TREND MICRO

OfficeScan™ Client/Server Edition 8

for Enterprise and Medium Business

for Windows™ Vista™

Installation and Deployment Guide

Endpoint Security

Document Part No. OSEM83231/70524

Release Date: May 2007

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

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

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

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

Please evaluate this documentation on the following site:

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

Contents

Chapter 1

Planning Client Installation

Topics in this chapter:

Installation Requirements

The following are the requirements for installing the OfficeScan client on computers running Windows Vista:

Operating system

- Microsoft Windows™ Vista™ Business 32-bit Edition
- Microsoft Windows Vista Enterprise 32-bit Edition
- Microsoft Windows Vista Ultimate 32-bit Edition
- Microsoft Windows Vista Business 64-bit Edition
- Microsoft Windows Vista Enterprise 64-bit Edition
- Microsoft Windows Vista Ultimate 64-bit Edition

Hardware

- 800MHz Intel Pentium processor or equivalent; AMD x64 or Extended Memory 64 Technology (EM64T) processor architectures also supported
- 1GB of RAM
- 200MB of available disk space
- Monitor that supports 800 x 600 resolution at 256 colors

Others

Microsoft Internet Explorer 7.0 or later if performing Web setup

Update Agent Requirements

- 800MHz Intel Pentium processor or equivalent
- 700MB available disk space
- 1GB of RAM

Unsupported Features

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

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

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

- Infection source notification (The Alerter Service is removed)

Installation Methods

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

Web install page

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

Client Packager

Create and send the client Setup or update files to client users (see *Installing with Client Packager* on page 2-3). If creating an MSI package using Client Packager, you can deploy the package using Active Directory™ or Microsoft SMS.

For details, see the following topics:

- *Deploying an MSI package using Active Directory* on page 2-7
- *Deploying an MSI package using Microsoft SMS* on page 2-8

Remote installation

From the Web console, install the client program on computers running supported platforms (see *Installing from the OfficeScan Web Console* on page 2-11).

Trend Micro Vulnerability Scanner (TMVS)

Install the client program on unprotected computers by running the Trend Micro™ Vulnerability Scanner (*Installing with Vulnerability Scanner* on page 2-13).

Summary

TABLE 1-1. OfficeScan client installation methods

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

Chapter 2

Installing the OfficeScan Client

Installation scenarios:

Recommended post-installation tasks:

Other task:

Performing Fresh Installation

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

Installing from the Web Install Page

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

Tip: You can use Vulnerability Scanner to determine the users that did not follow the instructions to install from the Web install page (see *Using Vulnerability Scanner to verify the client installation* on page 2-16 for more information).

Requirements:

- At least Microsoft Internet Explorer 7.0 with the security level set to allow ActiveX™ controls
- Built-in administrator privileges on the computer

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

To install from the Web install page:

Pre-installation

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

4. Under **ActiveX controls and plug-ins**, enable **Automatic prompting for ActiveX controls**.

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

Installation

1. Open an Internet Explorer window and type one of the following:
   - OfficeScan server with SSL:
     https://{OfficeScan_server_name}:{port}/officescan
   - OfficeScan server without SSL:
     http://{OfficeScan_server_name}:{port}/officescan
2. Click the link under **For Networked Computers**.
3. In the new screen that displays, click **Install Now** to start installing the OfficeScan client. The client installation starts.

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

Installing with Client Packager

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

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

Self-extracting files created by Client Packager

- **Executable:** This common file type has an .exe extension.
- **Microsoft Installer (MSI) Package Format:** This file type conforms to Microsoft's Windows Installer package specifications. You can send the MSI package through conventional media or use Active Directory and Microsoft SMS. See *Deploying an MSI package using Active Directory* on page 2-7 and *Deploying an MSI package using Microsoft SMS* on page 2-8 for details. For more information on MSI, see the Microsoft Web site.

