* on page 4-3).

Client Packager

Create and send the client Setup or update files to client users (see *Installing with Client Packager* on page 4-6). If creating an MSI package using Client Packager, you can deploy the package using Active Directory™ or Microsoft SMS.

For details, see the following topics:

- *Deploying an MSI package using Active Directory* on page 4-9
- *Deploying an MSI package using Microsoft SMS* on page 4-10

Remote installation

From the Web console, install the client program on computers running supported platforms (see *Installing from the OfficeScan Web Console* on page 4-13).

From a client disk image

Create and clone an image of an OfficeScan client, and then deploy to other computers on your network (see *Installing from a Client Disk Image* on page 4-15).

Trend Micro Vulnerability Scanner (TMVS)

Install the client program on unprotected computers by running the Trend Micro™ Vulnerability Scanner (*Installing with Vulnerability Scanner* on page 4-16).

Summary

TABLE 3-3. OfficeScan client installation methods

	Web Install Page	Login Script Setup	Client Package	Client Package Deployed Using Microsoft SMS	Client Package Deployed Using Active Directory	Remote Installation	Client Disk Image	TMVS
Suitable for deployment across the WAN	No	No	No	Yes	Yes	No	No	No
Suitable for centralized administration and management	No	No	No	Yes	Yes	Yes	No	Yes
Requires client user intervention	Yes	Yes	Yes	Yes/No	Yes/No	No	No	No
Requires IT resource	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Suitable for mass deployment	No	No	No	Yes	Yes	No	No	No
Bandwidth consumption	High	High, if clients start at the same time	Low, if scheduled	Low, if scheduled	High, if clients start at the same time	High	Low	High

Chapter 4

Installing and Upgrading the OfficeScan Client

Installation/Upgrade scenarios:

Recommended post-installation tasks:

Other task:

Performing Fresh Installation

Close any running applications on client computers before installing the client program. Otherwise, the installation process may take longer to complete.

Installing from the Web Install Page

If you installed the OfficeScan server to a computer running Windows 2000 Server or Windows Server 2003 with Internet Information Server (IIS) 5.0 or later or Apache 2.0, your client users can install the client program from the Web install page created during server installation. Instruct users to go to the Web install page and download the client Setup files.

Tip: You can use Vulnerability Scanner to determine the users that did not follow the instructions to install from the Web install page (see *Using Vulnerability Scanner to verify the client installation* on page 4-22 for more information).

Requirements:

- At least Microsoft Internet Explorer 5.0 (Windows 2000), 6.0 (Windows XP/Server 2003) or 7.0 (Windows Vista) with the security level set to allow ActiveX™ controls
- Administrator privileges on the computer

Send the following instructions to your users to install the OfficeScan client from the Web install page.

To install from the Web install page:

1. If installing to a computer running Windows Vista, perform pre-installation tasks. See page 5-2 for details. If the computer does not run Windows Vista, skip this step.
2. Open an Internet Explorer window and type one of the following:
   - OfficeScan server with SSL:

     https://{OfficeScan_server_name}:{port}/officescan
   - OfficeScan server without SSL:

     http://{OfficeScan_server_name}:{port}/officescan
3. Click the link under **For Networked Computers**.
4. In the new screen that displays, click **Install Now** to start installing the OfficeScan client. The client installation starts.

   The OfficeScan client icon appears in the Windows system tray after installation.

Installing with Login Script Setup

Login Script Setup automates the installation of the OfficeScan client to unprotected computers when they log on to the network. Login Script Setup adds a program called AutoPcc.exe to the server login script.

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 program files and the antivirus, anti-spyware and Damage Cleanup Services components

---

Note: Client computers must be part of the domain to be able to use AutoPcc through login script.

To add AutoPcc.exe to the login script using Login Script Setup:

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

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

2. Locate the server whose login script you want to modify, select it, and then click **Select**. The server must be a primary domain controller and you must have administrator access. Login Script Setup prompts you for a user name and password.

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

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

   - To modify the login script of a single or multiple user profiles, select 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 previously selected, click the name from the Selected users list, and 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 informs you that you have modified the server login scripts successfully.

5. Click **OK**. Login Script Setup returns to its initial screen.
   - To modify the login scripts of other servers, repeat steps 2 to 4.
   - To close Login Script Setup, click **Exit**.

Note: AutoPcc.exe automatically installs the OfficeScan client to an unprotected Windows 2000/XP/Server 2003 computer when it logs on to the server whose login scripts you modified.

However, AutoPcc.exe does not automatically install the client to Windows Vista computers. Users need to connect to the server computer, navigate to \\{server computer name}\ofcscan), right-click **AutoPcc.exe**, and select **Run as administrator**.

For remote desktop installation using AutoPcc.exe:

- The computer must be run in Mstsc.exe /console mode. This forces the AutoPcc.exe installation to run in session 0.

- Map a drive to the ofcscan share and execute AutoPcc.exe from that point.

The Windows 2000/Server 2003 scripts

If you already have an existing login script, Login Script Setup will append a command that executes AutoPcc.exe. Otherwise, OfficeScan creates a batch file called ofcscan.bat that contains the command to run AutoPcc.exe.

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

\\{Server_name}\ofcscan\autopcc

Where:

- {Server_name} is the computer name or IP address of the OfficeScan server computer
- "ofcscan" is the OfficeScan directory on the server
- "autopcc" is the link to the autopcc executable file that will install the OfficeScan client

Login script location (through a net logon shared directory):

- Windows 2000 server: \\Windows 2000 server\system drive\WINNT\SYSVOL\domain\scripts\ofcscan.bat
- Windows Server 2003 server: \\Windows 2003 server\system drive\windir\sysvol\domain\scripts\ofcscan.bat

Installing with Client Packager

Client Packager can compress Setup and update files into a self-extracting file, which you can then send to users using conventional media such as CD-ROM. When users receive the package, all they have to do is run the Setup program in the client computer.

Client Packager is especially useful when deploying the client Setup or update files to clients in low-bandwidth remote offices. OfficeScan clients you install using Client Packager report to the server where Client Packager created the Setup package.

Self-extracting files created by Client Packager

- **Executable:** This common file type has an .exe extension.
- **Microsoft Installer (MSI) Package Format:** This file type conforms to Microsoft's Windows Installer package specifications. You can send the MSI package through conventional media or use Active Directory and Microsoft SMS. See *Deploying an MSI package using Active Directory* on page 4-9 and *Deploying an MSI package using Microsoft SMS* on page 4-10 for details. For more information on MSI, see the Microsoft Web site.

Client computer requirements

- Minimum of 160MB free disk space
- Windows Installer 2.0 (to run an MSI package)

To create a package using Client Packager:

1. On the OfficeScan server computer, browse to \PCCSRV\Admin\Utility\ClientPackager.
2. Double-click ClnPack.exe to run the tool. The Client Packager console opens.

