TREND MICRO

OfficeScan™ 10

For Enterprise and Medium Business

Installation and Upgrade Guide

Endpoint Security

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 Web site at:

http://www.trendmicro.com/download

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 © 1998-2010 Trend Micro Incorporated. All rights reserved.

Document Part No. OSEM104325/91008

Release Date: September 2010

Protected by U.S. Patent No. 5,623,600; 5,889,943; 5,951,698; 6,119,165

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

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

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

Please evaluate this documentation on the following site:

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

Contents

Preface

OfficeScan Documentation vi
Audience vii
Document Conventions vii
Terminology viii

Chapter 1: Planning OfficeScan Installation and Upgrade

Fresh Installation Requirements 1-2
Upgrade Requirements 1-8
OfficeScan 8.x Server 1-8
OfficeScan 8.x Client 1-10
OfficeScan 7.x Server 1-10
OfficeScan 7.x Client 1-12
Product Versions and Keys 1-14
Full Version and Evaluation Version 1-14
The Registration Key and Activation Codes 1-15
Fresh Installation Considerations 1-15
Location of the OfficeScan Server 1-16
Remote Installation 1-16
Server Performance 1-16
Dedicated Server 1-17
Scan Method Deployment During Installation 1-17
Network Traffic 1-18
Third-party Security Software 1-20
Active Directory 1-20
Web Server 1-20
Upgrade Considerations 1-21
OfficeScan Settings and Configurations 1-21
Unsupported Operating Systems 1-22

Scan Method Deployment During Upgrade 1-23
Installation and Upgrade Checklist 1-23
Planning a Pilot Deployment 1-31
Known Compatibility Issues 1-31

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: Move Clients to an OfficeScan 10 SP1 Server 2-7
Upgrade Results 2-9
Upgrade Method 3: Enable Automatic Client Upgrade 2-10
Upgrade Results 2-11
Performing Silent Installation/Upgrade 2-11
Upgrading from an Evaluation Version 2-14
The Setup Installation Screens 2-15
License Agreement 2-18
Installation Destination 2-19
Prescan 2-21
Installation Path 2-22
Proxy Settings 2-23
Web Server Settings 2-24
Server Computer Identification 2-27
Registration and Activation 2-28
Integrated Smart Scan Server Installation 2-30
Remote Installation Destination 2-33
Target Computer Analysis 2-35
OfficeScan Programs 2-36
Cisco Trust Agent Installation/Upgrade 2-39
Cisco Trust Agent License 2-40
Trend Micro Smart Protection Network 2-41

Administrator Account Password 2-42
Client Installation Path 2-43
Antivirus Features 2-45
Anti-spyware Feature 2-46
Program Folder Shortcut 2-47
Installation Information 2-48
Policy Server Installation 2-49
OfficeScan Server Installation Completion 2-50

Post-installation Tasks 2-51
Verifying the Server Installation or Upgrade 2-51
Updating OfficeScan Components 2-53
Checking Default Settings 2-53
Using Client Mover for Legacy Platforms 2-54
Registering OfficeScan to Control Manager 2-56
Installing Plug-in Manager 2-57

Performing Server Uninstallation/Rollback 2-57
OfficeScan Server Uninstallation 2-58
Before Uninstalling the OfficeScan Server 2-58
Uninstalling the OfficeScan Server 2-60
Rolling Back to OfficeScan 10 2-64

Chapter 3: Getting Help

Troubleshooting Resources 3-2
Case Diagnostic Tool 3-2
Installation Logs 3-2
Server Debug Logs 3-3
Client Debug Logs 3-5

Contacting Trend Micro 3-6
Technical Support 3-6
The Trend Micro Knowledge Base 3-7
TrendLabs 3-8
Security Information Center 3-8
Sending Suspicious Files to Trend Micro 3-9
Documentation Feedback 3-9

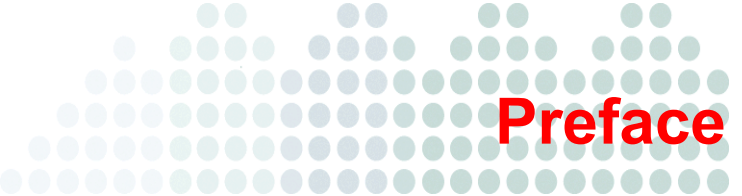
Appendix A: Sample Deployment

Basic Network A-2

Multiple Site Network A-2
Head Office Deployment A-4
Remote Site 1 Deployment A-5
Remote Site 2 Deployment A-6

Appendix B: Legacy OfficeScan Features

Index



Preface

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 viii

OfficeScan Documentation

OfficeScan documentation includes the following:

TABLE P-1. OfficeScan documentation

DOCUMENTATION	DESCRIPTION
Installation and Upgrade Guide	A PDF document that discusses requirements and procedures for installing the OfficeScan server, and upgrading the server and clients
Administrator's Guide	A PDF document that discusses getting started information, client installation procedures, and OfficeScan server and client management
Trend Micro Smart Scan for OfficeScan Getting Started Guide	A PDF document that helps users understand smart scan concepts, prepare the environment needed to use smart scan, and manage smart scan clients
Help	HTML files compiled in WebHelp or CHM format that provide "how to's", 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.
Readme file	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
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: http://esupport.trendmicro.com/support

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

http://www.trendmicro.com/download

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

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation or new technology components
TOOLS > CLIENT TOOLS	A "breadcrumb" 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.
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, C:\Program Files\<file_name> can be C:\Program Files\sample.jpg.

TABLE P-2. Document conventions (Continued)

CONVENTION	DESCRIPTION
Note: text	Provides configuration notes or recommendations
Tip: text	Provides best practice information and Trend Micro recommendations
WARNING! text	Provides warnings about activities that may harm computers on your network

Terminology

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

TABLE P-3. OfficeScan terminology

TERMINOLOGY	DESCRIPTION
Client	The OfficeScan client program
Client computer or endpoint	The computer where the OfficeScan client is installed
Client user (or user)	The person managing the OfficeScan client on the client computer
Server	The OfficeScan server program
Server computer	The computer where the OfficeScan server is installed

TABLE P-3. OfficeScan terminology (Continued)

TERMINOLOGY	DESCRIPTION
Administrator (or OfficeScan administrator)	The person managing the OfficeScan server
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**

TABLE P-3. OfficeScan terminology (Continued)

TERMINOLOGY	DESCRIPTION
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** 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>.
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

Chapter 1

Planning OfficeScan Installation and Upgrade

Topics in this chapter:

- *Fresh Installation Requirements* on page 1-2
- *Upgrade Requirements* on page 1-8
- *Product Versions and Keys* on page 1-14
- *Fresh Installation Considerations* on page 1-15
- *Upgrade Considerations* on page 1-21
- *Installation and Upgrade Checklist* on page 1-23
- *Planning a Pilot Deployment* on page 1-31
- *Known Compatibility Issues* on page 1-31

Fresh Installation Requirements

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

OfficeScan Server

The following are the requirements to perform a fresh installation of the OfficeScan server:

TABLE 1-1. OfficeScan server system requirements

RESOURCE	REQUIREMENTS
Operating system	**Windows 2000** • Microsoft™ Windows™ 2000 Server with Service Pack 4 • Windows 2000 Advanced Server with Service Pack 4 Install the following to use the Role-based Administration feature: • Microsoft patch KB890859 • Microsoft patch KB924270 • Windows 2000 Authorization Manager Runtime **Windows 2003** • Windows Server™ 2003 (Standard, Enterprise, and Datacenter Editions) with Service Pack 2 or later, 32-bit and 64-bit versions • Windows Server 2003 R2 (Standard, Enterprise, and Datacenter Editions) with Service Pack 2 or later, 32-bit and 64-bit versions • Windows Storage Server 2003, 32-bit and 64-bit versions • Windows Storage Server 2003 R2, 32-bit and 64-bit versions

TABLE 1-1. OfficeScan server system requirements (Continued)

RESOURCE	REQUIREMENTS
	Windows 2008 • Windows Server 2008 (Standard, Enterprise, Datacenter and Web Editions) with Service Pack 1 or later, 32-bit and 64-bit versions • Windows Server 2008 R2 (Standard, Enterprise, Datacenter and Web Editions), 64-bit versions **Note:** OfficeScan cannot be installed if Windows 2008 runs on the Server Core environment. OfficeScan automatically disables some features on server platforms. Refer to the Administrator's Guide for more information.
Virtualization	OfficeScan supports server installation on guest Windows 2000/2003/2008 operating systems hosted on the following virtualization applications: • VMware™ ESX™/ESXi Server 3.5 or 4 (Server Edition) • VMware Server 1.0.3 or later (Server Edition) • VMware Workstation and Workstation ACE Edition 6.0 The server can also be installed on guest Windows 2000, 2003 (32-bit/64-bit), and 2008 (32-bit/64-bit) operating systems hosted on: • Microsoft Virtual Server 2005 R2 with Service Pack 1 • Windows Server 2008 (64-bit) with Hyper-V™ • Windows Server 2008 R2 (64-bit) with Hyper-V • Microsoft Hyper-V Server 2008 R2 (64-bit) **Note:** OfficeScan automatically disables some features on server platforms. Refer to the Administrator's Guide for more information.

TABLE 1-1. OfficeScan server system requirements (Continued)

RESOURCE	REQUIREMENTS
Hardware (for Windows Server 2008)	**Processor** • At least 1GHz Intel™ Pentium™ or equivalent for x86 processors and 1.4GHz for x64 processors; 2GHz recommended • At least 1.86GHz Intel Core2Duo™ if installing the integrated Smart Scan Server • AMD™ 64 and Intel 64 processor architectures **RAM** • 512MB minimum, 2GB recommended • 1GB minimum if installing the integrated Smart Scan Server **Available disk space** • 3.1GB minimum if installing the OfficeScan server, OfficeScan client, Policy Server for Cisco™ NAC, and integrated Smart Scan Server locally • 3.5GB minimum if installing the OfficeScan server, OfficeScan client, and integrated Smart Scan Server remotely **Others** • Gigabit Network Interface Card (NIC) • Monitor that supports 1024 x 768 resolution at 256 colors or higher

TABLE 1-1. OfficeScan server system requirements (Continued)

RESOURCE	REQUIREMENTS
Hardware (for all other platforms)	**Processor** • 800MHz Intel Pentium or equivalent • At least 1.86GHz Intel Core2Duo™ if installing the integrated Smart Scan Server **RAM** • 512MB minimum, 1GB recommended • 1GB minimum if installing the integrated Smart Scan Server **Available disk space** • 3.1GB minimum if installing the OfficeScan server, OfficeScan client, Policy Server for Cisco NAC, and integrated Smart Scan Server locally • 3.5GB minimum if installing the OfficeScan server, OfficeScan client, and integrated Smart Scan Server remotely **Others** • Gigabit Network Interface Card (NIC) • Monitor that supports 1024 x 768 resolution at 256 colors or higher

TABLE 1-1. OfficeScan server system requirements (Continued)

RESOURCE	REQUIREMENTS

Web server	• Microsoft Internet Information Server (IIS)
	  • on Windows 2000: version 5.0
	  • on Windows Server 2003: version 6.0
	  • on Windows Server 2008: version 7.0
	• Apache™ Web server 2.0.x
	Note: 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.

Others	• Administrator or Domain Administrator access on the server computer • File and printer sharing for Microsoft Networks installed on the server computer • If you plan to install the Cisco Trust Agent (CTA) on the same computer as the OfficeScan server, do not install OfficeScan server on Windows Server 2003 x64 Edition. For more information on CTA requirements, see the *Administrator's Guide*.

