OfficeScan™ 10.6
For Enterprise and Medium Business

Installation and Upgrade Guide
Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro website at:


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

Copyright © 1998-2011 Trend Micro Incorporated. All rights reserved.

Document Part No. OSEM104849/110518

Release Date: August 2011

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 website.

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

### Preface

- OfficeScan Documentation ................................................................. vii
- Audience ............................................................................................ vii
- Document Conventions ........................................................................ vii
- Terminology ........................................................................................ ix

### Chapter 1: Planning OfficeScan Installation and Upgrade

- Fresh Installation and Upgrade Requirements ...................................... 1-2
- Product Versions and Keys ................................................................... 1-2
  - Full Version and Evaluation Version .................................................. 1-2
  - The Registration Key and Activation Codes ........................................ 1-3
- Fresh Installation Considerations ......................................................... 1-4
  - IPV6 Support ...................................................................................... 1-4
  - Location of the OfficeScan Server ...................................................... 1-5
- Remote Installation ................................................................................ 1-6
- Server Performance ............................................................................... 1-6
- Dedicated Server .................................................................................. 1-7
- Scan Method Deployment During Installation ....................................... 1-7
- Network Traffic .................................................................................... 1-8
- Third-party Security Software ............................................................... 1-10
- Active Directory ................................................................................... 1-10
- Web Server ........................................................................................... 1-10
- Upgrade Considerations ........................................................................ 1-11
  - IPV6 Support ...................................................................................... 1-11
  - Unsupported Operating Systems ......................................................... 1-12
  - OfficeScan Settings and Configurations ............................................. 1-13
  - Scan Method Deployment During Upgrade ......................................... 1-14
- Installation and Upgrade Checklist ....................................................... 1-17
- Planning a Pilot Deployment ................................................................. 1-24
Chapter 2: Installing and Upgrading OfficeScan

Performing a Fresh Installation of the OfficeScan Server ................. 2-2

Upgrading the OfficeScan Server and Clients ................................. 2-2
  Upgrade Method 1: Disable Automatic Client Upgrade ................. 2-4
    Upgrade Results (Online Clients) ........................................ 2-6
    Upgrade Results (Offline Clients) ...................................... 2-7
    Upgrade Results (Roaming Clients) ...................................... 2-7
  Upgrade Method 2: Upgrade Update Agents ............................... 2-8
    Upgrade Results (Online Clients) ........................................ 2-11
    Upgrade Results (Offline Clients) ...................................... 2-12
    Upgrade Results (Roaming Clients) ...................................... 2-12
  Upgrade Method 3: Move Clients to an OfficeScan 10.6 Server .... 2-13
    Upgrade Results ............................................................... 2-14
  Upgrade Method 4: Enable Automatic Client Upgrade ................. 2-15
    Upgrade Results ............................................................... 2-16

Performing Silent Installation/Upgrade ........................................ 2-16

Upgrading from an Evaluation Version ........................................ 2-19

The Setup Installation Screens ..................................................... 2-20
  License Agreement ................................................................. 2-23
  Client Deployment ................................................................. 2-24
  OfficeScan Server Settings .................................................. 2-25
  Installation Destination ......................................................... 2-26
  Prescan ............................................................................. 2-29
  Installation Path ................................................................. 2-31
  Proxy Settings ................................................................. 2-32
  Web Server Settings .......................................................... 2-33
  Server Computer Identification ............................................. 2-37
  Registration and Activation .................................................. 2-39
  Integrated Smart Protection Server Installation ......................... 2-41
  Enable Web Reputation Services ........................................... 2-44
  Remote Installation Destination ............................................. 2-46
  Target Computer Analysis .................................................... 2-49
  OfficeScan Programs .......................................................... 2-50
Cisco Trust Agent Installation/Upgrade .............................................. 2-53
Cisco Trust Agent License ................................................................. 2-54
Trend Micro Smart Protection Network .............................................. 2-55
Administrator Account Password .................................................... 2-57
Client Installation Path ...................................................................... 2-58
Antivirus Features ............................................................................. 2-60
Anti-spyware Feature ........................................................................ 2-61
Web Reputation Policy ...................................................................... 2-63
Program Folder Shortcut ................................................................. 2-65
Installation Information .................................................................. 2-66
Policy Server Installation ................................................................. 2-67
OfficeScan Server Installation Completion ...................................... 2-68

Post-installation Tasks ...................................................................... 2-69
Verifying the Server Installation or Upgrade .................................... 2-69
Verifying Integrated Smart Protection Server Installation ............ 2-72
Updating OfficeScan Components .................................................. 2-72
Checking Default Settings ............................................................... 2-73
Using Client Mover for Legacy Platforms ....................................... 2-74
Registering OfficeScan to Control Manager ................................... 2-77

Uninstallation and Rollback .............................................................. 2-77
OfficeScan Server Uninstallation ...................................................... 2-77
Before Uninstalling the OfficeScan Server .................................... 2-77
Uninstalling the OfficeScan Server .................................................. 2-80
Rolling Back to Previous OfficeScan Versions ......................... 2-84

Chapter 3: Getting Help

Troubleshooting Resources .............................................................. 3-2
Support Intelligence System ............................................................. 3-2
Case Diagnostic Tool ...................................................................... 3-2
Trend Micro Performance Tuning Tool ......................................... 3-2
Installation Logs ............................................................................ 3-4
Server Debug Logs ......................................................................... 3-5
Client Debug Logs .......................................................................... 3-7

Contacting Trend Micro ................................................................. 3-8
Technical Support ........................................................................... 3-8
The Trend Micro Knowledge Base .........................................................3-9
TrendLabs ..................................................................................................3-10
Security Information Center .................................................................3-10
Sending Suspicious Files to Trend Micro .............................................3-11
Documentation Feedback .......................................................................3-11

Appendix A: Sample Deployment

Basic Network .................................................................................................A-2
Multiple Site Network ....................................................................................A-3
  Head Office Deployment ...........................................................................A-5
  Remote Site 1 Deployment .....................................................................A-5
  Remote Site 2 Deployment .....................................................................A-6

Appendix B: Legacy OfficeScan Features

Index
Welcome to the Trend Micro™ OfficeScan™ Installation and Upgrade Guide. This document discusses requirements and procedures for installing the OfficeScan server, and upgrading the server and clients.

Note: For information on installing clients, see the Administrator’s Guide.

Topics in this chapter:

• OfficeScan Documentation on page vi
• Audience on page vii
• Document Conventions on page vii
• Terminology on page ix
OfficeScan Documentation

OfficeScan documentation includes the following:

**TABLE P-1. OfficeScan Documentation**

<table>
<thead>
<tr>
<th>DOCUMENTATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation and Upgrade Guide</td>
<td>A PDF document that discusses requirements and procedures for installing the OfficeScan server, and upgrading the server and clients</td>
</tr>
<tr>
<td>Administrator’s Guide</td>
<td>A PDF document that discusses getting started information, client installation procedures, and OfficeScan server and client management</td>
</tr>
<tr>
<td>Help</td>
<td>HTML files compiled in WebHelp or CHM format that provide &quot;how to's&quot;, usage advice, and field-specific information. The Help is accessible from the OfficeScan server, client, and Policy Server consoles, and from the OfficeScan Master Setup.</td>
</tr>
<tr>
<td>Readme file</td>
<td>Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>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 website: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>

Download the latest versions of the PDF documents and readme at:

Audience

OfficeScan documentation is intended for the following users:

- **OfficeScan Administrators**: Responsible for OfficeScan management, including server and client installation and management. These users are expected to have advanced networking and server management knowledge.

- **Cisco NAC administrators**: Responsible for designing and maintaining security systems with Cisco™ NAC servers and Cisco networking equipment. They are assumed to have experience with this equipment.

- **End users**: Users who have the OfficeScan client installed on their computers. The computer skill level of these individuals ranges from beginner to power user.

Document Conventions

To help you locate and interpret information easily, the OfficeScan documentation uses the following conventions:

**TABLE P-2. Document Conventions**

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL CAPITALS</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, options, and tasks</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>References to other documentation or new technology components</td>
</tr>
<tr>
<td><strong>TOOLS &gt; CLIENT</strong></td>
<td>A &quot;breadcrumb&quot; found at the start of procedures that helps users navigate to the relevant web console screen. Multiple breadcrumbs means that there are several ways to get to the same screen.</td>
</tr>
<tr>
<td>&lt;Text&gt;</td>
<td>Indicates that the text inside the angle brackets should be replaced by actual data. For example, C:\Program Files&lt;file_name&gt; can be C:\Program Files\sample.jpg.</td>
</tr>
<tr>
<td>CONVENTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Note:</strong> text</td>
<td>Provides configuration notes or recommendations</td>
</tr>
<tr>
<td><strong>Tip:</strong> text</td>
<td>Provides best practice information and Trend Micro recommendations</td>
</tr>
<tr>
<td><strong>WARNING!</strong> text</td>
<td>Provides warnings about activities that may harm computers on your network</td>
</tr>
</tbody>
</table>
## Terminology

The following table provides the official terminology used throughout the OfficeScan documentation:

<table>
<thead>
<tr>
<th>TERMINOLOGY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>The OfficeScan client program</td>
</tr>
<tr>
<td>Client computer or endpoint</td>
<td>The computer where the OfficeScan client is installed</td>
</tr>
<tr>
<td>Client user (or user)</td>
<td>The person managing the OfficeScan client on the client computer</td>
</tr>
<tr>
<td>Server</td>
<td>The OfficeScan server program</td>
</tr>
<tr>
<td>Server computer</td>
<td>The computer where the OfficeScan server is installed</td>
</tr>
<tr>
<td>Administrator (or OfficeScan administrator)</td>
<td>The person managing the OfficeScan server</td>
</tr>
</tbody>
</table>
| Console                                          | The user interface for configuring and managing OfficeScan server and client settings                                                                                                                                               
|                                                  | The console for the OfficeScan server program is called "web console", while the console for the client program is called "client console".                                                                    |
| Security risk                                    | The collective term for virus/malware, spyware/grayware, and web threats                                                                                                                                     |
| Product service                                  | Includes Antivirus, Damage Cleanup Services, and Web Reputation and Anti-spyware—all of which are activated during OfficeScan server installation                                                               |
| OfficeScan service                               | Services hosted by Microsoft Management Console (MMC). For example, ofcservice.exe, the OfficeScan Master Service.                                                                                       |
**Program**
Includes the OfficeScan client, Cisco Trust Agent, and Plug-in Manager

**Components**
Responsible for scanning, detecting, and taking actions against security risks

**Client installation folder**
The folder on the computer that contains the OfficeScan client files. If you accept the default settings during installation, you will find the installation folder at any of the following locations:

- **C:\Program Files\Trend Micro\OfficeScan Client**
- **C:\Program Files (x86)\Trend Micro\OfficeScan Client**

For example, if a particular file is found under \PCCSRV on the server installation folder, the full path to the file is:

**C:\Program Files\Trend Micro\OfficeScan\PCCSRV\<file_name>**.

**Server installation folder**
The folder on the computer that contains the OfficeScan server files. If you accept the default settings during installation, you will find the installation folder at any of the following locations:

- **C:\Program Files\Trend Micro\OfficeScan**
- **C:\Program Files (x86)\Trend Micro\OfficeScan**

**Smart scan client**
An OfficeScan client that has been configured to use smart scan

**Conventional scan client**
An OfficeScan client that has been configured to use conventional scan
**TABLE P-3. OfficeScan Terminology (Continued)**

<table>
<thead>
<tr>
<th>TERMINOLOGY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual-stack</td>
<td>An entity that has both IPv4 and IPv6 addresses. For example:</td>
</tr>
<tr>
<td></td>
<td>• A dual-stack endpoint is a computer with both IPv4 and IPv6 addresses.</td>
</tr>
<tr>
<td></td>
<td>• A dual-stack client refers to a client installed on a dual-stack endpoint.</td>
</tr>
<tr>
<td></td>
<td>• A dual-stack Update Agent distributes updates to clients.</td>
</tr>
<tr>
<td></td>
<td>• A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses.</td>
</tr>
<tr>
<td>Pure IPv4</td>
<td>An entity that only has an IPv4 address</td>
</tr>
<tr>
<td>Pure IPv6</td>
<td>An entity that only has an IPv6 address</td>
</tr>
<tr>
<td>Plug-in solutions</td>
<td>Native OfficeScan features and plug-in programs delivered through Plug-in Manager</td>
</tr>
</tbody>
</table>
Chapter 1

Planning OfficeScan Installation and Upgrade

This chapter describes preparation and pre-installation information for Trend Micro™ OfficeScan™ installation and upgrade.

Topics in this chapter:
• Fresh Installation and Upgrade Requirements on page 1-2
• Product Versions and Keys on page 1-2
• Fresh Installation Considerations on page 1-4
• Upgrade Considerations on page 1-11
• Installation and Upgrade Checklist on page 1-17
• Planning a Pilot Deployment on page 1-24
• Known Compatibility Issues on page 1-25
Fresh Installation and Upgrade Requirements

You can perform a fresh installation of the OfficeScan server and clients on supported Windows server platforms.

In addition, this version of OfficeScan supports upgrades from the following versions:

- OfficeScan 10.x
  - 10.5 Patch 1
  - 10.5
  - 10.0 Service Pack 1
  - 10.0
- OfficeScan 8.0 Service Pack 1

Visit the following website for a complete list of fresh installation and upgrade requirements:


Product Versions and Keys

Full Version and Evaluation Version

Install either a full or evaluation version of OfficeScan. Both versions require a different type of Activation Code. Register the product if you do not have an Activation Code.

Full Version

The full version includes all the product features and technical support, and provides a grace period (usually 30 days) after the license expires. If you do not renew the license after the grace period expires, you will not be able to obtain technical support and perform component updates. The scan engines will still scan computers using out-of-date components. These out-of-date components may not be able to protect computers completely from the latest security risks. Renew the license before or after it expires by purchasing a maintenance renewal.
Evaluation Version

The evaluation version includes all the product features. Upgrade an evaluation version to the full version at any time. If not upgraded at the end of the evaluation period, OfficeScan disables component updates, scanning, and all client features.

The Registration Key and Activation Codes

During installation, Setup prompts you to specify the Activation Codes for the following services:

- Antivirus
- Damage Cleanup Services™ (optional)
- Web Reputation and Anti-spyware

If you do not have the Activation Codes, use the Registration Key that came with the product. Setup automatically redirects you to the Trend Micro website where you can register your product.

http://olr.trendmicro.com

After registering your product, Trend Micro sends you the Activation Codes.

If you do not have either the Registration Key or Activation Codes, contact your Trend Micro sales representative. See Contacting Trend Micro on page 3-8 for details.

Fresh Installation Considerations

Consider the following when performing a fresh installation of the OfficeScan server:

- **IPV6 Support** on page 1-4
- **Location of the OfficeScan Server** on page 1-5
- **Remote Installation** on page 1-6
- **Server Performance** on page 1-6
- **Dedicated Server** on page 1-7
- **Scan Method Deployment During Installation** on page 1-7
- **Network Traffic** on page 1-8
- **Third-party Security Software** on page 1-10
- **Active Directory** on page 1-10
- **Web Server** on page 1-10

IPV6 Support

The IPv6 requirements for the OfficeScan server fresh installation are as follows:

- The OfficeScan server must be installed on Windows Server 2008. It cannot be installed on Windows Server 2003 because this operating system only supports IPv6 addressing partially.
- The server must use an IIS web server. Apache web server does not support IPv6 addressing.
- If the server will manage IPv4 and IPv6 clients, it must have both IPv4 and IPv6 addresses and must be identified by its host name. If a server is identified by its IPv4 address, IPv6 clients cannot connect to the server. The same issue occurs if pure IPv4 clients connect to a server identified by its IPv6 address.
• If the server will manage only IPv6 clients, the minimum requirement is an IPv6 address. The server can be identified by its host name or IPv6 address. When the server is identified by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.