3. Select the type of package you want to create:
   - **Setup:** Select if installing the OfficeScan client program. This will create an executable file.
   - **Update:** Select if updating OfficeScan client components only. This will also create an executable file.
   - **MSI Package:** Select if creating a package that conforms to the Microsoft Installer Package format
4. If creating an executable file, select the operating system for which you want to create the package.
5. Select from among the following installation options:
   - **Silent Mode:** Creates a package that installs on the client computer in the background, unnoticeable to the client and without showing an installation status window
   - **Update Agent:** Gives the client the ability to act as an update agent (Update Agents are alternative servers that help the OfficeScan server deploy components to clients.). If you install the OfficeScan client program using Client Packager and you enable the **Update Agent** option, you must use the Scheduled Update Configuration Tool to enable and configure scheduled updates (see *Using the Scheduled Update Configuration Tool* on page 4-9).

Tip: If you install the OfficeScan client program using Client Packager and you enable the Update Agent option, any OfficeScan server that registers with the client will not be able to synchronize or modify the following settings: the Update Agent privilege, client scheduled update, update from Trend Micro ActiveUpdate server, and updates from other update sources.

Trend Micro recommends installing only on client computers not registered with any OfficeScan server and configuring the Update Agent to get its updates from an update source other than an OfficeScan server. If you want to modify the Update Agent settings mentioned above, use a client program installation method other than Client Packager.

- **Force overwrite with latest version:** Overwrites old versions with the latest version; applicable only when you select **Update** as the package type.
- **Disable prescan (only for fresh install):** Disables the file scanning that OfficeScan performs before installation

6. Select the OfficeScan client utilities to include in the package.
   - **Outlook Mail Scan:** Scans Microsoft Outlook™ mailboxes for security risks
   - **Check Point SecureClient Support:** Support for Check Point™ SecureClient™ for Windows 2000/XP/Server 2003
7. Select the components to include in the installation package.
8. Next to **Source file**, ensure that the location of the ofcscan.ini file is correct. To modify the path, click ... to browse for the ofcscan.ini file. By default, this file is in the \PCCSRV folder of the OfficeScan server.
9. In **Output file**, click ... to specify the location where you want to create the client package and the file name (for example, ClientSetup.exe).
10. Click **Create**. When Client Packager finishes creating the package, the message "Package created successfully" appears. To verify successful package creation, check the output directory you specified.
11. Deploy the package.
    - Send the package to your users and ask them to run the client package on their computers by double-clicking the .exe or .msi file. For computers running Windows Vista, instruct users to right-click the .exe file and select **Run as administrator**.

      WARNING! *Send the package only to users whose OfficeScan client will report to the server where the package was created.*

    - If you created an .msi file, you can use Active Directory or Microsoft SMS. See *Deploying an MSI package using Active Directory* on page 4-9 or *Deploying an MSI package using Microsoft SMS* on page 4-10.

Using the Scheduled Update Configuration Tool

Use the Scheduled Update Configuration Tool to enable and configure scheduled updates on OfficeScan clients acting as Update Agents that you installed using Client Packager. This tool is available only on Update Agents that Client Packager installs.

To use the Scheduled Update Configuration Tool:

1. On the Update Agent that Client Packager installed, open Windows Explorer.
2. Go to the OfficeScan client folder.
3. Double-click SUCTool.exe to run the tool. The Schedule Update Configuration Tool console opens.
4. Select **Enable Scheduled Update**.
5. Specify the update frequency and time.
6. Click **Apply**.

Deploying an MSI package using Active Directory

You can take advantage of Active Directory features to deploy the MSI package simultaneously to multiple client computers. For instructions on creating an MSI file, see *Installing with Client Packager* on page 4-6.

To deploy an MSI package using Active Directory:

1. Open the Active Directory console.
2. Right-click the Organizational Unit (OU) where you want to deploy the MSI package and click **Properties**.
3. In the **Group Policy** tab, click **New**.
4. Choose between Computer Configuration and User Configuration, and open **Software Settings** below it.

Tip: Trend Micro recommends using **Computer Configuration** instead of **User Configuration** to ensure successful MSI package installation regardless which user logs on to the computer.

---

5. Below Software Settings, right-click **Software installation**, and then select **New** and **Package**.
6. Locate and select the MSI package.
7. Select a deployment method and then click **OK**.
   - **Assigned:** The MSI package is automatically deployed the next time users log on to the computer (if you select User Configuration) or when the computer restarts (if you select Computer Configuration). This method does not require any user intervention.
   - **Published:** To run the MSI package, inform users to go to Control Panel, open the Add/Remove Programs screen, and select the option to add/install programs on the network. When the OfficeScan client MSI package displays, users can proceed to install the client.

Deploying an MSI package using Microsoft SMS

You can deploy the MSI package using Microsoft System Management Server (SMS). However, you must have Microsoft BackOffice SMS installed on the server.

For instructions on creating an MSI file, see *Installing with Client Packager* on page 4-6.

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

The SMS server needs to obtain the MSI file from the OfficeScan server before it can deploy the package to target computers.

- **Local:** The SMS server and the OfficeScan server are on the same computer
- **Remote:** The SMS server and the OfficeScan server are on different computers

To obtain the package locally:

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 and select the MSI package file created by Client Packager, and then click **Open**. The MSI package name appears on the Package Definition screen. The package shows "Trend Micro OfficeScan Client" and the program version.
7. Click **Next**. The Source Files screen appears.
8. Click **Always obtain files from a source directory**, and then click **Next**.

   The Source Directory screen appears, displaying the name of the package you want to create and the source directory.
9. Click **Local drive on site server**.
10. Click **Browse** and select the source directory containing the MSI file.
11. Click **Next**. The wizard creates the package. When it completes the process, the name of the package appears on the SMS Administrator console.

To obtain the package remotely:

1. On the OfficeScan server, use Client Packager to create a Setup package with an .exe extension (you cannot create an .msi package). See *Installing with Client Packager* on page 4-6 for details.
2. On the computer where you want to store the source, create a shared folder.
3. Open the SMS Administrator console.
4. On the **Tree** tab, click **Packages**.
5. On the **Action** menu, click **New** > **Package From Definition**. The Welcome screen of the Create Package From Definition Wizard appears.
6. Click **Next**. The Package Definition screen appears.
7. Click **Browse**. The Open screen appears.
8. Browse for the MSI package file. The file is on the shared folder you created.
9. Click **Next**. The Source Files screen appears.

10. Click **Always obtain files from a source directory**, and then click **Next**. The Source Directory screen appears.
11. Click **Network path (UNC name)**.
12. Click **Browse** and select the source directory containing the MSI file (the shared folder you created).
13. 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 **All Windows NT Systems**.
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 your 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 to members of subcollections.
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.