Client computer requirements

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

To create a package using Client Packager:

1. On the OfficeScan server computer, browse to \PCCSRV\Admin\Utility\ClientPackager.
2. Double-click ClnPack.exe to run the tool. The Client Packager console opens.
3. Select the type of package you want to create:
   - **Setup:** Select if installing the OfficeScan client program. This will create an executable file.
   - **Update:** Select if updating OfficeScan client components only. This will also create an executable file.
   - **MSI Package:** Select if creating a package that conforms to the Microsoft Installer Package format
4. If creating an executable file, select the operating system for which you want to create the package.
5. Select from among the following installation options:
   - **Silent Mode:** Creates a package that installs on the client computer in the background, unnoticeable to the client and without showing an installation status window

- **Update Agent:** Gives the client the ability to act as an update agent (Update Agents are alternative servers that help the OfficeScan server deploy components to clients.). If you install the OfficeScan client program using Client Packager and you enable the **Update Agent** option, you must use the Scheduled Update Configuration Tool to enable and configure scheduled updates (see *Using the Scheduled Update Configuration Tool* on page 2-6).

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

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

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

6. Select the components to include in the installation package.
7. Next to **Source file**, ensure that the location of the ofcscan.ini file is correct. To modify the path, click  to browse for the ofcscan.ini file. By default, this file is in the \PCCSRV folder of the OfficeScan server.
8. In **Output file**, click  to specify the location where you want to create the client package and the file name (for example, ClientSetup.exe).
9. Click **Create**. When Client Packager finishes creating the package, the message "Package created successfully" appears. To verify successful package creation, check the output directory you specified.

10. Deploy the package.

- Send the package to your users and ask them to run the client package on their computers by right-clicking the .exe file and select **Run as administrator**.

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

- If you created an .msi file, you can use Active Directory or Microsoft SMS. See *Deploying an MSI package using Active Directory* on page 2-7 or *Deploying an MSI package using Microsoft SMS* on page 2-8.

Using the Scheduled Update Configuration Tool

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

To use the Scheduled Update Configuration Tool:

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

Deploying an MSI package using Active Directory

You can take advantage of Active Directory features to deploy the MSI package simultaneously to multiple client computers. For instructions on creating an MSI file, see *Installing with Client Packager* on page 2-3.

To deploy an MSI package using Active Directory:

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

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

---

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

Deploying an MSI package using Microsoft SMS

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

For instructions on creating an MSI file, see *Installing with Client Packager* on page 2-3.

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

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

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

To obtain the package locally:

1. Open the SMS Administrator console.
2. On the **Tree** tab, click **Packages**.
3. On the **Action** menu, click **New** > **Package From Definition**. The Welcome screen of the Create Package From Definition Wizard appears.
4. Click **Next**. The Package Definition screen appears.
5. Click **Browse**. The Open screen appears.
6. Browse and select the MSI package file created by Client Packager, and then click **Open**. The MSI package name appears on the Package Definition screen. The package shows "Trend Micro OfficeScan Client" and the program version.
7. Click **Next**. The Source Files screen appears.
8. Click **Always obtain files from a source directory**, and then click **Next**.

   The Source Directory screen appears, displaying the name of the package you want to create and the source directory.
9. Click **Local drive on site server**.

10. Click **Browse** and select the source directory containing the MSI file.
11. Click **Next**. The wizard creates the package. When it completes the process, the name of the package appears on the SMS Administrator console.

To obtain the package remotely:

1. On the OfficeScan server, use Client Packager to create a Setup package with an .exe extension (you cannot create an .msi package). See *Installing with Client Packager* on page 2-3 for details.
2. On the computer where you want to store the source, create a shared folder.
3. Open the SMS Administrator console.
4. On the **Tree** tab, click **Packages**.
5. On the **Action** menu, click **New** > **Package From Definition**. The Welcome screen of the Create Package From Definition Wizard appears.
6. Click **Next**. The Package Definition screen appears.
7. Click **Browse**. The Open screen appears.
8. Browse for the MSI package file. The file is on the shared folder you created.
9. Click **Next**. The Source Files screen appears.
10. Click **Always obtain files from a source directory**, and then click **Next**. The Source Directory screen appears.
11. Click **Network path (UNC name)**.
12. Click **Browse** and select the source directory containing the MSI file (the shared folder you created).
13. Click **Next**. The wizard creates the package. When it completes the process, the name of the package appears on the SMS Administrator console.

