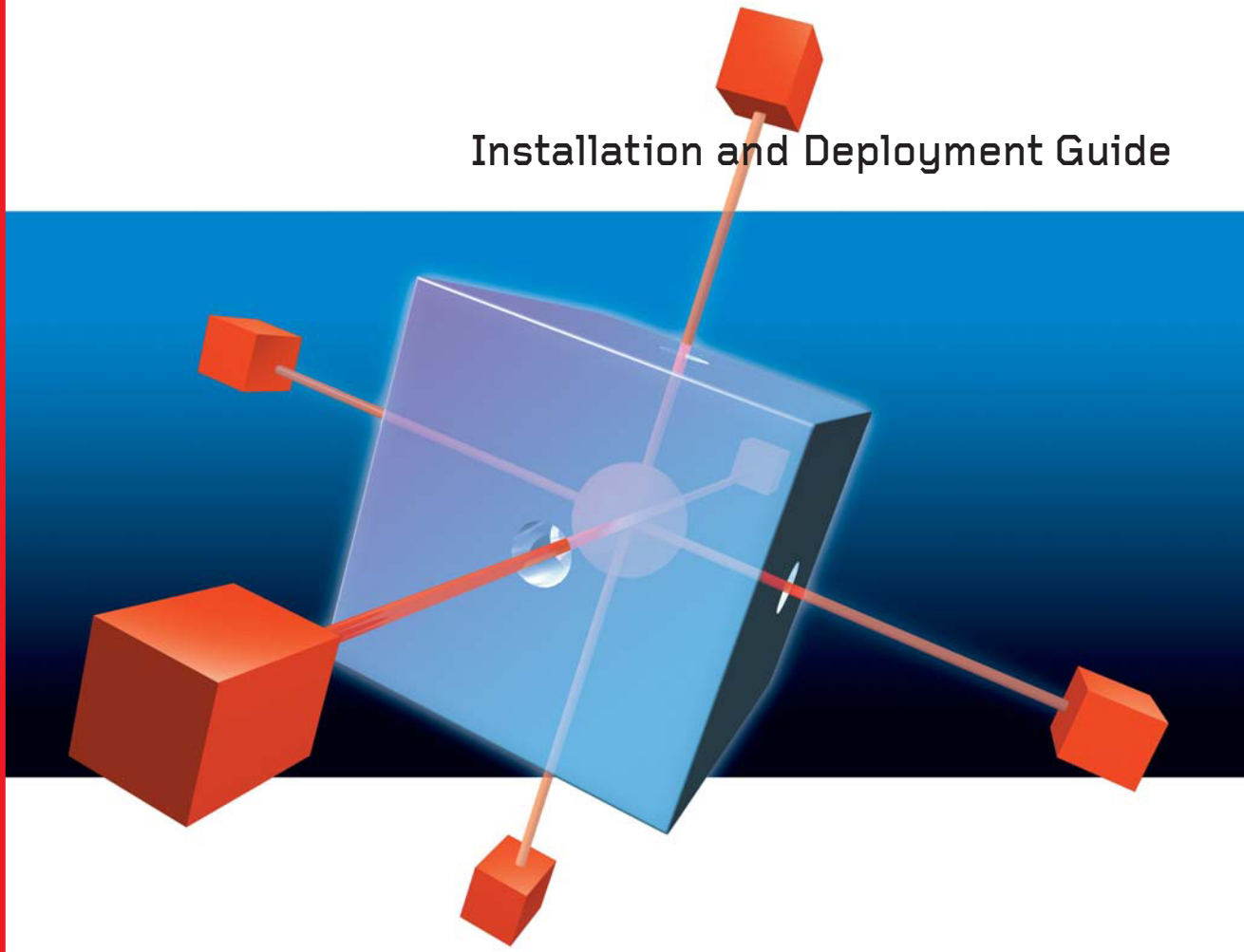
TREND MICRO™
OfficeScan™ 7

Comprehensive Security Protection for the Corporate Desktop

Installation and Deployment Guide



TREND MICRO™

Document Part No. OSEM72213/50217

Release Date: March, 2005

Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698; 6.119,165

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

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

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

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

Contents

Chapter 1

Introducing OfficeScan™

Trend Micro OfficeScan is a centrally managed antivirus and anti-spyware solution for desktops, notebook computers, and servers. OfficeScan helps protect your organization's Windows™ NT/2000/XP/Server 2003 and Windows 95/98/Me computers from a wide range of threats and potential nuisances, such as file viruses, macro viruses, malicious Java™ applets and ActiveX™ controls.

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

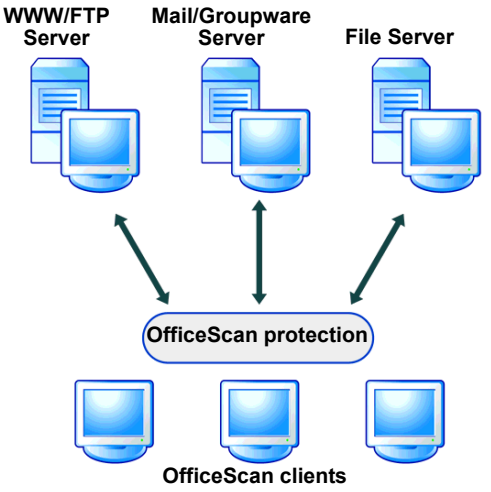


FIGURE 1-1 OfficeScan protection

OfficeScan includes the following:

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

What's New in OfficeScan 7.0

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

New Client-side Features

- **Protection against spyware and other types of grayware:** OfficeScan can help protect your computers from a variety of potential threats and nuisances that Trend Micro classifies as *grayware*, including the most notorious type– spyware (see *Understanding Spyware and Other Types of Grayware* on page 1-6 for more information). OfficeScan scans for and cleans spyware and other grayware just as it does viruses and Trojans. However, you may want to allow clients to keep certain applications that OfficeScan classifies as grayware. To prevent OfficeScan from continually labeling these applications as grayware, you can configure an grayware-specific exception list.
- **Windows server platform support for clients:** Install OfficeScan client on any Windows server operating system, such as Windows Server 2003. See *OfficeScan Client Requirements* on page 5-2 for details.
- **Incremental Update:** OfficeScan clients whose pattern files (including the spyware scan pattern, spyware cleanup pattern, and damage cleanup template) are within seven versions of the pattern files on the OfficeScan server, can update their files incrementally, instead of updating the entire files. This reduces the amount of time and the bandwidth required for OfficeScan clients to perform updates.
- **Client scheduled update enhancement:** Configure OfficeScan clients to perform component updates by schedule down to the minute. Also enable selected OfficeScan client users to modify scheduled update settings.
- **Adjustable file scanning:** To reduce the demand that file scanning puts on client CPU resources, manually adjust the wait time between the scanning of one file and the next.
- **Support for Windows server platforms on different processor architectures:** Run OfficeScan on Windows 2000, NT, and Server 2003 platforms. OfficeScan supports Windows XP/Server 2003 computers that use both x86 and Itanium 2 Architecture-64 (IA-64) processor architectures. See *32-bit and 64-bit Clients* on page 1-25 for more information.

- **Network virus log control/bandwidth reduction:** A single network virus can often cause a large number outbreaks in a short time. If OfficeScan detects multiple, recurring infections caused by the same network virus, it consolidates the network virus log entries made during detections and sends them to the OfficeScan server once an hour. This reduces the amount of network bandwidth required for log reporting and also reduces the number of virus detection notifications sent to your IT administrators.

New Server-side Features

- **Database backup integration:** Back up the OfficeScan database manually at any time or configure a schedule for automatic backup through the Web console. If there is ever an issue with the integrity of your OfficeScan database, you can recover your settings from the backup.
- **Multiple update sources:** Configure up to 10 update sources for both manual and scheduled updates.
- **ServerProtect Normal Server Migration Tool:** Use this Windows-based tool to help migrate computers running Trend Micro™ ServerProtect Normal Server to OfficeScan client.
- **Support for multi-server and remote server installation:** Install or upgrade OfficeScan server on several remote server machines at the same time.
- **Network virus log reporting to Control Manager:** Enable clients send their log for network viruses to the OfficeScan server, which will in turn send them to any registered Control Manager server. Use this information with Control Manager to create reports for network virus analysis.

OfficeScan Protection

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

Understanding Viruses

Tens of thousands of viruses exist, with more being created each day. In the past, most viruses were file-based and spread through the exchange of floppy disks. Today viruses commonly spread through the Internet, exploiting vulnerabilities in corporate networks, email systems and applications such as Web browsers.

Most computer viruses fall into the following categories:

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

Network Viruses

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the threats mentioned above, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of client

machines, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional disk-based file I/O scanning methods.

Enterprise Client Firewall works with a network virus pattern file to identify and block network viruses (see the *Administrator's Guide* and the OfficeScan server online help for more information on Enterprise Client Firewall).

Understanding Spyware and Other Types of Grayware

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

Types of Grayware

OfficeScan can detect several types of grayware, including the following:

- **Spyware:** gathers data, such as account user names, passwords, credit card numbers, and other confidential information, and transmits it to third parties
- **Adware:** displays advertisements and gathers data, such as Web surfing preferences that could be used for targeting future advertising at the user
- **Dialers:** change client Internet settings and can force a computer to dial pre-configured phone numbers through a modem. These are often pay-per-call or international numbers that can result it a significant expense for your organization.
- **Joke Programs:** cause a computer to behave abnormally, such as making the screen shake or modifying the appearance of the curser
- **Hacking Tools:** help malicious hackers enter a computer
- **Remote Access Tools:** help malicious hackers remotely access and control a computer
- **Password Cracking Applications:** help decipher account user names and passwords

- **Others:** other types of programs that are potentially malicious

How Spyware and Other Grayware Gets Into Your Network

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

Potential Risks and Threats

Spyware and other types of grayware on your network have the potential to introduce the following:

- **Reduced computer performance:** To perform their tasks, grayware applications often use significant CPU and system memory resources.
- **Increased Web browser-related crashes:** Certain types of grayware, such as adware, are often designed to create pop-up windows or display information in a browser frame or bar. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a system reboot.
- **Reduced user efficiency:** Grayware can unnecessarily distract users from their main tasks by forcing them to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs.
- **Degradation of network bandwidth:** Grayware often regularly transmits the data it collects to other applications running on your network or to locations outside of your network.
- **Loss of personal and corporate information:** Not all data that grayware applications collect is as simple as a list of Web sites users visited. Grayware can also collect user names and passwords that allow access to both personal user accounts, such as a bank account, and corporate accounts on your network.
- **Higher risk of legal liability:** If computer resources on your network are hijacked, hackers may be able to utilize your computers to launch attacks or install grayware on computers outside your network. The participation of your

network resources in these types of activities could leave your organization legally liable for damages incurred by third parties.

The Trend Micro Solution

This version of Trend Micro OfficeScan has the ability to scan for, detect, and remove a multitude of spyware and other grayware files and applications.

For instructions on configuring OfficeScan anti-spyware/grayware settings, see the *Administrator's Guide* and OfficeScan server online help.