    If you want Microsoft SMS to stop advertising the package on a specific date, click **Yes. This advertisement should expire**, and then specify the date and time in the **Expiration date and time** list boxes.

16. Click **Next**. The Assign Program screen appears.

17. Click **Yes, assign the program**, and then click **Next**.

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

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

Known Issues when Installing with Microsoft SMS

- "Unknown" appears in the Run Time column of the SMS console.
- If the installation is unsuccessful, the installation status may still show that the installation is complete on the SMS program monitor. For instructions on how to verify if the installation was successful, see *Using Vulnerability Scanner to verify the client installation* on page 4-22.

Installing from the OfficeScan Web Console

You can remotely install the OfficeScan client to one or several Windows XP, 2000, 2003 Server and Vista computers connected to the network. Ensure you have administrator rights to the target computers to perform remote installation. Remote installation will not install the OfficeScan client on a computer already running the OfficeScan server.

To install from the OfficeScan Web console:

1. If installing to a computer running Windows Vista, perform pre-installation tasks. See page 5-2 for details. If the computer does not run Windows Vista, skip this step.
2. In the Web console, click **Networked Computers > Client Installation > Remote**.

3. Select the target computers.
   - The **Domains and Computers** list displays all the Windows domains on your network. To display computers under a domain, double-click the domain name. Select a computer, and then click **Add**.
   - If you have a specific computer name in mind, type the computer name in the field on top of the page and click **Search**.

   OfficeScan will prompt you for the target computer's user name and password. Make sure to use an administrator account user name and password to continue.
4. Type your user name and password, and then click **Log in**. The target computer appears in the **Selected Computers** table.
5. Repeat steps 2 and 3 to add more computers.
6. Click **Install** when you are ready to install the client to your target computers. A confirmation box appears.
7. Click **Yes** to confirm that you want to install the client to the target computers. A progress screen appears as the program files copy to each target computer.

   When OfficeScan completes the installation to a target computer, the computer name disappears in 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 remote installation.

Note: If you install to multiple computers, OfficeScan will record any unsuccessful installation in the logs, but it will not postpone the other installations. You do not have to supervise the installation after you click **Install**. Check the logs later on to see the installation results.

Installing from a Client Disk Image

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

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

Note: Supported Windows platforms include Windows 2000, XP and Server 2003. This installation method does not support Microsoft Vista and x64 platforms.

To create a disk image of an OfficeScan client:

1. Install the OfficeScan client to a computer. You will use this client as the source of the disk image.
2. Copy ImgSetup.exe from the OfficeScan server's \PCCSRV\Admin\Utility\ImgSetup folder to this computer.
3. Run ImgSetup.exe on this computer. This creates a RUN registry key under HKEY_LOCAL_MACHINE.
4. Create a disk image of the OfficeScan client using your disk imaging software.
5. Restart the clone. ImgSetup.exe will automatically start and create one new GUID value. The client will report this new GUID to the server and the server will create a new record for the new client.

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

Installing with Vulnerability Scanner

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

This section explains how to install the OfficeScan client program with Vulnerability Scanner. For instructions on how to use Vulnerability Scanner to detect antivirus solutions, see the Administrative Tools section of the *Administrator's Guide* and the OfficeScan server online help.

Note: You can use Vulnerability Scanner on computers running Windows 2000 and Server 2003.

You cannot install OfficeScan clients with Vulnerability Scanner to a computer with the OfficeScan server installed.

To install OfficeScan client with Vulnerability Scanner:

1. If installing to a computer running Windows Vista, perform pre-installation tasks. See page 5-2 for details. If the computer does not run Windows Vista, skip this step.
2. In the computer where you installed OfficeScan server, open \OfficeScan\PCCSRV\Admin\Utility\TMVS. Double-click TMVS.exe. The Trend Micro Vulnerability Scanner console appears.
3. Click **Settings**.
4. Under **OfficeScan server settings**, type the OfficeScan server name and port number.
5. Select **Auto-Install OfficeScan client on unprotected computers**.
6. Click **OK** to begin checking the computers on your network and begin OfficeScan client installation.

Upgrading the OfficeScan Client

You can upgrade to a full version of OfficeScan from a previous version or from an evaluation version. When you upgrade the OfficeScan server, clients automatically upgrade when you perform client installation with any of the installation methods available (see *Installation Methods* on page 3-5 for information on installation methods).

You can also use the Client Mover tool. See the *Administrator's Guide* and OfficeScan server online help for details.

Migrating from Third-party Antivirus Applications

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

Note: If using Client Mover to move an un-upgraded OfficeScan client to a server already upgraded to this version, the client upgrades automatically. For more information on Client Mover, see the *Administrator's Guide* and the OfficeScan server online help.

Automatic Client Migration

Automatic client migration refers to replacing existing client antivirus software with the OfficeScan client. The client Setup program automatically uninstalls the existing software and replaces it with the OfficeScan client.

Note: OfficeScan only uninstalls clients, not servers.

To check the applications that OfficeScan automatically uninstalls, open the following files in \Trend Micro\OfficeScan\PCCSRV\Admin: tmuninst.ptn, tmuninst_as.ptn.

Client migration issues:

- If automatic client migration is successful but a user encounters problems with the OfficeScan client right after installation, restart the computer.
- If the client Setup program prompts you that it cannot automatically uninstall an existing client antivirus software on a user's computer, perform the following tasks:
  - Manually uninstall the existing client antivirus software. Depending on the uninstallation process of the software, the computer may or may not need to restart after uninstallation.
  - Install the OfficeScan client using any of the installation methods discussed in *Performing Fresh Installation* on page 4-2.
- If the client Setup program proceeded to install the OfficeScan client but did not uninstall any existing client antivirus software, there may be conflicts between the two client software installed on the same computer. In this case, uninstall both software, and then install the OfficeScan client using any of the installation methods discussed in *Performing Fresh Installation* on page 4-2.

Migrating from ServerProtect Normal Servers

The ServerProtect Normal Server Migration Tool is a Windows-based tool that helps migrate computers running ServerProtect Normal Server to OfficeScan client.

System Requirements

The ServerProtect Normal Server Migration Tool shares the same hardware and software specification as the OfficeScan server. Run the tool on Windows 2000/XP/Vista/Server 2003 computers.

When uninstallation of the ServerProtect Normal server is successful, it installs the OfficeScan client. However, it does not preserve and migrate the ServerProtect Normal server's settings to OfficeScan client settings.

Installing Server Protect Normal Server Migration Tool

On the OfficeScan server computer, open \OfficeScan\PCCSRV\Admin\Utility\SPNSXfr and copy the files SPNSXfr.exe and SPNSX.ini to \PCCSRV\Admin.

Use the local/domain administrator account to access the client computer. If you log on the remote computers with insufficient privileges, such as "Guest" or "Normal user", you will not be able to perform installation.