**Note:** The FQDN can only be specified when performing a local installation of the server. It is not supported on remote installations.

• Verify that the host machine’s IPv6 or IPv4 address can be retrieved using, for example, the “ping” or “nslookup” command.

• If you are installing the OfficeScan server to a pure IPv6 computer:
  • Set up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the OfficeScan server and the Internet to allow the server to successfully connect to Trend Micro hosted services, such as the ActiveUpdate server, the Online Registration website, and Smart Protection Network.
  • Do not install Policy Server for Cisco NAC and Cisco Trust Agent. These programs do not support IPv6 addressing.

**Location of the OfficeScan Server**

OfficeScan can accommodate a variety of network environments. For example, you can position a firewall between the OfficeScan server and its clients, or position both the server and all clients behind a single network firewall. If there is a firewall between the server and its clients, configure the firewall to allow traffic between the client and server listening ports.

**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.
Remote Installation

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

To ensure that installation can proceed:

• On each target computer, start the Remote Registry service using an administrator account and not a Local System account. Remote Registry service is managed from Microsoft Management Console (Click Start > Run, and type services.msc).
• Record the computer's host name and logon credentials (user name and password).
• Verify that the computer meets the OfficeScan server system requirements. Refer to Fresh Installation and Upgrade Requirements on page 1-2 for more information.

Server Performance

Enterprise networks require servers with higher specifications than those required for small and medium-sized businesses.

Tip: Trend Micro recommends at least 2GHz dual processors and over 2GB of RAM for the OfficeScan server.

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

The typical number of clients an OfficeScan server can manage are as follows:

• 3,000 to 5,000 clients for an OfficeScan server with 2GHz dual processor with 2GB of RAM
• 5,000 to 20,000 clients for an OfficeScan server with 2.13GHz Core2Duo™ processor with 4GB of RAM
Dedicated Server

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

- The CPU load the computer handles
- If the computer performs other functions

If the target computer has other functions, choose a computer that does not run critical or resource-intensive applications.

Scan Method Deployment During Installation

In this OfficeScan version, you can configure clients to use either smart scan or conventional scan.

Conventional Scan

Conventional scan is the scan method used in all earlier OfficeScan versions. A conventional scan client stores all OfficeScan components on the client computer and scans all files locally.

Smart Scan

Smart scan leverages threat signatures that are stored in-the-cloud. When in smart scan mode, the OfficeScan client first scans for security risks locally. If the client cannot determine the risk of the file during the scan, the client connects to a Smart Protection Server.

Smart scan provides the following features and benefits:

- Provides fast, real-time security status lookup capabilities in the cloud
- Reduces the overall time it takes to deliver protection against emerging threats
- Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud and not to many endpoints.
- Reduces the cost and overhead associated with corporate-wide pattern deployments
- Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.
Scan Method Deployment

On fresh installations, the default scan method for clients is the smart scan method. OfficeScan also allows you to customize the scan method for each domain after installing the server. Consider the following:

- If you did not change the scan method after installing the server, all clients that you install will use smart scan.
- If you want to use conventional scan on all clients, change the root level scan method to conventional scan after installing the server.
- If you want to use both conventional and smart scan, Trend Micro recommends retaining smart scan as the root level scan method and then changing the scan method on domains that you want to apply conventional scan.

Network Traffic

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

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

The client generates traffic when it does the following:

- Starts up
- Updates components
- Updates settings and installs a hot fix
- Scans for security risks
- Switches between roaming mode and normal mode
- Switches between conventional scan and smart scan
Network Traffic During Component Updates
OfficeScan generates significant network traffic when it updates a component. To reduce network traffic generated during component updates, OfficeScan performs component duplication. Instead of downloading an updated full pattern file, OfficeScan only downloads the "incremental" patterns (smaller versions of the full pattern file) and merges them with the old pattern file after the download.

Clients updated regularly only download the incremental pattern. Otherwise, they download the full pattern file.

Trend Micro releases new pattern files regularly. Trend Micro also releases a new pattern file as soon as a damaging and actively circulating virus/malware is discovered.

Update Agents and Network Traffic
If there are low-bandwidth or "heavy traffic" sections of the network between clients and the OfficeScan server, designate selected OfficeScan clients as Update Agents, or update sources for other clients. This helps distribute the burden of deploying components to all clients.

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

Trend Micro Control Manager and Network Traffic
Trend Micro Control Manager™ manages Trend Micro products and services at the gateway, mail server, file server and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for products and services throughout the network.

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

See the Control Manager documentation for more information on Control Manager.
Third-party Security Software

Remove third-party endpoint security software from the computer to which you will install OfficeScan server. These applications may prevent successful OfficeScan server installation or affect its performance. Install the OfficeScan server and client immediately after removing third-party security software to keep the computer protected from security risks.

**Note:** OfficeScan cannot automatically uninstall the server component of any third-party antivirus product, but can uninstall the client component. See the *Administrator's Guide* for details.

Active Directory

All OfficeScan servers must be part of an Active Directory domain to take advantage of the Role-based Administration and Security Compliance features.

Web Server

The OfficeScan web server’s functions are as follows:

- Allows users to access the web console
- Accepts commands from clients
- Allows clients to respond to server notifications

You can use an IIS web server or Apache web server. If you use an IIS web server, ensure that the server computer does not run IIS-locking applications. Setup automatically stops and restarts the IIS service during installation.

If you use an Apache web server, the administrator account is the only account created on the Apache web server. Create another account from which to run the web server to prevent compromising the OfficeScan server if a hacker takes control of the Apache web server.

Refer to [http://www.apache.org](http://www.apache.org) for the latest information on Apache web server upgrades, patches, and security issues.
Upgrade Considerations

Consider the following when upgrading the OfficeScan server and clients:

- IPv6 Support on page 1-11
- Unsupported Operating Systems on page 1-12
- OfficeScan Settings and Configurations on page 1-13
- Scan Method Deployment During Upgrade on page 1-14

IPv6 Support

The IPv6 requirements for the OfficeScan server and client upgrades are as follows:

- The OfficeScan server to be upgraded must be installed on Windows Server 2008. OfficeScan servers on Windows Server 2003 cannot be upgraded because Windows Server 2003 only supports IPv6 addressing partially.
- The OfficeScan server to be upgraded must be version 10.x or 8.0 SP1.
- The server must already be using an IIS web server. Apache web server does not support IPv6 addressing.
- Assign an IPv6 address to the server. In addition, the server must be identified by its host name, preferably its Fully Qualified Domain Name (FQDN). If the server is identified by its IPv6 address, all clients currently managed by the server will lose connection with the server. If the server is identified by its IPv4 address, it will not be able to deploy the client to pure IPv6 computers.
- Verify that the host machine’s IPv6 or IPv4 address can be retrieved using, for example, the “ping” or “nslookup” command.
Unsupported Operating Systems

OfficeScan no longer supports Windows 95, 98, Me, NT, 2000, or the Itanium architecture platform.

If you plan to upgrade to this version from OfficeScan 10.x/8.0 SP1 and you have OfficeScan 10.x/8.0 SP1 clients that run these operating systems:

• Do not upgrade all OfficeScan 10.x/8.0 SP1 servers to this OfficeScan version.
• Designate at least an OfficeScan 10.x or OfficeScan 8.0 SP1 server (parent server) to manage clients running unsupported operating systems.
• Before upgrading the other servers:
  • Open the web console and click Networked Computers > Client Management on the main menu.
  • On the client tree, select the clients that you want to move and then click Manage Client Tree > Move Client.
  • Specify the parent server’s computer name/IP address and server listening port under Move selected client(s) to another OfficeScan Server.
  • Click Move.

If you have upgraded the OfficeScan server but did not move unsupported clients, use a tool called Client Mover for Legacy Platforms to move the clients to a parent server that can manage them. For details about the tool, see Using Client Mover for Legacy Platforms on page 2-74.

dbbkup
OfficeScan Settings and Configurations

Back up the OfficeScan database and important configuration files before upgrading the OfficeScan server. Back up the OfficeScan server database to a location outside the OfficeScan program directory.

To back up and restore the OfficeScan database and configuration files:

1. Back up the database from the OfficeScan 10.x/8.0 SP1 web console by going to Administration > Database Backup.

   For detailed instructions, see the Administrator's Guide or Server Help for these product versions.

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

2. Stop the OfficeScan Master Service from the Microsoft Management Console.

3. Manually back up the following files and folders found under `<Server installation folder>\PCCSRV`:

   **Note:** Back up these files and folders to roll back OfficeScan only if you encounter upgrade issues.

   - **ofcscan.ini:** Contains global client settings
   - **ous.ini:** Contains the update source table for antivirus component deployment
   - **Private folder:** Contains firewall and update source settings
   - **Web\tmOPP folder:** Contains Outbreak Prevention settings
   - **Pccnt\Common\OfcPfw*.dat:** Contains firewall settings
   - **Download\OfcPfw*.dat:** Contains firewall deployment settings
   - **Log folder:** Contains system events and the connection verification logs
   - **Virus folder:** Contains quarantined files
   - **HTTPDB folder:** Contains the OfficeScan database
4. Upgrade the OfficeScan server.

Note: If you encounter upgrade issues, copy the backup files from step 3 to the `<Server installation folder>\PCCSRV` folder on the target computer and restart the OfficeScan Master Service.

---

**Scan Method Deployment During Upgrade**

In this OfficeScan version, you can configure clients to use either smart scan or conventional scan.

If you upgrade OfficeScan from an earlier version, you can retain or customize the scan method for each domain depending on the upgrade method chosen. Consider the following:

**Upgrading from OfficeScan 10.x:**

- If you plan to upgrade the OfficeScan 10.x server directly on the server computer, you do not need to make scan method changes from the web console because clients will retain their scan method settings after they upgrade.
- If you plan to upgrade OfficeScan 10.x clients by moving them to an OfficeScan 10.6 server:
  - In the OfficeScan 10.6 server, choose manual client grouping. This client grouping method allows you to create new domains.

  Note: If you plan to use automatic client grouping, enable it only after all clients have upgraded to ensure that all scan method settings are retained during client upgrade.

- Duplicate the domain structure and scan method settings in the OfficeScan 10.x server into the OfficeScan 10.6 server. If the domain structure and scan method settings on the two servers are not identical, some clients that move to the OfficeScan 10.6 server may not apply their original scan method settings.

**Upgrading from OfficeScan 8.0 SP1**

- If you plan to upgrade the OfficeScan 8.0 SP1 server directly on the server computer:
All Clients Use Smart Scan:

i. Prevent automatic updates and upgrade on clients.
   For details, see Part 1: Configure update settings on the OfficeScan 10.x or 8.0 SP1 server on page 2-4.

ii. Upgrade the OfficeScan server.
    For details, see Part 2: Upgrade the OfficeScan server on page 2-5.

iii. Change the root level scan method to smart scan.

iv. Upgrade clients.
    For details, see Part 3: Upgrade OfficeScan clients on page 2-5.

All Clients Use Conventional Scan:

i. Upgrade the OfficeScan server.
   For details on upgrading the server only and then staggering the client upgrade, see Part 2: Upgrade the OfficeScan server on page 2-5.
   For details on automatically upgrading the server and clients, see Part 2: Upgrade the OfficeScan server on page 2-15.

ii. Upgrade clients
    For details, see Part 3: Upgrade OfficeScan clients on page 2-5.

Most Clients Use Smart Scan:

Trend Micro recommends performing the following tasks:

i. Prevent automatic updates and upgrade on clients.
   For details, see Part 1: Configure update settings on the OfficeScan 10.x or 8.0 SP1 server on page 2-4.

ii. Upgrade the OfficeScan server.
    For details, see Part 2: Upgrade the OfficeScan server on page 2-5.

iii. Change the root level scan method to smart scan.

iv. Upgrade clients (All clients will use smart scan).
    For details, see Part 3: Upgrade OfficeScan clients on page 2-5.

v. Change the scan method of clients that you want to use conventional scan.
• If you plan to upgrade clients by moving them to an OfficeScan 10.6 server:

All Clients Use Smart Scan:

i. In the OfficeScan 8.0 SP1 server, move clients to the OfficeScan 10.6 server.

For details, see Upgrade Method 3: Move Clients to an OfficeScan 10.6 Server on page 2-13.

All Clients Use Conventional Scan:

i. In the OfficeScan 10.6 server, change the root level scan method to conventional scan.

ii. In the OfficeScan 8.0 SP1 server, move clients to the OfficeScan 10.6 server.

For details, see Part 2: Upgrade OfficeScan clients on page 2-14.

Most Clients Use Smart Scan:

i. In the OfficeScan 8.0 SP1 server:

• Identify which domains will apply smart scan and those that will apply conventional scan. For example, Domains A1, A2, and A3 will apply smart scan, and domains A4, A5, and A6 will apply conventional scan.

• Ensure that OfficeScan 8.0 SP1 clients that you want to use smart scan are grouped under Domain A1, A2, or A3.

• Ensure that OfficeScan 8.0 SP1 clients that you want to use conventional scan are grouped under Domain A4, A5, or A6.

ii. In the OfficeScan 10.6 server:

• Choose manual client grouping. This client grouping method allows you to create new domains.

• Create Domains A1, A2, A3, A4, A5, and A6. Use the exact domain names.

• Change the scan method of domains A4, A5, and A6 to conventional scan.

iii. In the OfficeScan 8.0 SP1 server:

• Move clients to the OfficeScan 10.6 server.

For details, see Part 2: Upgrade OfficeScan clients on page 2-14.
## Installation and Upgrade Checklist

Setup prompts you for the following information when you install or upgrade the OfficeScan server:

### TABLE 1-1. Installation Checklist

<table>
<thead>
<tr>
<th>INSTALLATION INFORMATION</th>
<th>INFORMATION NEEDED DURING</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LOCAL/SILENT FRESH INSTALL</td>
</tr>
<tr>
<td><strong>Installation path</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>The default server installation path is:</td>
<td></td>
</tr>
<tr>
<td>• C:\Program Files\Trend Micro\OfficeScan</td>
<td></td>
</tr>
<tr>
<td>• C:\Program Files (x86)\Trend Micro\OfficeScan (for x64 type platforms)</td>
<td></td>
</tr>
<tr>
<td>Identify the installation path if you choose not to use the default path. If the path does not exist, Setup creates it for you.</td>
<td></td>
</tr>
</tbody>
</table>

| **Proxy server settings** | Yes | Yes | No | Yes |
| If the OfficeScan server connects to the Internet through a proxy server, specify the following: | | | | |
| • Proxy type (HTTP or SOCKS 4) | | | | |
| • Server name or IP address | | | | |
| • Port | | | | |
| • Proxy authentication credentials | | | | |
### Web server settings

The web server (Apache or IIS web server) runs web console CGIs and accepts commands from clients. Specify the following:

- **HTTP port**: The default port is 8080. If you are using the IIS default web site, check the HTTP server’s TCP port.

**WARNING!** Many hacker and virus/malware attacks delivered over HTTP use ports 80 and/or 8080. Most organizations use these port numbers as the default TCP port for HTTP communications. Use other port numbers if you currently use the default port numbers.