To distribute the package to target computers:

1. On the **Tree** tab, click **Advertisements**.
2. On the **Action** menu, click **All Tasks** > **Distribute Software**. The Welcome screen of the Distribute Software Wizard appears.

3. Click **Next**. The Package screen appears.
4. Click **Distribute an existing package**, and then click the name of the Setup package you created.
5. Click **Next**. The Distribution Points screen appears.
6. Select a distribution point to which you want to copy the package, and then click **Next**. The Advertise a Program screen appears.
7. Click **Yes** to advertise the client Setup package, and then click **Next**. The Advertisement Target screen appears.
8. Click **Browse** to select the target computers. The Browse Collection screen appears.
9. Click **All Windows NT Systems**.
10. Click **OK**. The Advertisement Target screen appears again.
11. Click **Next**. The Advertisement Name screen appears.
12. In the text boxes, type a name and your comments for the advertisement, and then click **Next**. The Advertise to Subcollections screen appears.
13. Choose whether to advertise the package to subcollections. You can choose to advertise the program only to members of the specified collection or to members of subcollections.
14. Click **Next**. The Advertisement Schedule screen appears.
15. Specify when to advertise the client Setup package by typing or selecting the date and time.

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

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

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

Known Issues when Installing with Microsoft SMS

- "Unknown" appears in the Run Time column of the SMS console.
- If the installation is unsuccessful, the installation status may still show that the installation is complete on the SMS program monitor. For instructions on how to verify if the installation was successful, see *Using Vulnerability Scanner to verify the client installation* on page 2-16.

Installing from the OfficeScan Web Console

You can remotely install the OfficeScan client to one or several Vista computers connected to the network. Ensure you have built-in administrator rights to the target computers to perform remote installation. Remote installation will not install the OfficeScan client on a computer already running the OfficeScan server.

To install from the OfficeScan Web console:

Pre-installation:

1. On the Windows Vista computer, enable a built-in administrator account and set the password for the account.
2. Disable the Windows firewall.
   a. Click **Start > Programs > Administrative Tools > Windows Firewall with Advanced Security**.
   b. For Domain Profile, Private Profile, and Public Profile, set the firewall state to "Off".
3. Open the Windows Services screen (click **Start > Run** and type **services.msc**) and start the **Remote Registry** service.

Installation:

1. In the Web console, click **Networked Computers > Client Installation > Remote**.
2. Select the target computers.
   - The **Domains and Computers** list displays all the Windows domains on your network. To display computers under a domain, double-click the domain name. Select a computer, and then click **Add**.
   - If you have a specific computer name in mind, type the computer name in the field on top of the page and click **Search**.

   OfficeScan will prompt you for the target computer's user name and password. Make sure to use an administrator account user name and password to continue.
3. Type your user name and password, and then click **Log in**. The target computer appears in the **Selected Computers** table.
4. Repeat steps 2 and 3 to add more computers.
5. Click **Install** when you are ready 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 the program files copy to each target computer.

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

   When all target computers appear with red check marks in the **Domains and Computers** list, you have completed remote installation.

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

Installing with Vulnerability Scanner

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

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

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

To install the OfficeScan client with Vulnerability Scanner:

Pre-installation:

1. On the Windows Vista computer, enable a built-in administrator account and set the password for the account.
2. Disable the Windows firewall.
   a. Click **Start > Programs > Administrative Tools > Windows Firewall with Advanced Security**.
   b. For Domain Profile, Private Profile, and Public Profile, set the firewall state to "Off".
3. Open the Windows Services screen (click **Start > Run** and type **services.msc**) and start the **Remote Registry** service.

Installation:

1. In the computer where you installed OfficeScan server, open \OfficeScan\PCCSRV\Admin\Utility\TMVS. Double-click TMVS.exe. The Trend Micro Vulnerability Scanner console appears.
2. Click **Settings**.
3. Under **OfficeScan server settings**, type the OfficeScan server name and port number.