Web Console

The following are the requirements to launch and access the Web console:

TABLE 1-2. Web console requirements

RESOURCE	REQUIREMENT
Hardware	**Processor** 300MHz Intel Pentium processor or equivalent **RAM** 128MB minimum **Available disk space** 30MB minimum **Others** Monitor that supports 1024 x 768 resolution at 256 colors or higher
Browser	Microsoft Internet Explorer™ 6.0 or later

Upgrade Requirements

This version of OfficeScan supports upgrade from the following versions:

- 8.x
  - 8.0
  - 8.0 Service Pack 1

  If upgrading from version 8.x, the server and clients may need additional computer resources to run this OfficeScan version. For details, see *OfficeScan 8.x Server* on page 1-8 and *OfficeScan 8.x Client* on page 1-10.
- 7.x
  - 7.3
  - 7.0

  If upgrading from version 7.x, the server and clients may need additional computer resources to run this OfficeScan version. For details, see *OfficeScan 7.x Server* on page 1-10 and *OfficeScan 7.x Client* on page 1-12.

OfficeScan 8.x Server

All operating systems supported in version 8.x are supported in this version.

Before upgrading, perform the following tasks:

1. Apply the required Microsoft service packs.
   - Service Pack 4 for Windows 2000 Server
   - Service Pack 2 or later for Windows Server 2003

2. Check if the server computer needs additional resources to run this OfficeScan version. Refer to the following table for details.

TABLE 1-3. Differences between OfficeScan 10 SP1 and 8.x server minimum requirements

RESOURCE	OFFICESCAN 8.X SERVER REQUIREMENTS	OFFICESCAN 10 SP1 SERVER REQUIREMENTS
Processor	800MHz Intel Pentium or equivalent	1.86GHz Intel Core2Duo™ if installing the integrated Smart Scan Server
RAM	512MB	1GB if installing the integrated Smart Scan Server
Disk space	1GB	• 3.1GB if installing the OfficeScan server, OfficeScan client, Policy Server for Cisco NAC, and integrated Smart Scan Server locally • 3.5GB if installing the OfficeScan server, OfficeScan client, and integrated Smart Scan Server remotely
Web server	Apache Web server 2.0 or later	Apache Web server 2.0.x
Browser (for Web console and Web install page)	Microsoft Internet Explorer 5.5 with Service Pack 1 or later	Microsoft Internet Explorer 6.0 or later

OfficeScan 8.x Client

All operating systems supported in version 8.x are supported in this version.

Clients running Windows XP Professional and Windows Server 2008 require additional Microsoft service packs. Apply these service packs before upgrading.

- Service Pack 2 or later for Windows XP Professional
- Service Pack 2 or later for Windows Server 2003
- Service Pack 1 or later for Windows Server 2008

For other supported operating systems, the required service packs in version 8.x and in this version are the same.

OfficeScan 7.x Server

OfficeScan 7.x servers running the following operating systems can be upgraded:

- Windows 2000 Server
- Windows Server 2003

OfficeScan servers running the following operating systems cannot be upgraded:

- Windows NT series
- Windows XP Professional

Before upgrading, perform the following tasks:

1. Apply the required Microsoft service packs.
   - Service Pack 4 for Windows 2000 Server
   - Service Pack 2 or later for Windows Server 2003

2. Check if the server computer needs additional resources to run this OfficeScan version. Refer to the following table for details.

TABLE 1-4. Differences between OfficeScan 10 SP1 and 7.x server minimum requirements

RESOURCE	OFFICESCAN 7.X SERVER REQUIREMENTS	OFFICESCAN 10 SP1 SERVER REQUIREMENTS
Processor	300MHz Intel Pentium II processor or equivalent	• 800MHz Intel Pentium or equivalent • 1.86GHz Intel Core2Duo™ if installing the integrated Smart Scan Server
RAM	128MB	• 512MB • 1GB if installing the integrated Smart Scan Server
Disk space	• 600MB for OfficeScan 7.3 • 300MB for OfficeScan 7.0	• 3.1GB if installing the OfficeScan server, OfficeScan client, Policy Server for Cisco NAC, and integrated Smart Scan Server locally • 3.5GB if installing the OfficeScan server, OfficeScan client, and integrated Smart Scan Server remotely
Web server	Apache Web server 2.0 or later	Apache Web server 2.0.x
Browser (for Web console and Web install page)	Microsoft Internet Explorer 5.5 with Service Pack 1 or later	Microsoft Internet Explorer 6.0 or later

OfficeScan 7.x Client

OfficeScan 7.x clients running the following operating systems can be upgraded:

- Windows 2000
- Windows XP Professional
- Windows XP Home
- Windows Server 2003

OfficeScan 7.x clients running the following operating systems cannot be upgraded:

- Windows 95
- Windows 95 OSR2
- Windows 98
- Windows 98 SE
- Windows Me
- Windows NT 4.0
- Intel Itanium™ Architecture operating systems

Keep your OfficeScan 7.x server if you have clients running unsupported operating systems and you want to continue managing these clients. See *Unsupported Operating Systems* on page 1-22 for more information.

Tip: You can check the operating systems of your clients on the OfficeScan 7.x server Web console. Click **Clients** and go to the **Platform** column.

Windows 2000

Before upgrading clients running Windows 2000, perform the following tasks:

1. Apply Service Pack 4 or later.
2. Check if the client computer needs additional resources to run this OfficeScan version. Refer to the following table for details.

TABLE 1-5. Differences between OfficeScan 10 SP1 and 7.x client minimum requirements

RESOURCE	OFFICESCAN 7.X CLIENT REQUIREMENTS	OFFICESCAN 10 SP1 CLIENT REQUIREMENTS
Processor	150MHz Intel Pentium processor or equivalent	300MHz Intel Pentium processor or equivalent
RAM	64MB	256MB
Disk space	• 160MB for OfficeScan 7.3 • 80MB for OfficeScan 7.0	350MB

Windows XP Professional, Windows XP Home, and Windows Server 2003

Before upgrading clients running Windows XP Professional, XP Home, and Server 2003, perform the following tasks:

1. Apply the required Microsoft service packs.
   - Service Pack 2 or later for Windows XP Professional
   - Service Pack 3 for Windows XP Home
   - Service Pack 2 for later for Windows Server 2003

2. Check if the client computer needs additional resources to run this OfficeScan version. Refer to the following table for details:

TABLE 1-6. Differences between OfficeScan 10 SP1 and 7.x client minimum requirements

RESOURCE	OFFICESCAN 7.X CLIENT REQUIREMENTS	OFFICESCAN 10 SP1 CLIENT REQUIREMENTS
Disk space	• 160MB for OfficeScan 7.3 • 80MB for OfficeScan 7.0	350MB
RAM	128MB	256MB

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 Web site where you can register your product.

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

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 3-6 for details.

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

Fresh Installation Considerations

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

- *Location of the OfficeScan Server* on page 1-16
- *Remote Installation* on page 1-16
- *Server Performance* on page 1-16
- *Dedicated Server* on page 1-17
- *Scan Method Deployment During Installation* on page 1-17
- *Network Traffic* on page 1-18
- *Third-party Security Software* on page 1-20
- *Active Directory* on page 1-20
- *Web Server* on page 1-20

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* or the *OfficeScan Server Help*.

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 if the computer meets the OfficeScan server system requirements. Refer to *Fresh Installation 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:

- 3000 to 5000 clients for an OfficeScan server with 2GHz dual processor with 2GB of RAM
- 5000 to 8000 clients for an OfficeScan server with 3GHz dual 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 Scan 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

If you perform OfficeScan server fresh installation and did not change the scan method on the Web console after the installation, all clients that you install will use conventional scan. You can configure all or a certain number of clients to use smart scan after each client is installed. For more information, read the deployment guidelines in the Trend Micro Smart Scan for OfficeScan *Getting Started Guide*.

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

Verify if all OfficeScan servers are 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 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:

- *OfficeScan Settings and Configurations* on page 1-21
- *Unsupported Operating Systems* on page 1-22
- *Scan Method Deployment During Upgrade* on page 1-23

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 8.x/7.x 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. For details, see *Upgrading the OfficeScan Server and Clients* on page 2-2.

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.

Unsupported Operating Systems

OfficeScan no longer supports Windows 95, 98, Me, NT, or theItanium architecture platform. If you plan to upgrade to this version from OfficeScan 7.x and you have OfficeScan 7.x clients that run these operating systems:

1. Do not upgrade all OfficeScan 7.x servers to this OfficeScan version.
2. Designate at least one OfficeScan 7.x server (parent server) to manage clients running unsupported operating systems.
3. Before upgrading the other servers:
   a. Open the Web console for each server and click **Clients** on the main menu.
   b. From the client tree, select the clients you want to move, and then click **Move**.
   c. Specify the parent server's computer name/IP address and server listening port under **Move selected client(s) to another OfficeScan Server**.
   d. Click **Move**.

If you have upgraded the OfficeScan server but did not move unsupported clients, see *Using Client Mover for Legacy Platforms* on page 2-54 for instructions.

Scan Method Deployment During Upgrade

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

If you upgrade the OfficeScan server from an earlier version and automatic client upgrade is enabled, all clients that the server manages automatically use conventional scan after the upgrade. You can configure all or a certain number of clients to use smart scan after the upgrade. For more information, read the deployment guidelines in the Trend Micro Smart Scan for OfficeScan *Getting Started Guide*.

If you do not plan to deploy smart scan or if you will deploy it after all clients have upgraded, see *Upgrading the OfficeScan Server and Clients* on page 2-2.

Installation and Upgrade Checklist

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

TABLE 1-7. Installation checklist

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
Installation path The default server installation path is: • C:\Program Files\Trend Micro\OfficeScan • C:\Program Files (x86)\Trend Micro\OfficeScan *(for x64 type platforms)* Identify the installation path if you choose not to use the default path. If the path does not exist, Setup creates it for you.	Yes	Yes	No	Yes

TABLE 1-7. Installation checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
Proxy server settings 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	Yes	Yes	No	Yes

TABLE 1-7. Installation checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
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)	Yes	Yes	No	Yes

TABLE 1-7. Installation checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
Registration Register the product to receive the Activation Codes. To register, you need the following: *For returning users* • Online registration account (logon name and password) *For users without an account* • Registration Key	Yes	Yes	Yes	Yes
Activation Obtain the Activation Codes for the following product services: • Antivirus • Damage Cleanup Services • Web Reputation and Anti-spyware	Yes	Yes	Yes	Yes
Integrated Smart Scan Server installation If you choose to install the integrated server, specify the following: • SSL certificate validity period • SSL port	Yes	Yes	Yes	Yes

TABLE 1-7. Installation checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE

Remote installation destination
Identify the computers to which you will install/upgrade the OfficeScan server. Prepare the following:
• List of computer names or IP addresses
• (Optional) A text file with a list of target computers or IP addresses
Sample text file content:
`us-user_01`
`us-admin_01`
`123.12.12.123`
	No	Yes	No	Yes

Remote installation computer analysis Setup prompts you for the following information before performing target computer analysis: • User name and password for an administrator account with "logon as a service" privilege on the target computer	No	Yes	No	Yes
Install other OfficeScan programs If installing Cisco Trust Agent, prepare the following: • Cisco Trust Agent certificate file	Yes	No	No	No

TABLE 1-7. Installation checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
Administrator account password Setup creates a root account for Web console logon. Specify the following: • Root account password Prevent unauthorized uninstallation or unloading of the OfficeScan client by specifying the following: • Client uninstallation/unloading password	Yes	Yes	No	No
Client installation path Specify the directory on the client computer where the OfficeScan client will be installed. Specify the following: • Installation path: The default client installation path is $ProgramFiles\Trend Micro\ OfficeScan Client. Identify the installation path if you choose not to use the default path. If the path does not exist, Setup creates it during client installation. • Client communication port number: OfficeScan generates the port number randomly. Accept the generated port number or specify a new one.	Yes	Yes	No	No

TABLE 1-7. Installation checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
Program folder shortcut 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.	Yes	No	No	No

TABLE 1-7. Installation checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE

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).
	Yes	No	No	No

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:

1. Stop the World Wide Web Publishing service on the OfficeScan server computer.
2. Modify the URLScan configuration file to allow the file types specified above.
3. Restart the World Wide Web Publishing service.

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.