To use the Server Protect Normal Server Migration Tool:

1. Double click the SPNSXfr.exe file to open the tool. The Server Protect Normal Server Migration Tool console opens.
2. Select the OfficeScan server. The path of the OfficeScan server appears under OfficeScan server path. If it is incorrect, click **Browse** and select the PCCSRV folder in the directory where you installed OfficeScan.
   To enable the tool to automatically find the OfficeScan server again the next time you open the tool, select the **Auto find OfficeScan server** check box (selected by default).
3. Select the computers running ServerProtect Normal Server on which to perform the migration by clicking one of the following under **Target computer**:
   - **Windows network tree:** Displays a tree of domains on your network. To select computers by this method, click the domains on which to search for client computers.
   - **Information Server name:** Search by Information Server name. To select computers by this method, type the name of an Information Server on your network in the text box. To search for multiple Information Servers, enter a semicolon ";" between server names.
   - **Certain Normal Server name:** Search by Normal Server name. To select computers by this method, type the name of a Normal Server on your network in the text box. To search for multiple Normal Servers, enter a semicolon ";" between server names.

- **IP range search:** Search by a range of IP addresses. To select computers by this method, type a range of class B IP addresses under IP range.

Note: If a DNS server on your network does not respond when searching for clients, the search will hang. Wait for the search to time out.

4. Select to include computers running Windows Server 2003 in the search.
5. Select to restart computers running Windows Server 2003. For the migration to complete successfully on Windows 2003 computers, the computer must reboot. Selecting this check box ensures that it automatically reboots. If you do not select the **Restart Windows Server 2003 computers** check box, you must restart the computer manually after migration.
6. Click **Search**. The search results appear under ServerProtect Normal Servers.
7. Click the computers on which to perform the migration:
   - To select all computers, click **Select All**.
   - To deselect all computers, click **Unselect All**.
   - To export the list as a .CSV file, click **Export to CSV**.

   If logging on the target computers requires a user name and password, do the following:
   a. Select the **Use group account/password** check box.
   b. Click **Set User Logon Account**. The **Enter Administration Information** window appears.
   c. Type the user name and password.
   d. Click **Ok**.
   e. Click **Ask again if logon is unsuccessful** to be able to type the user name and password again during the migration process if you are unable to log on.

8. Click **Migrate**.

Note: The ServerProtect Normal Server Migration Tool does not uninstall the Control Manager agent for ServerProtect. For instructions on how to uninstall the agent, refer to your ServerProtect and/or Control Manager documentation.

While installing the OfficeScan client, the migration tool client installer may time out and the result may be shown as failed. However, the client may have been installed successfully. Verify the installation on the client computer from the OfficeScan Web console.

Migration fails under the following circumstances:
- If the remote client cannot use the NetBIOS protocol, or ports 455,337~339 are blocked
- If the remote client cannot use the RPC protocol
- If the Remote Registry Service stops

Post-installation Tasks

Trend Micro recommends performing the following post-installation tasks:

- *Verifying the Client Installation, Upgrade, or Migration* on page 4-21
- *Initiating Component Update* on page 4-24
- *Testing OfficeScan Using the EICAR Test Script* on page 4-25

Verifying the Client Installation, Upgrade, or Migration

After completing the installation or upgrade, verify the following:

- The Trend Micro OfficeScan Client shortcuts on the Windows **Start** menu of the client computer
- If "Trend Micro OfficeScan Client" is in the **Add/Remove Programs** list of the client computer's Control Panel

- OfficeScan client services included in Windows services:
  - OfficeScan NT Listener
  - OfficeScan NT Firewall (if firewall was enabled during installation)
  - OfficeScan NT Proxy Service
  - OfficeScanNT RealTime Scan
- Installation log: OFCNT.LOG in the following locations:
  - %windir% for all installation methods except MSI package
  - %temp% for the MSI package installation method
- Installation status using Vulnerability Scanner (see the next section)

Using Vulnerability Scanner to verify the client installation

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

Note: You can use Vulnerability Scanner on computers running Windows 2000 and Server 2003.

To verify client installation using Vulnerability Scanner:

1. On the OfficeScan server computer, open \OfficeScan\PCCSRV \Admin\Utility\ TMVS. Double-click TMVS.exe. The Trend Micro Vulnerability Scanner console appears.
2. Click **Settings**.
3. Under **Product query**, select the **OfficeScan Corporate Edition/Security Server** check box and specify the port that the server uses to communicate with clients.
4. Select whether to use Normal or Quick retrieval. 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 **Retrieve computer descriptions when available**.

5. To automatically send the results to yourself or to other administrators in your organization, select **Email results to the system administrator**. Then, click **Configure** to specify your email settings.
   - In **To**, type the email address of the recipient.
   - In **From**, type your email address. This will let the recipients know who sent the message.
   - In **SMTP server**, type the address of your SMTP server. For example, type smtp.company.com. This is a required information.
   - In **Subject**, type a new subject for the message or accept the default subject.
6. Click **OK** to save your settings.
7. To display an alert on unprotected computers, click the **Display notification on unprotected computers**. Then, click **Customize** to set the alert message. The Alert Message screen appears. Type a new alert message in the text box or accept the default message, and then click **OK**.
8. To save the results as a comma-separated value (CSV) data file, select **Automatically save the results to a CSV file**. By default, Vulnerability Scanner saves CSV data files to the TMVS folder. If you want to change the default CSV folder, click **Browse**, select a target folder on your computer or on the network, and then click **OK**.
9. 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** fields.
10. Click **OK**. The Vulnerability Scanner console appears.
11. To run a manual vulnerability scan on a range of IP addresses, do the following:

Note: Vulnerability Scanner only supports a class B subnet IP address range.

---

   a. In **Manual Scan**, type the IP address range of computers that you want to check for installed antivirus solutions.
   b. Click **Start** to begin checking the computers on your network.

12. To run a manual vulnerability scan on computers requesting IP addresses from a DHCP server, do the following:
    a. Click the **DHCP Scan** tab in the **Results** box. The **Start** button appears.
    b. Click **Start**. Vulnerability scanner begins listening for DHCP requests and performing vulnerability checks on computers as they log on to the network.

Vulnerability Scanner checks your network and displays the results in the **Results** table. Verify that all desktop and notebook computers 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.

Initiating Component Update

Notify your clients to update their components to ensure that they have the most up-to-date protection from security risks.

Note: This section shows you how to initiate manual update. For information on automatic update and update configurations, see the OfficeScan server online help.

To deploy the components to the clients:

1. Open the OfficeScan Web console.
2. Click **Updates** > **Networked Computers** > **Manual Update** on the main menu. The Manual Deployment screen appears showing a summary of components, versions, and the last update period.
3. Select the target clients. You can update clients with outdated components or manually select clients.
   - **Select clients with outdated components:** Optionally include roaming clients with functional connections to the server, and then click **Initiate Update**.
   - **Manually select clients:** After selecting this option, click **Select** to choose specific clients from the client tree. Select the clients you want to update and then click **Initiate Component Update** on top of the client tree.