4. Select **Auto-Install OfficeScan client on unprotected computers**.
5. Click **OK** to begin checking the computers on your network and begin OfficeScan client installation.

Upgrading the OfficeScan Client

You can upgrade to a full version of OfficeScan from an evaluation version. When you upgrade the OfficeScan server, clients automatically upgrade when you perform client installation with any of the installation methods available (see *Installation Methods* on page 1-3 for information on installation methods).

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.

Automatic Client Migration

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

Note: OfficeScan only uninstalls clients, not servers.

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

Client migration issues:

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

Post-installation Tasks

Trend Micro recommends performing the following post-installation tasks:

- *Verifying the Client Installation, Upgrade, or Migration* on page 2-15
- *Initiating Component Update* on page 2-18
- *Testing OfficeScan Using the EICAR Test Script* on page 2-19

Verifying the Client Installation, Upgrade, or Migration

After completing the installation or upgrade, verify the following:

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

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

Using Vulnerability Scanner to verify the client installation

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

To verify client installation using Vulnerability Scanner:

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

   If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting **Retrieve computer descriptions when available**.
5. To automatically send the results to yourself or to other administrators in your organization, select **Email results to the system administrator**. Then, click **Configure** to specify your email settings.
   - In **To**, type the email address of the recipient.

- In **From**, type your email address. This will let the recipients know who sent the message.
- In **SMTP server**, type the address of your SMTP server. For example, type smtp.company.com. This is a required information.
- In **Subject**, type a new subject for the message or accept the default subject.

6. Click **OK** to save your settings.
7. To display an alert on unprotected computers, click the **Display notification on unprotected computers**. Then, click **Customize** to set the alert message. The Alert Message screen appears. Type a new alert message in the text box or accept the default message, and then click **OK**.
8. To save the results as a comma-separated value (CSV) data file, select **Automatically save the results to a CSV file**. By default, Vulnerability Scanner saves CSV data files to the TMVS folder. If you want to change the default CSV folder, click **Browse**, select a target folder on your computer or on the network, and then click **OK**.
9. Under **Ping settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout** fields.
10. Click **OK**. The Vulnerability Scanner console appears.
11. To run a manual vulnerability scan on a range of IP addresses, do the following:

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

---

   a. In **Manual Scan**, type the IP address range of computers that you want to check for installed antivirus solutions.

   b. Click **Start** to begin checking the computers on your network.

12. To run a manual vulnerability scan on computers requesting IP addresses from a DHCP server, do the following:

   a. Click the **DHCP Scan** tab in the **Results** box. The **Start** button appears.

b. Click **Start**. Vulnerability scanner begins listening for DHCP requests and performing vulnerability checks on computers as they log on to the network.

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

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

Initiating Component Update

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

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

To deploy the components to the clients:

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

   The server starts notifying each client to download updated components.

Testing OfficeScan Using the EICAR Test Script

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

http://www.eicar.org

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

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

To test OfficeScan using the EICAR test script:

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

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

Uninstalling the Client

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

- *Uninstalling from the Web Console* on page 2-20
- *Running the Client Uninstallation Program* on page 2-21

Uninstalling from the Web Console

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

To uninstall the client from the Web console:

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

Running the Client Uninstallation Program

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

To run the client uninstallation program:

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

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

Chapter 3

Contacting Trend Micro

Topics in this chapter:

Technical Support

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

Trend Micro Incorporated provides worldwide support to all registered users.

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

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

Trend Micro, Inc.

10101 North De Anza Blvd., Cupertino, CA 95014

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

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

Fax: +1 (408) 257-2003

Web address: www.trendmicro.com

Email: support@trendmicro.com

Speeding Up Your Support Call

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

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

The Trend Micro Knowledge Base

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

http://esupport.trendmicro.com

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

TrendLabs

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

You can rely on the following post-sales service:

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

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

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

Information available:

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

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

Sending Suspicious Files to Trend Micro

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

http://subwiz.trendmicro.com/subwiz

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

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

Documentation Feedback

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

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