Unknown Viruses, Grayware, and Other Potentially Malicious Code

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, contact your support provider or visit the Trend Micro Submission Wizard URL:

```
http://subwiz.trendmicro.com/SubWiz
```

Understanding OfficeScan Components

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

- **Client program:** the OfficeScan client program, which uses the virus pattern file and scan engine to identify infections and perform actions on infected files
- **Scan engine:** the engine OfficeScan uses to scan for viruses
- **Virus pattern file:** a file that helps OfficeScan identify virus signatures– unique patterns of bits and bytes that signal the presence of a virus (see *About the Virus Pattern File* on page 1-9 for more information)
- **Damage cleanup engine:** the engine Damage Cleanup Services uses to scan for and remove Trojans and Trojan processes
- **Damage cleanup template:** used by the damage cleanup engine, this template helps identify Trojan files and processes so the engine can eliminate them
- **Spyware/Grayware scan pattern:** a file that helps OfficeScan identify unique patterns of bits and bytes that signal the presence of a certain types of potentially undesirable files and programs, such as adware and spyware

- **Spyware/Grayware cleanup pattern:** a file the damage cleanup engine uses to help eliminate spyware/adware files and processes
- **Common firewall driver:** the driver the Enterprise Client Firewall uses with the network virus pattern file to scan client machines for network viruses
- **Network virus pattern file:** like the virus pattern file, this file helps OfficeScan identify virus signatures
- **Cisco Trust Agent (if Policy Server for Cisco NAC is installed):** the program that enables communication between the OfficeScan client and routers supporting Cisco NAC
- **Hot fixes and security patches:** workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the OfficeScan server and/or client program

About the Virus Pattern File

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

All Trend Micro antivirus programs using the ActiveUpdate function can detect the availability of a new virus pattern file on the Trend Micro server, and/or can be scheduled to automatically poll the server every week, day, or hour to get the latest file.

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

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

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

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique

"signature" or string of tell-tale characters that distinguish it from any other code, the virus experts at TrendLabs™ capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When a match is found, a virus has been detected and a notification is sent via an email message to the system administrator.

Pattern File Numbering

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

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

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

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

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

About the Trend Micro Scan Engine

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

- "in the wild"– actively circulating
- "in the zoo" – controlled viruses not in circulation, but are developed and used for research

Rather than scan every byte of every file, the engine and pattern file work together to identify not only tell-tale characteristics of the virus code, but the precise location within a file that the virus would hide. If OfficeScan detects a virus, it can remove it and restore the integrity of the file.

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

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

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

- Frequent updates to the virus pattern file, which can be downloaded and read by the engine without the need for any changes to the engine code itself (see *About the Virus Pattern File* on page 1-9)
- Technological upgrades in the engine software prompted by a change in the nature of virus threats, such as a rise in mixed threats like SQL Slammer

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

Updating the Scan Engine

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

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

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

`http://www.trendmicro.com`

About Hot Fixes, Patches, and Service Packs

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

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

- **Hot fix:** a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes don't (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).
- **Security Patch:** a hot fix focusing on security issues that is suitable for deployment to all customers. Windows security patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Patch:** a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Service Pack:** a consolidation of hot fixes, patches, and feature enhancements significant enough to be considered a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

You can obtain hot fixes from your Technical Account Manager. Check the Trend Micro Knowledge Base to search for released hot fixes:

`http://kb.trendmicro.com/solutions/search/main/search/default.asp`

You check the Trend Micro Web site regularly to download patches and service packs:

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

All releases include a readme file with the information you need to install, deploy, and configure your product. Read the readme file carefully before installing the hot fix, patch, or service pack file(s).

Note: By default, the OfficeScan clients are allowed to receive hot fix deployments. To forbid clients from receiving hot fix deployments, change Client Privileges (see *Modifying the Default Scan Settings* on page 4-2).

What you can do with OfficeScan

Perform key administrative tasks using the OfficeScan Web console:

- Analyze Your Network's Protection
- Enforce Antivirus and Anti-spyware Policies
- Update Your Protection
- Perform Scans From One Location
- Rid Client Computers of Spyware and Grayware
- Quarantine Infected Files
- Control Outbreaks on the Network
- Manage OfficeScan Domains and Clients
- Protect clients from hacker attacks with Enterprise Client Firewall
- Protect Your PDAs from Viruses
- Evaluate Client Antivirus Status and Take Action on At-Risk Clients

Analyze Your Network's Protection

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

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

Enforce Antivirus and Anti-spyware Policies

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

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

Update Your Protection

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

Perform Scans From One Location

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

Rid Client Computers of Spyware and Grayware

In addition to scanning for viruses, OfficeScan also scans for spyware and other types of grayware, such as adware and joke programs.

Quarantine Infected Files

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

Control Outbreaks on the Network

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

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

Manage OfficeScan Domains and Clients

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

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

Protect clients from hacker attacks with Enterprise Client Firewall

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

Protect Your PDAs from Viruses

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

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

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

For more information on OfficeScan for Wireless, see the *Administrator's Guide*. In Windows Explorer, you can also open the Quick Start Guide by double-clicking `Wireless Protection Manager Manual.pdf` in the `Trend Micro\Wireless Protection Manager` folder.

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

Evaluate Client Antivirus Status and Take Action on At-Risk Clients

The Trend Micro™ Policy Server for Cisco Network Admission Control (NAC) evaluates client antivirus status and determines what actions the clients should perform, such as updating components or enabling Real-time Scan, based on policies you configure. Policy Server allows you to integrate OfficeScan clients with a Cisco NAC server and Network Access Devices, such as Cisco routers.

Benefits and Capabilities

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

Single Console Operation

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

Trend Micro Damage Cleanup Services

OfficeScan uses Damage Cleanup Services (DCS) to protect your Windows computers against Trojans (or Trojan horse programs), and to help rid your clients of potentially unwanted spyware and other types of grayware.

Trojans

A Trojan is a malicious program that masquerades as a harmless application. Unlike viruses, Trojans do not replicate but can be just as destructive. An application that claims to rid your computer of viruses when it actually introduces viruses onto your computer is an example of a Trojan. Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those that are already running on the system.

Grayware

Grayware refers to several types of files and applications that can be covertly installed on computers to track user Web surfing habits, display advertisements, log

key strokes, change Internet settings, cause abnormal computer behavior and even compromise system security (see *Understanding Spyware and Other Types of Grayware* on page 1-6 for a explanation of different types grayware. See the *Administrator's Guide* and the OfficeScan server online help for instructions on configuring OfficeScan to protect your clients from grayware).

The Damage Cleanup Services solution

To address the threats and nuisances posed by Trojans and grayware, DCS does the following:

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

To accomplish these tasks, DCS makes use of these components:

- **Damage cleanup engine:** the engine Damage Cleanup Services uses to scan for and remove Trojans and Trojan processes
- **Damage cleanup template:** used by the damage cleanup engine, this template helps identify Trojan files and processes so the engine can eliminate them
- **Spyware/Grayware cleanup pattern:** a file the damage cleanup engine uses to help eliminate spyware/adware files and processes

In OfficeScan, DCS runs on the client on these occasions:

- Client users perform a manual cleanup from the OfficeScan client main console
- You perform Cleanup Now on the client from the OfficeScan server Web console
- Client users run Manual Scan, Scheduled Scan, or Scan now (and cleaning for spyware and grayware is selected on the **Global Client Settings** screen for those clients. See the *Administrator's Guide* and OfficeScan server online help for details.)
- After hot fix or patch deployment (see *About Hot Fixes, Patches, and Service Packs* on page 1-12 for more information)
- When the OfficeScan service is restarted (the OfficeScan client Watchdog service must be selected to restart the client automatically if the client program unexpectedly terminates. Enable this feature on the **Global Client Settings**

screen. See the *Administrator's Guide* and OfficeScan server online help for details.)

Because DCS runs automatically, you do not need to configure it. Users are not even aware when it is executed because it runs in the background (when the client is running). However, OfficeScan may sometimes notify the user to restart their computer to complete the process of removing a Trojan or grayware application.

Virus Outbreak Monitor

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

Outbreak Prevention

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

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

Trend Micro IntelliScan

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

Using IntelliScan provides the following benefits:

- Performance optimization – IntelliScan does not affect crucial applications on the client because it uses minimal system resources

- Shorter scanning period – Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

Trend Micro ActiveAction

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

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

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

Secure Web Console Communication

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

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

OfficeScan Server Architecture

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

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

OfficeScan Server

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

The server performs these important functions:

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

HTTP-based Server

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

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

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

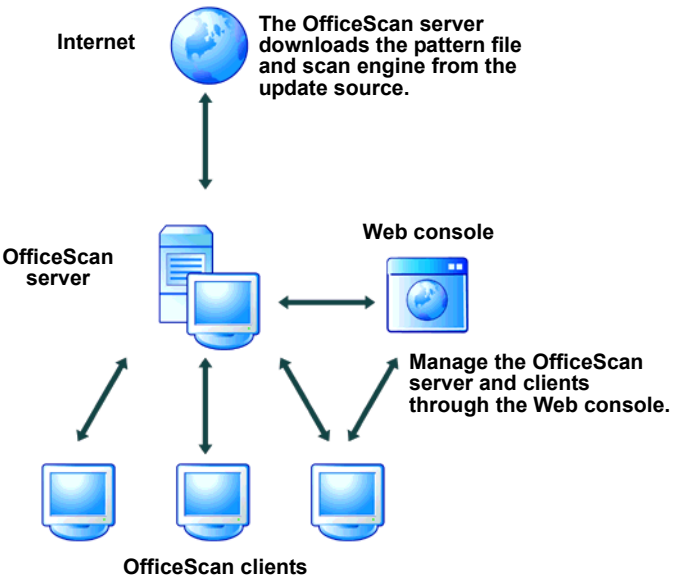


FIGURE 1-2 How the HTTP-based server works

OfficeScan Client

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

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

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

to remove the client program (see *Modifying the Default Client Privileges* on page 4-9 for more information).

There are two types of OfficeScan clients:

- Normal clients
- Roaming clients

Normal Clients

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

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

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

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

Roaming Clients

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

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

Roaming clients get updated only on these occasions:

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

For more information on how to update clients, see the *Administrator's Guide* and the OfficeScan server online help.

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

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

TABLE 1-2. Icons that appear on roaming clients

32-bit and 64-bit Clients

OfficeScan supports Windows XP/Server 2003 computers that use both x86 and Itanium 2 Architecture-64 (IA-64) processor architectures. The table below shows a comparison between OfficeScan features for both 32-bit and 64-bit client computers:

Feature	32-bit clients	64-bit clients
Manual, Real-time, and Scheduled Scan for viruses, spyware, and other types of grayware		
Roaming mode		
Damage Cleanup Services		N/A
Mailscan		N/A
Wireless Protection Manager		N/A
SecureClient Support		N/A

Web Console

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

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

- Deploy the client program to desktop and notebook computers
- Group desktop and notebook computers into logical domains for simultaneous configuration and management
- Set scan configurations and start Manual Scan on a single computer or on multiple computers

- Receive notifications and view log reports for virus activities
- Receive notifications when viruses are detected on clients and send virus outbreak alerts via email, pager, SNMP Trap, or Windows Event Log
- Control outbreaks by configuring and enabling Outbreak Prevention

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

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

Using the OfficeScan Documentation

The documentation set for OfficeScan includes the following:

- **Installation and Deployment Guide** – This guide helps you plan for and install the OfficeScan server program, modify important default client settings, and roll out your clients. The latest version of the *Installation and Deployment Guide* is available in electronic form at the following location:

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

- **Administrator's Guide** – This guide helps you configure OfficeScan options. The latest version of the *Administrator's Guide* is available in electronic form at the following location:

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

- **Online help** – The purpose of online help is to provide descriptions for performing the main tasks, usage advice, and field-specific information, such as valid parameter ranges and optimal values. Online help is accessible from the OfficeScan Web console.
- **Readme file** – The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and product release history.
- **Knowledge Base** – The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site:

  `http://kb.trendmicro.com`

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

`www.trendmicro.com/download/documentation/rating.asp`

Chapter 2

Preparing to Install OfficeScan

This chapter outlines the phases necessary for the successful installation and deployment of OfficeScan and provides instructions for the first phase: planning and testing. Read this chapter carefully before performing installation.

The information in this chapter includes:

Overview of Installation and Deployment

This section outlines the phases for OfficeScan installation and deployment. Each phase has corresponding sections that discuss in detail the tasks that you need to perform. This chapter contains instructions for completing the planning phase.