   The server starts notifying each client to download updated components.

Testing OfficeScan Using the EICAR Test Script

Trend Micro recommends testing OfficeScan and confirming that it works by using the EICAR test script. EICAR, the European Institute for Computer Antivirus Research, developed the test script as a safe way to confirm proper installation and configuration of antivirus software. Visit the EICAR Web site for more information:

http://www.eicar.org

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

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

To test OfficeScan using the EICAR test script:

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

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

Uninstalling the Client

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

- *Uninstalling from the Web Console* on page 4-26
- *Running the Client Uninstallation Program* on page 4-27

Note: If the client also has a Cisco Trust Agent (CTA) installation, uninstalling the OfficeScan client program may or may not remove the CTA. This depends on the settings you configured for the client for Cisco Agent Deployment (see the *Administrator's Guide* and the OfficeScan online help for more information).

Uninstalling from the Web Console

You can uninstall the client program from computers on the network using the Web console. Note that uninstalling the client program also removes security risk protection on selected clients.

To uninstall the client from the Web console:

1. On the OfficeScan Web console main menu, click **Networked Computers > Client Management**. The client tree displays.
2. In the client tree, select the clients to uninstall the OfficeScan client, and then click **Tasks > Client Uninstallation**.
3. In the Client Uninstallation screen, click **Initiate Uninstallation**. The server sends a notification to the clients.
4. Check the notification status and verify if there are clients that did not receive the notification.
   a. Click **Select Un-notified Computers** and then **Initiate Uninstallation** to immediately resend the notification to un-notified clients.
   b. Click **Stop Uninstallation** to prompt OfficeScan to stop notifying clients currently being notified. Clients already notified and already performing uninstallation will ignore this command.

Running the Client Uninstallation Program

If you granted users the privilege to uninstall the client program, instruct them to run the client uninstallation program from their computers. For more information, see the *Administrator's Guide* and the OfficeScan server online help.

To run the client uninstallation program:

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

The user does not need to restart the client computer to complete the uninstallation.

Chapter 5

FAQs and Troubleshooting

Topics in this chapter:

Frequently Asked Questions (FAQs)

I have several questions about OfficeScan registration. Where can I find the answers?

See the following Web site for frequently asked questions about registration:

http://kb.trendmicro.com/solutions/search/main/search/solutionDetail.asp?solutionID=16326

Which OfficeScan versions can upgrade to the current version?

This version of OfficeScan supports upgrade from any of the following versions: 7.3, 7.0, 6.5, 5.58.

Which operating systems are no longer supported in this version?

This version of OfficeScan no longer supports Windows 95, 98, Me, NT and IA64 architecture.

Can I upgrade the OfficeScan client from version 7.3 with patch to 8.0 from Terminal Service 2000?

No. OfficeScan 7.3 does not support Terminal Service.

What do I need to do before installing the OfficeScan client to computers running Windows Vista?

If you will install the OfficeScan client from the Web console (remote installation) or by using Vulnerability Scanner, perform the following steps on the Windows Vista computer:

1. Enable a built-in administrator account and set the password for the account.
2. Disable the Windows firewall.
   a. Click **Start > Programs > Administrative Tools > Windows Firewall with Advanced Security**.
   b. For Domain Profile, Private Profile, and Public Profile, set the firewall state to "Off".
3. Open the Windows Services screen (click **Start > Run** and type **services.msc**) and start the **Remote Registry** service.
4. Install the OfficeScan client using the built-in administrator account and password. See *Installing from the OfficeScan Web Console* on page 4-13or *Installing with Vulnerability Scanner* on page 4-16 for the procedure.

If users will install the OfficeScan client from the Web install page, instruct them to do the following:

1. Log on to the computer using a built-in administrator account.
2. Open Internet Explorer and click **Tools > Internet Options > Security**. The **Internet** zone is selected by default.
3. Click **Custom level...**

4. Under **ActiveX controls and plug-ins**, enable **Automatic prompting for ActiveX controls**.
5. Install the OfficeScan client. See *Installing from the Web Install Page* on page 4-2 for the procedure.

Note: During installation, users need to allow installation of ActiveX control to install the client successfully.

Can OfficeScan work in a network environment that utilizes Network Address Translation?

Yes. You must enable Scheduled Deployment in a NAT environment to ensure your clients can receive updated components. See the *Administrator's Guide* and for more information.

Can I manually uninstall the OfficeScan server and client?

Yes. However, Trend Micro recommends using the uninstallation program to uninstall the OfficeScan server and client. For the procedure, see *Uninstalling the Server* on page 2-27 and *Uninstalling the Client* on page 4-26.

Perform manual uninstallation only if you encounter problems with the uninstallation program. For the procedure, see *Server Uninstallation* on page 5-14 and *Solution: Manually uninstall the client.* on page 5-12.

What do I need to do if I do not want to use the OfficeScan firewall?

During OfficeScan server installation, do not select **Enable firewall** in the Antivirus Features screen.

If you enabled the OfficeScan firewall during installation, you can disable it from the Web console by doing the following:

1. Go to **Administration > Product License > Additional Services**.
2. In Firewall for networked computers, click **Disable**.
3. Log off from the Web console and then log on again.

Troubleshooting Resources

Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) collects necessary debugging information from a customer's product whenever problems occur. It automatically turns the product's debug status on and off and collects necessary files according to problem categories. Trend Micro uses this information to troubleshoot problems related to the product.

To obtain this tool and relevant documentation, contact your Support provider.

Installation Logs

Use the installation log files OfficeScan automatically generates to troubleshoot installation problems.

TABLE 5-1. Installation log files

Log File	File Name	Location
Server local installation/upgrade log	OFCMAS.LOG	%windir%
Server remote installation/upgrade log	OFCMAS.LOG (On the computer where you launched Setup) OFCMAS.LOG (On the target computer)	%windir%
Client installation log	OFCNT.LOG	%windir% (For all installation methods except MSI package) %temp% (For the MSI package installation method)

Server Debug Logs

You can enable debug logging before performing the following server tasks:

- Uninstall and then install the server again.
- Upgrade OfficeScan 8.0 to a new version.
- Perform remote installation/upgrade (Debug logging is enabled on the computer where you launched Setup and not on the remote computer.).

WARNING! *Debug logs may affect server performance and consume a large amount of disk space. Enable debug logging only when necessary and promptly disable it if you no longer need debug data. Remove the log file if the file size becomes huge.*

To enable debug logging on the OfficeScan server computer:

1. Copy the "LogServer" folder located in \PCCSRV\Private to C:\.
2. Create a file named ofcdebug.ini with the following content:

   [debug]

   DebugLevel=9

   DebugLog=C:\LogServer\ofcdebug.log
3. Save ofcdebug.ini to C:\LogServer.
4. Perform the appropriate task (that is, uninstall/reinstall the server, upgrade to a new server version, or perform remote installation/upgrade).
5. Check ofcdebug.log in C:\LogServer.