OfficeScan automatically excludes all Microsoft Exchange 2000/2003 directories from scanning. This setting can be configured on the Web console (**Networked Computers > Global Client Settings > Virus/Malware Scan Settings**). For Microsoft Exchange 2007, refer to http://technet.microsoft.com/en-us/library/bb332342.aspx for scan exclusion details.

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

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 2-11
- *Upgrading from an Evaluation Version* on page 2-14
- *The Setup Installation Screens* on page 2-15
- *Post-installation Tasks* on page 2-51
- *Performing Server Uninstallation/Rollback* on page 2-57

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 Requirements* on page 1-2. For information on the installation screens and configuration options, see *The Setup Installation Screens* on page 2-15.

Note: You do not need to run two installation packages separately because the OfficeScan 10 SP1 package automatically installs the service pack after installing OfficeScan 10.

After installing the server, configure OfficeScan server settings from the Web console and then install the OfficeScan client to computers.

For client fresh installation methods and instructions, see the *Administrator's Guide* or *OfficeScan Server Help*.

Upgrading the OfficeScan Server and Clients

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.

Note: The OfficeScan 10 SP1 package automatically installs the service pack after installing OfficeScan 10. This also applies when upgrading OfficeScan clients.

If you plan to upgrade clients and deploy smart scan at the same time, see the Trend Micro Smart Scan for OfficeScan *Getting Started Guide*.

Before Upgrading the OfficeScan Server and Clients

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

- This service pack includes updates to OfficeScan firewall drivers. If you have enabled the OfficeScan firewall in your current OfficeScan version, deploying the service pack may cause client computer disruptions

After deploying the service pack, 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, open the Web console, go to **Networked Computers > Global Client Settings** and check the option under **Alert Settings**.

- The OfficeScan server cannot upgrade to this service pack if a client is running Login Script (AutoPcc.exe) at the time of server upgrade. Ensure that no client is running Login Script before installing this service pack.
- The network bandwidth needed to upgrade to this service pack are as follows:
  - By hot fix mechanism 26 MB
  - By Login Script (AutoPcc.exe) 102.4 MB

Upgrade Methods

If all clients will use conventional scan after the upgrade, use one of following upgrade methods:

- *Upgrade Method 1: Disable Automatic Client Upgrade* on page 2-4
- *Upgrade Method 2: Move Clients to an OfficeScan 10 SP1 Server* on page 2-7
- *Upgrade Method 3: Enable Automatic Client Upgrade* on page 2-10

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 upgrading a large number of clients.

Part 1: Configure update settings and privileges on the OfficeScan 8.x or 7.x server

For OfficeScan 8.x:

1. Go to **Updates > Networked Computers > Automatic Update**.
2. Disable the following options:
   - 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)
3. Go to **Networked Computers > Client Management**.
4. From the client tree, select the root icon to select all clients.
5. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
6. Enable **Clients can update components but not upgrade the client program or deploy hot fixes**.
7. Click **Apply to All Clients**.

For OfficeScan 7.x:

1. Go to **Updates > Client Deployment > Automatic Deployment**.
2. Disable the following options:
   - Deploy to clients immediately after the OfficeScan server downloads a new component.
   - Deploy to clients for OfficeScan clients only and excluding roaming clients when they are restarted.
3. Click **Clients** on the main menu.
4. From the client tree, select the root icon to select all clients.
5. Click **Client Privileges/Settings**.
6. Under Update Settings, enable **Forbid program upgrade and hot fix deployment**.

7. Click **Apply to All**.

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 2-15 for details on upgrading the OfficeScan server.

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 **Networked Computers > Client Management**.
2. On the client tree, select the clients you want to upgrade. Stagger the upgrade by selecting a domain or specific clients from a domain.

   Tip: Upgrade Update Agents first. Update Agents help reduce traffic directed to the OfficeScan server by acting as an update source for other clients.

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. Go to **Updates > Networked Computers > Automatic Update**.
6. Enable the following options:
   - 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).

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 computers to finish upgrading the clients.

Upgrade Results (Online Clients)

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 2000, 2003, and 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 2000, 2003, XP Professional, 2008, or Vista™ (all editions except Vista 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 or Vista Home, instruct the user to right-click **AutoPcc.exe**, and select **Run as administrator**.
- Initiate manual client update.

To initiate manual client update:

1. Go to **Updates > Networked Computers > Manual Update**.
2. Select **Manually select clients** 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: Move Clients to an OfficeScan 10 SP1 Server

Perform a fresh installation of the OfficeScan 10 SP1 server and then move clients to this server. When you move the clients, they automatically upgrade to OfficeScan 10 SP1.

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

1. Perform a fresh installation of the OfficeScan 10 SP1 server on a computer. For details, see *The Setup Installation Screens* on page 2-15.
2. Open the OfficeScan 10 SP1 Web console and go to **Updates > Networked Computers > Automatic Update**.
3. Enable the following options:
   - 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)

4. Go to **Networked Computers > Client Management**.
5. From the client tree, select the root icon.
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 SP1 server information. Specify this information on the OfficeScan 8.x/7.x server when moving 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.

Part 2: Upgrade OfficeScan clients

For OfficeScan 8.x:

1. On the 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 SP1 server.

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

3. Go to **Networked Computers > Client Management**.
4. From the client tree, select the clients you want to upgrade. Select only online clients because offline and roaming clients can not be moved.

   Tip: Upgrade Update Agents first. Update Agents help reduce traffic directed to the OfficeScan server by acting as an update source for other clients.

5. Click **Manage Client Tree > Move Client**.

6. Specify the OfficeScan 10 SP1 server computer name/IP address and server listening port under **Move selected client(s) online to another OfficeScan Server**.
7. Click **Move**.

For OfficeScan 7.x:

1. On the Web console, click **Clients** on the main menu.
2. From the client tree, select the clients you want to upgrade. Select only online clients because offline and roaming clients can not be moved.

> **Tip:** Upgrade Update Agents first. Update Agents help reduce traffic directed to the OfficeScan server by acting as an update source for other clients.

3. Click **Move**.
4. Specify the OfficeScan 10 SP1 server computer name/IP address and server listening port under **Move selected client(s) online to another OfficeScan Server**.
5. 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 SP1 client.

> **Note:** Restart computers to finish upgrading the clients. You can uninstall the OfficeScan 7.x or 8.x server after all clients have been upgraded.

Upgrade Method 3: 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 settings on the OfficeScan 8.x or 7.x server

For OfficeScan 8.x:

1. Go to **Updates > Networked Computers > Automatic Update**.
2. Enable the following options:
   - 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)
3. Go to **Networked Computers > Client Management**.
4. From the client tree, select the root icon.
5. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
6. Disable **Clients can update components but not upgrade the client program or deploy hot fixes**.
7. Click **Apply to All Clients**.

For OfficeScan 7.x:

1. Go to **Updates > Client Deployment > Automatic Deployment**.
2. Enable the following options:
   - Deploy to clients immediately after the OfficeScan server downloads a new component.
   - Deploy to clients for OfficeScan clients only and excluding roaming clients when they are restarted.
3. Click **Clients** on the main menu.
4. From the client tree, select the root icon to select all clients.
5. Click **Client Privileges/Settings**.
6. Under Update Settings, disable **Forbid program upgrade and hot fix deployment**.

7. Click **Apply to All**.

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 2-15 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 computers to finish upgrading the clients. You can uninstall the OfficeScan 7.x or 8.x server after all clients have been upgraded.

Performing Silent Installation/Upgrade

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

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

- This service pack includes updates to OfficeScan firewall drivers. If you have enabled the OfficeScan firewall in your current OfficeScan version, deploying the service pack may cause client computer disruptions

  After deploying the service pack, 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, open the Web console, go to **Networked Computers > Global Client Settings** and check the option under **Alert Settings**.

- The OfficeScan server cannot upgrade to this service pack if a client is running Login Script (AutoPcc.exe) at the time of server upgrade. Ensure that no client is running Login Script before installing this service pack.
- The network bandwidth needed to upgrade to this service pack are as follows:
  - By hot fix mechanism 26 MB
  - By Login Script (AutoPcc.exe) 102.4 MB

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 2-15 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

SCREENS	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
Welcome	✓	✓	✓	✓
License Agreement	✓	✓	✓	✓
Installation Destination	✓	✓	✓	✓
Prescan	✓	✓	✓	✓
Setup Status (Computer Analysis) **Note:** Analysis may take some time to complete, especially during HTTP server initialization.	✓		✓	
Installation Path	✓	✓		✓
Proxy Settings	✓	✓		✓
Web Server Settings	✓	✓		✓
Server Computer Identification	✓	✓		✓

TABLE 2-1. Installation screens and tasks (Continued)

SCREENS	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
Registration and Activation	✓	✓	✓	✓
Integrated Smart Scan Server Installation	✓	✓	✓	✓
Remote Installation Destination		✓		✓
Target Computer Analysis		✓		✓
OfficeScan Programs	✓	✓		✓
Cisco Trust Agent Installation/Upgrade	✓			
Cisco Trust Agent License	✓			
Trend Micro Smart Protection Network	✓	✓		
Administrator Account Password	✓	✓		
Client Installation Path	✓	✓		
Antivirus Features	✓	✓		

TABLE 2-1. Installation screens and tasks (Continued)

SCREENS	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
Anti-spyware Feature When performing a local upgrade, this screen does not display if the Web Reputation and Anti-spyware license has been activated previously.	✓	✓	✓	✓
Program Folder Shortcut	✓			
Installation Information	✓	✓	✓	✓
OfficeScan Server Installation	✓	✓	✓	✓
Policy Server Installation	✓			
OfficeScan Server Installation Completion	✓	✓	✓	✓

License Agreement

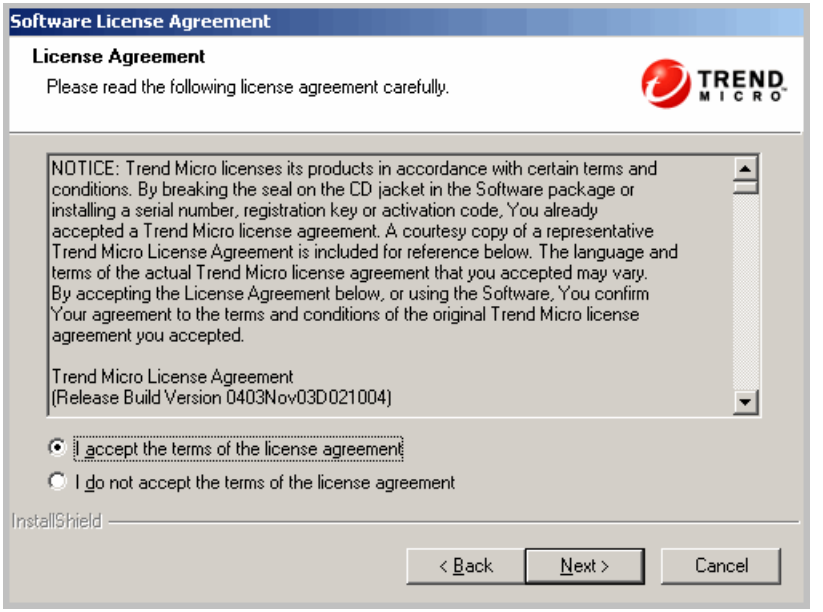


FIGURE 2-1. License Agreement screen

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.