Phase 1: Initial Planning

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

Determining the Location of the OfficeScan Server on page 2-4

Determining the Number of Clients on page 2-4

Planning for Network Traffic on page 2-5

Planning the Placement of the Program Files on page 2-6

Determining the Number of Domains on page 2-6

Deciding How to Deploy the Client on page 2-7

Planning a Pilot Deployment on page 2-7

Phase 2: OfficeScan Server Installation

During this phase, start implementing the plan you created in Phase 1. Complete this phase by performing the following tasks:

Verifying Server System Requirements on page 3-2

Preparing for Server Installation on page 3-5

Installing or Upgrading OfficeScan Server on page 3-12

Verifying the Server Installation or Upgrade on page 3-24

Phase 3: Post-Installation Configuration

Before installing your clients, modify the default settings if necessary to ensure that the settings are in line with your antivirus and anti-spyware initiative:

Modifying the Default Scan Settings on page 4-2

Modifying the Default Global Client Settings on page 4-6

Modifying the Default Client Privileges on page 4-9

Phase 4: OfficeScan Client Installation

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

Verifying Client System Requirements on page 5-2

Choosing an Installation Method on page 5-4

Installing, Upgrading, or Migrating OfficeScan Client on page 5-6

Deploying the Latest Components on page 5-29

Verifying the Client Installation, Upgrade, or Migration on page 5-31

Testing the Client Installation with the EICAR Test Script on page 5-34

Completing Phase 1: Initial Planning

The steps in this phase help you develop a plan for OfficeScan installation and deployment. Trend Micro highly recommends creating an installation and deployment plan before performing installation. This will help ensure that you incorporate OfficeScan's capabilities into your existing antivirus and anti-spyware initiative.

Determining the Location of the OfficeScan Server

OfficeScan is flexible enough to 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.

Note: If a firewall is located between the server and its clients, you must configure the firewall to allow traffic between the client listening port and the server listening port (see *Understanding OfficeScan Ports* on page 3-9 for more information on the types of ports the client and server use to communicate)

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).

Determining the Number of Clients

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

If you have a heterogeneous client base (that is, if your network has different Windows operating systems, such as Windows NT/2000/XP/Server 2003 and 95/98/Me), identify how many clients are using a specific Windows version. Use this

information to decide which client deployment method will work best in your environment.

Note: A single OfficeScan server can manage up to **50,000** OfficeScan clients. If you have more then this amount, Trend Micro suggests installing more than one OfficeScan server.

Planning for Network Traffic

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

The server generates traffic when it does the following:

- Connects to the Trend Micro 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
- Performs scheduled update
- Switches between roaming mode and normal mode
- Performs Update Now

Network Traffic During Pattern File Updates

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

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

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

Deciding on a Dedicated Server

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

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

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

Planning the Placement of 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 that you use the default settings, unless you have a compelling reason (such as insufficient disk space) to change them.

The default client installation path is:

```
C:\Program Files\Trend Micro\OfficeScan Client
```

Determining the Number of Domains

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

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

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

Deciding How to Deploy the Client

OfficeScan provides several client deployment methods. Determine which ones are most suitable for your environment. For a complete list of available client deployment methods, see *Completing Phase 4: Installing OfficeScan Clients* on page 5-2.

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

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

Planning a Pilot Deployment

Before performing a full-scale deployment, Trend Micro recommends that you first conduct a pilot deployment in a controlled environment. A pilot deployment provides an opportunity to determine how features work and the level of support you will likely need after full deployment.

It also gives 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.

Tip: Although this phase is optional, Trend Micro highly recommends conducting a pilot deployment before doing a full-scale deployment.

Choosing a Pilot Site

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

Creating a Rollback Plan

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

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

Deploying Your Pilot

Evaluate the different deployment methods (see *Overview of Installation and Deployment* on page 2-2) to see which ones are suitable for your particular environment.

Evaluating Your Pilot Deployment

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

Chapter 3

Installing OfficeScan Server

This chapter explains the steps necessary for the next phase: OfficeScan server installation or upgrade. It also provides information on uninstalling the server program.

The information in this chapter includes:

Completing Phase 2: Installing the OfficeScan Server

The steps in this phase help you prepare for OfficeScan server installation and outline how to perform a fresh install or an upgrade.

Tip: You can preserve your client settings when you ugrade to this version of OfficeScan or if you need to reinstall this version of OfficeScan server. See *Upgrading from a Previous Version* on page 3-19 for instructions.

Verifying Server System Requirements

The computer(s) running the OfficeScan server program and any computer accessing the server Web console need to meet the minimum requirements listed in this section.

OfficeScan Server Requirements

To install OfficeScan server, the following are required:

Operating System Requirements

Microsoft™ Windows™ NT series (Service Pack 6a)

Windows 2000 Series (Service Pack 2 or above)

Windows XP (Professional Edition only, Service Pack 1)

Windows Server 2003

Hardware Requirements

300MHz Intel™ Pentium™ II processor or equivalent

128MB of RAM

300MB of disk space

Monitor that supports 800 x 600 resolution at 256 colors or higher

Microsoft Internet Explorer 5.5 or later

Web Server Requirements

- Microsoft Internet Information Server™ (IIS)

  on Windows NT: version 4.0

  on Windows 2000: version 5.0

  on Windows XP: version 5.1

  on Windows Server 2003: version 6.0
- Apache Web server 2.0 or later (for Windows 2000/XP[Service pack 1 or later]/Server 2003 only)

WARNING! *You have the option of installing Apache 2.0.52 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; otherwise the OfficeScan server may become compromised if a malicious hacker takes control of the Apache server.*
Before installing the Apache Web server, refer to the Apache Web site for the latest information on upgrades, patches, and security issues: ***www.apache.org***.

Other Requirements

- Administrator or Domain Administrator access on the server computer
- File and printer sharing for Microsoft Networks installed
- Transmission Control Protocol/Internet Protocol (TCP/IP) support installed

---

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

Web Console Requirements

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

Hardware Requirements

133MHz Intel Pentium processor or equivalent

64MB of RAM

30MB of free disk space

Monitor that supports 800 x 600 resolution at 256 colors or higher

Software Requirements

Microsoft Internet Explorer 5.5 or later

Considering Server Performance

Enterprise networks require servers with higher specifications than those required for small and medium-sized businesses. Ideally, the computer on which OfficeScan server is installed would have the following:

- dual processors
- over 1 GB of memory

Note: Both single and dual processor servers perform approximately the same; both can process up to 50,000 clients. However, a single processor server consumes 100% more CPU cycles than dual processor servers. Consider this when choosing your server computer.

Preparing for Server Installation

This section provides background information you will need to understand before performing installation.

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. The existence of other antivirus and anti-spyware applications on the same computer may hinder proper OfficeScan server installation and 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 5-23 for instructions and for a list of third party applications OfficeScan can remove).

Known Compatibility Issues

This sections explains compatibility issues that may arise if you install OfficeScan server on the same computer with certain other third-party applications. Always refer to the documentation of all third-party applications that are installed on the same computer on which you will install OfficeScan server.

Microsoft Small Business Server™

Before installing OfficeScan on a computer running Microsoft Small Business Server that is also running Microsoft Internet Security Acceleration server (ISA), record the server port in use by ISA. By default, both OfficeScan server and ISA use port 8080.

Therefore, chose another server listening port when installing OfficeScan server.

Domain Controllers

Domain controllers may conflict with proper OfficeScan server installation and performance. Uninstall any domain controllers on the computer you will install OfficeScan server.

Microsoft Exchange Server

During installation of the OfficeScan server, you will be prompted to install virus protection to the same computer on which you are installing OfficeScan server. If you choose to install virus protection, OfficeScan needs access to all files you want to scan. Since Microsoft Exchange Server queues messages in local directories, you must exclude these directories from the Real-time Scan. Not doing so may prevent the Exchange Server from properly processing email messages.

Exclude the directories in Table 3-1.

MS Exchange Version	Directories to be Excluded
Exchange 5.5	\Exchsvr\ImcData\In
	\Exchsvr\ImcData\Out
	\Exchsvr\MDBData
Exchange 2000	\Exchsvr\MdbData
	\Exchsvr\MtaData
	\Exchsvr\server_name.log
	\Exchsvr\Mailroot (may contain several subfolders)
	\Exchsvr\SrsData
	\%SystemRoot%\System32\Inetsrv
Exchange 2003	\Exchsvr\MdbData
	\Exchsvr\MtaData
	\Exchsvr\server_name.log
	\Exchsvr\Mailroot (may contain several subfolders)
	\Exchsvr\SrsData
	\Exchsvr\MdbDataUtility

TABLE 3-1 Microsoft Exchange directories to exclude from Real-time Scan

For Exchange 2000 and 2003, also exclude from Real-time Scan the Windows Installable File System (IFS) drive (**Drive M** by default). The IFS drive shares mailboxes and public stores with Windows applications such as Word, Internet Explorer and the command prompt.

Trend Micro™ ScanMail for Microsoft Exchange can properly protect your Exchange server from viruses and other potential threats. See the Trend Micro Web site (`www.trendmicro.com`) or your sales contact for details.

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 XP SP2 and Windows Server 2003 provides a built-in firewall named Internet Connection Firewall (ICF). Trend Micro highly recommends removing any third-party firewall applications if you want to install OfficeScan Enterprise Client 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 *Understanding OfficeScan Ports* on page 3-9 for information on listening ports and see your firewall documentation for details on how to configure exception lists).

Full version and Trial Version

You can install either a full version of OfficeScan or a free, trial version.

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

Note: Both versions require an different type of Activation Code to perform installation. If you do not have an Activation Code, register your version (see *The Registration Key and Activation Codes* on page 3-8).

The Registration Key and Activation Codes

Your version of OfficeScan comes with a Registration Key. During installation, OfficeScan prompts you to enter an different Activation Code for the OfficeScan program and for Damage Cleanup Services (optional).

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 can automatically redirect 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 Technical Support* on page 6-12).

Note: If you have questions about registration, please consult the Trend Micro Web site at the following address:
`http://kb.trendmicro.com/solutions/search/main/search/solutionDetail.asp?solutionID=16326`

Information to Prepare Before Installation

The master installer will prompt you for the following information during installation:

- **Proxy server details:** If a proxy server handles Internet traffic on your network, you must configure proxy server information (including the proxy server user name and password). This information is necessary to download the latest components, including the virus pattern file, scan engine and program from the Trend Micro update server. You can enter proxy server information either during installation or at a later time through the OfficeScan Web console.

- **Console password:** To prevent unauthorized access to the OfficeScan Web console, you can specify a password that will be required of anyone who tries to open the console.
- **Custom client alert messages:** When OfficeScan detects a virus on a computer during Real-time Scan or when it detects a firewall violation, an alert message appears on the client computer. You can customize this message either during installation or at a later time through the OfficeScan Web console.
- **Client software installation path:** Configure the client installation path where OfficeScan files will be copied to during client setup.
- **Trend Micro™ Control Manager server information:** If you plan to install Control Manager agent so your Control Manager server can manage the OfficeScan server, you will need the Control Manager host name or IP address and the encryption key.

Understanding OfficeScan Ports

OfficeScan utilizes two types of ports:

- **Server listening port (HTTP port):** used to access 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 sever virtual Web site: 8080

  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 in the OfficeScan server Web console after installation. You cannot modify the client listening port.

WARNING! *Many hacker and virus attacks are delivered over HTTP and are directed at ports 80 and/or 8080– commonly used in most organizations as the default Transmission Control Protocol (TCP) ports for HTTP communications.*

If your organization is currently using one of these ports as the HTTP port, Trend Micro recommends using another port number.

OfficeScan Server Prescan

Before the master installer begins the installation process it performs a prescan. This prescan includes a virus scan and Damage-Cleanup Services scan to help ensure the target computer does not contain viruses, Trojans, spyware, other grayware, or other potentially malicious code (see *Understanding Viruses* on page 1-5 and *Understanding Spyware and Other Types of Grayware* on page 1-6 for more information).