Client Debug Logs

You can also enable debug logging before installing the OfficeScan client.

WARNING! *Debug logs may affect client performance and consume a large amount of disk space. Enable debug logging only when necessary and promptly disable it if you no longer need debug data. Remove the log file if the file size becomes huge.*

To enable debug logging on the OfficeScan client computer:

1. Create a file named ofcdebug.ini with the following content:

   [Debug]

   Debuglog=C:\ofcdebug.log

   debuglevel=9

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
2. Send ofcdebug.ini to client users, instructing them to save the file to C:\.
3. LogServer.exe automatically runs each time the client computer starts. Instruct users NOT to close the LogServer.exe command window that opens when the computer starts as this prompts OfficeScan to stop debug logging. If users close the command window, they can start debug logging again by running LogServer.exe located in \OfficeScan Client.
4. For each client computer, you can check ofcdebug.log in C:\.
5. To disable debug logging for the OfficeScan client, delete ofcdebug.ini.

Knowledge Base

Some solutions in this section direct you to the Trend Micro Knowledge Base. Please make sure you have Internet connection to open the Knowledge Base.

Troubleshooting Installation Issues

Client Installation

PROBLEM 1:

The OfficeScan client does not install on computers running Windows XP.

Solution:

Disable **Simple File Sharing** on computers running Windows XP (see your Windows documentation for instructions).

PROBLEM 2:

After installing Windows 2003 Service Pack 1, the client tree in the Web console's Remote Installation screen (**Networked Computers > Client Installation > Remote**) does not display the domains and client computers.

Solution:

Option 1: Change the anonymous user account in the Internet Information Services (IIS) Manager

1. Open the IIS console by clicking **Start > Programs > Administrative Tools > Internet Services Manager.**
2. Click the **OfficeScan** virtual directory, select **officescan > console > remoteinstallcgi**, and double-click **cgiRemoteInstall.exe**.
3. In the **File Security** tab, then click **Edit > Browse > Advanced > Find Now**.
4. Select Administrator (if any), then click **OK**.
5. Double-click cgiGetNTDomain.exe. Repeat steps 3 and 4.

6. Double-click cgiGetNTClient.exe. Repeat steps 3 and 4.

Option 2: Install OfficeScan using any of the following installation methods:

- Login Script Setup. See *Installing with Login Script Setup* on page 4-3.
- Web Installation. See *Installing from the Web Install Page* on page 4-2.
- Client Packager. See *Installing with Client Packager* on page 4-6.

PROBLEM 3:

Some client computers do not appear in the Remote Installation screen (**Networked Computers > Client Installation > Remote**) even when they are online. The client computers and the server computer are on the same subnet and can communicate with each other (verified using ping).

Explanation:

The computers are not visible on the network.

Solution:

Make the computers visible on the network by enabling File and Print Sharing for Microsoft Networks in Network Connection.

PROBLEM 4:

The Web install page containing the link for the OfficeScan client installation does not display.

Explanation:

The settings in the Internet options may have been configured incorrectly.

Solution:

Perform the following steps on the target computers:

1. If the user can download the client Setup files but cannot install the OfficeScan client, verify the following:
   - The user has Administrator rights on the computer.

- The target computer meets the minimum system requirements for OfficeScan client installation.
- The computer runs a supported Windows operating system.

2. Open Internet Explorer and click **Tools > Internet Options**.
3. Click the **Connections** tab and select **LAN Settings**.
4. Disable **Bypass proxy server for local addresses**.
5. Click **OK** to save the changes.
6. Install the OfficeScan client again from the Web install page.

PROBLEM 5:

When using the Login Script Setup to install the OfficeScan client, the following error message appears:

"Error – Failed to logon. Please make sure the selected server {Server Name} is a Windows server, and enter the correct user name and password."

Solution:

Use an account with Domain Administrator privileges when installing the OfficeScan client.

PROBLEM 6:

If you install the Check Point SecureClient Support tool in OfficeScan 7.3 with patch 2 and you upgrade to this version, there will be issues with the tool after the upgrade.

Solutions:

- Use Client Packager to deploy Check Point SecureClient Support.
- Install the tool from the OfficeScan client console.

Migration from Third-party Antivirus Software

PROBLEM 1:

The OfficeScan client Setup program is unable to automatically uninstall third-party antivirus software installed on the client computer.

Explanation:

The Setup program for the OfficeScan client utilizes the third-party software's uninstallation program to automatically remove it from the client computer and replace it with the OfficeScan client. Automatic uninstallation fails for the following reasons:

- The third-party software's version number or product key is inconsistent.
- The third-party software's uninstallation program does not work.
- Certain files for the third-party software are either missing or corrupted.
- Setup cannot clean the registry key for the third-party software.
- The third-party software has no uninstallation program.

Solutions:

- Manually remove the third-party software.
- Stop the service for the third-party software.
- Unload the service or process for the third-party software.

To manually remove the third-party software:

- If the third-party software registers to the Add/Remove Programs
  a. Open the Control Panel.
  b. Double-click **Add/Remove Programs**.
  c. Select the third-party software from the list of installed programs.
  d. Click **Remove**.

- If the third-party software does not register to the Add/Remove Programs
  - **a.** Open the Windows registry.
  - **b.** Go to HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Uninstall.
  - **c.** Locate the third-party software and run the uninstall string value.
  - **d.** If the third-party software's Setup program is in MSI format:
    - Locate the product number
    - Verify the product number
    - Run the uninstall string

Note: Some product uninstallation keys are in the Product Key folder.

To modify the service for the third-party software:

1. Restart the computer in Safe mode.
2. Modify the service startup from automatic to manual.
3. Restart the system again.
4. Manually remove the third-party software.

To unload the service or process for the third-party software:

WARNING! *This procedure may cause undesirable effects to your computer if performed incorrectly. Trend Micro highly recommends backing up your system first.*

1. Unload the service for the third-party software.
2. Open the Windows registry, then locate and delete the product key.
3. Locate and delete the run or run service key.

Verify that the service registry key in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services has been removed.

Client Uninstallation

PROBLEM 1:

The client does not uninstall using the client uninstallation program.

Solution: Manually uninstall the client.