If enabling secure connections:

- SSL certificate validity period
- SSL port (Default: 4343)

<table>
<thead>
<tr>
<th><strong>Web server settings</strong></th>
<th>LOCAL/SILENT FRESH INSTALL</th>
<th>REMOTE FRESH INSTALL</th>
<th>LOCAL/SILENT UPGRADE</th>
<th>REMOTE UPGRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 1-1. Installation Checklist (Continued)

<table>
<thead>
<tr>
<th>Installation Information</th>
<th>Local/ Silent Fresh Install</th>
<th>Remote Fresh Install</th>
<th>Local/ Silent Upgrade</th>
<th>Remote Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Register the product to receive the Activation Codes. To register, you need the following:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>For returning users</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Online registration account (logon name and password)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>For users without an account</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Registration Key</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Activation</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Obtain the Activation Codes for the following product services:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Antivirus</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Damage Cleanup Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Web Reputation and Anti-spyware</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrated Smart Protection Server installation</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>If you choose to install the integrated server, specify the following:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SSL certificate validity period</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SSL port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-1. Installation Checklist (Continued)

<table>
<thead>
<tr>
<th>INSTALLATION INFORMATION</th>
<th>INFORMATION NEEDED DURING</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LOCAL/SILENT FRESH INSTALL</td>
</tr>
<tr>
<td>Remote installation destination</td>
<td>No</td>
</tr>
<tr>
<td>Identify the computers to which you will install/upgrade the OfficeScan server. Prepare the following:</td>
<td></td>
</tr>
<tr>
<td>• List of computer names or IP addresses</td>
<td></td>
</tr>
<tr>
<td>• (Optional) A text file with a list of target computers or IP addresses</td>
<td></td>
</tr>
<tr>
<td>Sample text file content:</td>
<td></td>
</tr>
<tr>
<td>us-user_01</td>
<td></td>
</tr>
<tr>
<td>us-admin_01</td>
<td></td>
</tr>
<tr>
<td>123.12.12.123</td>
<td></td>
</tr>
<tr>
<td>Remote installation computer analysis</td>
<td>No</td>
</tr>
<tr>
<td>Setup prompts you for the following information before performing target computer analysis:</td>
<td></td>
</tr>
<tr>
<td>• User name and password for an administrator account with &quot;logon as a service&quot; privilege on the target computer</td>
<td></td>
</tr>
<tr>
<td>Install other OfficeScan programs</td>
<td>Yes</td>
</tr>
<tr>
<td>If installing Cisco Trust Agent, prepare the following:</td>
<td></td>
</tr>
<tr>
<td>• Cisco Trust Agent certificate file</td>
<td></td>
</tr>
<tr>
<td>INSTALLATION INFORMATION</td>
<td>INFORMATION NEEDED DURING</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td>LOCAL/SILENT FRESH INSTALL</td>
</tr>
<tr>
<td>Administrator account password</td>
<td>Yes</td>
</tr>
<tr>
<td>Setup creates a root account for web</td>
<td></td>
</tr>
<tr>
<td>console logon. Specify the following:</td>
<td></td>
</tr>
<tr>
<td>• Root account password</td>
<td></td>
</tr>
<tr>
<td>Prevent unauthorized uninstallation or</td>
<td></td>
</tr>
<tr>
<td>unloading of the OfficeScan client by</td>
<td></td>
</tr>
<tr>
<td>specifying the following:</td>
<td></td>
</tr>
<tr>
<td>• Client uninstallation/unloading</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td></td>
</tr>
<tr>
<td>Client installation path</td>
<td>Yes</td>
</tr>
<tr>
<td>Specify the directory on the client</td>
<td></td>
</tr>
<tr>
<td>computer where the OfficeScan client</td>
<td></td>
</tr>
<tr>
<td>will be installed. Specify the following:</td>
<td></td>
</tr>
<tr>
<td>• Installation path: The default client</td>
<td></td>
</tr>
<tr>
<td>installation path is $ProgramFiles\Trend Micro\OfficeScan Client. Identify the</td>
<td></td>
</tr>
<tr>
<td>installation path if you choose not to</td>
<td></td>
</tr>
<tr>
<td>use the default path. If the path does</td>
<td></td>
</tr>
<tr>
<td>not exist, Setup creates it during</td>
<td></td>
</tr>
<tr>
<td>client installation.</td>
<td></td>
</tr>
<tr>
<td>• Client communication port number:</td>
<td></td>
</tr>
<tr>
<td>OfficeScan generates the port number</td>
<td></td>
</tr>
<tr>
<td>randomly. Accept the generated port</td>
<td></td>
</tr>
<tr>
<td>number or specify a new one.</td>
<td></td>
</tr>
</tbody>
</table>
**TABLE 1-1. Installation Checklist (Continued)**

<table>
<thead>
<tr>
<th>INSTALLATION INFORMATION</th>
<th>INFORMATION NEEDED DURING</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LOCAL/ SILENT FRESH INSTALL</td>
</tr>
<tr>
<td>Program folder shortcut</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The shortcut to the OfficeScan server installation folder displays from the Windows Start menu. The default shortcut name is **Trend Micro OfficeScan Server-<Server_name>**. Identify a different name if you do not want to use the default name.
**Policy server installation**

Prepare the following information if you choose to install Policy Server for Cisco NAC:

- **Installation Path**: If you do not accept the default installation path, specify a location on the local computer where Policy Server will be installed.

- **Web Server Configuration**: Specify the following settings for the selected web server:
  - HTTP port (Default: 8081)
  - If enabling secure connections:
    - SSL certificate validity period
  - SSL port (Default: 4344)
  - Web Console Password: Specify the password to log on to the Policy Server console.

- **ACS Server Authentication**: An ACS server receives OfficeScan client antivirus data from the client through the Network Access Device and passes it to an external user database for evaluation. Specify the logon credentials (user name and password).
Planning a Pilot Deployment

Before performing a full-scale deployment, 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 may need after full deployment. It gives your installation team a chance to rehearse and refine the deployment process. It also allows you to test if the deployment plan meets your organization’s security initiative.

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

**Choosing a Pilot Site**

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

**Creating a Rollback Plan**

Create a recovery or rollback plan in case there are issues with the installation or upgrade process.

**Evaluating the Pilot Deployment**

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

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

**Microsoft Small Business Server**

Before installing the OfficeScan server on a computer running Microsoft Small Business Server™ and Microsoft Internet Security Acceleration server (ISA), record the server port used by ISA. By default, both the OfficeScan server and ISA use port 8080. Choose another server listening port when installing the OfficeScan server.

**Microsoft Lockdown Tools and URLScan**

If you use the Microsoft IIS Lockdown Tool or URLScan, lockdown of the following OfficeScan files may block OfficeScan client and server communication:

- Configuration (.ini) files
- Data (.dat) files
- Dynamic link library (.dll) files
- Executable (.exe) files

**To prevent URLScan from interfering with client-server communication:**

2. Modify the URLScan configuration file to allow the file types specified above.

**Microsoft Exchange Server**

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

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

Internet Connection Firewall (ICF)
Windows Server 2003 provides a built-in firewall called Internet Connection Firewall (ICF). If you want to run ICF, add the OfficeScan listening ports to the ICF exception list. See the firewall documentation for details on how to configure exception lists.
Chapter 2

Installing and Upgrading OfficeScan

This chapter describes the steps in installing or upgrading Trend Micro™ OfficeScan™.

Topics in this chapter:

- Performing a Fresh Installation of the OfficeScan Server on page 2-2
- Upgrading the OfficeScan Server and Clients on page 2-2
- Performing Silent Installation/Upgrade on page 2-16
- Upgrading from an Evaluation Version on page 2-19
- The Setup Installation Screens on page 2-20
- Post-installation Tasks on page 2-69
- Uninstallation and Rollback on page 2-77
Performing a Fresh Installation of the OfficeScan Server

To perform a fresh installation, run Setup on a computer that meets the OfficeScan server fresh installation and upgrade requirements. Setup installs the OfficeScan server and Plug-in Manager 2.0. This Plug-in Manager version provides the widget functionality in OfficeScan. For information on the installation screens and configuration options, see the setup installation screens (on page 2-20).

For client fresh installation methods and instructions, see the Administrator's Guide.

Upgrading the OfficeScan Server and Clients

Running Setup on a computer with an OfficeScan 10.x or 8.0 SP1 server upgrades the server. If Plug-in Manager is installed on the computer, Setup also upgrades Plug-in Manager to version 2.0. If Plug-in Manager is not installed, version 2.0 will automatically be installed. This Plug-in Manager version provides the widget functionality in OfficeScan.

Depending on network bandwidth and the number of clients the OfficeScan server manages, stagger the client upgrade in groups or upgrade all clients immediately after the server upgrades.

Tip: Trend Micro highly recommends restarting the OfficeScan clients after upgrading to ensure that all OfficeScan components have been updated.
Before Upgrading the OfficeScan Server and Clients

Before upgrading the OfficeScan server and clients, take note of the following:

1. The installation package includes updates to OfficeScan firewall drivers. If you have enabled the OfficeScan firewall in your current OfficeScan version, deploying the package may cause the following client computer disruptions:

   - When Common Firewall Driver update starts, client computers will be temporarily disconnected from the network. Users are not notified before disconnection.
     
     An option on the OfficeScan 10 SP1 or later web console, which is enabled by default, postpones the Common Firewall Driver update until a client computer is restarted. To avoid the disconnection issue, ensure that this option is enabled. To check the status of this option, navigate to Networked Computers > Global Client Settings and go to the Firewall Settings section. The option is Update the OfficeScan firewall driver only after a system reboot.

   - After deploying the package, the OfficeScan TDI driver's previous version still exists on the client computer and the new version will not be loaded until the computer is restarted. Users are likely to encounter problems with the OfficeScan client if they do not restart immediately.

     If the option to display the restart notification message is enabled on the web console, users will be prompted to restart. However, users who decide to postpone the restart are not prompted again. If the option is disabled, users are not notified at all.

     The option to display the restart notification message is enabled by default. To check the status of this option, navigate to Networked Computers > Global Client Settings and go to the Alert Settings section. The option is Display a notification message if the client computer needs to restart to load a kernel mode driver.
2. The OfficeScan server cannot upgrade to this version if:
   • A client is running Login Script (AutoPcc.exe) at the time of server upgrade. Ensure that no client is running Login Script before upgrading the server.
   • The server is performing database-related tasks. Before upgrading, check the status of the OfficeScan database (DbServer.exe). For example, open Windows Task Manager and verify that CPU usage for DbServer.exe is 00. If CPU usage is higher, wait until usage is 00, which signals that database-related tasks have been completed. If you run an upgrade and encounter upgrade problems, it is possible that database files have been locked. In this case, restart the server computer to unlock the files and then run another upgrade.

Upgrade Methods
Use one of following upgrade methods:
• Upgrade Method 1: Disable Automatic Client Upgrade on page 2-4
• Upgrade Method 2: Upgrade Update Agents on page 2-8
• Upgrade Method 3: Move Clients to an OfficeScan 10.6 Server on page 2-13
• Upgrade Method 4: Enable Automatic Client Upgrade on page 2-15

Upgrade Method 1: Disable Automatic Client Upgrade
By disabling automatic client upgrade, you can upgrade the server first and then upgrade clients in groups. Use this upgrade method if you are upgrading a large number of clients.

Part 1: Configure update settings on the OfficeScan 10.x or 8.0 SP1 server
1. Go to Networked Computers > Client Management.
2. On the client tree, click the root domain icon to select all clients.
3. Click Settings > Privileges and Other Settings and go to the Other Settings tab.
4. Enable Clients can update components but not upgrade the client program or deploy hot fixes.
5. Click **Apply to All Clients**.

**Tip:** It may take a while to deploy the settings to online clients if you have a complex network environment and a large number of clients. Before the upgrade, allocate sufficient time for settings to deploy to all clients. Clients that do not apply the settings will automatically upgrade.

### Part 2: Upgrade the OfficeScan server

See *The Setup Installation Screens* on page 2-20 for details on upgrading the OfficeScan server.

**Note:** To speed up the upgrade process, unload the OfficeScan client before upgrading an OfficeScan server running Windows Server 2008 Standard 64-bit.

Configure OfficeScan server settings using the web console immediately after completing the installation and before upgrading clients.

For detailed instructions on how to configure OfficeScan settings, refer to the *Administrator's Guide* or *OfficeScan Server Help*.

### Part 3: Upgrade OfficeScan clients

1. Go to **Updates > Networked Computers > Automatic Update** and ensure that the following options are enabled:
   - Initiate component update on clients immediately after the OfficeScan server downloads a new component.
   - Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)
2. Go to **Networked Computers > Client Management**.
3. On the client tree, select the clients that you want to upgrade. You can select one or several domains, or individual/all clients within a domain.
4. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
5. Disable **Clients can update components but not upgrade the client program or deploy hot fixes**.
6. Click Save.
7. Check the upgrade results.
   - Upgrade Results (Online Clients) on page 2-6
   - Upgrade Results (Offline Clients) on page 2-7
   - Upgrade Results (Roaming Clients) on page 2-7
8. Restart the client computers to finish upgrading the clients.
9. Repeat step 2 to step 8 until all clients have been upgraded.

Upgrade Results (Online Clients)

Note: Restart the client computers after the upgrade.

Automatic Upgrade
Online clients start to upgrade when any of the following events occur:
- The OfficeScan server downloads a new component and notifies clients to update.
- The client reloads.
- The client restarts and then connects to the OfficeScan server.
- A client computer running Windows Server 2003 or Windows XP Professional logs on to a server whose login script you modified using Login Script Setup (AutoPcc.exe).
- Schedule update runs on the client computer (only for clients with scheduled update privileges).

Manual Upgrade
If none of the above events have occurred, perform any of the following tasks to upgrade clients immediately:
- Create and deploy an EXE or MSI client package.

Note: See the Administrator's Guide for instructions on creating a client package.
- Instruct client users to run Update Now on the client computer.
• If the client computer runs Windows Server 2003, XP Professional, Server 2008, Vista™ (all editions except Vista Home), or 7™ (all editions except 7 Home) instruct the user to perform the following steps:
  • Connect to the server computer.
  • Navigate to `\<server computer name>\ofcscan`.
  • Launch `AutoPcc.exe`.
• If the client computer runs Windows XP Home, Vista Home, or 7 Home, instruct the user to right-click `AutoPcc.exe`, and select `Run as administrator`.
• Initiate manual client update.

To initiate manual client update:
2. Select the Manually select clients option and click Select.
3. In the client tree that opens, choose the clients to upgrade.
4. Click Initiate Component Update on top of the client tree.

Upgrade Results (Offline Clients)
Offline clients upgrade when they become online.

Upgrade Results (Roaming Clients)
Roaming clients upgrade when they become online or, if the client has scheduled update privileges, when scheduled update runs.
Upgrade Method 2: Upgrade Update Agents

Use this upgrade method if you have a large number of clients updating from Update Agents. These clients will upgrade from their respective Update Agents.

Clients that do not update from Update Agents will upgrade from the OfficeScan server.

Part 1: Configure update settings on the OfficeScan 10.x or 8.0 SP1 server

1. Go to Networked Computers > Client Management.
2. On the client tree, click the root domain icon  to select all clients.
3. Click Settings > Privileges and Other Settings and go to the Other Settings tab.
4. Enable Clients can update components but not upgrade the client program or deploy hot fixes.
5. Click Apply to All Clients.

Tip: It may take a while to deploy the settings to online clients if you have a complex network environment and a large number of clients. Before the upgrade, allocate sufficient time for settings to deploy to all clients. Clients that do not apply the settings will automatically upgrade.

Part 2: Upgrade the OfficeScan server

See The Setup Installation Screens on page 2-20 for details on upgrading the OfficeScan server.

Configure OfficeScan server settings using the web console immediately after completing the installation and before upgrading Update Agents.

For detailed instructions on how to configure OfficeScan settings, refer to the Administrator's Guide or OfficeScan Server Help.
Part 3: Upgrade Update Agents

1. Go to Networked Computers > Client Management.
2. On the client tree, select the Update Agents that you want to upgrade.

   **Tip:** To locate Update Agents easily, select a domain, go to the Client tree view on top of the client tree and then select Update agent view.

3. Click Settings > Privileges and Other Settings and go to the Other Settings tab.
4. Disable Clients can update components but not upgrade the client program or deploy hot fixes.
5. Click Save.
7. Select the Manually select clients option and click Select.
8. In the client tree that opens, choose the Update Agents to upgrade.