Installation Destination

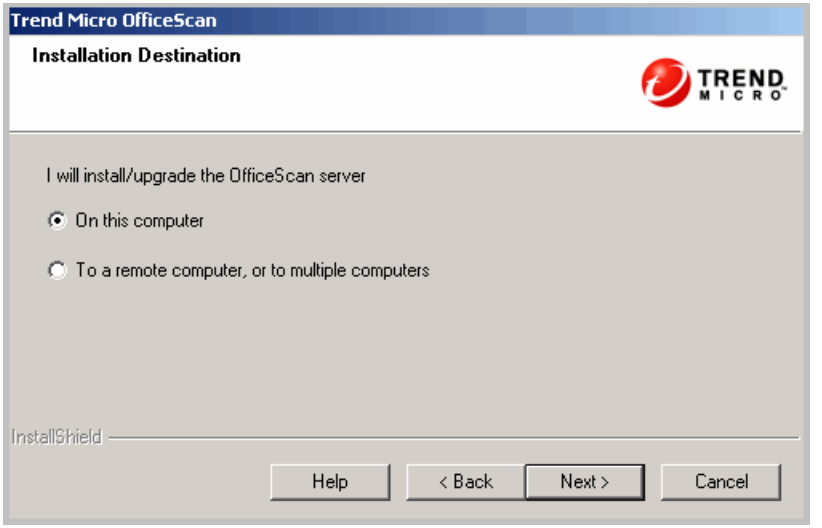


FIGURE 2-2. Installation Destination screen

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:

- 8.0
- 8.0 Service Pack 1
- 7.3
- 7.0

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 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.

Prescan

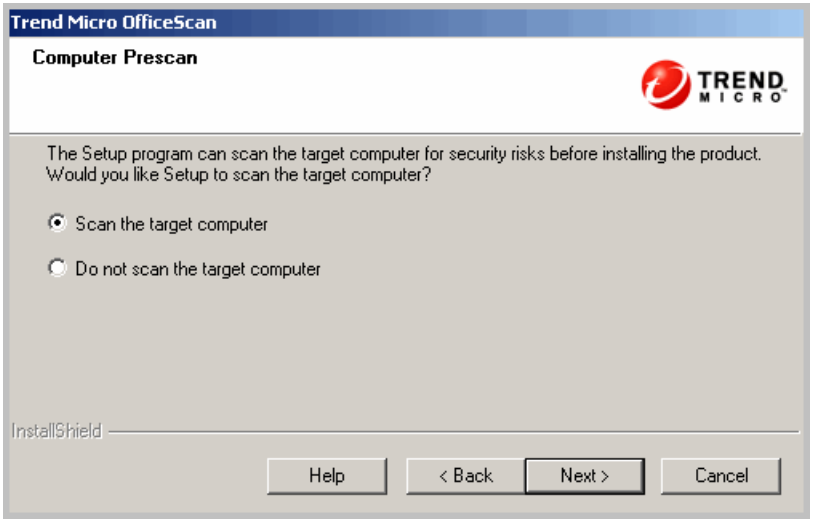


FIGURE 2-3. Computer Prescan screen

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

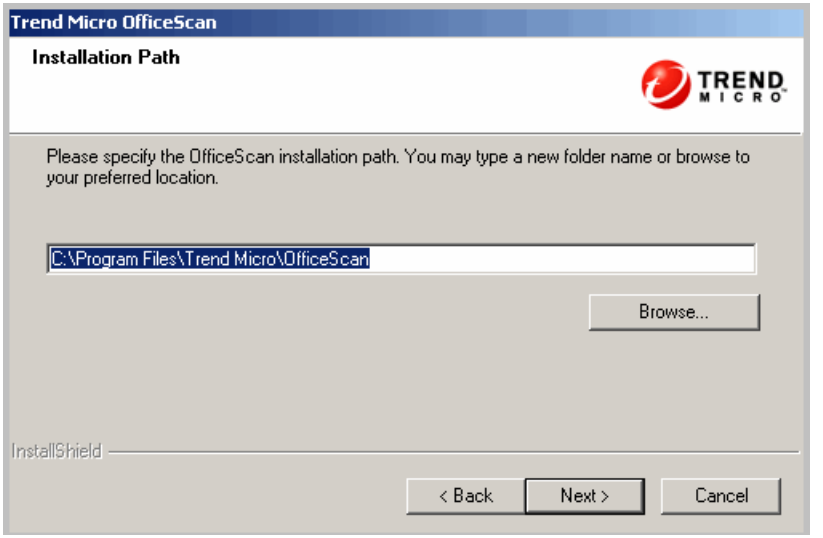


FIGURE 2-4. Installation Path screen

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 Settings

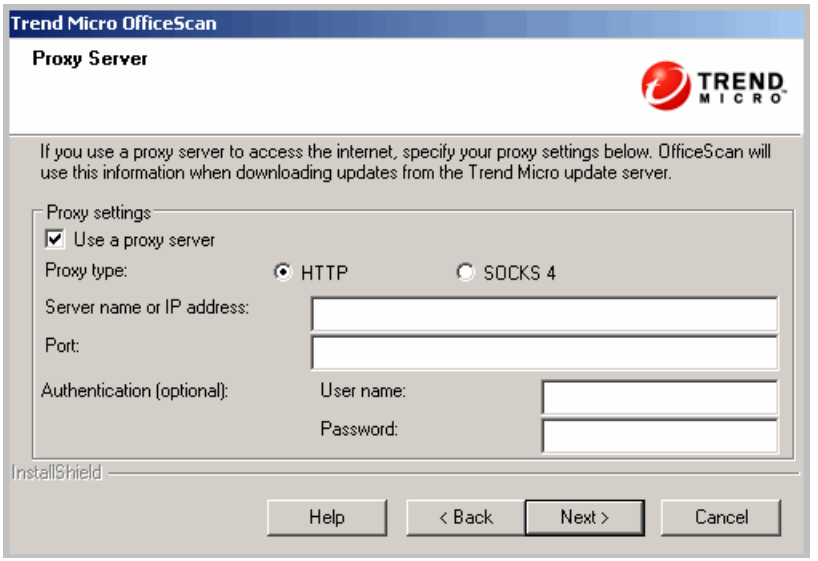


FIGURE 2-5. Proxy Server screen

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.

Web Server Settings

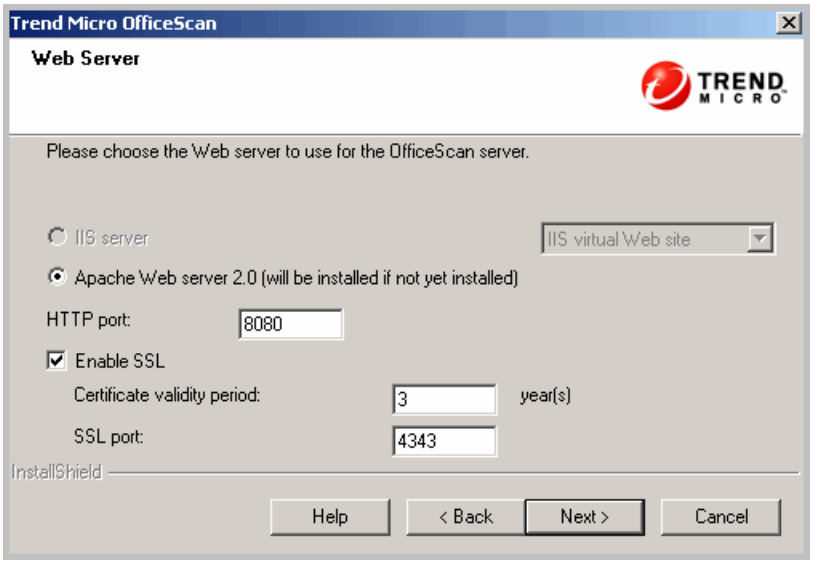


FIGURE 2-6. Web Server screen

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.

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 and can only be used on Windows 2000, XP, 2003, and 2008. 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 Web site for the latest information on upgrades, patches, and security issues.

If using an IIS Web server:

- Microsoft Internet Information Server (IIS) version 5.0 is required for Windows 2000, version 6.0 for Windows Server 2003, and version 7.0 for Windows Server 2008.
- 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.

OfficeScan uses the same port number that the HTTP server uses for TCP traffic. In many organizations, this is port 80 or 8080. The OfficeScan default port is 8080.

If you enable SSL, OfficeScan uses the SSL port (4343 is the default port) instead of the HTTP port.

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.

Each SSL certificate has a validity period of three 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.

Server Computer Identification

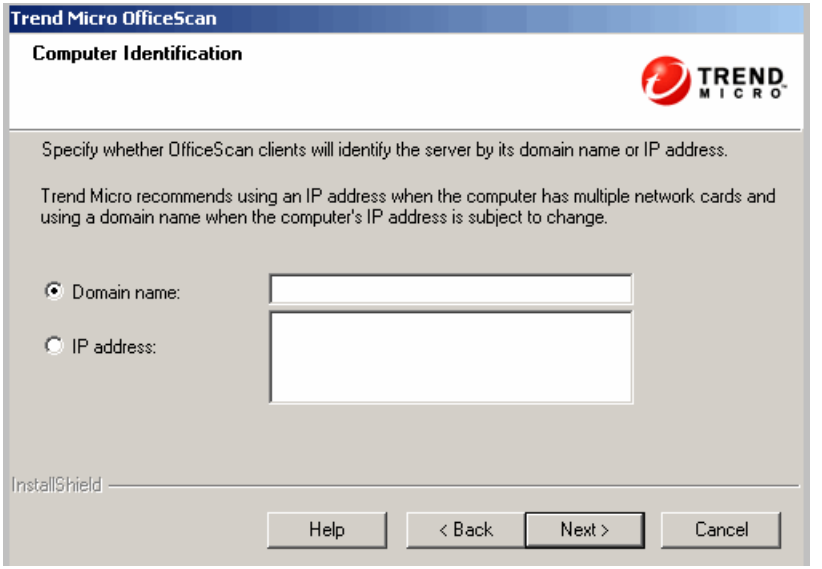


FIGURE 2-7. Computer Identification screen

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 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 domain name and you change its domain name.

In most networks, the server computer's IP address is more likely to change than its domain name, thus it is usually preferable to identify the server computer by a domain 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 domain name to ensure successful client-server communication.

Registration and Activation

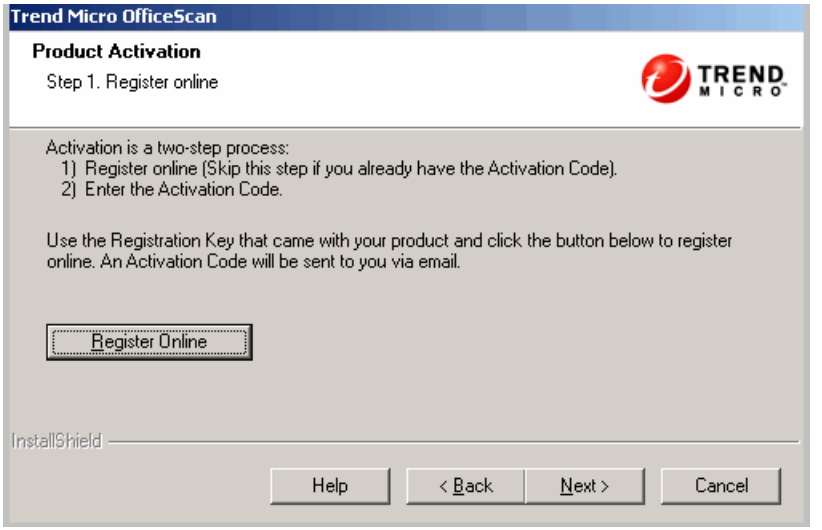


FIGURE 2-8. Product Registration screen

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 Web site. After you complete the registration form, Trend Micro sends an email with the Activation Codes. You can then continue with the installation process

.