WARNING! *This procedure requires you to delete registry keys. Before doing so, make sure you understand how to restore it if a problem occurs. Making incorrect changes to your registry can cause serious system problems. Always make a backup copy before making any registry changes. For more information, refer to the Registry Editor Help.*

To manually uninstall the OfficeScan client:

1. Stop the following services:
   - OfficeScan NT Firewall (if enabled)
   - OfficeScan NT Listener
   - OfficeScan NT Proxy Service
   - OfficeScanNT RealTime Scan
2. Open Registry Editor. On the Start menu, click **Start > Run** and type **regedit**.
3. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services and delete the following keys (if available):
   - ntrtscan
   - tmcfw
   - tmcomm
   - TmFilter
   - tmlisten
   - TmPfw
   - TmPreFilter
   - TmProxy
   - tmtdi

4. Go to HKEY_LOCAL_MACHINE \SOFTWARE\TrendMicro and delete the following keys (if available):

   Note: For 64-bit clients, look for HKEY_LOCAL_MACHINE \SOFTWARE \Wow6432Node\TrendMicro.

   - CFW
   - NSC
   - OfcWatchDog
   - Pc-cillinNTCorp or OfficeScanCorp (depending on the client)

5. Go to HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft\Windows\CurrentVersion\Run and delete the key **OfficeScanNT Monitor**.
6. Delete the OfficeScan client shortcut from the Windows Start menu.
7. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall and delete the **OfficeScanNT** key.
8. If the OfficeScan firewall is enabled, open Control Panel and select **Network Connections > Local Area Connection**. Click **Properties** and then uninstall Trend Micro Common Firewall Driver.
9. Restart the computer.
10. Delete the directories that contain the OfficeScan client program files.

PROBLEM 2:

OfficeScan client cannot be uninstalled using the "per-user" uninstallation method on Microsoft SMS and Active Directory's Group Policy Object.

Explanation:

The OfficeScan client needs to check the uninstallation password. For the "per-system" uninstallation from Microsoft SMS and Active Directory, OfficeScan skips password checking by account name (SYSTEM and SMSCliToknAcct&). However, for the "per-user" uninstallation, OfficeScan cannot skip password checking if the privilege "Allow the user to uninstall the OfficeScan client" is not set.

Solutions:

- Use "per-system" installation and uninstallation to finish the deployment.
- In the Web console, enable the privilege "Allow the user to uninstall the OfficeScan client".

Server Uninstallation

PROBLEM 1:

The server does not uninstall using the server uninstallation program.

Solution:

Manually uninstall the server.

WARNING! *This procedure requires you to delete registry keys. Before doing so, make sure you understand how to restore it if a problem occurs. Making incorrect changes to your registry can cause serious system problems. Always make a backup copy before making any registry changes. For more information, refer to the Registry Editor Help.*

To manually uninstall the OfficeScan server:

1. Stop the OfficeScan Master Service from the Windows Services screen.
2. Delete the OfficeScan program shortcut from the Start menu.
3. Delete the files in the \Trend Micro\OfficeScan directory. This deletes the DBBackup and PCCSRV folders.
4. Delete the IIS Virtual Directories.
   a. Open the Internet Information Services console. You can open the console from the Windows Start menu (**Start > Programs > Administrative Tools > Internet Services Manager**).
   b. Search and delete the **OfficeScan** folder.
5. Delete the OfficeScan registry keys.
   a. Open Registry Editor. On the Start menu, click **Start > Run** and type **regedit**.
   b. Go to HKEY_LOCAL_MACHINE\Software\TrendMicro and delete the **OfficeScan** key.
   c. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version Uninstall\ and delete the **OfficeScan Management Console** key.
   d. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ and delete the **ofcservice** key.

Apache Web Server

Policy Server and Plug-in Manager handle some of the Web requests using Internet Server Application Programming Interface (ISAPI). ISAPI is not compatible with Apache Web server versions 2.0.56 to 2.0.59 and versions 2.2.3 to 2.2.4.

You can restore an unsupported Apache Web server version. For example, you can restore version 2.0.59 to version 2.0.54.

To restore Apache Web server version 2.0.59 to 2.0.54:

1. Upgrade the OfficeScan server or Policy Server to this version.
2. Back up the following files on the **Apache2** folder on the OfficeScan installation folder:
   - httpd.conf
   - httpd.conf.tmbackup
   - httpd.default.conf
3. Uninstall Apache 2.0.59 from the Add/Remove Programs screen.
4. Install Apache 2.0.54.
   a. Launch apache.msi from \PCCSRV\Admin\Utility\Apache.
   b. In the Server Information screen, enter the required information.
   c. In the Destination Folder screen, change the destination folder by clicking change and browsing to \PCCSRV.
   d. Complete the installation.
5. Copy the backup files back to the **Apache2** folder.
6. Restart the Apache service.

Chapter 6

Contacting Trend Micro

Topics in this chapter:

Technical Support

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

Trend Micro Incorporated provides worldwide support to all registered users.

- Get a list of the worldwide support offices at http://www.trendmicro.com/support.
- Get the latest Trend Micro product documentation at http://www.trendmicro.com/download.

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

Trend Micro, Inc.

10101 North De Anza Blvd., Cupertino, CA 95014

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

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

Fax: +1 (408) 257-2003

Web address: www.trendmicro.com

Email: support@trendmicro.com

Speeding Up Your Support Call

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

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

The Trend Micro Knowledge Base

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

http://esupport.trendmicro.com

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

TrendLabs

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

You can rely on the following post-sales service:

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

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

Comprehensive security information is available at the Trend Micro Web site:
http://www.trendmicro.com/vinfo/

Information available:

- List of viruses and malicious mobile code currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories

- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

Sending Suspicious Files to Trend Micro

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

http://subwiz.trendmicro.com/subwiz

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

- Send an email to: virusresponse@trendmicro.com, and specify "Phish or Disease Vector" as the Subject.
- Use the Web-based submission form: http://subwiz.trendmicro.com/subwiz.

Documentation Feedback

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

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

Appendix A

Sample Deployment

This section illustrates how best to deploy OfficeScan based on network topology and available network resources. You can use this as a reference when planning OfficeScan deployment in your organization.

Basic Network

Figure 1-1 illustrates a basic network with the OfficeScan server and clients connected directly. Most business networks have this configuration where the LAN (and /or WAN) access speed is 10Mbps, 100Mbps or 1Gbps. In this scenario, a computer that meets the OfficeScan system requirements and has adequate resources is a prime candidate for the installation of the OfficeScan server.