   **Tip:** To locate Update Agents easily, select a domain, go to the Client tree view on top of the client tree and then select Update agent view.

9. Click Initiate Component Update on top of the client tree.
10. Check the upgrade results.
    - Online Update Agents upgrade immediately after you initiated component update.
    - Offline Update Agents upgrade when they become online.
    - Roaming Update Agents upgrade when they become online or, if the Update Agent has scheduled update privileges, when scheduled update runs.
11. Restart the Update Agents’ computers to finish upgrading the agents.
12. Repeat step 1 to step 11 until all Update Agents have been upgraded.
Part 4: Configure Update Agent settings
1. Go to Networked Computers > Client Management.
2. Select Update Agents in the client tree.

   **Tip:** To locate Update Agents easily, select a domain, go to the Client tree view on top of the client tree and then select Update agent view.

3. Ensure that Update Agents have the latest components.
4. Click Settings > Update Agent Settings.
5. Select the following options:
   - Component updates
   - Domain settings
   - Client programs and hot fixes
6. Click Save. Wait for the Update Agent to finish downloading the client program before proceeding to Part 5.
7. Repeat step 1 to step 6 until all Update Agents have applied the necessary settings.

Part 5: Upgrade OfficeScan clients
1. Go to Updates > Networked Computers > Automatic Update and ensure that the following options are enabled:
   - Initiate component update on clients immediately after the OfficeScan server downloads a new component.
   - Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)
2. Go to Networked Computers > Client Management.
3. On the client tree, select the clients that you want to upgrade. You can select one or several domains, or individual/all clients within a domain.
4. Click Settings > Privileges and Other Settings and go to the Other Settings tab.
5. Disable Clients can update components but not upgrade the client program or deploy hot fixes.
6. Click Save.
7. Check the upgrade results.
   • Upgrade Results (Online Clients) on page 2-11
   • Upgrade Results (Offline Clients) on page 2-12
   • Upgrade Results (Roaming Clients) on page 2-12

8. Restart the client computers to finish upgrading the clients.

9. Repeat step 2 to step 8 until all clients have been upgraded.

**Upgrade Results (Online Clients)**

*Note:* Restart the client computers after the upgrade.

**Automatic Upgrade**

Online clients start to upgrade when any of the following events occur:

• The OfficeScan server downloads a new component and notifies clients to update.
• The client reloads.
• The client restarts and then connects to the OfficeScan server.
• A client computer running Windows Server 2003 or Windows XP Professional logs on to a server whose login script you modified using Login Script Setup (AutoPcc.exe).
• Schedule update runs on the client computer (only for clients with scheduled update privileges).

**Manual Upgrade**

If none of the above events have occurred, perform any of the following tasks to upgrade clients immediately:

• Create and deploy an EXE or MSI client package.

  *Note:* See the *Administrator's Guide* for instructions on creating a client package.

• Instruct client users to run **Update Now** on the client computer.
• If the client computer runs Windows Server 2003, XP Professional, Server 2008, Vista (all editions except Vista Home), or 7 (all editions except 7 Home), instruct the user to perform the following steps:
  • Connect to the server computer.
  • Navigate to \\<server computer name>\ofcscan.
  • Launch AutoPcc.exe.
• If the client computer runs Windows XP Home, Vista Home, or 7 Home, instruct the user to right-click AutoPcc.exe, and select Run as administrator.
• Initiate manual client update.

To initiate manual client update:
2. Select the Manually select clients option and click Select.
3. In the client tree that opens, choose the clients to upgrade.
4. Click Initiate Component Update on top of the client tree.

Upgrade Results (Offline Clients)
Offline clients upgrade when they become online.

Upgrade Results (Roaming Clients)
Roaming clients upgrade when they become online or, if the client has scheduled update privileges, when scheduled update runs.
Upgrade Method 3: Move Clients to an OfficeScan 10.6 Server

Perform a fresh installation of the OfficeScan 10.6 server and then move clients to this server. When you move the clients, they automatically upgrade to OfficeScan 10.6.

Part 1: Perform a fresh installation of the OfficeScan server and then configure update settings

1. Perform a fresh installation of the OfficeScan 10.6 server on a computer. For details, see The Setup Installation Screens on page 2-20.
2. Open the OfficeScan 10.6 web console.
3. Go to Updates > Networked Computers > Automatic Update and ensure that the following options are enabled:
   a. Initiate component update on clients immediately after the OfficeScan server downloads a new component.
   b. Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)
4. Go to Networked Computers > Client Management.
5. On the client tree, click the root domain icon 🚀 to select all clients.
6. Click Settings > Privileges and Other Settings and go to the Other Settings tab.
7. Disable Clients can update components but not upgrade the client program or deploy hot fixes.
8. Click Apply to All Clients.
9. Record the following OfficeScan 10.6 server information. Specify this information on the OfficeScan 10.x/8.0 SP1 server when moving clients:
   a. Computer name or IP address
   b. Server listening port
   To view the server listening port, go to Administration > Connection Settings. The port number displays on the screen.
Part 2: Upgrade OfficeScan clients

1. On the OfficeScan 10.x/8.0 SP1 web console, go to Updates > Summary.

2. Click Cancel Notification. This function clears the server notification queue, which will prevent problems moving clients to the OfficeScan 10.6 server.

   WARNING! Perform the succeeding steps immediately. If the server notification queue gets updated before you move clients, clients might not move successfully.


4. On the client tree, select the clients that you want to upgrade. Select only online clients because offline and roaming clients cannot be moved.

5. Click Manage Client Tree > Move Client.

6. Specify the OfficeScan 10.6 server computer name/IP address and server listening port under Move selected client(s) online to another OfficeScan Server.

7. Click Move.

Upgrade Results

- Online clients start to move and upgrade.
- Tips for managing offline and roaming clients:
  - Disable roaming mode on clients so you can upgrade them.
  - For offline clients, instruct users to connect to the network so that the client can become online. For clients that are offline for an extended period of time, instruct users to uninstall the client from the computer and then use a suitable client installation method (such as client packager) discussed in the OfficeScan Administrator's Guide to install the OfficeScan 10.6 client.

Note: Restart the client computers to finish upgrading the clients.
Upgrade Method 4: Enable Automatic Client Upgrade

After upgrading the OfficeScan server to this version, the server immediately notifies all clients it manages to upgrade.

If the server manages a small number of clients, consider allowing clients to upgrade immediately. You can also use the upgrade methods discussed previously.

Part 1: Configure update settings on the OfficeScan 10.x or 8.0 SP1 server

1. Go to Updates > Networked Computers > Automatic Update and ensure that the following options are enabled:
   - Initiate component update on clients immediately after the OfficeScan server downloads a new component.
   - Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)
2. Go to Networked Computers > Client Management.
3. On the client tree, click the root domain icon to select all clients.
4. Click Settings > Privileges and Other Settings and go to the Other Settings tab.
5. Disable Clients can update components but not upgrade the client program or deploy hot fixes.
6. Click Apply to All Clients.

Tip: Allocate sufficient time for settings to deploy to all clients before upgrading the OfficeScan server.

Part 2: Upgrade the OfficeScan server

See The Setup Installation Screens on page 2-20 for details on upgrading the OfficeScan server.
Upgrade Results

- Online clients upgrade immediately after server upgrade is complete.
- Offline clients upgrade when they become online.
- Roaming clients upgrade when they become online or, if the client has scheduled update privileges, when scheduled update runs.

*Note:* Restart the client computers to finish upgrading the clients.

Performing Silent Installation/Upgrade

Install or upgrade multiple OfficeScan servers silently if the servers will use identical installation settings.

When silent installation runs on the target computer, Setup installs OfficeScan 10.6 and Plug-in Manager 2.0. If an earlier OfficeScan or Plug-in Manager version exists, Setup performs an upgrade. Plug-in Manager 2.0 provides the widget functionality in OfficeScan.

Before upgrading the OfficeScan server and clients, take note of the following:

1. The installation package includes updates to OfficeScan firewall drivers. If you have enabled the OfficeScan firewall in your current OfficeScan version, deploying the package may cause the following client computer disruptions:
   - When Common Firewall Driver update starts, client computers will be temporarily disconnected from the network. Users are not notified before disconnection.

   An option on the OfficeScan 10 SP1 or later web console, which is enabled by default, postpones the Common Firewall Driver update until a client computer is restarted. To avoid the disconnection issue, ensure that this option is enabled. To check the status of this option, navigate to Networked Computers > Global Client Settings and go to the Firewall Settings section. The option is Update the OfficeScan firewall driver only after a system reboot.
• After deploying the package, the OfficeScan TDI driver's previous version still exists on the client computer and the new version will not be loaded until the computer is restarted. Users are likely to encounter problems with the OfficeScan client if they do not restart immediately.

If the option to display the restart notification message is enabled on the web console, users will be prompted to restart. However, users who decide to postpone the restart are not prompted again. If the option is disabled, users are not notified at all.

The option to display the restart notification message is enabled by default. To check the status of this option, navigate to Networked Computers > Global Client Settings and go to the Alert Settings section. The option is Display a notification message if the client computer needs to restart to load a kernel mode driver.

2. The OfficeScan server cannot upgrade to this version if a client is running Login Script (AutoPcc.exe) at the time of server upgrade. Ensure that no client is running Login Script before upgrading the server.

Silent installation involves two procedures:

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

   Important:
   • Setup only shows screens for local installation (fresh installation or upgrade). See The Setup Installation Screens on page 2-20 for the relevant screens that will display.
   • If you plan to upgrade OfficeScan servers to this version, create the response file from a computer with an OfficeScan server installed.
   • If you plan to perform a fresh installation, create a response file from a computer without an OfficeScan server installed.

2. Run Setup from a command prompt and point Setup to the location of the response file to use for silent installation.
To record Setup configuration to a response file:

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

1. Open a command prompt and type the directory of the OfficeScan `setup.exe` file. For example, "CD C:\OfficeScan Installer\setup.exe".
2. Type the following:
   ```
   setup.exe -r
   ```
   The `-r` parameter triggers Setup to launch and record the installation details to a response file.
3. Perform the installation steps in Setup.
4. After completing the steps, check the response file `setup.iss` in `%windir%`.

To run silent installation:

1. Copy the installation package and `setup.iss` to the target computer.
2. In the target computer, open a command prompt and type the directory of the installation package.
3. Type the following:
   ```
   setup.exe -s <-f1path>setup.iss <-f2path>setup.log
   ```
   For example: `C:\setup.exe -s -f1C:\setup.iss -f2C:\setup.log`
   Where:
   - `-s`: Triggers Setup to perform a silent installation
   - `<-f1path>setup.iss`: Location of the response file. If the path contains spaces, enclose the path with quotes ("). For example, `-f1"C:\osce script\setup.iss"`.
   - `<-f2path>setup.log`: Location of the log file that Setup will create after installation. If the path contains spaces, enclose the path with quotes ("). For example, `-f2"C:\osce log\setup.log"`.
4. Press Enter. Setup silently installs the server to the computer.
5. To determine if installation was successful, check the OfficeScan program shortcuts on the target computer. If the shortcuts are not available, retry the installation.
Upgrading from an Evaluation Version

When the evaluation version is about to expire, OfficeScan displays a notification message on the Summary screen. Upgrade from an evaluation version to the full version of OfficeScan through the web console without losing any configuration settings. When you have a full version license, you will receive a Registration Key or an Activation Code.

**To upgrade from an evaluation version:**

1. Open the OfficeScan web console.
2. Click **Administration > Product License**. The Product License screen appears.
3. If you have an Activation Code, type it in the **New Activation Code** field and click **Save**.
4. If you do not have an Activation Code, click **Register Online** and use the Registration Key to obtain an Activation Code.
The Setup Installation Screens

Below is a list of the installation screens (arranged sequentially) that display when you install or upgrade the OfficeScan server locally, remotely, or silently.

**TABLE 2-1. Installation Screens and Tasks**

<table>
<thead>
<tr>
<th>SCREENS</th>
<th>LOCAL/SILENT FRESH INSTALL</th>
<th>REMOTE FRESH INSTALL</th>
<th>LOCAL/SILENT UPGRADE</th>
<th>REMOTE UPGRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>License Agreement</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Client Deployment</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>OfficeScan Server Settings</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Installation Destination</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Prescan</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Setup Status (Computer Analysis)</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Note:** Analysis may take some time to complete, especially during HTTP server initialization.

| Installation Path | ✔️ | ✔️ | ✔️ |
| Proxy Settings     | ✔️ | ✔️ | ✔️ |
### Table 2-1. Installation Screens and Tasks (Continued)

<table>
<thead>
<tr>
<th>Screens</th>
<th>Local/Silent Fresh Install</th>
<th>Remote Fresh Install</th>
<th>Local/Silent Upgrade</th>
<th>Remote Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server Settings</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Server Computer Identification</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Registration and Activation</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Integrated Smart Protection Server Installation</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Enable Web Reputation Services</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Remote Installation Destination</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Target Computer Analysis</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>OfficeScan Programs</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Cisco Trust Agent Installation/Upgrade</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Cisco Trust Agent License</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Trend Micro Smart Protection Network</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Administrator Account Password</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Client Installation Path</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>SCREENS</td>
<td>LOCAL/SILENT FRESH INSTALL</td>
<td>REMOTE FRESH INSTALL</td>
<td>LOCAL/SILENT UPGRADE</td>
<td>REMOTE UPGRADE</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------</td>
<td>----------------------</td>
<td>----------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Antivirus Features</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-spyware Feature</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Reputation Policy</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program Folder Shortcut</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation Information</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OfficeScan Server Installation</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Server Installation</td>
<td>❏</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OfficeScan Server Installation Completion</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
license

License Agreement

![License Agreement screen](image)

**FIGURE 2-1.** License Agreement screen

Read the license agreement carefully and accept the license agreement terms to proceed with installation. Installation cannot proceed if you do not accept the license agreement terms.
Client Deployment

There are several methods for installing or upgrading OfficeScan clients. This screen lists the different deployment methods and approximate network bandwidth needed. These measurements will change if the OfficeScan server is updated because OfficeScan components currently available in the server will be included in the client installation package.

Use this screen to estimate the size required on the servers and the amount of bandwidth that will be consumed when deploying clients to the target endpoints.
Note: All these installation methods require local administrator rights on the target computers.

usage

OfficeScan Server Settings

If you are upgrading to this version of OfficeScan, Trend Micro recommends backing up the OfficeScan server settings before upgrading.

If you have installed Trend Micro Control Manager, you can use its configuration replication feature to apply the settings of another OfficeScan server to this server. See the Control Manager documentation for details.

If you are upgrading to this version of OfficeScan, Trend Micro recommends backing up the OfficeScan database from the OfficeScan web console. The OfficeScan server database contains all OfficeScan settings, including scan settings and privileges. When backing up the database, OfficeScan automatically defragments the database and repairs any possible corruption to the index file.
Do not use any other type of back up tool or application. For details on backing up the database, see OfficeScan Settings and Configurations (on page 1-13).

You can also use Trend Micro Control Manager to back up or replicate server settings. Use these server settings to either restore the OfficeScan server if any issues occur during upgrades, or copy the server settings to another OfficeScan server. For details, see the Trend Micro Control Manager Administrator's Guide.

**instdest**

**Installation Destination**

![Installation Destination screen](image)

**FIGURE 2-4. Installation Destination screen**

Run Setup and install the OfficeScan server either on the computer where you launched it or to other computer(s) on the network. If Setup detects an earlier version of OfficeScan on the target computer, it prompts you to upgrade. Only the following versions of OfficeScan can upgrade to this version:

- 10.5 Patch 1
• 10.5
• 10.0 Service Pack 1
• 10.0
• 8.0 Service Pack 1
Remote Installation/Upgrade Notes

If you install/upgrade remotely, Setup checks if the target computer meets the requirements for server installation/upgrade. Before you proceed:

• Ensure that you have administrator rights to the target computer.
• Record the computer's host name and logon credentials (user name and password).
• Verify that the target computers meet the requirements for installing the OfficeScan server.
• Ensure the computer has Microsoft IIS server 5.0 or later if using this as the web server. If you choose to use Apache web server, Setup automatically installs this server if not present in the target computer.