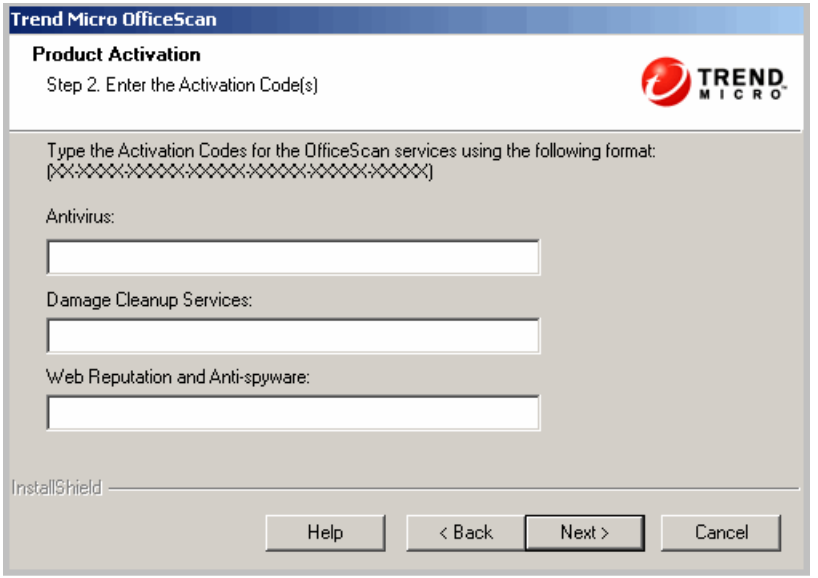


FIGURE 2-9. Product Activation screen

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

Integrated Smart Scan Server Installation

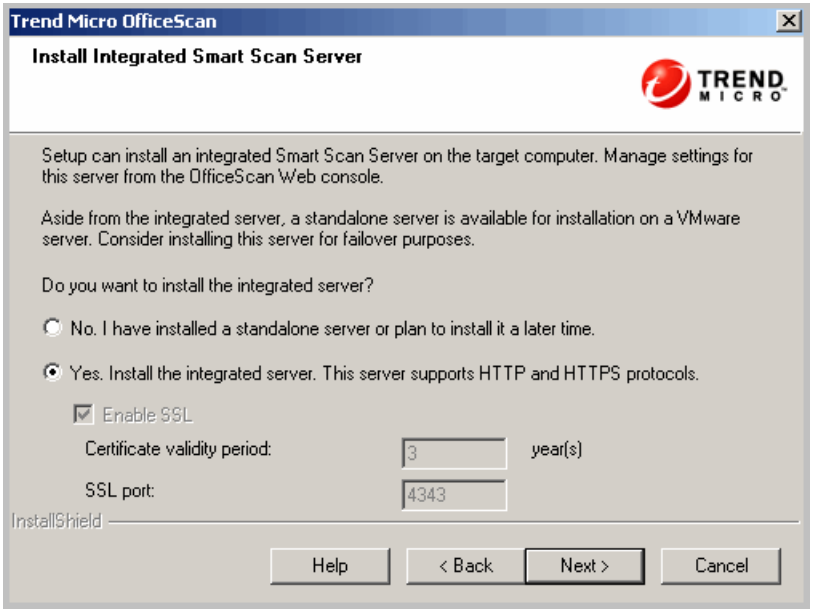


FIGURE 2-10. Integrated Smart Scan Server Installation screen

The OfficeScan smart scan solution makes use of lightweight patterns that work together to provide the same protection provided by conventional anti-malware and anti-spyware patterns. These patterns originate from the Trend Micro ActiveUpdate server and are made available to Smart Scan Servers and the OfficeScan server.

A Smart Scan Server hosts the Smart Scan Pattern, which is updated hourly and contains majority of the pattern definitions. Smart scan clients do not download this pattern. Clients verify potential threats against the pattern by sending scan queries to the Smart Scan Server.

Note: The other pattern used in the smart scan solution, called Smart Scan Agent Pattern, is hosted on the OfficeScan server and downloaded by clients.

If a client can connect to the corporate network, it sends scan queries to a local Smart Scan Server. Setup includes a local Smart Scan Server (called integrated Smart Scan Server) that installs on the same computer where the OfficeScan server is installed. Manage settings for the integrated server on the OfficeScan server Web console.

Install several local Smart Scan Servers for failover purposes. Aside from the integrated server, a standalone Smart Scan Server is available for installation on a VMware server. The standalone server has the same functions and capabilities as the integrated server. It has a separate management console and is not managed from the OfficeScan Web console. See the Trend Micro Smart Scan for OfficeScan *Getting Started Guide* for information on the standalone server.

Tip: Because the integrated Smart Scan 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 Scan Server as the primary scan source and the integrated server as a backup source. See the *Administrator's Guide* for information on configuring scan 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 2-28 for more information on the OfficeScan licenses.

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

Client Connection Protocols

Clients can connect to the integrated Smart Scan Server using HTTP and HTTPS protocols. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

The SSL port number used for secure connections depends on the Web server (Apache or IIS) you want to use for the OfficeScan server. See *Web Server Settings* on page 2-24 for more information.

TABLE 2-1. SSL port numbers for the OfficeScan server and Integrated Smart Scan Server

OFFICESCAN WEB SERVER SETTINGS	OFFICESCAN SERVER SSL PORT	INTEGRATED SMART SCAN SERVER SSL PORT
Apache Web server with SSL enabled	4343	4343
Apache Web server with SSL disabled	N/A	4345
IIS default Web site with SSL enabled	443	443
IIS default Web site with SSL disabled	N/A	443
IIS virtual Web site with SSL enabled	4343	4345
IIS virtual Web site with SSL disabled	N/A	4345

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.

Remote Installation Destination

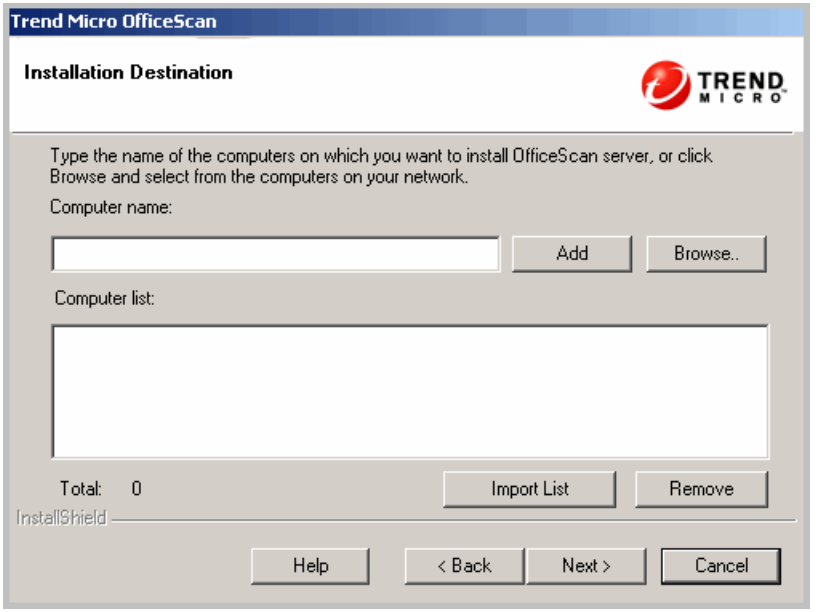


FIGURE 2-11. Remote Installation Destination screen

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).
- Use only the following characters: a-z, A-Z, 0-9, periods (.), and hyphens (-).

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 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

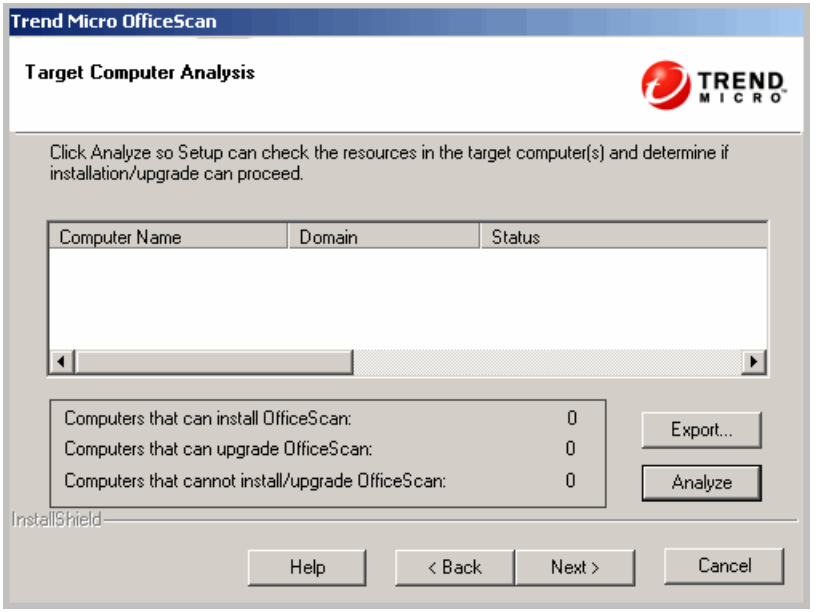


FIGURE 2-12. Target Computer Analysis screen

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).

OfficeScan Programs

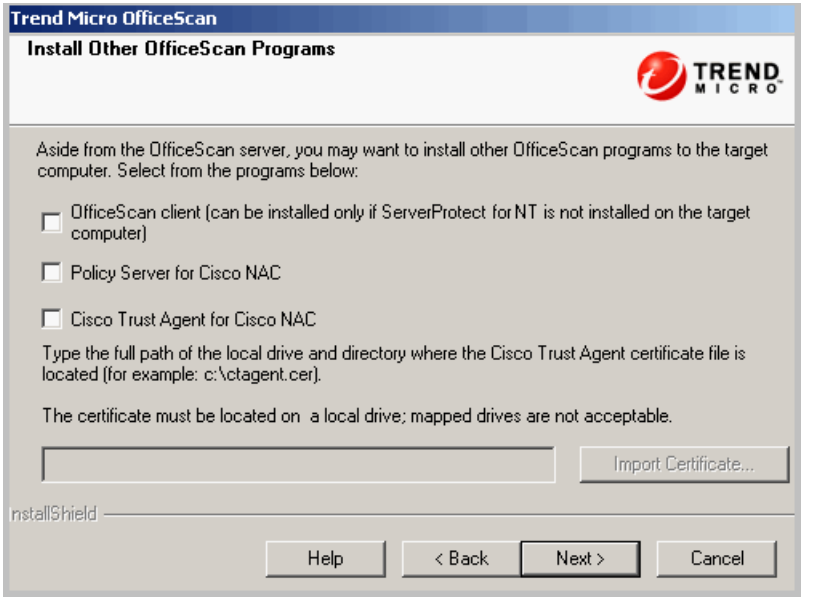


FIGURE 2-13. OfficeScan Programs Installation screen

Choose to install the following OfficeScan programs:

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 Web site, 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

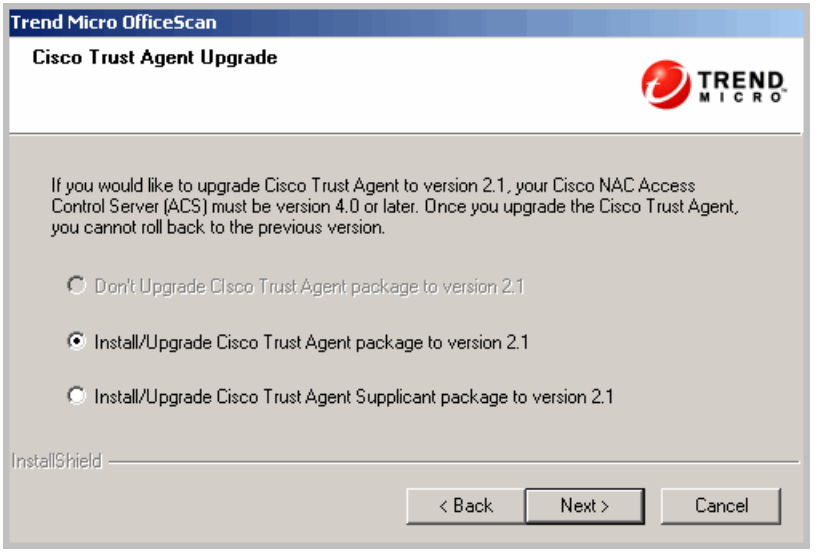


FIGURE 2-14. Cisco Trust Agent Upgrade screen

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

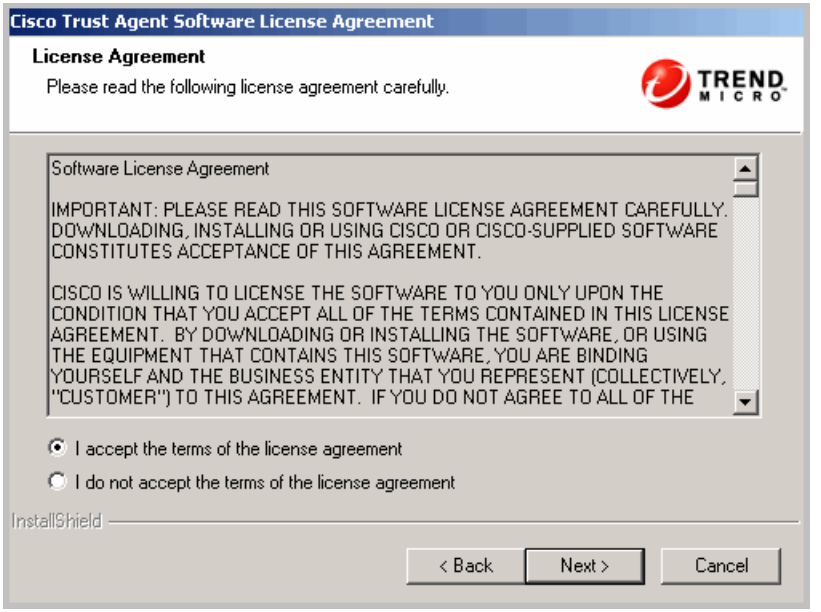


FIGURE 2-15. Cisco Trust Agent License Agreement screen

Read the license agreement carefully and accept the license agreement terms to proceed with installation.

