TREND MICRO™

11.0 OfficeScan™

Installation and Upgrade Guide

For Enterprise and Medium Business

Endpoint Security

Protected Cloud

Web Security

TREND MICRO SMART PROTECTION NETWORK™

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/enterprise/officescan.aspx

Document Part No.: OSEM115885_130313

Release Date: April 2014

Protected by U.S. Patent No.: 5,951,698

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

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.

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Chapter 1: Planning OfficeScan Installation

Chapter 2: Installing OfficeScan

Chapter 3: Upgrading OfficeScan

Chapter 4: Post-installation Tasks

Chapter 5: Uninstalling and Rolling Back OfficeScan

Chapter 6: Getting Help

Appendix A: Sample Deployment

Index

Preface

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 agents.

Topics in this chapter:

- *OfficeScan Documentation on page viii*
- *Audience on page viii*
- *Document Conventions on page ix*
- *Terminology on page x*

Note

For information on installing agents, see the *Administrator's Guide*.

OfficeScan Documentation

OfficeScan documentation includes the following:

TABLE 1. OfficeScan Documentation

DOCUMENTATION	DESCRIPTION
Installation and Upgrade Guide	A PDF document that discusses requirements and procedures for installing the OfficeScan server
Administrator’s Guide	A PDF document that discusses getting started information, agent installation procedures, and OfficeScan server and agent management
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, agent, 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 website: http://esupport.trendmicro.com

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

http://docs.trendmicro.com/en-us/enterprise/officescan.aspx

Audience

OfficeScan documentation is intended for the following users:

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

- End users: Users who have the OfficeScan agent installed on their endpoints. The endpoint skill level of these individuals ranges from beginner to power user.

Document Conventions

The documentation uses the following conventions.

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Terminology

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

Table 3. OfficeScan Terminology

Terminology	Description
Administrator (or OfficeScan administrator)	The person managing the OfficeScan server
Agent endpoint	The endpoint where the OfficeScan agent is installed

`Agent installation folder`	The folder on the endpoint that contains the OfficeScan agent 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\Trend Micro (x86)\OfficeScan Client`

Agent user (or user)	The person managing the OfficeScan agent on the agent endpoint
Components	Responsible for scanning, detecting, and taking actions against security risks
Console	The user interface for configuring and managing OfficeScan server and agent settings The console for the OfficeScan server program is called "web console", while the console for the OfficeScan agent program is called "agent console".
Conventional scan agent	Any OfficeScan agent that has been configured to use conventional scan

Terminology	Description
Dual-stack	Entities that have both IPv4 and IPv6 addresses. For example: • Endpoints with both IPv4 and IPv6 addresses • OfficeScan agents installed on dual-stack endpoints • Update Agents that distribute updates to agents • A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses
License service	Includes Antivirus, Damage Cleanup Services, and Web Reputation and Anti-spyware—all of which are activated during OfficeScan server installation
OfficeScan agent	The OfficeScan agent program
OfficeScan service	Services hosted through Microsoft Management Console (MMC). For example, `ofcservice.exe`, the OfficeScan Master Service.
Plug-in solutions	Native OfficeScan features and plug-in programs delivered through Plug-in Manager
Program	Includes the OfficeScan agent, Cisco Trust Agent, and Plug-in Manager
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address
Security risk	The collective term for virus/malware, spyware/grayware, and web threats
Server	The OfficeScan server program
Server computer	The endpoint where the OfficeScan server is installed

Terminology	Description

`Server installation folder`	The folder on the endpoint 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\Trend Micro (x86)\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 agent	Any OfficeScan agent that has been configured to use smart scan

Chapter 1

Planning OfficeScan Installation

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

Topics in this chapter:

- *Fresh Installation and Upgrade Requirements on page 1-2*
- *Product Versions on page 1-2*
- *Registration Key and Activation Codes on page 1-3*
- *Fresh Installation Considerations on page 1-4*
- *Installation and Upgrade Checklist on page 1-15*
- *Planning a Pilot Deployment on page 1-21*
- *Known Compatibility Issues on page 1-22*

Fresh Installation and Upgrade Requirements

Perform a fresh installation of the OfficeScan server and agents on supported Windows server platforms.

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

- 10.6 Service Pack 3
- 10.6 Service Pack 2
- 10.6 Service Pack 1 Patch 1
- 10.6
- 10.5 Patch 5
- 10.0 Service Pack 1 Patch 5

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

http://docs.trendmicro.com/en-us/enterprise/officescan.aspx

Product Versions

Install either a full or trial version of OfficeScan. Both versions require a different type of Activation Code. To obtain an Activation Code, register the product with Trend Micro.