For local upgrades, OfficeScan preserves the original settings from the previous installation, including the server name, proxy server information, and port numbers. You cannot modify these settings when upgrading. Modify them after the upgrade from the OfficeScan web console.

For remote upgrades, you need to re-enter all the settings. However, these settings will be disregarded after the server upgrades because the server will use the previous version's settings.
Before the OfficeScan server installation commences, Setup can scan the target computer for viruses and malware. Setup scans the most vulnerable areas of the computer, which include the following:

- Boot area and boot directory (for boot viruses)
- Windows folder
- Program Files folder
Setup can perform the following actions against detected virus/malware and Trojan horse programs:

- **Delete**: Deletes an infected file
- **Clean**: Cleans a cleanable file before allowing full access to the file, or lets the specified next action handle an uncleanable file.
- **Rename**: Changes the infected file's extension to "vir". Users cannot open the file initially, but can do so if they associate the file with a certain application. Virus/Malware may execute when opening the renamed infected file.
- **Pass**: Allows full access to the infected file without doing anything to the file. A user may copy/delete/open the file.

If you are performing a local installation, scanning occurs when you click Next. If you are performing a remote installation, scanning occurs right before the actual installation.
Installation Path

FIGURE 2-6. Installation Path screen

Accept the default installation path or specify a new one.

The installation path you specify applies only when you are performing a remote fresh installation. For remote upgrades, OfficeScan will use the previous version’s settings.
proxy

Proxy Settings

The OfficeScan server uses the HTTP protocol for client-server communication and to connect to the Trend Micro ActiveUpdate server and download updates. If a proxy server handles Internet traffic on the network, OfficeScan needs the proxy settings to ensure that the server can download updates from the ActiveUpdate server.

You can skip specifying proxy settings during installation and do so after installation from the OfficeScan web console.

Proxy settings apply only if you are performing a remote fresh installation. For remote upgrade, OfficeScan will use the previous version’s settings.

FIGURE 2-7. Proxy Server screen
IPv6 Support

If you are installing the OfficeScan server on a pure IPv6 computer, set up a dual-stack proxy server that can convert between IP addresses. This allows the server to connect to the ActiveUpdate server successfully.

wserver

Web Server Settings

The OfficeScan web server hosts the web console, allows the administrator to run console Common Gateway Interfaces (CGIs), and accepts commands from clients. The web server converts these commands to client CGIs and forwards them to the OfficeScan Master Service.
Web server settings only apply if you are performing a remote fresh installation. If you are performing a remote upgrade, OfficeScan will use the previous version’s settings.

**IPv6 Support**

For fresh installations, select IIS server to enable IPv6 support. Apache web server does not support IPv6 addressing. If the target computer only has an IPv6 address and you choose Apache, the installation will not proceed. If the target computer has both IPv6 and IPv4 addresses, you can choose Apache but IPv6 support will not be enabled after the server is installed.

If you are upgrading to this OfficeScan version, the OfficeScan server to be upgraded must already be using IIS. If the server is using Apache, configure it to use IIS before the upgrade.

**Web Server**

If Setup detects both IIS and Apache web servers installed on the target computer, you may choose either of the two web servers. If neither exists on the target computer, you cannot select IIS and OfficeScan installs Apache web server 2.0.63 automatically.

*If using an Apache web server:*

- Apache web server 2.0.x is required. If Apache web server exists on the computer but the version is not 2.0.x, OfficeScan will install and use version 2.0.63. The existing Apache web server is not removed.
- If enabling SSL and Apache web server 2.0.x exists, the Apache web server must have SSL settings preconfigured.
- By default, the administrator account is the only account created on the Apache web server.

*Tip:* 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 website for the latest information on upgrades, patches, and security issues.
If using an IIS web server:

- The following Microsoft Internet Information Server (IIS) versions are required:
  - Version 6.0 on Windows Server 2003
  - Version 7.0 on Windows Server 2008
  - Version 7.5 on Windows Server 2008 R2
- Do not install the web server on a computer running IIS-locking applications because this could prevent successful installation. See the IIS documentation for more information.

**HTTP Port**

The web server listens for client requests on the HTTP port and forwards these requests to the OfficeScan Master Service. This service returns information to clients at the designated client communication port. Setup randomly generates the client communication port number during installation.

**SSL Support**

Enable Secure Sockets Layer (SSL) if you want secure communication between the web console and the server. SSL provides an extra layer of protection against hackers. Although OfficeScan encrypts the passwords specified on the web console before sending them to the OfficeScan server, hackers can still sniff the packet and, without decrypting the packet, "replay" it to gain access to the console. SSL tunneling prevents hackers from sniffing packets traversing the network.

The SSL version used depends on the version that the web server supports.

When you select SSL, Setup automatically creates an SSL certificate, which is a requirement for SSL connections. The certificate contains server information, public key, and private key.

The SSL certificate should have a validity period between 1 and 20 years. The administrator can still use the certificate after it expires. However, a warning message appears every time SSL connection is invoked using the same certificate.
How communication through SSL works:
1. The administrator sends information from the web console to the web server through SSL connection.
2. The web server responds to the web console with the required certificate.
3. The browser performs key exchange using RSA encryption.
4. The web console sends data to the web server using RC4 encryption.

Although RSA encryption is more secure, it slows down the communication flow. Therefore, it is only used for key exchange, and RC4, a faster alternative, is used for data transfer.

**Web Server Ports**
The following table lists the default port numbers for the web server:

**TABLE 2-1. Port Numbers for the OfficeScan Web Server**

<table>
<thead>
<tr>
<th>Web Server and Settings</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HTTP</td>
</tr>
<tr>
<td>Apache web server with SSL enabled</td>
<td>8080 (configurable)</td>
</tr>
<tr>
<td>Apache web server with SSL disabled</td>
<td>8080 (configurable)</td>
</tr>
<tr>
<td>IIS default website with SSL enabled</td>
<td>80 (not configurable)</td>
</tr>
<tr>
<td>IIS default website with SSL disabled</td>
<td>80 (not configurable)</td>
</tr>
<tr>
<td>IIS virtual website with SSL enabled</td>
<td>8080 (configurable)</td>
</tr>
<tr>
<td>IIS virtual website with SSL disabled</td>
<td>8080 (configurable)</td>
</tr>
</tbody>
</table>
The option you select on this screen applies only if you are performing a remote fresh installation. For remote upgrade, OfficeScan will use the previous version's settings.

Specify if OfficeScan clients will identify the server computer by its host (domain) name or IP address.

If the server computer is identified by IP address and you change its IP address, the OfficeScan server and clients will not be able to communicate. The only way to restore communication is to redeploy all the clients. The same situation applies if the server computer is identified by a host name and you change its host name.
In most networks, the server computer's IP address is more likely to change than its host name, thus it is usually preferable to identify the server computer by a host name. Changing the IP address is also not recommended if OfficeScan obtains an IP address from a DHCP server.

If you use static IP addresses, identify the server by its IP address. In addition, if the server computer has multiple network interface cards (NICs), consider using one of the IP addresses instead of the host name to ensure successful client-server communication.

**IPV6 Support**

If the server will manage IPv4 and IPv6 clients, it must have both IPv4 and IPv6 addresses and must be identified by its host name. If a server is identified by its IPv4 address, IPv6 clients cannot connect to the server. The same issue occurs if pure IPv4 clients connect to a server identified by its IPv6 address.

If the server will manage only IPv6 clients, the minimum requirement is an IPv6 address. The server can be identified by its host name or IPv6 address. When the server is identified by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.

---

**Note:** The FQDN can only be specified when performing a local installation of the server. It is not supported on remote installations.
Registration and Activation

Register OfficeScan using the Registration Key that came with the product and then obtain the Activation Codes. If you already registered and received the Activation Codes, skip this step.

If you do not have the Activation Codes, click **Register Online**. Setup directs you to the Trend Micro registration website. After you complete the registration form, Trend Micro sends an email with the Activation Codes. You can then continue with the installation process.
If you are installing the OfficeScan server on a pure IPv6 computer, set up a dual-stack proxy server that can convert between IP addresses. This allows the server to connect to the Trend Micro registration website successfully.

**FIGURE 2-11. Product Activation screen**

If you already have the Activation Codes, continue with the installation process and specify the codes. The Activation Codes are case-sensitive.

If you obtained an Activation Code that is valid for all services:

1. Select **Use the same Activation Code for Damage Cleanup Services and Web Reputation and Anti-spyware**.
2. Type the Activation Code in the **Antivirus** text box.
**Integrated Smart Protection Server Installation**

Setup will install the integrated Smart Protection Server on the target computer. The integrated server provides File Reputation Services and Web Reputation Services. It is managed from within the OfficeScan web console.

Trend Micro recommends installing the standalone Smart Protection Server, which has the same function as the integrated server but can serve more clients. The standalone server is installed separately.

Do you want to install the integrated server?
- No. I have installed a standalone server or plan to install it a later time.
- Yes. Install the integrated server.

**File Reputation Services settings:**
- **Certificate validity period:** 3
- **SSL port:** 4345

**FIGURE 2-12. Integrated Smart Protection Server Installation screen**

Setup can install the integrated Smart Protection Server on the target computer. The integrated server provides File Reputation Services to clients that use smart scan and Web Reputation Services to clients subject to web reputation policies. The integrated server is managed from within the OfficeScan web console.
Trend Micro recommends installing the standalone Smart Protection Server, which has the same functions as the integrated server but can serve more clients. The standalone server is installed separately and has its own management console. See the Trend Micro Smart Protection Server Administrator's Guide for information on the standalone server.

**Tip:** Because the integrated Smart Protection Server and the OfficeScan server run on the same computer, the computer’s performance may reduce significantly during peak traffic for the two servers. To reduce the traffic directed to the OfficeScan server computer, assign a standalone Smart Protection Server as the primary smart protection source and the integrated server as a backup source. See the Administrator's Guide for information on configuring smart protection sources for clients.

**Licenses**

Activate the licenses for the following services to use smart scan:

- Antivirus
- Web Reputation and Anti-spyware

See Registration and Activation on page 2-39 for more information on the OfficeScan licenses.

If you do not activate the licenses, you can still install the integrated Smart Protection Server but clients will not be able to use smart scan or connect to any Smart Protection Server. Contact your Trend Micro representative for license and activation concerns.

**Client Connection Protocols for File Reputation Services**

Clients can connect to the integrated Smart Protection Server’s File Reputation Services using HTTP and HTTPS. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

**Note:** If clients connect to the integrated server through a proxy server, you need to configure internal proxy settings from the web console. See the Administrator's Guide for information on configuring proxy settings.

The port numbers used for File Reputation Services depend on the web server (Apache or IIS) you want to use for the OfficeScan server. See Web Server Settings on page 2-33 for more information.
The HTTP port is not displayed on the installation screen. The HTTPS port is displayed and may or may not be configured.

**TABLE 2-2. Ports for the Integrated Smart Protection Server’s File Reputation Services**

<table>
<thead>
<tr>
<th><strong>WEB SERVER AND SETTINGS</strong></th>
<th><strong>PORTS FOR FILE REPUTATION SERVICES</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HTTP</td>
</tr>
<tr>
<td>Apache web server with SSL enabled</td>
<td>8080</td>
</tr>
<tr>
<td>Apache web server with SSL disabled</td>
<td>8080</td>
</tr>
<tr>
<td>IIS default website with SSL enabled</td>
<td>8082</td>
</tr>
<tr>
<td>IIS default website with SSL disabled</td>
<td>8082</td>
</tr>
<tr>
<td>IIS virtual website with SSL enabled</td>
<td>8082</td>
</tr>
<tr>
<td>IIS virtual website with SSL disabled</td>
<td>8082</td>
</tr>
</tbody>
</table>

**Integrated Server Not Installed**

If you are performing a fresh installation or upgrading from OfficeScan 8.0 SP1 and you chose not to install the integrated server:

- Conventional scan will become the default scan method.
- If you choose to enable web reputation policies in a separate installation screen (for details, see *Web Reputation Policy* on page 2-63), clients will not be able to send web reputation queries because it is assumed that no Smart Protection Server has been installed.
If a standalone server is available after installing or upgrading OfficeScan, perform the following tasks from the OfficeScan web console:

- Change the scan method to smart scan.
- Add the standalone server to the smart protection source list so that clients can send file and web reputation queries to the server.

If you are upgrading from an OfficeScan 10.x server where the integrated server has been disabled, the integrated server will not be installed. Clients retain their scan methods and the smart protection sources to which they send queries.

**wrepsvc**

**Enable Web Reputation Services**

![Enable Web Reputation Services](image)

*FIGURE 2-13. Enable Web Reputation Service screen*
Web Reputation Services evaluates the potential security risk of all requested URLs at the time of each HTTP request. Depending on rating returned by the database and the security level configured, web reputation either blocks or approves the request. The integrated Smart Protection Server installed with the OfficeScan server provides Web Reputation Services.

Enabling Web Reputation Services (running under the process name LWCSService.exe) helps reduce the overall bandwidth consumption. This is because OfficeScan clients obtain web reputation data from a local server, instead of connecting to the Smart Protection Network.

**Client Connection Protocols for Web Reputation Services**

Clients can connect to the integrated Smart Protection Server’s Web Reputation Services using HTTP.

The HTTP port number used for Web Reputation Services depends on the web server (Apache or IIS) you want to use for the OfficeScan server. See *Web Server Settings* on page 2-33 for more information.

**TABLE 2-3. Ports for the Integrated Smart Protection Server’s Web Reputation Services**

<table>
<thead>
<tr>
<th>WEB SERVER AND SETTINGS</th>
<th>HTTP PORT FOR WEB REPUTATION SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache web server with SSL enabled</td>
<td>8080 (not configurable)</td>
</tr>
<tr>
<td>Apache web server with SSL disabled</td>
<td>8080 (not configurable)</td>
</tr>
<tr>
<td>IIS default website with SSL enabled</td>
<td>80 (not configurable)</td>
</tr>
<tr>
<td>IIS default website with SSL disabled</td>
<td>80 (not configurable)</td>
</tr>
<tr>
<td>IIS virtual website with SSL enabled</td>
<td>5274 (configurable)</td>
</tr>
<tr>
<td>IIS virtual website with SSL disabled</td>
<td>5274 (configurable)</td>
</tr>
</tbody>
</table>
Remote Installation Destination

Specify the target computer to which you will install OfficeScan. You can manually type the computer's host name or IP address. Click **Browse** to search for computer(s) in the network.

You can also import computer name(s) from a text file by clicking **Import List**. If you install to multiple computers simultaneously and all computers pass the analysis, Setup installs the OfficeScan server in the order in which they are listed in the text file.

In the text file:

- Specify one computer name per line.
- Use the Unified Naming Convention (UNC) format (for example, `\test`).

**FIGURE 2-14. Remote Installation Destination screen**
• Use only the following characters: a-z, A-Z, 0-9, periods (.), and hyphens (-).
For example:
\\domain1\test-abc
\\domain2\test-123
\\domain3\test.xyz

Tips to ensure that remote installation can proceed:

- Ensure that you have administrator rights to the target computer.
- Record the computer's host name and logon credentials (user name and password).
- Verify that the target computers meet the system requirements for installing the OfficeScan server.
- Ensure the computer has Microsoft IIS server 5.0 or later if using this as the web server. If you choose to use Apache web server, Setup automatically installs this server if not present in the target computer.
- Do not specify the computer where you launched Setup as a target computer. Run local installation on the computer instead.