The prescan targets the most vulnerable areas of the computer, which include the following:

- the Boot area and boot directory (for boot viruses)
- the Windows folder
- the Program files folder

Actions for Prescan Detections

If the OfficeScan setup program detects viruses, Trojans, spyware, other grayware, or other potentially malicious code, you can take the following actions:

- **Clean** – cleans an infected file by removing the virus or grayware application. OfficeScan encrypts and renames the file if the file is uncleanable.
- **Rename** – encrypts the file and changes the file extension to .VIR, VIR1, VIR2... The file remains in the same location.
- **Delete** – deletes the file
- **Pass** – does nothing to the file

Tip: Trend Micro recommends cleaning or deleting infected files.

Other Installation Notes

Installing the OfficeScan server does not require you to restart the computer. After completing the installation, immediately configure the server, and then proceed to rolling out clients. If using an IIS Web server, the setup program automatically stops and restarts the IIS service during Web server installation.

WARNING! *Make sure that you do not install the Web server on a computer that is running applications that might lock IIS. This could prevent successful installation. See your IIS documentation for more information.*

If you do not install the firewall, Control Manager agent, or Policy Server for Cisco NAC during OfficeScan server installation, you can do so at a later time.

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

Installing or Upgrading OfficeScan Server

This section provides information on the following:

- Performing a fresh OfficeScan server install with the master installer (see *Performing a Fresh Install with the Master Installer* on page 3-12)
- Upgrading from a previous version of OfficeScan to the current version (see *Upgrading the OfficeScan Server* on page 3-19)
- Backing up program settings and restoring them if you reinstall OfficeScan or want to roll back to previous settings (see *Restoring Program Settings after Rollback or Reinstallation* on page 3-22)

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

Tip: You can preserve your client settings when you ugrade to this version of OfficeScan or if you need to reinstall this version of OfficeScan server. See *Upgrading from a Previous Version* on page 3-19 for instructions.

Performing a Fresh Install with the Master Installer

Follow the procedure below if this is the first time you are installing OfficeScan server on the target computer.

To install OfficeScan server:

1. Open the folder that contains the setup files and double-click **Setup** (`SETUP.EXE`). The **Welcome** screen appears.
2. Click **Next**. The **OfficeScan Software License Agreement** screen appears.
3. Read the agreement carefully, and then click **Yes** to agree to all the terms. The **Cisco NAC License Agreement** screen appears.
4. Read the agreement carefully, and then click **Yes** to agree to all the terms. If you do not agree at this time, you cannot deploy Cisco NAC Policy Servers. You can choose not to agree at this time and later agree to this license on the OfficeScan server Web console. The **Choose Destination** screen appears.

5. Choose where to install or upgrade to this version of OfficeScan by clicking one of the following:
   - **I will install/upgrade OfficeScan Server on this computer**
   - **I will install/upgrade OfficeScan Server on a remote computer or on multiple computers**

   If you selected to install on the computer you are currently using, the **Web Server** screen appears.

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

   a. Type the computer name or click **Browse** and select a computer on your network.

   b. Click **Add**. The computer name appears in the text box. Continue adding as many computers as necessary.

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

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

   c. Click **Next**.

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

---

6. Choose the Web server for the OfficeScan server:
   - **IIS server:** click **Install OfficeScan server on the IIS server** to install OfficeScan on an existing IIS installation
   - **Apache 2.0:** click **Install OfficeScan server on Apache Web server 2.0** to install Apache 2.0.52 on an existing installation. If an Apache Web server version 2.0 or later installation is not found, Apache 2.0.52 will be installed automatically.

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

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

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

     Tip: Clicking **IP address** is not recommended if the OfficeScan obtains an IP address from a DHCP server.

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

   - If you selected to install OfficeScan on an IIS server, select one of the following in the **IIS Website** section:
     - **IIS default Web site** – click to install as an IIS default Web site (in the IIS default Web site folder)
     - **IIS virtual Web site** – click to install as an IIS virtual Web site (in the IIS virtual Web site folder)
   - Under **Port number**, type a port to use as the server listening port. The OfficeScan server's address will be the following:

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

- You also have the option of enabling Secured Socket Layer (SSL) security. Select the **Enable SSL** check box. Type the number of years to keep the SSL certificate valid (the default is 3 years) and type an SSL port number. If you enable SSL, this port number will serve as the server's listening port. The OfficeScan server's address will be as follows:

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

  Tip: Trend Micro highly recommends enabling SSL to enhance security between the Web console and the server.

- To change the target directory location to install OfficeScan server, click **Browse** and select or create a new folder.

9. Click **Next**. A confirmation window appears. Verify that the port number is correct. OfficeScan uses the same TCP port number that your HTTP server is using. Setup automatically retrieves this port number and displays it on this screen.
   Make sure your HTTP port number and the port are the same. This will be the port number on the server through which the administrator connects to the Web console.
10. Click **Yes** to continue
    - If installing OfficeScan on the current computer (if you selected **I will install/upgrade OfficeScan Server on this computer** on the Choose Destination screen) the **Proxy Server** screen appears. Go to Step 11.
    - If performing a remote install or installing on multiple computers (if you selected **I will install/upgrade OfficeScan Server on a remote computer or on multiple computers** on the **Choose Destination** screen), the **Target Server Analysis** screen appears. Do the following:
      i. Click **Analysis**. The installer checks the computer to find out if it requires a new OfficeScan server program installation or an upgrade. You may need to type the administrator user name and password for that computer. If so, click **OK** after typing the information. The result appears under **Status** on the **Target Server Analysis** screen.

      Note: If the installer cannot determine this information for any computers you selected, **Failed** appears under **Status**, and the installer will not install

OfficeScan server on the selected computers. At least one computer must pass the analysis before the installation can continue.

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

iii. Click **Next**.

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

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

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

12. Create OfficeScan administrator passwords for access to the Web console and for clients to unload/uninstall the client program. Confirm the passwords in the text boxes. This helps prevent unauthorized users from accessing the Web console and modifying your settings or removing the clients.

13. Click **Next**. The **Components Selection** screen appears.

14. Select the check boxes next to the components to install or enable:

    - **Install client protection to target OfficeScan server:** install the OfficeScan client program on the same machine you are installing the OfficeScan server

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

    - **Install Control Manager agent:** install the Control Manager agent to allow Control Manager to manage the OfficeScan server (see the *Administrator's Guide* and the OfficeScan online help for more information)

- **Install Policy Server for Cisco NAC:** install Policy Server for Cisco NAC (see the *Administrator's Guide* and the OfficeScan online help for more information)
- **Enable Agent Deployment for Cisco NAC:** automatically deploy the Cisco Trust Agent when deploying OfficeScan clients. You can also deploy the Cisco Trust Agent at a later time through the Web console (see the *Administrator's Guide* and the OfficeScan online help for more information).

Note: Installation for Control Manager agent and Policy Server for Cisco NAC continues after OfficeScan server installation (see Step 35).

---

15. Click **Next**. The **World Virus Tracking Program** screen appears.
16. Read the statement and click **Yes** to enroll in the World Virus Tracking Program or click **No** to decline to participate.
17. Click **Next**. The **Server Settings Finished** screen appears.
18. Click **Next**. The **Product Activation** screen appears.
19. If you have the Activation Code for OfficeScan, click **Next**. The **Product Activation** screen appears.
    If you do not have the Activation Code, click **Register online**. Your Web browser opens to the Trend Micro registration Web site.
20. Type the Activation Codes for the following:
    - **Standard Antivirus:** to install OfficeScan
    - **Damage Cleanup Services:** to install Damage Cleanup Services (optional)
21. Click **Next**. The **Product Registration Settings Finished** screen appears.
22. Confirm that the correct items will be installed.

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

---

23. Click **Next**. The **Client Installation Path** screen appears.
24. Do the following to set an installation path:
    - Type an installation path

- Click **Enable network scan for mapped drives and shared folders** to have OfficeScan client include mapped drives and shared folders during scanning
- Modify the trusted port number so that it does not conflict with any other ports used in your internal network. This is a randomly generated port number through which the server will communicate with its clients.

25. Click **Next**. A confirmation screen appears.
26. Verify the port number and click **OK** to continue. The **Client Alert Message** screen appears.
27. Modify the default alert messages that appear on client machines if OfficeScan detects a virus, spyware or grayware application, a firewall violation, and/or a network virus.
28. Click **Next**. The **Client Security Level** screen appears.
29. Click one of the following:
    - **Normal:** assigns the access privileges already configured for the client Program Files and registry files to OfficeScan client files and OfficeScan client registries.
    - **High:** restricts access privileges to OfficeScan client files and OfficeScan client registries.

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

30. Select **Enable Spyware/Grayware Scan/Clean** to enable OfficeScan to scan for spyware and other types of grayware and attempt to clean grayware files.
31. Click **Next**. The **Client Settings Finished** screen appears.
32. Click **Next**. The **Select Program Folder** screen appears.
33. The Master Installer adds program icons to the folder listed under **Program Folder**. Modify it if necessary.
34. Click **Next**. The OfficeScan installation process commences. After installation completes, the **Shared Folder** screen appears.

If you selected **I will install/upgrade OfficeScan Server on a remote computer or on multiple computers** on the **Choose Destination** screen, a confirmation screen appears. Click **OK** to complete the installation.

35. Click **Next**. If you selected to install Control Manager agent or Policy Server for Cisco NAC, the installation commences (see the *Administrator's Guide* and the OfficeScan online help for more information).
36. Click **Next**. The **Setup Complete** screen appears.

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

Note: You can configure the OfficeScan settings using the Web console immediately after completing the installation and before deploying the clients. To start configuring basic OfficeScan settings, see *Completing Phase 3: Performing Post-Installation Configuration* on page 4-2.

Upgrading the OfficeScan Server

You can upgrade to a full version of OfficeScan from a previous version or from a trial version (see *Full version and Trial Version* on page 3-7 for more information on the differences between the full and trial versions).

Upgrading from a Previous Version

OfficeScan 7.0 supports upgrade from any of the following versions:

- **6.5**
- **5.58**
- **5.5 + NPF Service Pack**

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

Tip: You can preserve your client settings when you ugrade to this version of OfficeScan or if you need to reinstall this version of OfficeScan server.

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.

To upgrade to this version of OfficeScan:

- Run the master installer program on the target computer. Upgrading is very similar to performing a fresh install, but you will not be prompted to enter configuration information, such as port numbers or proxy server information. OfficeScan uses the same existing configuration information on the computer (see *Performing a Fresh Install with the Master Installer* on page 3-12 for instructions).

Upgrading from a Trial Version

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

To upgrade from a trial version:

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

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

Upgrading from OfficeScan 5.5x via Control Manager

This section explains how to simultaneously upgrade multiple OfficeScan 5.5x servers to the current version via the Trend Micro™ Control Manager management console. To perform the upgrade, you need to register your OfficeScan 5.5x servers to a Control Manager server (versions 2.5 or 3.0).

To upgrade from OfficeScan 5.5x via Control Manager:

1. Contact your support provider to obtain the `PatchAgent.dll` file.
2. Copy the all of the OfficeScan setup files and folders from your installation CD to a single folder on your computer (it does not have to be the Control Manager server computer).
3. Create a multi-line, comma-delimited text file with the following contents:

   ```
   Hostname, admin account name, password
   ```

   For example:

   ```
   officescanserver1, adminaccount1, password1
   officescanserver2, adminaccount2, password2
   officescanserver3, adminaccount3, password3
   ```

4. Save the file with the following name: `pass.csv`.
5. Create a response file on the environment on which the OfficeScan 5.5x server was installed:
   a. Open a command prompt and navigate to the folder you created in Step 2.
   b. Type **`setup -r`** and press the Enter key. Windows creates the response file `setup.iss`. in the `c:\winnt` or `c:\windows` directory.
6. Open the Control Manager management console and select **Products** > **Tasks**.
7. Select the OfficeScan server to which you want to deploy the package.
8. Under select a task, select **Deploy program files** from the drop down list.