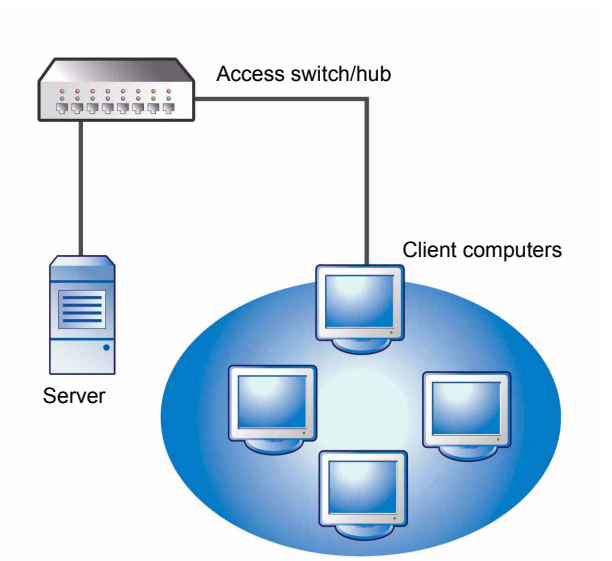


FIGURE 1-1 Basic network topology

Multiple Site Network

For a network with multiple access points and multiple remote sites with different bandwidths, analyze the consolidation points in terms of offices and network bandwidth, and determine their current bandwidth utilization. This presents a clearer picture as to how best to deploy OfficeScan.

Figure 1-2 illustrates a multiple site network topology.

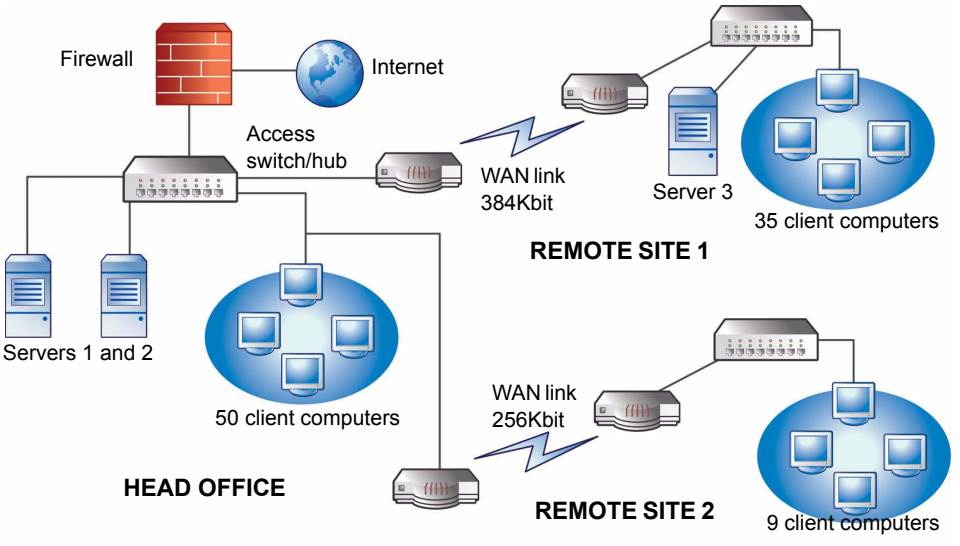


FIGURE 1-2 Multiple site network topology

Network information:

- Remote Site 1 WAN link averages around 70 percent utilization during business hours. There are 35 client computers on this site.
- Remote Site 2 WAN link averages around 40 percent utilization during business hours. There are 9 client computers on this site.
- Server 3 only functions as a file and print server for the group at Remote Site 1. This computer is a possible candidate for installing an OfficeScan server, but may not be worth the extra management overhead. All servers run Windows 2000. The network uses Active Directory, but mainly for network authentication.
- All client computers in Head Office, Remote Site 1, and Remote Site 2 run Windows 2000 or Windows XP.

Tasks:

1. Identify the computer where you will install the OfficeScan server. See *Installing or Upgrading the OfficeScan Server* on page 2-2 for the installation procedure.
2. Identify the available installation methods and eliminate methods that do not fit the requirement. See *Installation Methods* on page 3-5 for more information.

   Possible installation methods:

   Login Script Setup

   Login Script Setup works well if there is no WAN in place because local traffic does not matter. However, given that more than 50MB of data transmits to each computer, this option is not viable.

   Remote installation from the Web console

   This method is valid for all the LAN-connected computers at the head office. Because these computers all run Windows 2000, it is simple to deploy the package to the computers.

   Due to the low link speed between the two remote sites, this deployment method may impact available bandwidth if OfficeScan deployment occurs during business hours. You can use the whole link capacity to deploy OfficeScan during non-business hours when most people are no longer at work. However, if users turn off their computers, OfficeScan deployment to these computers will not be successful.

   Client package deployment

   Client package deployment seems to be the best option for remote site deployment. However, at Remote Site 2, there is no local server to facilitate this option properly. Looking at all options in-depth, this option provides the best coverage for most computers.

Head Office Deployment

The easiest client deployment method to implement at the head office is remote installation from the OfficeScan Web console. See *Installing from the OfficeScan Web Console* on page 4-13 for the procedure.

Remote Site 1 Deployment

Deployment to Remote Site 1 requires configuration of the Microsoft Distributed File System (DFS). For more information about DFS, refer to http://support.microsoft.com/?kbid=241452. After configuring DFS, Server 3 at Remote Site 1 needs to enable DFS, replicating the existing DFS environment or creating a new one.

A suitable deployment method is the creation of a client package in Microsoft Installer Package (MSI) format and the deployment of the client package to the DFS share. See *Installing with Client Packager* on page 4-6 for the procedure. Since the package will be replicated to Server 3 during the next scheduled update, client package deployment has minimal bandwidth impact.

You can also use a new Active Directory (AD) Policy. See *Deploying an MSI package using Active Directory* on page 4-9 for more information.

To minimize the impact of component updates across the WAN:

- Designate a client to act as an Update Agent for Remote Site 1. To do this, open the Web console and go to **Networked Computers > Client Management**. In the client tree, select the client that will act as the Update Agent and click **Settings > Update Agent Settings**.
- After designating an Update Agent, select the clients in Remote Site 1 that will update components from the Update Agent. To do this, go to **Updates > Networked Computers > Update Source**. Select **Customized Update Source** and click **Add**. In the screen that displays, enter the IP address range of the client computers in Remote Site 1, select the **Update source** button, and then select the designated Update Agent from the dropdown list.

Remote Site 2 Deployment

The key issue in Remote Site 2 is low bandwidth. However, 60 percent of the bandwidth is free during business hours. During business hours when there is 40 percent utilization, there is approximately 154 Kbits of available bandwidth available.

The best way to install the OfficeScan client is to use the same client package in MSI format used at Remote Site 1. However, since there is no available server, you cannot use a Distributed File System (DFS). You can configure a computer running Windows 2000 or XP as a DFS host but this is outside the scope of this document. You need to explore other options.

One option is to use third-party management tools that will allow administrators to configure or create shares on remote computers without having physical access to them. After creating this share on a single computer, copying the client package to the share requires less overhead than installing the client to nine computers.

You can use another Active Directory policy, but again, not specifying the DFS share as the source.

These methods keep the installation traffic local to the network, minimizing the traffic hit across the WAN.

To minimize the impact of component updates across the WAN, you can also designate a client to act as Update Agent. See the procedure in Remote Site 1 for more information.

Index

W