When you have specified the target computer(s), click **Next**. Setup checks if the computer(s) meet the OfficeScan installation requirements.
Target Computer Analysis

Before allowing remote installation to proceed, Setup needs to first determine if the target computer(s) you selected can install the OfficeScan server. To start the analysis, click Analyze. Setup may require you to provide the administrator user name and password used to log on to the target computer. After the analysis, Setup displays the result in the screen.

If you install to multiple computers, installation proceeds if at least one of the computers pass the analysis. Setup installs the OfficeScan server to that computer and ignores the ones that did not pass the analysis.

During remote installation, the installation progress only displays in the computer where you launched Setup and not on the target computer(s).
osprograms

OfficeScan Programs

Choose to install the following OfficeScan programs:

- OfficeScan client
- Policy Server for Cisco NAC
- Cisco Trust Agent

Note: If you are installing the OfficeScan server to a pure IPv6 computer, do not install Policy Server for Cisco NAC and Cisco Trust Agent. These programs do not support IPv6 addressing.
OfficeScan Client

The client program provides the actual protection against security risks. Therefore, to protect the OfficeScan server computer against security risks, it needs to also have the client program. Choosing to install the client during server installation is a convenient way to ensure that the server is automatically protected. It also removes the additional task of installing the client after server installation.

**Note:** Install the client to other computers on the network after server installation. See the *Administrator's Guide* for the client installation methods.

If you are upgrading OfficeScan, this screen does not display.

If a Trend Micro or third-party endpoint security software is currently installed on the server computer, OfficeScan may or may not be able to automatically uninstall the software and replace it with the OfficeScan client. Contact your support provider for a list of software that OfficeScan automatically uninstalls. If the software cannot be uninstalled automatically, manually uninstall it first before proceeding with OfficeScan installation.

Cisco Network Admission Control (NAC) Programs

Cisco NAC focuses on controlling security risks inside the network by enforcing admission privileges and antivirus and security policies. It allows client computers to communicate with the network about security issues.

Like OfficeScan, Cisco NAC has a server component (Policy Server for Cisco NAC) and a client component (Cisco Trust Agent or CTA). To use Cisco NAC, you need to have Cisco routers that support it and you need to connect to the Cisco Admission Control Server (ACS).

**Note:** Cisco NAC programs are unavailable if you do not activate the Antivirus service.

You cannot install/upgrade the Policy Server or CTA if performing a remote server installation. After performing a remote installation, install the CTA to clients from the OfficeScan web console, and the Policy Server by running the Policy Server installer from the OfficeScan Setup package. Refer to the *Administrator's Guide* for more information about Cisco NAC.
Policy Server for Cisco NAC

Similar to the OfficeScan web console, the Policy Server for Cisco NAC is a web-based console where you configure network admission policies. The Policy Server continually verifies that client pattern files and scan engines are up-to-date.

You may run the OfficeScan server and Policy Server on the same computer and the same default website, or install them on different computers. If installing them on the same computer, Setup can install them simultaneously during server installation or you can install the Policy Server later. If installing the Policy Server to another computer, run the Policy Server installer on that computer.

Access the Policy Server installer from the OfficeScan Setup package.

Cisco Trust Agent (CTA) for Cisco NAC

CTA, a program hosted within the OfficeScan server and installed to clients, enables the OfficeScan client to report antivirus information to Cisco ACS.

If you select this option during server installation, the OfficeScan server automatically installs CTA to all clients that the server will manage. In the next screen, Setup prompts you whether to install Cisco Trust Agent or Cisco Trust Agent Supplicant. The only difference between the two versions is that the Supplicant package provides layer 2 authentication for the computer and end user.

If you do not select this option, you can still install CTA to clients from the web console (Cisco NAC > Agent Deployment). However, you need to do this every time a new client is added to the server. Refer to the OfficeScan Server Help for information on installing CTA from the web console.

CTA installation requires a certificate file (.cer), which CTA uses to create an encrypted communication session with Cisco ACS. A Certificate Authority (CA) server generates the certificate file. Request a certificate file from your Trend Micro representative, and enter the certificate during server installation or from the web console (Cisco NAC > Client Certificate).
Cisco Trust Agent Installation/Upgrade

**FIGURE 2-17. Cisco Trust Agent Upgrade screen**

If you are performing a fresh installation, this screen displays only if you choose to install Cisco Trust Agent in the previous screen. Select the CTA package to install to clients.

If you are upgrading, this screen displays only if you have previously installed CTA. Choose whether to upgrade CTA to the current version (2.1). If upgrading, select the CTA upgrade package.

If you did not select to install CTA during server installation, you can still install it from the web console.
Cisco Trust Agent License

![Cisco Trust Agent License Agreement screen](image)

**FIGURE 2-18. Cisco Trust Agent License Agreement screen**

Read the license agreement carefully and accept the license agreement terms to proceed with installation.
Trend Micro Smart Protection Network

Trend Micro™ Smart Protection Network is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both local and hosted solutions to protect users whether they are on the network, at home, or on the go, using light-weight clients to access its unique in-the-cloud correlation of email, web and file reputation technologies, and threat databases. Customers’ protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users. The smart protection network solution leverages Smart Protection Network for in-the-cloud protection.

![Smart Protection Network screen](image)

**FIGURE 2-19.** Smart Protection Network screen
Smart Feedback

Trend Micro Smart Feedback provides communication between Trend Micro products and the company’s 24/7 threat research centers and technologies. Each new threat identified through a single customer's routine reputation check automatically updates all of Trend Micro's threat databases, blocking any subsequent customer encounters of a given threat. For example, routine reputation checks sent to Trend Micro Smart Protection Network. By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security. This is much like an automated neighborhood watch that involves the community in protection of others. The privacy of a customer's personal or business information is always protected because the threat information gathered is based on the reputation of the communication source.

Trend Micro Smart Feedback is designed to collect and transfer relevant data from clients' Trend Micro Smart Protection Server to Trend Micro back-end server side. So that further analysis can be conducted, and consequently, advanced solutions can evolve and be deployed to protect clients.

You can terminate your participation to the program anytime from the web console.

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com
Administrator Account Password

FIGURE 2-20. Administration Account Password screen

Specify passwords to perform the following:

Access the Web Console

Setup creates a root account during installation. The root account has full access to all OfficeScan web console functions. Logging on using this account also allows the administrator to create custom user accounts that other users can use to log on to the web console. Users can configure or view one or several web console functions depending on the access privileges for their accounts.

Specify a password known only to you and other OfficeScan administrators. If you forget the password, contact your support provider for help in resetting the password.
Unload and Uninstall the OfficeScan Client

Specify a password to prevent unauthorized uninstallation or unloading of the OfficeScan client. Uninstall or unload the client only if there are problems with client functions and promptly install/reload it.

**clinstpath**

Client Installation Path

![OfficeScan Client Installation Path screen](image)

The same installation path will be used for installing the OfficeScan client to all the computers that the OfficeScan server will manage. Please type the installation path below.

Warning: The installation path cannot be changed after setup is complete.

![ProgramFiles\Trend Micro\OfficeScan Client](image)

- Port number:
- Security level:
  - Normal: Assigns the access privileges already configured for the computer's Program Files and registry files to OfficeScan client files and registries.
  - High: Restricts access to OfficeScan client files and registries.

Accept the default client installation settings or specify a different client installation path. Change the path if there is insufficient disk space on the installation directory.

**Tip:** Trend Micro recommends using the default settings.
If specifying a different installation path, type a static path or use variables. If the path you type includes a directory that does not exist on the client, Setup creates the directory automatically during client installation.

To type a static client installation path, type the drive path, including the drive letter. For example, C:\Program Files\Trend Micro\OfficeScan Client.

**Note:** The client installation path cannot be modified after you finish installing the OfficeScan server. All OfficeScan clients that will be installed will use the same installation path.

When specifying variables for the client installation path, use the following:

- **$BOOTDISK:** The drive letter of the hard disk that the computer boots from, by default C:\
- **$WINDIR:** The Windows directory, by default C:\Windows
- **$ProgramFiles:** The Program Files directory automatically set up in Windows and usually used for installing software, by default C:\Program Files

Also on this screen, configure the following:

- **Port number:** Setup randomly generates this port number, which the OfficeScan server uses to communicate with clients. You can specify a different port number.
- **Client security level:** After installing OfficeScan, you can change the security level from the OfficeScan console (Networked Computers > Client Management > Settings > Privileges and Other Settings > Other Settings)
  - **Normal:** This permission grants all users (the user group "Everyone") full rights to the client program directory and client registry entries.
  - **High:** The client installation directory inherits the rights of the Program Files folder and the client's registry entries inherit permissions from the HKLM\Software key. For most Active Directory configurations, this automatically limits “normal” users (those without administrator privileges) to read-only access.
Avfeat

Antivirus Features

![Antivirus Features screen](image)

**Figure 2-22. Antivirus Features screen**

This screen displays only if you activate the Antivirus service.

**OfficeScan Firewall**

The OfficeScan firewall protects clients and servers on the network using stateful inspections, high performance network virus scans, and elimination. Create rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.

You can choose to disable the firewall and enable it later from the OfficeScan server web console.
Optionally enable the firewall on server platforms. If you are upgrading and the firewall service is already enabled on server platforms, select **Enable firewall on server platforms** so that OfficeScan does not disable the firewall service after the upgrade.

### asfeat

**Anti-spyware Feature**

![Anti-spyware Feature screen](image)

**FIGURE 2-23. Anti-spyware Feature screen**

This screen displays only if you activate the Web Reputation and Anti-spyware service. When in assessment mode, all clients managed by the server will log spyware/grayware detected during Manual Scan, Scheduled Scan, Real-time Scan, and Scan Now but will not clean spyware/grayware components. Cleaning terminates processes or deletes registries, files, cookies, and shortcuts.
Trend Micro provides assessment mode to allow you to evaluate items that Trend Micro detects as spyware/grayware and then configure the appropriate action based on your evaluation. For example, detected spyware/grayware that you do not consider a security risk can be added to the spyware/grayware approved list.

After the installation, refer to the *Administrator's Guide* for some recommended actions to take during assessment mode.

Configure assessment mode to take effect only for a certain period of time by specifying the number of weeks in this screen. After the installation, you can change assessment mode settings from the web console (*Networked Computers > Global Client Settings > Spyware/Grayware Settings*).
Web Reputation Policy

![Web Reputation Feature screen](image)

**FIGURE 2-24. Web Reputation Feature screen**

Web reputation policies dictate whether OfficeScan will block or allow access to a website. For details about policies, see the *Administrator’s Guide*.

Selecting **Enable web reputation policy** enables policies for internal and external clients installed on desktop platforms, such as Windows XP, Vista, and 7. Select **Enable web reputation policy on server platforms** if server platforms, such as Windows Server 2003 and Windows Server 2008, require the same level of web threat protection as desktop platforms.

Clients use the location criteria you have set in the web console’s Computer Location screen to determine their location and the policy to apply. Clients switch policies each time the location changes.
You can configure web reputation policy settings from the web console after installation. OfficeScan administrators typically configure a stricter policy for external clients.

Web reputation policies are granular settings in the OfficeScan client tree. You can enforce specific policies to client groups or individual clients. You can also enforce a single policy to all clients.

If you enable web reputation policies, be sure to install Smart Protection Servers (integrated or standalone) and add them to the smart protection source list on the OfficeScan web console. Clients send web reputation queries to the servers to verify the safety of websites that users are accessing.

**Note:** The integrated server is installed with the OfficeScan server. For details, see *Integrated Smart Protection Server Installation* on page 2-41. The standalone server is installed separately.
shortcut

Program Folder Shortcut

![Program shortcuts screen](image)

**FIGURE 2-25. Program shortcuts screen**

Accept the default folder name or specify a new one. You can also select an existing folder to which Setup adds the program shortcuts.
Installation Information

![Installation Information screen](image)

**Figure 2-26. Installation Information screen**

This screen provides a summary of the installation settings. Review the installation information and click **Back** to change any of the settings or options. To start the installation, click **Install**.
psinst

Policy Server Installation

FIGURE 2-27. Policy Server Installation screen

This screen displays if you chose to install Policy Server for Cisco NAC. The settings and options on the Policy Server installation screens that display are similar to most settings you specify during OfficeScan server installation.

- **License Agreement**: Accept the terms of the license agreement to proceed.
- **Installation Path**: Accept the default installation path or specify a location on the local computer where Policy Server will be installed.
- **Web Server**: Specify whether to use an IIS or Apache web server
- **Web Server Configuration**: Specify settings for the selected web server.
• **Web Console Password:** Specify the password to access the Policy Server console. The console is separate from the OfficeScan server console, although you can launch the console from OfficeScan.

• **ACS Server Authentication:** An ACS server receives OfficeScan client antivirus data from the client through the Network Access Device and passes it to an external user database for evaluation. Later in the process, the ACS server also passes the result of the evaluation, which may include instructions for the OfficeScan client, to the Network Access Device.

• **Installation Information:** Review the installation information.

**instcomp**

**OfficeScan Server Installation Completion**

![Installation Complete screen](image)

**FIGURE 2-28. Installation Complete screen**
When the installation is complete, view the readme file for basic information about the product and known issues.

You can also launch the web console to start configuring OfficeScan settings.

**Post-installation Tasks**

Perform the following post-installation tasks:

- *Verifying the Server Installation or Upgrade* on page 2-69
- *Updating OfficeScan Components* on page 2-72
- *Checking Default Settings* on page 2-73
- *Using Client Mover for Legacy Platforms* on page 2-74. Perform this task only if you have clients running Windows 95, 98, Me, NT, 2000, or Itanium architecture.
- *Registering OfficeScan to Control Manager* on page 2-77. Control Manager registration only applies to newly installed OfficeScan servers.

**Verifying the Server Installation or Upgrade**

After completing the installation or upgrade, verify the following:

<table>
<thead>
<tr>
<th>ITEM TO VERIFY</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OfficeScan server shortcuts</td>
<td>The Trend Micro OfficeScan server shortcuts appear on the Windows <em>Start</em> menu on the server computer.</td>
</tr>
<tr>
<td>Programs list</td>
<td><strong>Trend Micro OfficeScan Server</strong> is listed on the <em>Add/Remove Programs</em> list on the server computer’s Control Panel.</td>
</tr>
</tbody>
</table>
**TABLE 2-4.  Items to Verify After Installing or Upgrading OfficeScan (Continued)**

<table>
<thead>
<tr>
<th>ITEM TO VERIFY</th>
<th>DETAILS</th>
</tr>
</thead>
</table>
| OfficeScan web Console | Type the following URLs on the Internet Explorer browser:  
  - HTTP connection: http://<OfficeScan server name>:<port number>/OfficeScan  
  - HTTPS connection: https://<OfficeScan server name>:<port number>/OfficeScan  
  Where <OfficeScan server name> is the name or IP address of the OfficeScan server.  
The web console logon screen displays. |
The following OfficeScan server services display on the Microsoft Management Console:

- **OfficeScan Active Directory Integration Service**: This service displays if the Active Directory integration and Role-based Administration features work properly.

- **OfficeScan Control Manager Agent**: The status for this service should be "Started" if the OfficeScan server has been registered to Control Manager.

- **OfficeScan Master Service**: The status for this service should be "Started".

- **OfficeScan Plug-in Manager**: The status for this service should be "Started".

- **Trend Micro Smart Scan Server**: The status for this service should be "Started".

- **Trend Micro Local Web Classification Server**: The status for this service should be "Started" if Web Reputation Services was enabled during installation.

- **Trend Micro Policy Server for Cisco NAC**: The status for this service should be "Started" if Policy Server was installed.

When you open Windows Task Manager, DBServer.exe is running.

The server installation log, OFCMSAS.LOG, exists in %windir%.

The following registry key exists:

HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan
Verifying Integrated Smart Protection Server Installation

OfficeScan automatically installs the integrated Smart Protection Server during a fresh installation.