WARNING! *Ensure that the OfficeScan server computer are up and running during upgrade. If the servers are shut down during deployment, the upgrade will be unsuccessful.*

---

9. This will deploy the setup package to all selected OfficeScan 5.5x servers registered with the Control Manager server.
10. To verify the upgrade, go to the Control Manager management console and select **Administration** > **Command Tracking**. Verify that the OfficeScan deployment was successful.
11. Log into the OfficeScan server Web console to verify the upgrade. The Web console address and password are the same as your previous installation.

Note: If the deployment was unsuccessful, obtain the debug log on the OfficeScan server at the following location: `installation drive:\OSCE 7005\pass.log` (this directory does not appear if the installation is successful).

Restoring Program 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 are experiencing 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 (see the *Administrator's Guide* or 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 verify connection log
   - **`Virus` folder** – the folder in which OfficeScan quarantines infected files
   - **`HTTDB` folder** – contains the OfficeScan database
3. Uninstall OfficeScan (see *Uninstalling the OfficeScan Server* on page 3-25).

4. Perform a fresh install (see *Performing a Fresh Install with the Master Installer* on page 3-12).
5. After the master installer finishes, stop the OfficeScan service on the target computer:
   a. Open **Windows Task Manager** (see your Windows documentation for details).
   b. Select the **Processes** tab.
   c. Stop the following process: `ofcservice.exe`.
6. With the backups you created, overwrite the OfficeScan server database and the relevant files and folders on the target machine in the `PCCSRV` folder.
7. Restart the OfficeScan service.

Verifying the Server Installation or Upgrade

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

To verify the installation, do the following:

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

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

  or if using SSL:

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

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

Uninstalling the OfficeScan Server

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

To remove the OfficeScan server:

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

   A confirmation screen appears.
2. Click **Yes**. Master Uninstaller, the server uninstallation program, prompts you for the administrator password.
3. Type the administrator password in the text box and click **OK**. Master Uninstaller then starts removing the server files. A confirmation message appears.
4. Click **OK** to close the uninstallation program.

Chapter 4

Performing Post-Installation Configuration

The OfficeScan server program installs with default client settings that affect how your OfficeScan clients scan for viruses, spyware, and other types of grayware. If the default settings do not conform to your antivirus and anti-spyware initiative, modify and save the settings in the Web console before deploying your clients.

The information in this chapter includes:

Completing Phase 3: Performing Post-Installation Configuration

The steps in this phase help you modify basic OfficeScan client default settings. For instructions on configuring the full range of OfficeScan server and client settings, see the *Administrator's Guide* and OfficeScan server online help.

Note: This section only provides basic instructions on modifying default settings. For more detailed explanation of OfficeScan features, see the *Administrator's Guide* and OfficeScan server online help.

Modifying the Default Scan Settings

OfficeScan provides the following types of scans to protect your clients from virus threats, spyware, and other types of grayware:

- **Manual Scan**: occurs after you executes the scan from the OfficeScan server Web console
- **Real-time Scan**: occurs when any file is opened or saved
- **Scheduled Scan**: occurs according to a configurable schedule
- **Scan Now:** occurs when the client user selects Scan Now on the client console

If you do not modify these scan options, your clients will scan files using the default settings, which provide an adequate level of protection for most environments.

The default scan settings are shown in Table 4-1.

Feature	Possible Options	Manual Scan	Real-time Scan	Scheduled Scan (not enabled by default)	Scan Now
Scan Target	All scannable files				
	Intelliscan (a method for automatically identifying certain types of flies to scan)	✔	✔	✔	✔
	Files with extensions you can specify				
	Compressed files (2 layers)	✔	✔	✔	✔
	Scan exclusion list	Enabled	Enabled	Enabled	Enabled
	RAM memory	✔	N/A	✔	✔
	Boot area	✔	✔	✔	✔
	Hidden folders		N/A	N/A	N/A
	Spyware/Grayware				
	Mapped drives			N/A	
	Incoming file	N/A		N/A	N/A
	Outgoing file	N/A		N/A	N/A
	Incoming and outgoing file	N/A	✔	N/A	N/A
	Floppy during system shutdown	N/A		N/A	N/A

Feature	Possible Options	Manual Scan	Real-time Scan	Scheduled Scan (not enabled by default)	Scan Now
Scan Action	Display an alert message on client when virus detected	N/A	✓	✓	N/A
	ActiveAction (a Trend Micro pre-configured set of actions)				
	Customized action based on the following types of potential threats:				
	Joke	Quarantine	Quarantine	Quarantine	Quarantine
	Trojan	Quarantine	Quarantine	Quarantine	Quarantine
	Virus	Clean and Quarantine	Clean and Quarantine	Clean and Quarantine	Clean and Quarantine
	Test Virus	Pass	Pass	Pass	Pass
	Spyware/Grayware	Quarantine	Quarantine	Quarantine	Quarantine
	Other	Clean and Quarantine	Clean and Quarantine	Clean and Quarantine	Clean and Quarantine
	Use the same action for all types	✓	✓	✓	✓
		Clean and Quarantine	Clean and Quarantine	Clean and Quarantine	Clean and Quarantine
CPU Usage	**High:** scan files one after another (without pausing between scans)	✓	N/A	✓	✓
	Medium: pause slightly between file scans		N/A		
	Low: increase pause between file scans		N/A		

TABLE 4-1. Default scan settings

To modify scan settings:

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

2. Click the root OfficeScan server domain.
3. On the sidebar, click **Scan Options**. The sidebar expands to reveal the available types of scans.
4. Click the type of scan settings you want to modify. The selected scan settings screen appears.
5. Modify the settings.
6. Click **Save**.

Modifying the Default Global Client Settings

OfficeScan provides several types of settings that apply to all clients registered to the server.

The default global client settings are show in Table 4-2.

Feature	Possible Options	Explanation	Default
Scan Settings	Configure scan settings for compressed files	Allows clients to skip scanning compressed files based on the size of each extracted file or number of files contained within the compressed file.	✔
	Clean compressed files	Performs the clean action on compressed files that are infected.	
	Scan a configurable amount of Object Linking and Embedding (OLE) layers	Scans OLE layers and specify how many layers to scan. OLE allows users to create objects with one application and then link or embed them in a second application.	✔
	Add Manual Scan to client Windows shortcut menu	Allows client users to scan files and folders by just right-clicking a file or folder on the Windows desktop or in Windows Explorer and clicking Scan with OfficeScan Client.	
	Enable Damage Cleanup Services to clean spyware and other grayware (running applications only)	Performs Damage Cleanup Services (DCS) cleanup on running spyware and other grayware applications and processes.	✔
	Enable and exclusion list for spyware and other grayware	Allows clients to exclude from scanning a list of applications and files that OfficeScan may consider spyware or other grayware.	
	Exclude the folder of OfficeScan server database from real-time scanning	Prevents OfficeScan from scanning its own database during Real-time Scans only.	✔

Feature	Possible Options	Explanation	Default
Alert Settings	Show the OfficeScan splash screen at startup	Displays the OfficeScan splash screen on the client computer during startup.	
	Show the alert icon on the Windows taskbar if the virus pattern file is not updated after { } days	Displays the alert icon on your clients when the pattern file is outdated.	
Scheduled Clean Settings	Enable Scheduled Clean	Activate automatic Damage Cleanup Services cleanup.	
Reserved Disk Space and Watchdog Settings	Enable OfficeScan client Watchdog service	Enables the watchdog service attempt to restart the client program if it unexpectedly shuts down.	
	Enable anti-hacking mode	Gives the Watchdog service a random name, which helps prevent any virus or other type of threat from identifying the service and terminating it.	
	Reserve a configurable amount of disk space for updates	Allows a certain amount of space on clients hard disks for hot fixes, pattern files, scan engines, and program updates (20MB by default).	
Connection Settings	Connect to the OfficeScan server using its fully qualified domain name (FQDN)	Allows Windows 95/98/Me clients to use the server's FQDN.	
Network Virus Log Consolidation		Instructs clients to send their network virus log to the OfficeScan server, which will in turn send them to any registered Control Manager server.	
Virus Log Bandwidth Settings		Instructs OfficeScan clients to consolidate virus log entries when detecting multiple infections from the same virus or grayware application over a short period of time.	

Feature	Possible Options	Explanation	Default
Grouping Rule	NetBios Domain	Group clients in the domain tree by NetBios name.	✔
	Active Directory Domain	Group clients in the domain tree by Active Directory name.	
	DNS Domain	Group clients in the domain tree by DNS name.	

TABLE 4-2. Default global client settings

To modify global settings:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the root OfficeScan server domain.
3. On the sidebar, click **Global Client Settings**. The **Global Client Settings** screen appears.
4. Modify the settings.
5. Click **Save**.

Modifying the Default Client Privileges

OfficeScan provides several types of privileges you can allow your clients to have.

The default client privileges are shown in Table 4-3.

Privilege	Possible Options	Explanation	Default
Antivirus	Manual Scan settings	Allows clients to modify these scan settings from their client console.	
	Real-time Scan settings		
	Scheduled Scan settings		
	Stop Scheduled Scan		
	Enable roaming mode	Allows clients to enable roaming mode.	
Enterprise Client Firewall	Display Enterprise Client Firewall tab	Allows clients to view the Enterprise Client Firewall tab on their client console and change the status of these firewall features.	
	Allow clients to enable or disable the Enterprise Client Firewall, the Intrusion Detection System, and the firewall alert message		
Mail Scan	Display the mail scan tab	Allows clients to view the mail scan tab on their client console and modify these mail scan settings.	
	Install/upgrade POP3 mail scan module		
	Real-time POP3 mail scan settings		
	Install/upgrade Outlook mail scan module		
	Run Outlook folder scan		

Privilege	Possible Options	Explanation	Default
Toolbox	Display toolbox tab	Allows client users to access the toolbox from their client console, install protection for wireless computers and support for SecureClient VPN connections.	☑
	Install/upgrade Wireless Protection Manager		☑
	Run Wireless Protection Manager		☑
	Install CheckPoint Secure Client support		☑
Proxy Setting		Allows clients to configure their own proxy settings.	☑
Update Privileges	Perform Update Now!	Allows clients to perform component updates on demand.	☑
	Enable Scheduled Update	Allows the client user to turn on/off the Scheduled Update option from the client console.	
Update Settings	Download from the Trend Micro ActiveUpdate server	Allows clients to receive updates directly from Trend Micro's ActiveUpdate server.	
	Enable Scheduled Update	Allows client users to perform Scheduled Update.	
	Forbid program upgrade and hot fix deployment	Forbids clients from performing upgrades and receiving hot fixes.	
	Act as an Update Agent	Allows the client to deploy components to other clients.	
Uninstallation	Allow the client user to uninstall OfficeScan	Allows users to unload (or turn off) the client without requiring a password.	
	Require a password for the client user to uninstall OfficeScan client	Allows only users with the unload password to be able to turn off the client.	☑
Unloading	Allow the client user to unload OfficeScan	Allows users to unload (or turn off) the client without requiring a password.	
	Require a password for the client user to unload OfficeScan client	Allows only users with the unload password to be able to turn off the client.	☑

Privilege	Possible Options	Explanation	Default
Client Security	High	Restricts clients from accessing OfficeScan client folders, files, and registries.	
	Normal	Allows clients read/write access to the OfficeScan client folders, files, and registries on client computers.	✓

TABLE 4-3. Default client privileges

To modify client privileges:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the root OfficeScan server domain.
3. On the sidebar, click **Client Privileges/Settings**. The **Client Privileges and Settings** screen appears.
4. Modify the settings.
5. Click **Save**.

Chapter 5

Installing OfficeScan Client

This chapter explains the steps necessary for successful OfficeScan client installation and upgrade. It also provides information on uninstalling the client program.