Trend Micro Smart Protection Network

The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to protect customers from Web threats. Smart Feedback is a key element of the Smart Protection Network.

.

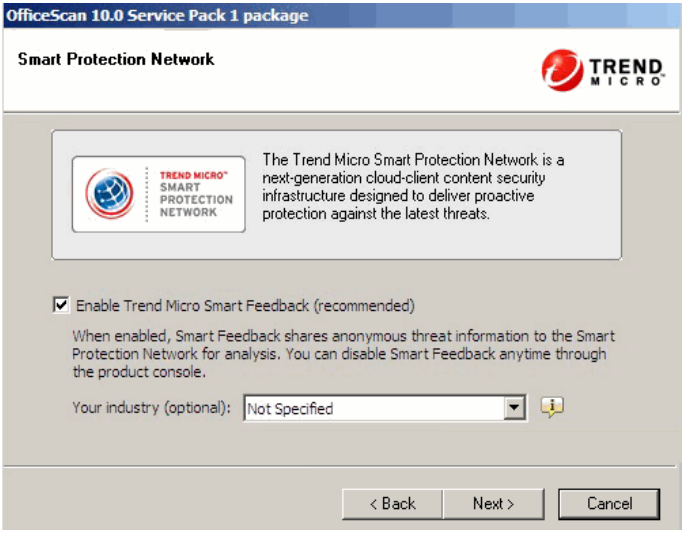


FIGURE 2-16. Smart Protection Network screen

Smart Feedback

Trend Micro Smart Feedback continually gathers and analyzes threat information to provide better protection. Select the Industry type to help Trend Micro understand your organization. Your participation in this program can benefit the attempt to better understand the development and spread of security risks.

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

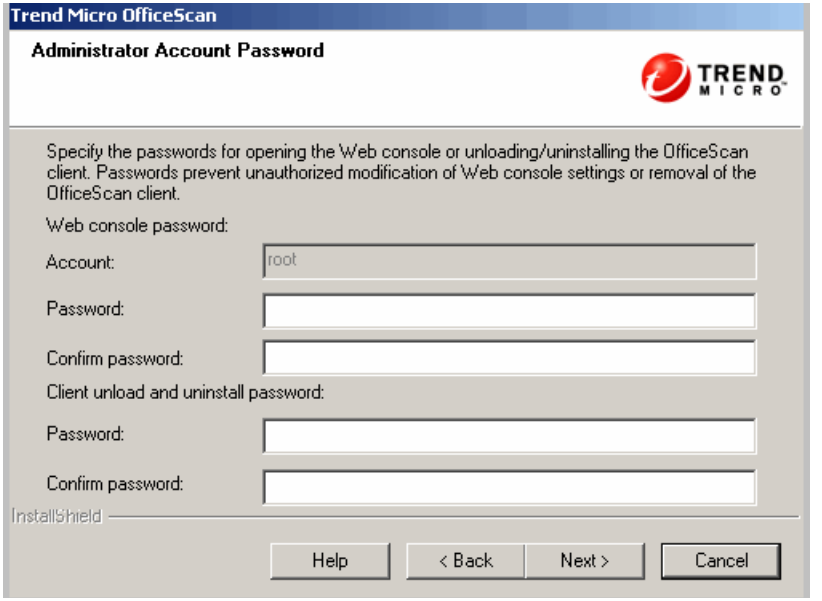


FIGURE 2-17. Administration Account Password screen

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.

Client Installation Path

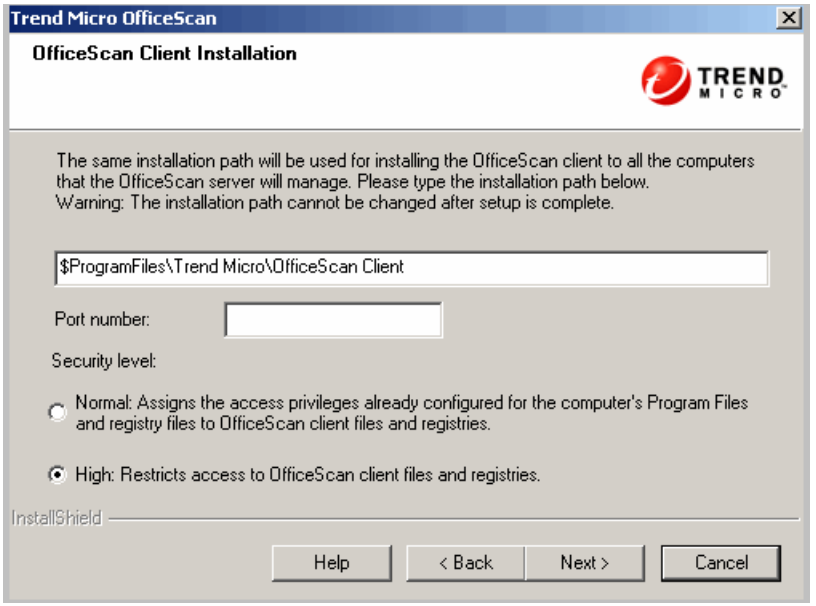


FIGURE 2-18. OfficeScan Client Installation Path screen

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:** Allows clients read/write access to the OfficeScan client folders, files, and registries on client computers.
  - **High:** Restricts clients from accessing OfficeScan client folders, files, and registries (default). If you select High, the access permissions settings of the OfficeScan folders, files, and registries are inherited from the Program Files folder (for client computers running Windows 2000, XP, or Server 2003).

Antivirus Features

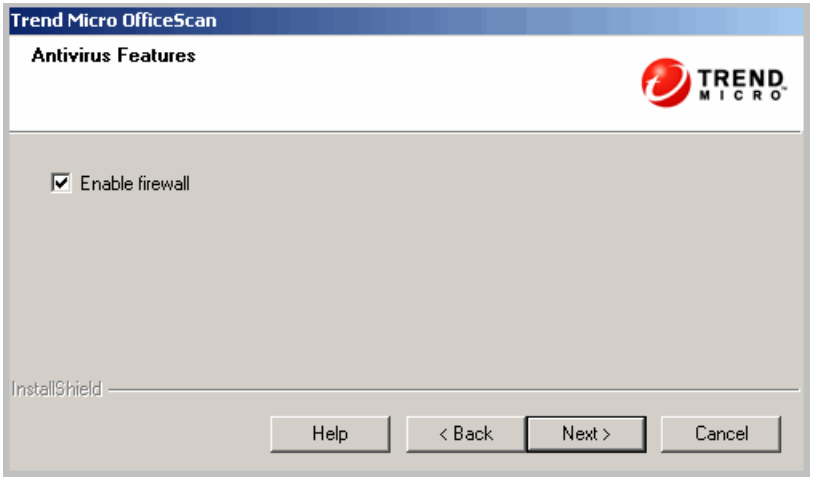


FIGURE 2-19. Antivirus Features screen

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.

Anti-spyware Feature

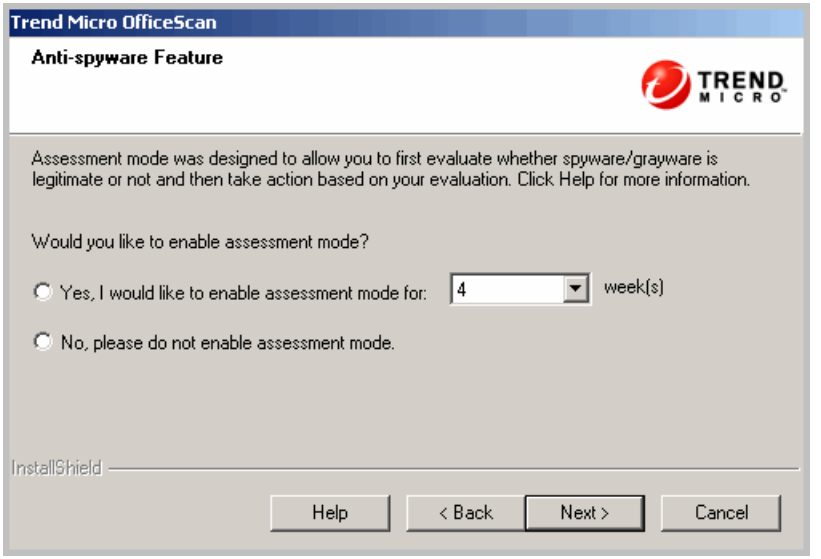


FIGURE 2-20. Anti-spyware Feature screen

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**).

Program Folder Shortcut

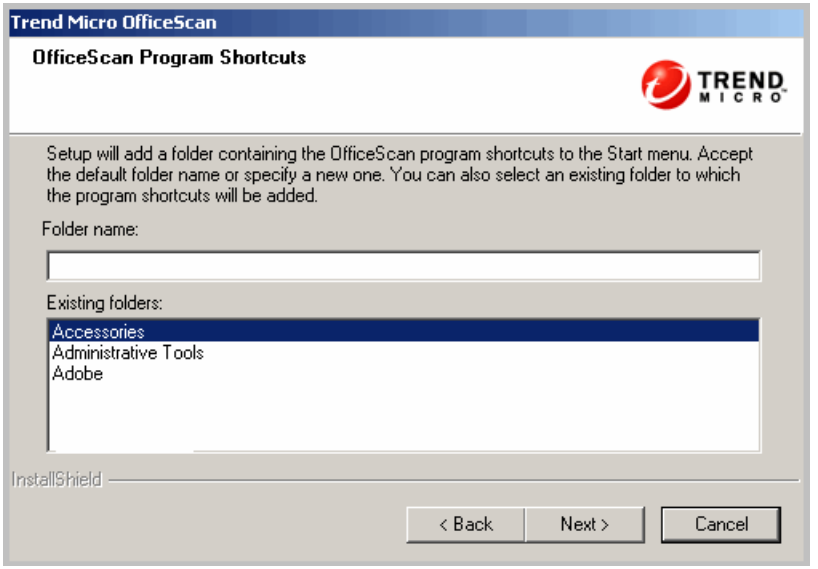


FIGURE 2-21. Program shortcuts screen

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

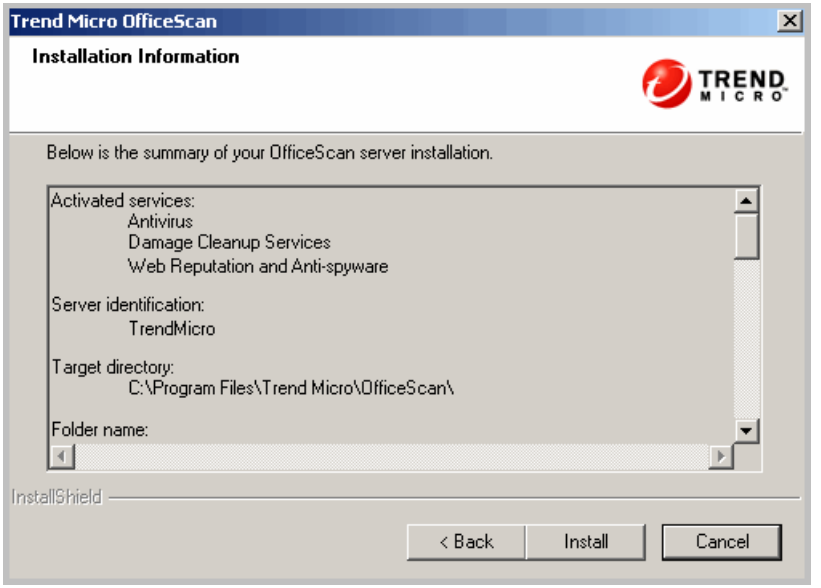


FIGURE 2-22. Installation Information screen

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**.