To verify the integrated Smart Protection Server installation:
1. On the OfficeScan server web console, navigate to Smart Protection > Smart Protection Sources.
2. Click the standard list link.
3. On the screen that opens, click Integrated Smart Protection Server.
4. On the screen that displays, click Test Connection. Connection with the integrated server should be successful.

Updating OfficeScan Components

After installing or upgrading OfficeScan, update components on the server.

Note: This section shows you how to perform a manual update. For information on scheduled update and update configurations, see the OfficeScan Server Help.

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

Checking Default Settings

OfficeScan installs with default settings. If these settings do not conform to your security requirements, modify the settings on the web console. Refer to the OfficeScan Server Help and Administrator's Guide for details on the settings available on the web console.

Scan Settings

OfficeScan provides several types of scans to protect computers from security risks. Modify the scan settings from the web console by going to Networked Computers > Client Management > Settings > {Scan Type}.

Global Client Settings

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

Client Privileges

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

cplat
Using Client Mover for Legacy Platforms

The OfficeScan client no longer supports the Windows 95, 98, Me, NT, or 2000 operating systems, and the Itanium architecture platform. If OfficeScan clients run any of these platforms and you upgraded the server that manages them to version 10.6:

- The OfficeScan clients will not be upgraded.
- The OfficeScan 10.6 server stops managing the clients. The clients' status becomes "Disconnected".
- The OfficeScan 10.6 server saves the clients’ information to a file named `unsupCln.txt`. Use this file to "move" clients to a server with the same version. Move means designating a new server to manage the clients.
- On the OfficeScan 10.6 server computer, run a tool called Client Mover for Legacy Platforms. This tool notifies clients that they will be managed by a new server and checks if clients were moved successfully. When clients receive the notification, they register to their new parent server.

To move clients:

1. Prepare a new parent server. This server’s version should be the same as the version of the clients to be moved.
2. Record the server’s computer name/IP address and server listening port. These details are required when you move the clients.
   
   Obtain the server listening port from the server’s web console by going to Administration > Web Server.
3. On the OfficeScan 10.6 server computer, navigate to `<Server Installation Folder>\PCCSRV\Admin\Utility\ClientMover` and run `clientmover.exe`. 


4. In the command window, type the following command:

ClientMover /P:<ExportDataPath> /S:<ServerIP:port> /N

Where:

- **ExportDataPath:** The path and file name of the file (unsupCln.txt) containing client information.
- **ServerIP:port:** The IP address and server listening port number of the new parent server.
- **/N:** A command that notifies and then moves the clients to the new parent server. This command is used in conjunction with the /V command.

For example:

ClientMover /P:"C:\Program Files\TrendMicro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:123.12.12.123:23456 /N

5. Use the /V command to verify that the tool successfully moved the clients. This command compares the IP addresses of the OfficeScan 10.6 server and the new parent server. If the IP addresses are the same, the tool was unable to move the clients.

For example:

ClientMover /P:"C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:123.12.12.123:23456 /V

6. To check the result:

   a. Access the resulting log in \PCCSRV\Private\. The log’s file name is unsupcln.txt.log.<date_time>.

      For example: unsupcln.txt.log.20080101_123202

   b. Also in the same folder, verify that OfficeScan updated and backed up the unsupcln.txt file. The backup file’s name is unsupcln.txt.bak.
Sample entry in the updated unsupcln.txt file:

------------------------------------------------------------
x12xx345-6xxx-78xx-xx91-234x567x8x91 1234567891 23456 0
------------------------------------------------------------

Where:

- "x12xx345-6xxx-78xx-xx91-234x567x8x91" is the client's GUID.
- "1234567891" is the client's IP address in decimal notation.
- "23456" is the client listening port.
- "0" is the result and it means notification was completed.

Other possible results:

- 1 = Client notification successful
- 2 = Client notification unsuccessful
- 3 = Verification successful
- 4 = Verification unsuccessful

Sample entry in the unsupcln.txt.log.<date_time> file:

------------------------------------------------------------
x12xx345-6xxx-78xx-xx91-234x567x8x91 123.12.12.123:23456
Unable to send the notification. Please check the network or client status.
------------------------------------------------------------

Where:

- "x12xx345-6xxx-78xx-xx91-234x567x8x91" is the client’s GUID.
- "123.12.12.123:23456" is the client’s IP address and listening port.
- Result is "Unable to send the notification. Please check the network or client status".

7. Use the /F command to force the notification or verification without checking the current client status.
Registering OfficeScan to Control Manager

If you want a Control Manager server to manage newly installed OfficeScan servers, register OfficeScan to Control Manager after installation. You can do so from the OfficeScan web console by going to Administration > Control Manager Settings. See the OfficeScan Server Help or OfficeScan Administrator’s Guide for the procedure.

Uninstallation and Rollback

If you experience problems with OfficeScan, you can:

- Use the uninstallation program to safely remove the OfficeScan server from the computer. Before uninstalling the server, move the clients it manages to another OfficeScan server.
- Roll back clients to version previous OfficeScan versions instead of uninstalling the OfficeScan server. See Rolling Back to Previous OfficeScan Versions on page 2-84.

OfficeScan Server Uninstallation

Use the uninstallation program to safely remove the OfficeScan server.

Before Uninstalling the OfficeScan Server

Before uninstalling the server, move the clients it manages to an OfficeScan server with the same version. Consider backing up the server database and configuration files if you plan to reinstall the server later.

Moving Clients to Another OfficeScan Server

The OfficeScan web console provides an option to move clients managed by the server to another OfficeScan server.
To move clients to another OfficeScan server:

1. Record the following information for the other OfficeScan server. You will need the information when you move the clients.
   - Computer name or IP address
   - Server listening port
     To view the server listening port, go to Administration > Connection Settings. The port number displays on the screen.

2. On the web console of the server you want to uninstall, go to Networked Computers > Client Management.

3. On the client tree, select the clients that you want to upgrade and then click Manage Client Tree > Move Client.

4. Under Move selected client(s) to another OfficeScan Server, specify the server computer name/IP address and server listening port of the other OfficeScan server.

5. Click Move.

If all clients were moved and are already being managed by the other OfficeScan server, it is safe to uninstall the OfficeScan server.

Backing Up and Restoring the OfficeScan Database and Configuration Files

Back up the OfficeScan database and important configuration files before uninstalling the OfficeScan server. Back up the OfficeScan server database to a location outside the OfficeScan program directory.

To back up and restore the OfficeScan database and configuration files:

1. Back up the database from the OfficeScan web console by going to Administration > Database Backup. See the Administrator's Guide or the OfficeScan Server Help for instructions.

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

2. Stop the OfficeScan Master Service from the Microsoft Management Console.
3. Manually back up the following files and folders found under `<Server installation folder>\PCCSRV`:
   - `ofcscan.ini`: Contains global client settings
   - `ous.ini`: Contains the update source table for antivirus component deployment
   - **Private folder**: Contains firewall and update source settings
   - `Web\tmOPP folder`: Contains Outbreak Prevention settings
   - `Pccnt\Common\OfcPfw*.dat`: Contains firewall settings
   - `Download\OfcPfw.dat`: Contains firewall deployment settings
   - **Log folder**: Contains system events and the connection verification logs
   - `Virus folder`: Contains quarantined files
   - **HTTPDB folder**: Contains the OfficeScan database

4. Uninstall the OfficeScan server. For details, see *OfficeScan Server Uninstallation* on page 2-77.

5. Perform a fresh installation. See *Performing a Fresh Installation of the OfficeScan Server* on page 2-2 for details.

6. After Setup finishes, open the Microsoft Management Console (click **Start > Run** and type **services.msc**).

7. Right-click **OfficeScan Master Service** and then click **Stop**.

8. Copy the backup files to the `<Server installation folder>\PCCSRV` folder on the target computer. This overwrites the OfficeScan server database and the relevant files and folders.

9. Restart the OfficeScan Master Service.
Uninstalling the OfficeScan Server

Use the uninstallation program to uninstall the OfficeScan server and the integrated Smart Protection Server.

If you encounter problems with the uninstallation program, manually uninstall the server.

Note: For OfficeScan client uninstallation instructions, see the Administrator’s Guide.

To uninstall the OfficeScan server using the uninstallation program:

1. If you performed a fresh installation on the server computer, skip this step.
   If you upgraded the server from an earlier version to this version:
   a. If Plug-in Manager is currently installed, uninstall Plug-in Manager.
   b. If Plug-in Manager is not installed, delete the AOS registry key found in HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\.

2. Run the uninstallation program. There are two ways to access the uninstallation program.

   Method A
   a. On the OfficeScan server computer, click Start > Programs > Trend Micro OfficeScan Server > Uninstall OfficeScan. A confirmation screen appears.
   b. Click Yes. The server uninstallation program prompts you for the administrator password.
   c. Type the administrator password and click OK. The server uninstallation program starts removing the server files. A confirmation message appears.
   d. Click OK to close the uninstallation program.
Method B

a. Double-click the OfficeScan server program on the Windows Add/Remove Programs screen.

b. Click Control Panel > Add or Remove Programs. Locate and double-click "Trend Micro OfficeScan Server". Follow the on-screen instructions until you are prompted for the administrator password.

c. Type the administrator password and click OK. The server uninstallation program starts removing the server files. A confirmation message appears.

d. Click OK to close the uninstallation program.

To manually uninstall the server:

Part 1: Integrated Smart Protection Server uninstallation

1. Open the Microsoft Management Console and stop the OfficeScan Master Service.
2. Open a command prompt and then go to \<Server installation folder>\PCCSRV.
3. Run the following command:

   \SVRSVCSETUP.EXE -uninstall

   This command uninstalls OfficeScan-related services but does not remove configuration files or the OfficeScan database.
4. Navigate to \<Server installation folder>\PCCSRV\private and open ofcserver.ini.
5. Modify the following settings:

   **TABLE 2-5. ofcserver.ini Settings**

<table>
<thead>
<tr>
<th>SETTING</th>
<th>INSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSS_INSTALL=1</td>
<td>Change 1 to 0</td>
</tr>
<tr>
<td>WSS_ENABLE=1</td>
<td>Delete this line</td>
</tr>
<tr>
<td>WSS_URL=https://&lt;computer_name&gt;:4345/tmcss/</td>
<td>Delete this line</td>
</tr>
</tbody>
</table>
6. Navigate to `<Server installation folder>\PCCSRV` and open `OfUninst.ini`. Delete the following lines:
   - If using IIS web server:
     ```ini
     [WSS_WEB_SERVER]
     ServerPort=8082
     IIS_VhostName=Smart Protection Server (Integrated)
     IIS_VHostIdx=5
     ```
   
   **Note:** The value for IIS_VHostIdx should be the same as the "isapi" value indicated on the following line:
   ```ini
   ROOT=/tmcss,C:\Program Files\Trend Micro\OfficeScan\PCCSRV\WSS\isapi,,<value>
   ```
   ```ini
   [WSS_SSL]
   SSLPort=<SSL port>
   ```
   - If using Apache web server:
     ```ini
     [WSS_WEB_SERVER]
     ServerPort=8082
     [WSS_SSL]
     SSLPort=<SSL port>
     ```

7. Open a command prompt and then go to `<Server installation folder>\PCCSRV`.

8. Run the following commands:
   ```bash
   Svrsvcsetup -install
   Svrsvcsetup -enablessl
   Svrsvcsetup -setprivilege
   ```

9. Verify that the following items were removed:
   - Trend Micro Smart Protection Server service from the Microsoft Management Console
   - Smart Protection Server performance counters
   - Smart Protection Server (Integrated) website
Part 2: OfficeScan server uninstallation

1. Open Registry Editor and perform the following steps:

   **WARNING!** The next steps require you to delete registry keys. Making incorrect changes to the registry can cause serious system problems. Always make a backup copy before making any registry changes. For more information, refer to the Registry Editor Help.

   a. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\. 
   b. Verify that the ofcservice hive has been deleted. 
   c. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\ and delete the OfficeScan hive. 
      For 64-bit computers, the path is HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\. 
   d. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ and delete the OfficeScan Management Console-<Server Name> folder.

2. Navigate to <Server installation folder>\PCCSRV folder and unshare the PCCSRV folder.

3. Restart the server computer.

4. Navigate to <Server installation folder>\PCCSRV and delete the PCCSRV folder.

5. Delete the OfficeScan website from the Internet Information Services (IIS) console.
   a. Open the IIS console.
   b. Expand ServerName. 
   c. If you installed OfficeScan on a separate website, go to the Web Sites folder and then delete OfficeScan.
   d. If you installed OfficeScan virtual directories under the default website, go to Default Web Site and then delete the OfficeScan virtual directory.
Rolling Back to Previous OfficeScan Versions

If you encounter problems upgrading OfficeScan clients, you can roll back the clients to their previous version.

To roll back successfully, prepare the following:

- An OfficeScan server that will manage the clients that will be rolled back. The server version should be any of the following:
  - 10.5 Patch 1
  - 10.5
  - 10.0 Service Pack 1
  - 10.0
  - 8.0 Service Pack 1
- A computer that will act as update source. This update source contains the rollback files and components. When a client to be rolled back updates from this source, the client will be uninstalled and then the previous version of the client will be installed.
- The OfficeScan 10.6 server managing the clients to be rolled back
- The OfficeScan 10.6 clients to be rolled back

Part 1: Preparing the previous OfficeScan server version

1. Prepare a computer with the previous OfficeScan server version installed.
2. Apply the latest hot fixes, patches, or service packs for the previous OfficeScan server version.
3. Replicate the following OfficeScan 10.6 server settings to the previous OfficeScan server version.

   Consider the following settings:
   a. Client settings
      - Scan
      - Update Agents
      - Privileges
      - Spyware/Grayware Approved List (for OfficeScan 8.0 SP1 or later)
      - Behavior Monitoring Exception List (for OfficeScan 10.0 SP1 or later)
   b. Global client settings
c. Web Reputation settings (for OfficeScan 8.0 SP1 or later)
   • Computer location
   • Policies
   • Proxy

d. OfficeScan firewall settings
   • Policy
   • Profiles

e. Connection verification schedule

f. Update settings
   • Server scheduled update
   • Server update source
   • Client scheduled update
   • Client update source

g. Log maintenance settings

h. Notifications - all notification settings

i. Administration settings
   • Quarantine Manager
   • Control Manager
   • Database backup

4. On the previous OfficeScan server version, run Client Packager twice to create two client installation packages, one for x86 computers and another for x64 computers.

   Settings on the client installation package for x86 computers:
   • Package type: Setup
   • Windows operating system type: 32-bit
   • Output file: InstNTPkg.exe
Settings on the client installation package for x64 computers:
• Package type: Setup
• Windows operating system type: 64-bit
• Output file: InstNTPkg.exe

Because the two output files have the same file name, save them to separate locations so that one file does not overwrite the other.

**Part 2: Preparing an update source for clients that will be rolled back**

1. Prepare a computer that will act as update source.

2. On the OfficeScan 10.6 server computer, navigate to `<Server Installation Folder>\PCCSRV` and copy the **Download** folder (including subfolders) to the update source computer (the computer prepared in the previous step).