The information in this chapter includes:

Completing Phase 4: Installing OfficeScan Clients

The steps in this phase help you prepare for OfficeScan client installation and outline the various methods for a fresh install or an upgrade.

Verifying Client System Requirements

The computers running the OfficeScan client program need to meet the minimum requirements listed in this section.

OfficeScan Client Requirements

To install OfficeScan client, the following are required:

Windows 95/98/Me client

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

- 133MHz Intel™ Pentium™ processor or equivalent
- Microsoft Windows 95/98/98 SE/Me
- 64MB of RAM (20 MB free)
- 80MB of disk space
- Monitor that supports 640 x 480 resolution at 256 colors or higher
- Microsoft Internet Explorer 4.01 or later
- Microsoft Internet Explorer 5.0 or later if need to perform Web setup
- Gigabit Network Interface Card (NIC)- supported

Windows NT/2000 client

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

- 150MHz Intel Pentium processor or equivalent
- Microsoft Windows NT 4.0 Workstation/Server with SP6a or above, Windows 2000 Server/Advanced Server/Professional with SP2 or above

- 64MB of RAM (20 MB free)
- 80MB of disk space
- Monitor that supports 640 x 480 resolution at 256 colors or higher
- Microsoft Internet Explorer 4.01 or later
- Microsoft Internet Explorer 5.0 or later if need to perform Web setup
- Gigabit Network Interface Card (NIC)- supported

Windows XP/Server 2003

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

- 300MHz Intel Pentium processor or equivalent
- 128MB of RAM (20 MB free)
- 80MB of disk space
- Monitor that supports 800 x 600 resolution at 256 colors
- Microsoft Internet Explorer 6.0 or later if need to perform Web setup
- Gigabit Network Interface Card (NIC)- supported

Note: You must disable **Simple File Sharing** on Windows XP clients before they can successfully install the OfficeScan client program (see your Windows documentation for instructions).

Choosing an Installation Method

OfficeScan provides several methods to install the client. This section provides a summary of the different methods available to help you decide which is most suitable for your network environment.

- **Internal Web page** – instruct the users in your organization to go to the internal Web page and download the client setup files (see *Installing from the Internal Web Page* on page 5-6)
- **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 5-7)
- **Client Packager** – deploy the client setup or update files to client via email (see *Installing with Client Packager* on page 5-10)
- **MSI Package** – use Client Packager to create a Windows Installer MSI file to deploy the client setup or update files to client via email. This is especially useful if you are already using Windows Active Directory (see *Installing with an MSI file* on page 5-14).
- **Windows Remote Install** – install the client program on all Windows NT/2000/XP/Server 2003 clients from your Web console (*Installing with Windows Remote Install* on page 5-15)
- **From a client disk image** – create an image of an OfficeScan client, make clones of it, and deploy to other computers on your network (*Installing from a Client Disk Image* on page 5-16)
- **Trend Micro™ Vulnerability Scanner (TMVS)** – install the client program on all Windows NT/2000/XP(Professional)/Server 2003 clients with the Trend Micro Vulnerability Scanner (*Installing with Vulnerability Scanner* on page 5-17)
- **Microsoft System Management Server (SMS)** – use Microsoft System Management Server (SMS) to distribute the client program (see *Installing the client using Microsoft SMS* on page 5-17)

Table 5-1 summarizes each client deployment method.

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

TABLE 5-1 OfficeScan client deployment methods

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

Installing, Upgrading, or Migrating OfficeScan Client

This section provides information on the following:

- Performing a fresh OfficeScan server install with your chosen installation method (see *Performing a Fresh Install* on page 5-6)
- Upgrading from a previous version of OfficeScan to the current version (see *Upgrading the OfficeScan Client* on page 5-21)
- Migrating from a third-party antivirus installation to the current version of OfficeScan (see *Migrating from Third-party Antivirus Applications* on page 5-23)
- Migrating from a Trend Micro ServerProtect™ Normal Server installation to the current version of OfficeScan (see *Migrating from ServerProtect Normal Servers* on page 5-25)

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

Performing a Fresh Install

Follow the procedure below if this is the first time you are installing OfficeScan server on the target computer.

Installing from the Internal Web Page

If you installed OfficeScan server to a computer running Windows NT, Windows 2000, Windows XP, or Windows Server 2003 with Internet Information Server (IIS) 4.0 or later or Apache 2.0.52 (only on Windows 2000/XP/Server 2003 machines), your client users can install the client program from the internal Web server created during master setup.

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

Tip: You can use Vulnerability Scanner to see which clients have not followed the instructions to install from the Web console (see *Using Vulnerability Scanner to Verify the Client Installation* on page 5-31 for more information).

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

To install from the internal Web page:

1. Open an Internet Explorer window and type one of the following:
   - **OfficeScan server with SSL:**

     `https://{OfficeScan_server_name}:{port}/officescan/console/clientinstall`
   - **OfficeScan server without SSL:**

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

   Alternatively, click the **Click here** link under **Install OfficeScan Client** on the main page of the OfficeScan server Web console.
2. Click **Install Now** to start installing the OfficeScan client.

   The client installation starts. Once installation is completed, the screen displays the message, "Client installation is complete".
3. Verify the installation by checking if the OfficeScan client icon appears in the Windows system tray.

Installing with Login Script Setup

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

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

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

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

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

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

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

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

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

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

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

4. Click **Apply** when all the target users are in the **Selected users** list.

   A message appears informing you that you have modified the server login scripts successfully.

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

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

Installing with Windows NT/2000/Server 2003 scripts

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

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

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

where:

`{Server_name}` is the computer name or IP address of the computer where the OfficeScan server is installed

`ofcscan` is the OfficeScan directory on the server

`installation_path` is the directory where you installed the server files (by default, the `PCCSRV` folder)

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

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

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

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

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

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

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

Installing with Client Packager

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

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

Note: Client packager requires a minimum of 140MB free disk space on the client. Windows Installer 2.0 is necessary for the client to run an MSI package.

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

- **Executable** – this common file type has an `.exe` extension
- **Microsoft Installer Package Format (MSI)** – this file type conforms to Microsoft's Windows Installer package specifications. For more information on MSI, see the Microsoft Web site.

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

Note: Install **Microsoft Outlook** to use the Client Packager send mail option.

To create a package with the Client Packager GUI:

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

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

4. In **Target operating system**, select the operating system for which you want to create the package.
5. Select the type of package you want to create:
   - **Setup:** select if installing the OfficeScan client program
   - **Update:** select if updating OfficeScan client components only
6. Select from among the following installation options under **Options**:
   - **Silent Mode** – creates a package that installs on the client machine in the background, unnoticeable to the client without showing an installation status window
   - **MSI Package** – creates a package that conforms to the Microsoft Windows Installer Package Format

---

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

   - **Disable Prescan (only for fresh-install)** – disables the normal file scanning that OfficeScan performs before starting setup
   - **Force overwrite with latest version:** overwrites old versions with the latest version (this check box is enabled only when you select **Update** for **Package type**). This option appears only when creating a package for Windows NT/2000/XP/Server 2003, including for Windows NT/2000/XP/Server 2003 clients with IA-64 processor architecture.
   - **Update Agent:** gives the client the ability to act as an Update Agent

---

Tip: If you install the OfficeScan client program using Client Packager and the **Update Agent** option is enabled, 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.

Tip: Trend Micro recommends installing only on client machines that are 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 be able to modify the Update Agent settings mentioned above, use another client program installation method other then Client Packager.

Note: If you install the OfficeScan client program using Client Packager and the **Update Agent** option is enabled, you must use the Scheduled Update Configuration Tool to enable and configure scheduled updates (see *The Scheduled Update Configuration Tool* on page 5-14).

7. Under **Components**, select the components to include in the installation package:
   - **Program** – all components (if you select **Program**, Client Packager automatically selects the other components)
   - **Scan engine** – the latest scan engine on the OfficeScan server
   - **Virus pattern/Spyware/Grayware pattern** – the latest virus pattern file and Spyware/Grayware scan and cleanup file on the OfficeScan server
     - **Spyware/Grayware scan pattern** – a file that helps OfficeScan identify grayware files and programs, such as adware and spyware
   - **Common Firewall Driver** – the driver for Enterprise Client Firewall
   - **Network Virus Pattern** – the latest pattern file specifically for network viruses
   - **DCE/DCT** – the latest damage cleanup engine and template on the OfficeScan server
   - **Spyware/Grayware cleanup** – used by the damage cleanup engine, this template helps identify spyware/adware files and processes so the damage cleanup engine can eliminate them
8. Select the OfficeScan client utilities to include in the package:
   - **POP3 Mail Scan** – performs a virus scan on the client's Post Office Protocol 3 (POP3) mail messages and attachments as they are downloaded from the mail server
   - **Outlook Mail Scan** – performs a virus scan on the client's Microsoft Outlook folders
   - **Wireless Protection** – an antivirus module to protect your Personal Digital Assistants (PDA). This is not available with Silent Mode or MSI packages.

- **Check Point SecureClient** – support for Check Point SecureClient for Windows NT/2000/XP/Server 2003

9. Ensure that the location of the `ofcscan.ini` file is correct next to **Source file**. To modify the path, click ... to browse for the ofcscan.ini file. By default, this file is located in the \PCCSRV folder of the OfficeScan server.
10. In **Output file**, click ... to specify the file name (for example, `ClientSetup.exe`) and the location to create the client package.
11. Click **Create** to build the client package. When Client Packager finishes creating the package, the message "Package created successfully." appears. To verify successful package creation, check the output directory you specified.
12. Send the package to your users via email, or copy it to a CD or similar media and distribute among your users.

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

Sending the Package via Email

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

To send the package from the console:

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

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 the **Enable Scheduled Update** check box.
5. Click one of the following:
   - **Hours, every { } hour(s):** click to perform scheduled update every hour and select a number of hours from the list
   - **Daily:** click to perform scheduled update every day and select the start time from the list boxes. Also select a number of hours which represent a time period during which OfficeScan will perform the update. OfficeScan performs the update at a random time during this time period, which begins after the start time you specify.
   - **Weekly:** click to perform scheduled update once a week. You must select a day from the list, a start time, and a period of time during which OfficeScan will perform the update.
6. Click **Apply**.

Installing with an MSI file

If you are using Active Directory, you can install OfficeScan client by creating a Microsoft Windows Installer file. Use Client Packager to create a file with an `.msi` extension. You can take advantage of Active Directory features by automatically deploying the OfficeScan client program to all your clients simultaneously with the MSI file, rather than requiring each client to separately install OfficeScan client themselves.

For more information on MSI, see the Microsoft Web site (`www.microsoft.com`). For instructions on creating an MSI file, see *Installing with Client Packager* on page 5-10).

Installing with Windows Remote Install

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

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

To install with Windows Remote Install:

1. From the OfficeScan Web console sidebar, click **Clients** > **Remote Install** on the OfficeScan server sidebar.

   The **Remote Install** screen appears. The domains and computers list displays all the Windows domains on your network.
2. From the list of computers, select a client, and then click **Add >>**. OfficeScan prompts you for a user name and password to the target computer. You need administrator rights to the target computer.
3. Type your user name and password, and then click **Login**. The target computer appears in the selected computers list.
4. Repeat these steps until the list displays all the Windows computers to install OfficeScan client.
5. Click **Install** to install the client to your target computers. A confirmation box appears.
6. Click **Yes** to confirm that you want to install the client to the target computers. A progress screen appears as OfficeScan copies the program files to each target computer.

When OfficeScan completes the installation to a target computer, the installation status will appear in the **Result** field of the selected computers list, and the computer name appears with a green check mark.

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

Installing from a Client Disk Image

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

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

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

To create a disk image of an OfficeScan client:

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

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

Installing with Vulnerability Scanner

Use Vulnerability Scanner to detect installed antivirus solutions, search for unprotected computers on your network, and install OfficeScan client on 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 machines running Windows 2000 or Server 2003; however, the machines cannot be running Terminal Server.