Policy Server Installation

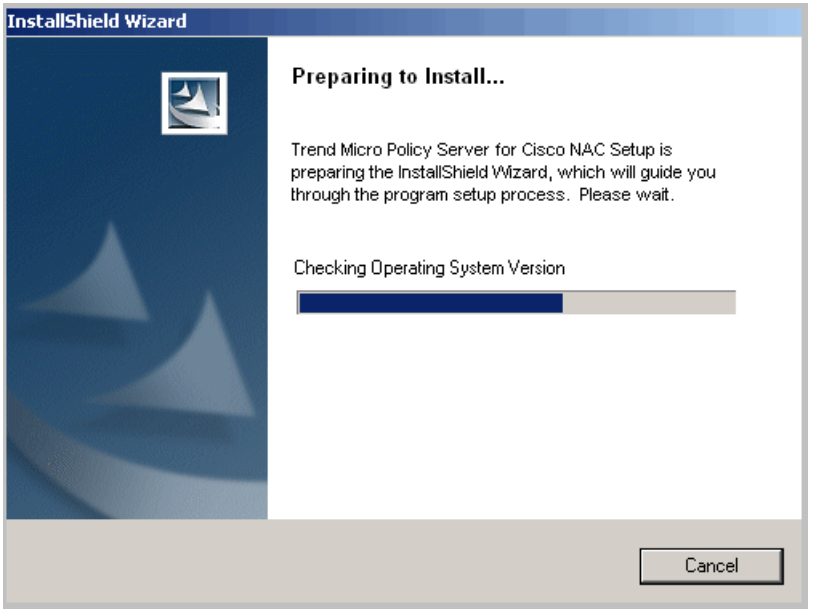


FIGURE 2-23. Policy Server Installation screen

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.

OfficeScan Server Installation Completion

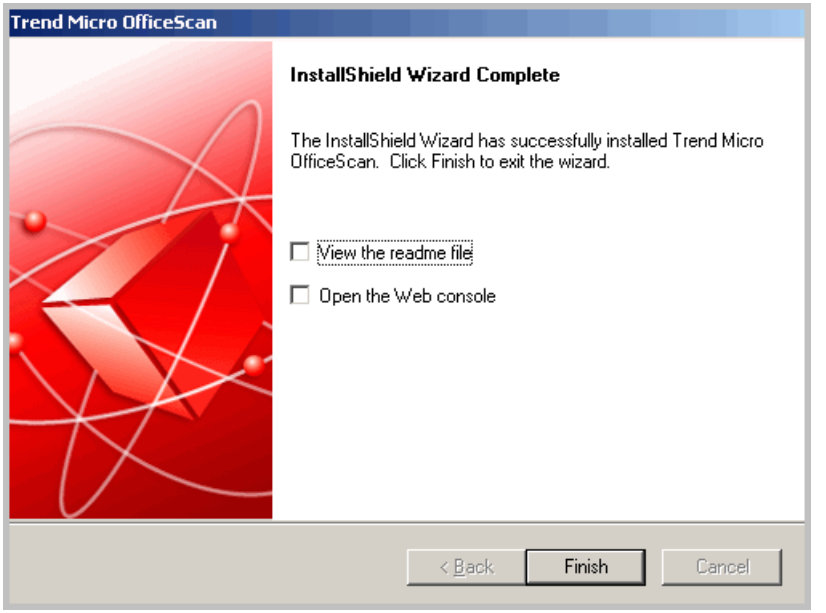


FIGURE 2-24. Installation Complete screen

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 2-51
- *Updating OfficeScan Components* on page 2-53
- *Checking Default Settings* on page 2-53
- *Using Client Mover for Legacy Platforms* on page 2-54. Perform this task only if you have clients running Windows 95, 98, Me, NT, or Itanium architecture.
- *Registering OfficeScan to Control Manager* on page 2-56. Control Manager registration only applies to newly installed OfficeScan servers.
- *Installing Plug-in Manager* on page 2-57

Verifying the Server Installation or Upgrade

After completing the installation or upgrade, verify the following:

TABLE 2-2. Items to verify after installing or upgrading OfficeScan

ITEM TO VERIFY	DETAILS
OfficeScan server shortcuts	The Trend Micro OfficeScan server shortcuts appear on the Windows **Start** menu on the server computer.
Programs list	**Trend Micro OfficeScan Server** is listed on the **Add/Remove Programs** list on the server computer's Control Panel.
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.

TABLE 2-2. Items to verify after installing or upgrading OfficeScan (Continued)

ITEM TO VERIFY	DETAILS
OfficeScan server services	The following OfficeScan server services display on the Microsoft Management Console: • OfficeScan Master Service (should be running) • Trend Micro Smart Scan Server, if you installed the integrated Smart Scan Server (the startup type is "manual") • Trend Micro Policy Server for Cisco NAC, if installed • OfficeScan Active Directory Integration Service, if the Role-based Administration function works properly • OfficeScan Control Manager Agent
OfficeScan server processes	When you open Windows Task Manager, the following OfficeScan processes are running: • OfcService.exe • DBServer.exe • iCRCService.exe, if the integrated Smart Scan Server was installed • OfcCMAgent.exe, if the OfficeScan server has been registered to Control Manager
Server installation log	The server installation log, OFCMAS.LOG, exist in %windir%.
Registry keys	The following registry key exists: HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan
Program folder	The OfficeScan server files are found under the <Server installation folder>.

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**.

Using Client Mover for Legacy Platforms

The OfficeScan client no longer supports Windows 95, 98, Me, NT, or the Itanium architecture platform. If OfficeScan clients run any of these platforms and you upgraded the server that manages them to version 10 SP1:

- The OfficeScan clients will not be upgraded.
- The OfficeScan 10 SP1 server stops managing the clients. The clients' status becomes "Disconnected".
- The OfficeScan 10 SP1 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 SP1 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 SP1 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 if the tool successfully moved the clients. This command compares the IP addresses of the OfficeScan 10 SP1 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 if 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.

Installing Plug-in Manager

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

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

Note: Refer to the Plug-in Manager readme file for installation requirements and instructions.

Performing Server Uninstallation/Rollback

If you experience problems with OfficeScan, you can:

- Use the uninstallation program to safely remove the OfficeScan server from your computer and then reinstall OfficeScan. Move all clients before removing the server.
- Roll back to version 10.0 instead of uninstalling the OfficeScan server. See *Rolling Back to OfficeScan 10* on page 2-64.

Note: There is no rollback tool available, which means you need to perform manual rollback. You cannot roll back from OfficeScan 10.0 Service Pack 1 server directly because Service Pack 1 includes some kernel drivers that cannot be rolled back automatically. You need to prepare another computer with OfficeScan 10.0 server installed.

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. From the client tree, select the clients 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 2-58.
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 Scan 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 Scan 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 as follows:

TABLE 2-3. ofcserver.ini settings

SETTING	INSTRUCTION
WSS_INSTALL=1	Change 1 to 0
WSS_ENABLE=1	Delete this line
WSS_URL=https://<computer_name>:4345/tmcss/	Delete this line

6. Navigate to <Server installation folder>\PCCSRV and open **OfUninst.ini**. Delete the following lines:
   - If using IIS Web server:

     ```
     [WSS_WEB_SERVER]
     ServerPort=8082
     IIS_VhostName=Smart Scan Server (Integrated)
     ```

     IIS_VHostIdx=5

     Note: The value for IIS_VHostidx should be the same as the "isapi" value indicated on the following line:

     ROOT=/tmcss,C:\Program Files\Trend Micro\OfficeScan\PCCSRV\WSS\isapi,,<value>

     ```
     [WSS_SSL]
     SSLPort=<SSL port>
     ```
   - If using Apache Web server:

     ```
     [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:

   ```
   Svrsvcsetup -install
   Svrsvcsetup -enablessl
   Svrsvcsetup -setprivilege
   ```
9. Verify if the following items were removed:
   - Trend Micro Smart Scan Server service from the Microsoft Management Console
   - Smart Scan Server performance counters
   - Smart Scan Server (Integrated) Web Site

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 if 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 Web site from the Internet Information Services (IIS) console.

   a. Open the IIS console.

   b. Expand **ServerName**.

   c. If you installed OfficeScan on a separate Web site, go to the **Web Sites** folder and then delete **OfficeScan**.

   d. If you installed OfficeScan virtual directories under the Default Web Site, go to **Default Web Site** and then delete the OfficeScan virtual directory.

Rolling Back to OfficeScan 10

Roll back to OfficeScan 10.0 instead of uninstalling the OfficeScan server.

Part 1: Rollback preparation

1. Prepare a computer with OfficeScan 10.0 server installed.
2. Apply hot fixes and patches released after version 10.0 to this server.
3. Duplicate or reconfigure settings on the OfficeScan 10.0 server.

   Consider the following settings:

   a. Client settings
      - Scan
      - Update Agents
      - Privileges
      - Spyware/Grayware Approved List
      - Behavior Monitoring Exception List

   b. Global client settings

   c. Web Reputation settings
      - 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 messages

i. Administration settings

- Quarantine Manager
- Control Manager Agent
- Database backup

4. Run Client Packager on the OfficeScan 10.0 server to create a client installation package.

   Settings on Client Packager screen:

   a. Package type: Setup

   b. Output file: \InstNTPkg.exe

5. Prepare an update source (another computer that will act as update source) that has components similar to or newer than the components on the current OfficeScan 10.0 Service Pack 1 server.

Tip: You can copy all component files directly from the OfficeScan 10.0 server's PCCSRV\Download folder to the update source.

Note: If you have older components on the update source, you cannot perform rollback from the server's Web console.

---

6. Package the following files:

   - RollbackAgent.dll (under \PCCSRV\Admin)
   - ClientRollback.exe (under \PCCSRV\Admin)
   - InstNTPkg.exe (for x86 computers)
   - InstNTPkg.exe (for x64 computers)

   a. Compress RollbackAgent.dll as RollbackAgent.zip.

   b. Create two folders: RollBackNTPkg and RollBackNTpkgx64.

   c. Copy ClientRollback.exe and NT Client Packager (InstNTPkg.exe) to the RollbackNTPkg folder.

d. Copy the ClientRollback.exe and NT x64 Client Packager (InstNTPkg.exe) to the RollbackNTPkgx64 folder.

e. Compress the RollbackNTPkg folder as RollbackNTPkg.zip and the RollbackNTPkgx64 folder as RollbackNTpkgx64.zip.

f. Modify the update source download file and server.ini file.

i. Copy RollbackAgent.zip, RollbackNTPkg.zip and RollbackNTPkgx64.zip to the computer acting as update source, under the folder Download\Product\.

ii. Add the server.ini file and modify as follows:

Note: Modify only the following lines. Do not change any other setting.

```
[All_Product]
MaxProductID=109
Product.109=OfficeScan Rollback, 3.5, 8.0

[Info_109_35000_1_1]
Version=10.0
Update_Path=product/RollbackAgent.zip, 90517
Path=product/RollBackNTPkg.zip, xx

[Info_109_35000_1_5633]
Version=10.0
Update_Path=product/RollbackAgent.zip, 90517
Path=product/RollBackNTPkg x64.zip, yy
```

Where:

`xx` - File size of "RollBackNTPkg.zip".