   For example, copy the **Download** folder to the following directory on the update source computer:

   C:\OfficeScanUpdateSource

3. On the OfficeScan 10.6 server computer:
   a. Create a temporary folder.
   b. Navigate to `<Server Installation Folder>\PCCSRV\Admin` and copy the following files to the temporary folder:
      • RollbackAgent.dll
      • RollbackAgent_64x.dll
      • ClientRollback.exe
   c. In the temporary folder, compress RollbackAgent.dll as RollbackAgent.zip.
   d. In the temporary folder, compress RollbackAgent_64x.dll as RollbackAgent_64x.zip.
   e. Create a subfolder in the temporary folder and name it RollBackNTPkg.
   f. Copy the following files to the RollBackNTPkg subfolder:
      • ClientRollback.exe
      • The client installation package for x86 computers (InstPkg.exe) created in Part 1, step 4
g. Compress the RollbackNTPkg subfolder as RollbackNTPkg.zip.

h. Create a subfolder in the temporary folder and name it RollBackNTPkgx64.

i. Copy the following files to the RollBackNTPkgx64 subfolder:
   - ClientRollback.exe
   - The client installation package for x64 computers (InstPkg.exe) created in Part 1, step 4

j. Compress the RollbackNTPkgx64 subfolder as RollbackNTPkgx64.zip.

k. Copy the following compressed files from the temporary folder to the update source computer:
   - RollbackAgent.zip
   - RollbackAgent_64x.zip
   - RollbackNTPkg.zip
   - RollbackNTPkgx64.zip

Note: Copy the files to the \\Download\\Product folder on the update source computer. For example, copy the files to C:\OfficeScanUpdateSource\Download\Product.

4. On the update source computer:

a. Ensure that the "Internet Guest Account" has read access to the following compressed files in \\Download\\Product (for example, C:\OfficeScanUpdateSource\Download\Product):
   - RollbackAgent.zip
   - RollbackAgent_64x.zip
   - RollbackNTPkg.zip
   - RollbackNTPkgx64.zip

Tip: To check the access permission, right-click each file and select Properties. In the Security tab, the permission for Internet Guest Account should be "Read".
b. In the \Download\Product folder, open the server.ini file using a text editor such as Notepad.

c. Modify the following lines in the server.ini file and then save the file:

WARNING!  Do not change any other settings in the server.ini file.

[All_Product]
MaxProductID=109
Product.109=OfficeScan Rollback, 3.5, <Current OfficeScan version>

[Info_109_35000_1_1]
Version=<Previous OfficeScan version>
Update_Path=product/RollbackAgent.zip, <RollbackAgent file size>
Path=product/RollBackNTPkg.zip, <RollBackNTPkg file size>

[Info_109_35000_1_5633]
Version=<Previous OfficeScan version>
Update_Path=product/RollbackAgent_64x.zip, <RollbackAgent64 file size>
Path=product/RollBackNTPkgx64.zip, <RollBackNTPkg64 file size>

Where:
•  <RollbackAgent file size>: File size of "RollbackAgent.zip" in bytes. For example, 90517.
•  <RollBackNTPkg file size>: File size of "RollbackNTPkg.zip" in bytes. For example, 32058256.
•  <RollbackAgent64 file size>: File size of "RollbackAgent_64x.zip" in bytes. For example, 90517.
Part 3: Rolling back the OfficeScan clients

1. On the OfficeScan 10.6 web console:
   a. Go to Updates > Networked Computers > Update Source.
   b. Select Customized Update Source.
   d. Type the IP addresses of the clients to be rolled back.
   e. Type the update source URL. For example, type:
      http://<IP address of update source>/OfficeScanUpdateSource/
   f. Click Save. The screen closes.
   g. Click Notify All Clients.

When a client to be rolled back updates from the update source, the client will be uninstalled and the previous client version will be installed.

2. After the previous client version is installed, inform the user to restart the computer. After the restart, the client will report to the OfficeScan server prepared in Part 1.
Getting Help

This chapter describes troubleshooting issues that may arise and how to contact support.

Topics in this chapter:

- *Troubleshooting Resources* on page 3-2
- *Contacting Trend Micro* on page 3-8
Troubleshooting Resources

Support Intelligence System
Support Intelligence System is a page wherein you can easily send files to Trend Micro for analysis. This system determines the OfficeScan server GUID and sends that information with the file you send. Providing the GUID ensures that Trend Micro can provide feedback regarding the files sent for assessment.

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

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

Trend Micro Performance Tuning Tool
Trend Micro provides a standalone performance tuning tool to identify applications that could potentially cause performance issues. The Trend Micro Performance Tuning Tool should be run on a standard workstation image and/or a few target workstations during the pilot process to preempt performance issues in the actual deployment of Behavioral Monitoring and Device Control.

Note: The Trend Micro Performance Tuning Tool only supports 32-bit platforms.
To identify system-intensive applications:

1. Download Trend Micro Performance Tuning Tool from:
   

2. Unzip TMPftool.zip to extract TMPftool.exe.

3. Place TMPftool.exe in the <Client installation folder> or in the same folder as TMBMCLI.dll.

4. Right-click TMPftool.exe and select Run as administrator.

5. Read and accept the end user agreement and then click OK.

6. Click Analyze. The tool starts to monitor CPU usage and event loading. A system-intensive process is highlighted in red.

   ![Screen capture of the Trend Micro Performance Tuning Tool](image)

   **FIGURE 3-1.** System-intensive process highlighted

7. Select a system-intensive process and click the Add to the exception list (allow) button.
8. Check if the system or application performance improves.
9. If the performance improves, select the process again and click the Remove from the exception list button.
10. If the performance drops again, perform the following steps:
   a. Note the name of the application.
   b. Click Stop.
   c. Click the Generate report button and then save the .xml file.
   d. Review the applications that have been identified as conflicting and add them to the Behavior Monitoring exception list. For details, see the Administrator’s Guide.

**Installation Logs**

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

**TABLE 3-1. Installation Log Files**

<table>
<thead>
<tr>
<th>LOG FILE</th>
<th>FILE NAME</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server local installation/upgrade log</td>
<td>OFCMAS.LOG</td>
<td>%windir%</td>
</tr>
<tr>
<td>Server remote installation/upgrade log</td>
<td>OFCMAS.LOG (On the computer where you launched Setup)</td>
<td>%windir%</td>
</tr>
<tr>
<td></td>
<td>OFCMAS.LOG (On the target computer)</td>
<td>%windir%</td>
</tr>
<tr>
<td>Client installation log</td>
<td>OFCNT.LOG</td>
<td>%windir% (For all installation methods except MSI package)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%temp% (For the MSI package installation method)</td>
</tr>
</tbody>
</table>
Server Debug Logs

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

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

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

To enable debug logging on the OfficeScan server computer:

Option 1:
1. Log on to the web console.
2. On the banner of the web console, click the first "c" in "OfficeScan". This opens the Debug Log Setting screen.
4. Click Save.
5. Check the log file (ofcdebug.log) in the default location: <Server installation folder>\PCCSRV\Log.
Option 2:

1. Copy the "LogServer" folder located in <Server installation folder>\PCCSRV\Private to C:.

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

   [debug]
   DebugLevel=9
   DebugLog=C:\LogServer\ofcdebug.log
   debugLevel_new=D
   debugSplitSize=10485760
   debugSplitPeriod=12
   debugRemoveAfterSplit=1

3. Save ofcdebug.ini to C:\LogServer.

4. Perform the appropriate task (that is, uninstall/reinstall the server, upgrade to a new server version, or perform a remote installation/upgrade).

5. Check ofcdebug.log in C:\LogServer.

---

**Note:** If an OfficeScan client is present on the OfficeScan server, then the client will also output its debug logs in the server's debug logs.
Client Debug Logs

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

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

To enable debug logging on the OfficeScan client computer:

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

   [Debug]
   Debuglog=C:\ofcdebug.log
   debuglevel=9
   debugLevel_new=D
   debugSplitSize=10485760
   debugSplitPeriod=12
   debugRemoveAfterSplit=1

2. Send ofcdebug.ini to client users, instructing them to save the file to C:\.

   LogServer.exe automatically runs each time the client computer starts. Instruct users NOT to close the LogServer.exe command window that opens when the computer starts as this prompts OfficeScan to stop debug logging. If users close the command window, they can start debug logging again by running LogServer.exe located in \OfficeScan Client.

3. For each client computer, check ofcdebug.log in C:\.

4. To disable debug logging for the OfficeScan client, delete ofcdebug.ini.
Contacting Trend Micro

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://esupport.trendmicro.com

• Get the latest Trend Micro product documentation at:

  http://docs.trendmicro.com

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:
http://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 website, 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](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℠ 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 website.

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 website 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 the following address and specify "Phish or Disease Vector" as the subject.

  virusresponse@trendmicro.com

• You can also use the web-based submission form at:

  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
Sample Deployment

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

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

![Basic network topology](image)

**FIGURE A-1.** Basic network topology
Multiple Site Network

For a network with multiple access points and multiple remote sites with different bandwidths:

• Analyze the consolidation points in terms of offices and network bandwidth.
• Determine the current bandwidth utilization for each office.

This presents a clearer picture as to how best to deploy OfficeScan. Figure A-2 illustrates a multiple site network topology.

**FIGURE A-2.** Multiple site network topology

Network information:

• Remote Site 1 WAN link averages around 70 percent utilization during business hours. There are 35 client computers on this site.
• Remote Site 2 WAN link averages around 40 percent utilization during business hours. There are 9 client computers on this site.
• Server 3 only functions as a file and print server for the group at Remote Site 1. This computer is a possible candidate for installing an OfficeScan server, but may not be worth the extra management overhead. All servers run Windows Server 2003. The network uses Active Directory, but mainly for network authentication.

• All client computers in Head Office, Remote Site 1, and Remote Site 2 run Windows Server 2003 or Windows XP.

Tasks:
1. Identify the computer where you will install the OfficeScan server. See *Performing a Fresh Installation of the OfficeScan Server* on page 2-2 for the installation procedure.
2. Identify the available client installation methods and eliminate methods that do not fit the requirement. See the *Administrator's Guide* for more information on the client installation methods.

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

• Remote installation from the web console
  
  This method is valid for all the LAN-connected computers at the head office. Because these computers all run Windows Server 2003, it is simple to deploy the package to the computers.

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

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

The easiest client deployment method to implement at the head office is remote installation from the OfficeScan web console. See the Administrator's Guide for the procedure.

Remote Site 1 Deployment

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

A suitable deployment method is the creation of a client package in Microsoft Installer Package (MSI) format and the deployment of the client package to the DFS. See the Administrator's Guide for the procedure. Since the package will be replicated to Server 3 during the next scheduled update, client package deployment has minimal bandwidth impact.

You can also deploy a client package through Active Directory. See the Administrator's Guide for details.

To minimize the impact of component updates across the WAN:

1. Designate a client to act as an Update Agent on Remote Site 1.
   a. Open the web console and go to Networked Computers > Client Management.
   b. In the client tree, select the client that will act as the Update Agent and click Settings > Update Agent Settings.

2. Select the clients in Remote Site 1 that will update components from the Update Agent.
   a. Go to Updates > Networked Computers > Update Source.
   b. Select Customized Update Source and click Add.
c. In the screen that displays, type the IP address range of the client computers in Remote Site 1.

d. Select **Update source** and then select the designated Update Agent from the drop-down list.

**Remote Site 2 Deployment**

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

The best way to install the OfficeScan client is to use the same client package in MSI format used in Remote Site 1. However, since there is no available server, you cannot use a Distributed File System (DFS).

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

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

These methods keep the installation traffic within the local network and minimizes the traffic across the WAN.

To minimize the impact of component updates across the WAN, you can also designate a client to act as an Update Agent. See **Remote Site 1 Deployment** on page A-5 for more information.
Legacy OfficeScan Features

This section provides a list of features available in previous OfficeScan versions that are no longer available in this version.

**TABLE B-1. Legacy OfficeScan Features**

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>STATUS IN OFFICE SCAN 10.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>OfficeScan Watchdog</td>
<td>The OfficeScan Watchdog’s function (restarting OfficeScan client services that stopped unexpectedly) is performed by the OfficeScan client. Service restart settings are configured on the web console.</td>
</tr>
</tbody>
</table>
Index

A
ACS Server 1-23, 2-51, 2-68
activation 1-19, 2-39
Activation Code 1-3, 1-19, 2-39, 2-42
Active Directory 1-10, A-5
Apache Web server 1-10, 2-34, 2-67
assessment mode 2-61
automatic client upgrade 2-4, 2-6, 2-11, 2-15

B
backup
OfficeScan database 1-13, 2-78
OfficeScan server files and folders 1-13,
2-79

C
Case Diagnostic Tool 3-2
Cisco NAC 2-51
Cisco Trust Agent 1-20, 2-52–2-54
client debug logs 3-7
client installation path 1-21, 2-58
Client Mover 2-77
Client Mover for Legacy Platforms 2-74
Client Packager A-4
compatibility issues 1-25
component duplication 1-9
component updates 1-9
components 2-72
considerations
fresh installation 1-4
upgrade 1-11
Control Manager 1-9, 2-77
conventional scan 1-7, 2-4

database backup 1-13, 2-78
debug logs
client 3-7
server 3-5
default settings
client privileges 2-73
global client settings 2-73
scan settings 2-73
Distributed File System (DFS) A-5
documentation feedback 3-11

E
evaluation version 1-3, 2-19
Exceptions
performance tuning tool 3-2

F
firewall 2-60
fresh installation 2-2
checklist 1-17
considerations 1-4
silent 2-16
summary 2-66
system requirements 1-2
verification 2-69
full version 1-2

H
HTTP port 1-18, 1-23, 2-35

I
IIS Web server 1-10, 2-34, 2-67
incremental pattern 1-9
installation
logs 3-4
Policy Server 1-23, 2-67
post-installation tasks 2-69
screens and tasks 2-20
silent 2-16
installation destination 2-26
installation path
client 1-21, 2-58
server 1-17, 2-31
integrated Smart Protection Server 1-7, 2-80
client connection protocols 2-42, 2-45
installation 1-19, 2-41
uninstallation 2-81
Internet Connection Firewall 1-26
IPv6 support 1-4

K
Knowledge Base 3-9

L
legacy features B-1
lockdown tools 1-25
Login Script Setup A-4

M
manual client upgrade 2-6, 2-11
manual update 2-72
Microsoft Exchange Server 1-25
MSI package deployment A-5

N
network traffic 1-8

O
OfficeScan client
debug logs 3-7

P
passwords 1-21, 1-23, 2-57, 2-68
Performance Tuning Tool 3-2
pilot deployment
evaluation 1-24
pilot site 1-24
rollback plan 1-24
Policy Server 1-23, 2-52, 2-67
port
client communication port 1-21, 2-59
HTTP port 1-18, 2-35
ISA port 1-25
proxy server port 1-17
server listening port 1-12, 2-13
SSL port 1-18, 2-45
post-installation 2-69
prescan 2-29
program folder shortcut 1-22, 2-65, 2-69
program settings 2-78
proxy server 1-17, 2-32

R
readme file 2-69
registration 1-19, 2-39
Registration Key 1-3
remote installation 1-6, 1-20, 2-28, 2-46, 2-49, A-4
response file 2-17
root account 1-21, 2-57
RSA encryption 2-36

S
sample deployment A-1
scan action 2-30
scan method 1-7–1-8, 1-14
Security Compliance 1-10
Security Information Center 3-10
Setup 2-20
silent installation 2-16
Smart Feedback 2-56
Smart Protection Network 2-55
Smart Protection Server 1-7, 1-19, 2-41–2-42, 2-45, 2-80–2-81
smart scan 1-7
SQL server 1-26
SSL port 1-18, 1-23, 2-35, 2-45
SSL tunneling 2-35
Support Intelligence System 3-2
suspicious files 3-11
system requirements
  fresh installation 1-2

T
Technical Support 3-8
third-party security software 1-10
TMPerftool 3-2
troubleshooting 3-2
troubleshooting resources 3-2

U
uninstallation 2-77
  manual 2-81
    using the uninstallation program 2-80
unsupported operating systems 1-12, 2-74
Update Agent 1-9
updates 1-9
upgrade
  checklist 1-17
  client base size 2-4
  clients 2-6, 2-11, 2-14, 2-16
  considerations 1-11
  from an evaluation version 2-19
  methods 2-4
  server and clients 2-2
  silent 2-16
  summary 2-66
  verification 2-69
URLScan 1-25

W
Watchdog B-1
Web console 2-57, 2-69–2-70
Web server 1-10, 1-18, 2-33