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

To install OfficeScan client with Vulnerability Scanner:

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

Installing the client using Microsoft SMS

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

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

1. Create the setup package

2. Distribute or "advertise" the package to the target computers

---

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

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

- **Local drive:** the SMS server and the OfficeScan server are on the same machine
- **Remote location:** the SMS server and the OfficeScan server are on different machines

To create the setup package on the local drive:

1. Open the SMS Administrator console.
2. On the **Tree** tab, click **Packages**.
3. On the **Action** menu, click **New** > **Package From Definition**. The **Welcome** screen of the **Create Package From Definition Wizard** appears.
4. Click **Next**. The **Package Definition** screen appears.
5. Click **Browse**. The **Open** screen appears.
6. Browse for the package description file (PDF) on the server. The location of the PDF depends on the operating system of the target clients. The PDF for the Windows NT/2000/XP/Server 2003 client is in `\PCCSRV\PCCNT\Disk1\setup.pdf`. The PDF for the Windows 95/98/Me client is in `\PCCSRV\PCC95\Disk1\setup.pdf`.
7. Select the PDF for the target clients, and then click **OK**.

   The package name for the PDF you have selected appears on the **Package Definition screen**. If you selected the PDF for the Windows NT/2000/XP/Server 2003 Server client, it will show "OfficeScan Client NT/2K/XP/Server 2003 setup 7.0". If you selected the PDF for the Windows 95/98/Me client, it will show "OfficeScan Client 95/98/Me setup 7.0".
8. Click **Next**. The **Source Files** screen appears.
9. Click **Always obtain files from a source directory**, and then click **Next**.

   The **Source Directory** screen appears, displaying the name of the package you are creating and the source directory.
10. Click **Local drive on site server**.

11. Click **Browse** and select the source directory where the PDF file is located.
12. Click **Next**. The wizard creates the package. When it completes the process, the name of the package appears on the SMS Administrator console.

To create a setup package on a remote location:

1. On the OfficeScan server, use Client Packager to create a setup package with an `.exe` extension. (the `.msi` package is not supported). See *Installing with Client Packager* on page 5-10.
2. On the computer where you want to store the source, create a shared folder.
3. Browse for the package description file (PDF).

   The location of the PDF depends on the operating system of your target clients. The PDF for the Windows NT/2000/XP/Server 2003 client is in `\PCCSRV\PCCNT\Disk1\setup.pdf`. The PDF for the Windows 95/98/ME client is in `\PCCSRV\PCC95\Disk1\setup.pdf`.
4. Copy the installation package you created with Client Packager and the `setup.pdf` file to the shared folder.
5. Open the `setup.pdf` file with a text editor, and change the `IS-CmdLine` and `CommandLine` parameters to the package name (for example: `IS-CmdLine=package_name.exe`).
6. Open the SMS Administrator console.
7. On the **Tree** tab, click **Packages**.
8. On the **Action** menu, click **New** > **Package From Definition**. The **Welcome** screen of the **Create Package From Definition Wizard** appears.
9. Click **Next**. The **Package Definition** screen appears.
10. Click **Browse**. The **Open** screen appears.
11. Browse for the package description file (PDF), which is located in the shared folder you created.
12. Click **Next**. The **Source Files** screen appears.
13. Click **Always obtain files from a source directory**, and then click **Next**. The **Source Directory** screen appears.
14. Click **Network path (UNC name)**.
15. Click **Browse** and select the source directory where the PDF file is located (the shared folder you created).

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

To distribute the package to target computers:

1. On the **Tree** tab, click **Advertisements**.
2. On the **Action** menu, click **All Tasks** > **Distribute Software**. The **Welcome** screen of the Distribute Software Wizard appears.
3. Click **Next**. The **Package** screen appears.
4. Click **Distribute an existing package**, and then click the name of the setup package you created.
5. Click **Next**. The **Distribution Points** screen appears.
6. Select a distribution point to which you want to copy the package, and then click **Next**. The **Advertise a Program** screen appears.
7. Click **Yes** to advertise the client setup package, and then click **Next**. The **Advertisement Target** screen appears.
8. Click **Browse** to select the target computers. The **Browse Collection** screen appears.
9. Click the collection to which you want to distribute the setup package.
   - If you created a client setup package for Windows NT/2000/XP/Server 2003, click **All Windows NT Systems**.
   - If you created a client setup package for Windows 98, click **All Windows 98 Systems**.

Note: You can distribute the setup package to Windows 98 computers, not Windows 95 and Me computers. To distribute the client setup package to Windows Me computers, you must create a new collection. For instructions on how to create a new collection, refer to the Microsoft SMS documentation.

---

10. Click **OK**. The **Advertisement Target** screen appears again.
11. Click **Next**. The **Advertisement Name** screen appears.
12. In the text boxes, type a name and comments for the advertisement, and then click **Next**. The **Advertise to Subcollections** screen appears.

13. Choose whether to advertise the package to subcollections. You can choose to **Advertise the program only to members of the specified collection** or **Advertise the program to members of subcollections as well**.
14. Click **Next**. The **Advertisement Schedule** screen appears.
15. Specify when to advertise the client setup package by typing or selecting the date and time in the list boxes.

    If you want Microsoft SMS to stop advertising the package on a specific date, click **Yes**. **This advertisement should expire**, and then specify the date and time in the **Expiration date and time** list boxes.
16. Click **Next**. The **Assign Program** screen appears.
17. Click **Yes, assign the program**, and then click **Next**.

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

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

Known Issues when Installing with Microsoft SMS:

- "Unknown" appears in the Run Time and Disk Space columns of the SMS console.
- If the installation is unsuccessful, the installation status may still show that the installation is complete on the SMS program monitor. For instructions on how to verify if the installation was successful, see *Using Vulnerability Scanner to Verify the Client Installation* on page 5-31.

Upgrading the OfficeScan Client

You can upgrade to a full version of OfficeScan from a previous version or from a trial version. When you upgrade the OfficeScan server, clients can be automatically upgraded when you perform client installation with any of the installation methods available (see *Choosing an Installation Method* on page 5-4 for information on installation methods).

Note: For upgrade to take place automatically, event triggered deployment must be enabled. Confirm this on the **Updates** > **Client Deployment** > **Automatic Deployment** screen.

You can also use the Client Mover I 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 I to move an OfficeScan 5.58 client registered with an OfficeScan 5.58 server to the current version of the server, the client will be upgraded automatically. For more information on the Client Mover I tool, see the *Administrator's Guide* and the OfficeScan server online help.

Automatic Client Migration

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

Refer to Table 5-2 for a list of third-party client applications that OfficeScan can automatically remove.

Note: OfficeScan only removes the following client installations, not server installations.

Trend Micro
PC-cillin™ (Internet Security) 2005, 2004, 2003, 2002, 2000, 98, 6, NT, 97 2.0, 97 3.0, 95 1.0, 95 1.0 Lite
ServerProtect™ for Windows NT
Virus Buster™ 2001, 2000, 2000 for NT ver.1.00, 2000 for NT ver.1.20, 98 for NT, 98, NT, VirusBuster™ 95 1.0, Lite 1.0, Lite 2.0, 97, 97 Lite
Symantec™
Norton™ Internet Security™ 2004
Norton Antivirus™ 2004 Pro, 2004, 2003, 2002, 2001, 2000, CE 8.1, CE 8.0, CE 7.61, CE 7.6, CE 7.51, CE 7.5, CE 7.0, CE 6.524, 5.32, 5.31, 5.0, 4.0, 2.0 NT, Symantec Antivirus CE 9.0

McAfee™
VirusScan™ Enterprise 8.0, 7.1, 7.0, VirusScan ASaP, 95 {3.20,4.01,4.02, 4.03(#4023),4.03a (#4059)}, NT 4.03a (#4019), 5.15, 5.16, 5.21, 6.01, 4.5, 4.51, Thin Client (TC)
NetShield™ NT 4.03a (build #4014, #4019), 4.5 (Build #4062)
Internet Security Suite™ 6.0
ePOAgent™1000, 2000, 3000
Dr.Solomon™ 4.0.3 95 (Build #4023,#4066), 4.0.3 NT (Build #4019), 7.77 NT, 7.95 NT
LANDesk™
VirusProtect™ 5.0
Computer Associates™
eTrust AntiVirus™ 7.1
InocuLAN™ NT 4.5, 9.x, 4.53
eTrust InoculateIT™ 7.0, 6.0
InocuLAN™ 5
Cheyenne AntiVirus™ 9x, NT
Ahnlab™
V3 Pro™ 2000 Deluxe, 98, 98 Deluxe
Panda Software™
Platinum™ 7.0
Antivirus 6.0, 5.0, Local Networks, Windows NT WS
F-Sercure™
Anti-Virus™ 4.04, 4.08, 4.2, 4.3, 5.3
Backweb™
Management Agent™
Kaspersky™
Antivirus Personal 4.0, Workstation 3.5, 5.4

Sophos™
Anti-Virus 3.37,3.47, 3.51~3.61.
Hauri™
ViRobot 2k Professional™
Authentium™
Command AntiVirus™ 2.80.5, 4.64 for win 9x/ME, 4.8 Standalone, 4.9 Enterprise
Tegam™
ViGUARD™ 9.25e for Windows NT
Grisoft™
ViGUARD™ 9.25e for Windows NT
Aladdin™
eSafe™ 3.0, 3.1, eSafe Desktop™ 3.0
PER Antivirus™
Antivirus
Others
The Hacker Anti-Virus 5.5

TABLE 5-2 Removable third-party client applications

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 of the OfficeScan server. Run the tool on Windows NT/2000/XP/Server 2003 machines.

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

Installing the Server Protect Normal Server Migration Tool

- Copy the files `SPNSXfr.exe` and `SPNSX.ini` to the `PCCSRV\Admin` folder on the OfficeScan server.

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

To perform the migration using 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. Under **OfficeScan server**, select the OfficeScan server on which you are running the tool. 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 timeout.

4. To include computers running Windows Server 2003 in the search, select the **Include Windows Server 2003** check box.
5. Select the **Restart Windows Server 2003 computers** check box 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 don't 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. Under **Server list**, 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 a user name and password are required to log on the target computers, 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 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. Very the installation on the client machine from the OfficeScan Web console.

Migration will be unsuccessful 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 is stopped

Deploying the Latest Components

To ensure your clients have the most up-to-date protection from viruses and spyware, update the server with the latest OfficeScan components and deploy them to the clients.

Note: This section shows you how to perform Manual Update and Manual Deployment. For information on other update and deployment methods, see the *Administrator's Guide* and the OfficeScan server online help.

To update the OfficeScan server:

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

To deploy the components to the clients:

1. Open the OfficeScan Web console.
2. Click **Updates** > **Client Deployment** > **Manual Deployment** on the sidebar. The **Manual Deployment** screen appears showing a summary of components, versions, and the last time OfficeScan updated them.
3. Under **Update Target**, choose to update either specified clients or all clients whose components are out of date:
   - To update all online clients, including roaming clients with functional connections to the server, click **Select clients with out-of-date components** and select the **Include roaming client(s)** check box.

- To update specific clients, click **Manually select clients**. Then click the **Select** button to choose specific clients. The **Manual Deployment** screen shows the client tree. Click the clients you want to update or click the root icon to update all clients.

4. After selecting all clients to update, click **Notify**. The server starts notifying each client to download the updates.

Verifying the Client Installation, Upgrade, or Migration

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

To verify the installation, do the following:

- Look for the OfficeScan program shortcuts on the Windows **Start** menu of the OfficeScan client
- Check if OfficeScan is in the **Add/Remove Programs** list of the OfficeScan client's Control Panel
- Use 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 machines running Windows 2000 and Server 2003; however, the machines cannot be running Terminal Server.