For example, 32058256.

yy - File size of RollBackNTPkg x64.zip.

For example, 36930773.

To get the file size, right-click the zip file and click **Properties**. Take note of the size, not the size on disk.

Part 2: Rolling back the OfficeScan clients

1. On the OfficeScan 10.0 Service Pack 1 Web console, configure all clients to update from the update source configured in Part 1.
   a. Go to **Updates > Networked Computers > Update Source**.
   b. Select **Customized Update Source**.
   c. On the **Customized Update Source List**, add the update source, which should contain the patch agent and client packages.
   d. Click **Notify All Clients**.

      Clients will use the patch agent to uninstall and then reinstall the OfficeScan 10.0 client during client update.
2. After reinstalling the client, inform users to restart their client computers.

   After restarting client computers, all clients will report to the OfficeScan 10.0 server prepared in Part 1.

Chapter 3

Getting Help

Topics in this chapter:

- *Troubleshooting Resources* on page 3-2
- *Contacting Trend Micro* on page 3-6

Troubleshooting Resources

Case Diagnostic Tool

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

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

Installation Logs

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

TABLE 3-1. Installation log files

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

Server Debug Logs

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

- Uninstall and then install the server again.
- Upgrade OfficeScan 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".
3. Specify debug log settings.
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://www.trendmicro.com/support

- Get the latest Trend Micro product documentation at:

  http://www.trendmicro.com/download

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

Trend Micro, Inc.

10101 North De Anza Blvd., Cupertino, CA 95014

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

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

Fax: +1 (408) 257-2003

Web address:

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

http://esupport.trendmicro.com

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

TrendLabs

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

You can rely on the following post-sales service:

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

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

Comprehensive security information is available at the Trend Micro Web site.

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

Information available:

- List of viruses and malicious mobile code currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

Sending Suspicious Files to Trend Micro

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

http://subwiz.trendmicro.com/subwiz

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

- Send an email to 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

Appendix A

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.

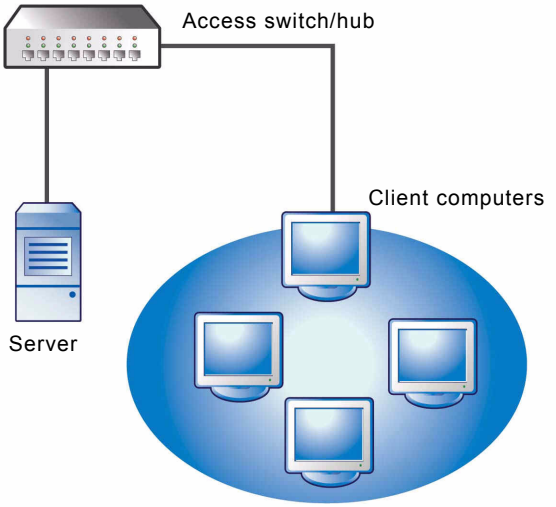


FIGURE A-1. Basic network topology

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.

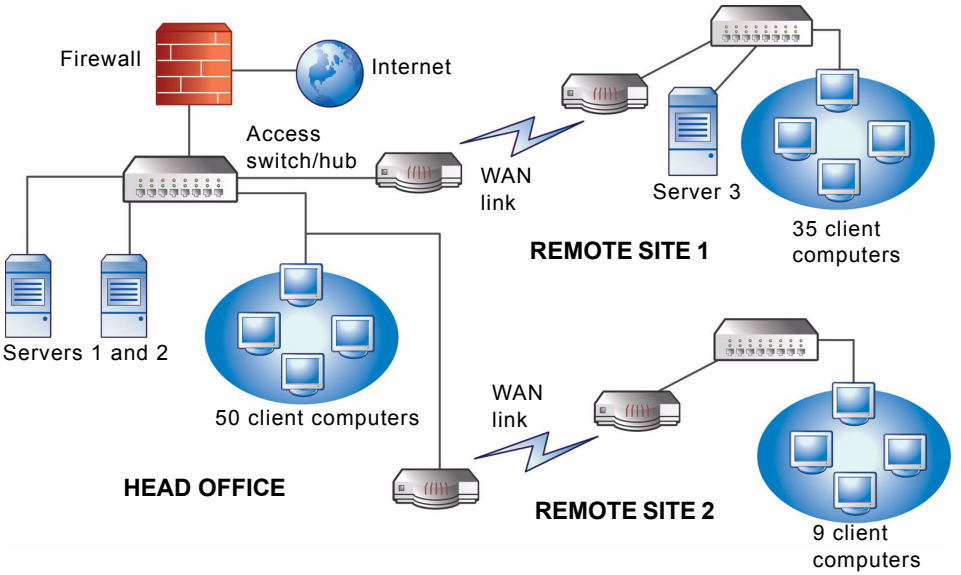


FIGURE A-2. Multiple site network topology

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 2000. The network uses Active Directory, but mainly for network authentication.
- All client computers in Head Office, Remote Site 1, and Remote Site 2 run Windows 2000 or Windows XP.

Tasks:

1. Identify the computer where you will install the OfficeScan server. See *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 2000, it is simple to deploy the package to the computers.

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

   - Client package deployment

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

Head Office Deployment

The easiest client deployment method to implement at the head office is remote installation from the OfficeScan Web console. See 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.

Appendix B

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-2. Legacy OfficeScan features

FEATURE	AVAILABILITY		STATUS IN OFFICESCAN 10 SP1
	8.x	7.x	
Trend Micro OfficeScan for Wireless	No	Yes	Trend Micro OfficeScan for Wireless has been replaced by Trend Micro Mobile Security™, which is available as a plug-in program.
Wireless Protection Manager	No	Yes	Wireless Protection Manager has been replaced by Trend Micro Mobile Security, which is available as a plug-in program.
DCS scan (client-initiated)	No	Yes	DCS scan is performed automatically during scanning.

TABLE B-2. Legacy OfficeScan features (Continued)

FEATURE	AVAILABILITY		STATUS IN OFFICESCAN 10 SP1
	8.x	7.x	
DCS Cleanup Now (server-initiated)	No	Yes	DCS Cleanup Now is performed automatically during scanning.
Scheduled clean (a global client setting)	No	Yes	Scheduled clean is performed automatically during scanning.
Virus Outbreak Monitor	No	Yes	Virus Outbreak Monitor settings are configured under **Notifications > Administrator Notifications > Outbreak Notifications > Shared Folder Session**.
Firewall Outbreak Monitor	No	Yes	Firewall Outbreak Monitor settings are configured under **Notifications > Administrator Notifications > Outbreak Notifications > Firewall Violations**.
OfficeScan Watchdog	Yes	Yes	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's Global Client Settings screen.

Index

A

ACS Server 1-30, 2-37, 2-50
activation 1-26, 2-28
Activation Code 1-15, 1-26, 2-28, 2-31
Active Directory 1-20, A-5
Apache Web server 1-20, 2-24, 2-49
assessment mode 2-46
automatic client upgrade 2-4, 2-6, 2-10

B

backup
  OfficeScan database 1-21, 2-59
  OfficeScan server files and folders 1-21, 2-59

C

Case Diagnostic Tool 3-2
Cisco NAC 2-37
Cisco Trust Agent 1-27, 2-38–2-40
client debug logs 3-5
client installation path 1-28, 2-43
Client Mover 2-58
Client Mover for Legacy Platforms 2-54
Client Packager A-4
compatibility issues 1-31
component duplication 1-19
component updates 1-19
components 2-53
considerations
  fresh installation 1-15
  upgrade 1-21
Control Manager 1-19, 2-56
conventional scan 1-17, 2-3

D

database backup 1-21, 2-59
debug logs
  client 3-5
  server 3-3
default settings
  client privileges 2-54
  global client settings 2-53
  scan settings 2-53
Distributed File System (DFS) A-5
documentation feedback 3-9

E

evaluation version 1-14, 2-14

F

firewall 2-45
fresh installation 2-2
  checklist 1-23
  considerations 1-15
  silent 2-11
  summary 2-48
  system requirements 1-2
  verification 2-51
full version 1-14

H

HTTP port 1-25, 1-30, 2-25

I

IIS Web server 1-20, 2-24, 2-49
incremental pattern 1-19
installation
  logs 3-2

Policy Server 1-30, 2-49
post-installation tasks 2-51
screens and tasks 2-15
silent 2-11
installation destination 2-19
installation path
client 1-28, 2-43
server 1-23, 2-22
integrated Smart Scan Server 1-17, 2-60
client connection protocols 2-31
installation 1-26, 2-30
uninstallation 2-61
Internet Connection Firewall 1-32

K

Knowledge Base 3-7

L

legacy features B-1
lockdown tools 1-32
Login Script Setup A-4

M

manual client upgrade 2-6
manual update 2-53
Microsoft Exchange Server 1-32
MSI package deployment A-5

N

network traffic 1-18

O

OfficeScan client
debug logs 3-5
installation 2-36
security level 2-44
unload 2-43
upgrade 2-2
OfficeScan firewall 2-45
OfficeScan server
capacity 1-17
debug logs 3-3
default settings 2-53
fresh installation 2-2
functions 1-17
identification 2-27
installation logs 2-52
installation summary 2-48
location 1-16
manage using Control Manager 1-19
manual update 2-53
master service 2-24, 2-52
performance 1-16
processes 2-52
product services 1-15
register to Control Manager 2-56
registry keys 2-52
services 2-52
silent installation/upgrade 2-11
uninstallation 2-57
upgrade 2-2
outbreak monitor B-2

P

passwords 1-28, 1-30, 2-42, 2-49
pilot deployment
evaluation 1-31
pilot site 1-31
rollback plan 1-31
Plug-in Manager 2-57
Policy Server 1-30, 2-37, 2-49
port
client communication port 1-28, 2-44
HTTP port 1-25, 2-25

ISA port 1-31
proxy server port 1-24
server listening port 1-22, 2-8
SSL port 1-25, 2-25, 2-32
post-installation 2-51
prescan 2-21
program folder shortcut 1-29, 2-47, 2-51
program settings 2-59
proxy server 1-24, 2-23

R

readme file 2-50
registration 1-26, 2-28
Registration Key 1-15
remote installation 1-16, 1-27, 2-20, 2-33, 2-35, A-4
response file 2-12
Role-based Administration 1-2
root account 1-28, 2-42
RSA encryption 2-26

S

sample deployment A-1
scan action 2-21
scan method 1-17–1-18, 1-23
scheduled clean B-2
Security Compliance 1-20
Security Information Center 3-8
Setup 2-15
silent installation 2-11
Smart Feedback 2-41
Smart Protection Network 2-41
smart scan 1-17, 2-30
Smart Scan Server 1-17, 1-26, 2-30–2-31, 2-60–2-61
SQL server 1-32
SSL port 1-25, 1-30, 2-26, 2-32
SSL tunneling 2-26
standalone Smart Scan Server 2-31
suspicious files 3-9
system requirements
fresh installation 1-2
upgrade 1-8

T

Technical Support 3-6
third-party security software 1-20
troubleshooting 3-2
troubleshooting resources 3-2

U

uninstallation 2-57
manual 2-61
using the uninstallation program 2-60
unsupported operating systems 1-22, 2-54
Update Agent 1-19
updates 1-19
upgrade
checklist 1-23
client base size 2-3
clients 2-6, 2-9, 2-11
considerations 1-21
from an evaluation version 2-14
from version 7.x 1-10, 1-12
from version 8.x 1-8, 1-10
methods 2-3
server and clients 2-2
silent 2-11
summary 2-48
system requirements 1-8
verification 2-51
URLScan 1-32

V

virtualization applications 1-3

W

Watchdog B-2
Web console 1-7, 2-42, 2-50–2-51
Web server 1-6, 1-20, 1-25, 2-24
Wireless Protection Manager B-1