To verify client installation using Vulnerability Scanner:

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

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

5. To automatically send the results to yourself or to other administrators in your organization, select the **Email results to the system administrator** check box under **Alert Settings**. Then, click **Configure** to specify your email settings.
   - In **To**, type the email address of the recipient
   - In **From**, type your email address. If you are sending it to other administrators in your organization, this will let the recipients know who sent the message
   - In **SMTP server**, type the address of your SMTP server. For example, type `smtp.company.com`. The SMTP server information is required
   - In **Subject**, type a new subject for the message or accept the default subject
6. Click **OK** to save your settings.
7. To display an alert on unprotected computers, click the **Display alert on unprotected computers** check box. Then, click **Customize** to set the alert message. The **Alert Message** screen appears.
8. Type a new alert message in the text box or accept the default message, and then click **OK**.
9. To save the results as a comma-separated value (CSV) data file, select the **Automatically save the results to a CSV file** check box. By default, 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**.
10. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout fields**.
11. Click **OK**. The Vulnerability Scanner console appears.
12. To run a manual vulnerability scan on a range of IP addresses, do the following:

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

---

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

13. 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 **DHCP Start** button appears.
    b. Click **DHCP 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.

Testing the Client Installation with the EICAR Test Script

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

`http://www.eicar.org`

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

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

To test the client installation with the EICAR test script:

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

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

To test the client installation HTTP scanning capability:

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

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

  `http://www.eicar.org/anti_virus_test_file.htm`

OfficeScan should show that it detected the EICAR test file.

Removing the Client

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

- Remove the client from the OfficeScan Web console, also known as Uninstall Now (see page 5-35)
- Remove the client using its uninstallation program (see page 5-36)

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).

Removing the Client from the OfficeScan Web Console

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

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

To remove the client using Uninstall Now

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

To stop notifications

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

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

Removing the Client Using its Uninstallation Program

If you granted users the privilege to remove the client program, instruct them to run the client uninstallation program from their computers. For more information, see 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 uninstall password.
2. Type the uninstall password, and then click **OK**. The **OfficeScan Client Uninstallation** screen shows the progress of the uninstallation.

When uninstallation is complete, the message "Uninstallation is complete" appears. You may need to restart the client computer to complete the uninstallation.

Chapter 6

FAQs, Troubleshooting and Technical Support

This chapter provides answers to commonly asked questions about installation and deployment, describes how to troubleshoot problems that may arise with OfficeScan, and provides information you'll need to contact Trend Micro technical support.

In this chapter, you will learn about the following:

Frequently Asked Questions (FAQs)

The following is a list of frequently asked questions and answers.

Registration

I have several questions on registering OfficeScan. 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
```

Installation, Upgrade, and Compatibility

Which OfficeScan versions can upgrade to the current version?

This version of OfficeScan supports upgrade from any of the following versions: **6.5, 5.58, 5.5 + NPF Service Pack**.

Which client installation method is best for my network environment?

See *Choosing an Installation Method* on page 5-4 for a summary and brief comparison of the various client installation methods available.

Can OfficeScan server be installed remotely using Citrix or Windows Terminal Services?

No. The OfficeScan server cannot be installed remotely with Citrix or Windows Terminal Services. The only approved remote install methods is the following:

- The master installer (select **I will install/upgrade OfficeScan Server on a remote computer or on multiple computers**)

Can OfficeScan work in an 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 OfficeScan server online help for more information.

Does OfficeScan support 64-bit platforms?

Yes. A scaled down version of OfficeScan client is available for 64-bit platforms (see *32-bit and 64-bit Clients* on page 1-25 for details).

What should I do if I'm locking down my Web server with a lockdown tool, such as the MicroSoft IIS Lockdown Tool?

If you're using the Microsoft IIS Lockdown Tool™, the lockdown of OfficeScan configuration (`.ini`) and executable (`.exe`) files may be causing the problem. See your Microsoft documentation for ways to configure the lockdown tool to allow these files to be accessed and execute.

Can I upgrade to OfficeScan from Trend Micro™ ServerProtect?

Yes. See *Migrating from ServerProtect Normal Servers* on page 5-25.

Configuring Settings

I have several questions on configuring OfficeScan settings. Where can I find the answers?

Refer to the *Administrator's Guide*. You can download all OfficeScan documentation from the following site:

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

Documentation

What documentation is available with this version of OfficeScan?

This version of OfficeScan includes the following: *Installation and Deployment Guide*, *Administrator's Guide*, readme file, and help files for the OfficeScan server Web console (you are currently viewing), client, Master Installer, Policy Server Web console, and Policy Server installer.

Can I download the OfficeScan documentation?

Yes. You can download the Installation and Deployment Guide, Administrator's Guide, and readme file from the following site:

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

I have questions/issues with the documentation. How can I provide feedback to Trend Micro?

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents,

please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Troubleshooting

This section helps you troubleshoot issues that may arise during installation, upgrade, migration, and deployment.

OfficeScan Client will not Install on Windows XP Computers

You must disable **Simple File Sharing** on Windows XP clients before they can successfully install the OfficeScan client program (see your Windows documentation for instructions).

Some OfficeScan Components are not Installed

Licenses to various components of Trend Micro products may differ by region. You may not have received a license for the Enterprise Client Firewall, for protection, and/or Damage Cleanup Services. After installation, you will see a summary of the components your Registration Key/Activation Code allows you to use. Check with your vendor or reseller to verify the components for which you have licenses.

Unable to Access the Web Console

There are several potential causes of this problem.

Browser Cache

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

SSL Certificate

Also verify that your Web server is functioning properly. If you are using SSL, verify that the SSL certificate is still valid. See your Web server documentation for details.

Web Server Lockdown

If you're using the Microsoft IIS Lockdown Tool™, the lockdown of OfficeScan configuration (`.ini`) and executable (`.exe`) files may be causing the problem. See your Microsoft documentation for ways to configure the lockdown tool to allow these files to be accessed and execute.

Virtual Directory Settings

There may be a problem with the virtual directory settings If you are running the OfficeScan server Web console on an IIS server and the following message appears:

The page cannot be displayed
HTTP Error 403.1 - Forbidden: Execute access is denied.
Internet Information Services (IIS)

This message may appear when either of the following addresses is used to access the console:

```
http://<server name>/officescan/
```

```
http://<server name>/officescan/default.htm
```

However, the console may open without any problems when using the following address:

```
http://<server name>/officescan/console/cgi/cgichkmasterpwd.exe
```

To resolve this issue, check the execute permissions of the OSCE virtual directory.

Do the following:

1. Open the Internet Information Services (IIS) manager.
2. In the OSCE virtual directory, select **Properties**.
3. Select the **Virtual Directory** tab and change the execute permissions to **Scripts** instead of none.

Also change the execute permissions of the client install virtual directory.

Incorrect Number of Clients on the Web Console

You may see that the number of clients reflected on the Web console is incorrect.

This happens if you retain client records in the database after client program removal. For example, if client-server communication is lost while removing the client, the server does not receive notification about the client removal. The server retains client information in the database and still shows the client icon on the console. When you reinstall the client, the server creates a new record in the database and displays a new icon on the console.

Use the Verify Connection feature through the OfficeScan server Web console to check for duplicate client records. See the *Administrator's Guide* and OfficeScan server online help for more information.

Unsuccessful Installation from Web page or Remote Install

If users report that they cannot install from the internal Web page or if installation with Remote Install is unsuccessful, try the following:

- Verify that client -server communication exists by using ping and telnet
- Verify that you have administrator privileges to the target computer where you want to install the client
- Check if TCP/IP on the client is enabled and properly configured
- Check if the target computer meets the minimum system requirements
- Check if any file has been locked
- If you have limited bandwidth, check if it causes connection timeout between the server and the client
- If you are using a proxy server for client-server communication, check if the proxy settings are configured correctly
- Open a Web browser on the client, type `http://{Server name}:{server port} /officeScan/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client.

Client Icon Does Not Appear on Web Console After Installation

You may discover that the client icon does not appear on the console after you install the client. This happens when the client is unable to send its status to the server.

To resolve this, do the following:

- Verify that client-server communication exists by using ping and telnet
- If you have limited bandwidth, check if it causes connection timeout between the server and the client
- Check if the \PCCSRV folder on the server has shared privileges and if all users have been granted full control privileges
- Verify that the OfficeScan server proxy settings are correct
- Open a Web browser on the client, type `http://{OfficeScan_Server_Name}:{port number}/officeScan/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client.
- If you moved the client to a new OfficeScan server with the Client Mover I tool, you may need to restart the OfficeScan master service (`ofservice.exe`) on the new server.

Note: If this does not help you find the real cause of the issue, use ActiveSupport to collect `Ofcdebug.log` from the client, then contact Trend Micro technical support. See the OfficeScan client help for information on running Active Support.

Issues During Migration from Third-party Antivirus Software

This section discusses some issues you may encounter when migrating from third-party antivirus software.

Client Migration

The setup program for the OfficeScan client utilizes the third-party software's uninstallation program to automatically remove it from your users' system and replace it with the OfficeScan client. If automatic uninstallation is unsuccessful, users get the following message:

```
Uninstallation failed.
```

There are several possible causes for this error:

- The third-party software's version number or product key is inconsistent
- The third-party software's uninstallation program is not working
- Certain files for the third-party software are either missing or corrupted
- The registry key for the third-party software cannot be cleaned
- The third-party software has no uninstallation program

There are also several possible solutions for this error:

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

To manually remove the third-party software:

- If the third-party software is registered to the Add/Remove Programs
  - **a.** Open the Control Panel.
  - **b.** Double-click **Add/Remove Programs**.
  - **c.** Select the third-party software from the list of installed programs.
  - **d.** Click **Remove**.
- If the third-party software is not registered to the Add/Remove Programs
  - **a.** Open the Windows registry.
  - **b.** Go to `HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Uninstall`.
  - **c.** Locate the third-party software and run the uninstall string value.
  - **d.** If the third-party software's setup program is in MSI format:
    - Locate the product number
    - Verify the product number
    - Run the uninstall string

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

To modify the service for the third-party software

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

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

---

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

---

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

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

Contacting Trend Micro

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

`http://www.trendmicro.com/en/about/contact/overview.htm`

Note: The information on this Web site is subject to change without notice.

The Trend Micro Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

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

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of threats expected to trigger in the current week, and describes the 10 most prevalent threats around the globe for the current week
- View a Virus Map of the top 10 threats around the globe
- Consult the Virus Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
  - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other threats
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security threat terminology
- Download comprehensive industry white papers

- Subscribe to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Web masters
- Read about TrendLabs[SM], Trend Micro's global antivirus research and support center

Known Issues

Known issues are features in OfficeScan software that may temporarily require a work around. Known issues are typically documented in the Readme document you received with your product. Readme's for Trend Micro products can also be found in the Trend Micro Update Center:

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

Known issues can be found in the technical support Knowledge Base:

`http://kb.trendmicro.com/solutions/`

Trend Micro recommends that you always check the Readme text for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

Contacting Technical Support

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

You can contact Trend Micro via fax, phone, and email, or visit us at:

`http://www.trendmicro.com`

Speeding Up Your Support Call

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

- Microsoft Windows and Service Pack versions

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

The Trend Micro Knowledge Base

Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in Knowledge Base are product FAQs, important tips, preventive antivirus advice, and regional contact information for support and sales.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

`http://kb.trendmicro.com/solutions/`

If you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

Sending Suspicious Files to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, contact your support provider or visit the Trend Micro Submission Wizard URL:

`http://subwiz.trendmicro.com/SubWiz`

Click the link under the type of submission you want to make.

Note: Submissions made via the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you submit your case, an acknowledgement screen displays. This screen also displays a case number. Make note of the case number for tracking purposes.

If you prefer to communicate by email message, send a query to the following address:

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAV, or 877-873-6328

About TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

Index

Numerics

A

B

C

T

U

V

W