TABLE 1-1. Version Comparison

VERSION	DESCRIPTION
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. After the grace period expires, technical support and component updates are not available. The scan engines continue to scan endpoints using out-of-date components. These out-of-date components may not be able to protect endpoints completely from the latest security risks. Renew the license before or after it expires by purchasing a maintenance renewal.
Trial Version	The trial version includes all the product features. Upgrade a trial version to the full version at any time. If not upgraded at the end of the trial period, OfficeScan disables component updates, scanning, and all agent features.

Registration Key and Activation Codes

During installation, specify the Activation Codes for the following services:

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

Use the Registration Key that came with the product to obtain Activation Codes (if not already obtained). Setup automatically redirects to the Trend Micro website for product registration.

http://olr.trendmicro.com

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

Contact a Trend Micro sales representative to obtain the Registration Key or Activation Codes, if neither is available at the time of installation. See *Contacting Trend Micro on page 6-10* 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:

- *IPv6 Support on page 1-4*
- *Location of the OfficeScan Server on page 1-5*
- *Remote Installation on page 1-6*
- *Server Performance on page 1-6*
- *Dedicated Server on page 1-7*
- *Scan Method Deployment During Installation on page 1-7*
- *Network Traffic on page 1-8*
- *Third-Party Security Software on page 1-10*
- *Active Directory on page 1-10*
- *Web Server on page 1-10*

IPv6 Support

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

- The OfficeScan server must be installed on Windows Server 2008 or Windows Server 2012. It cannot be installed on Windows Server 2003 because this operating system only supports IPv6 addressing partially.
- The server must use an IIS web server. Apache web server does not support IPv6 addressing.

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

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

Note

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

- Verify that the host machine's IPv6 or IPv4 address can be retrieved using, for example, the "`ping`" or "`nslookup`" command.

- If you are installing the OfficeScan server to a pure IPv6 endpoint:

    - Set up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the OfficeScan server and the Internet to allow the server to successfully connect to Trend Micro hosted services, such as the ActiveUpdate server, the Online Registration website, and Smart Protection Network.

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 agents, or position both the server and all agents behind a single network firewall. If there is a firewall between the server and its agents, configure the firewall to allow traffic between the agent and server listening ports.

Note

For information on resolving potential problems when managing OfficeScan agents on a network that uses Network Address Translation, see the *Administrator's Guide*.

Remote Installation

Remote installation allows launching the installation on one endpoint and installing OfficeScan on another endpoint. When performing a remote installation, Setup checks if the target endpoint meets the requirements for server installation.

To ensure that installation can proceed:

- On each target endpoint, 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 endpoint's host name and logon credentials (user name and password).
- Verify that the endpoint meets the OfficeScan server system requirements. Refer to *Fresh Installation and Upgrade Requirements on page 1-2* for more information.

Server Performance

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

Tip

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

The number of networked endpoint agents 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 agents the server can manage.

The typical number of agents the OfficeScan server can manage are as follows:

- 3,000 to 5,000 agents for OfficeScan servers with 2GHz dual processor with 2GB of RAM
- 5,000 to 20,000 agents for OfficeScan servers with 2.13GHz Core2Duo™ processor with 4GB of RAM

Dedicated Server

When selecting the endpoint to host the OfficeScan server, consider the following:

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

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

Scan Method Deployment During Installation

In this OfficeScan version, you can configure agents 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 agent stores all OfficeScan components on the agent endpoint 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 agent first scans for security risks locally. If the agent cannot determine the risk of the file during the scan, the agent connects to a Smart Protection Server.

Smart Scan provides the following features and benefits:

- Provides fast, real-time security status lookup capabilities in the cloud

- Reduces the overall time it takes to deliver protection against emerging threats
- Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud and not to many agents.
- 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

During fresh installations, the default scan method for agents is the Smart Scan method. OfficeScan also allows you to customize the scan method for each domain after installing the server. Consider the following:

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

Network Traffic

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

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

The OfficeScan agent 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.

OfficeScan agents 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 agents and the OfficeScan server, designate selected OfficeScan agents as Update Agents, or update sources for other agents. This helps distribute the burden of deploying components to all agents.

For example, if you have a remote office with 20 or more endpoints, designate an Update Agent to replicate updates from the OfficeScan server and act as a distribution point for other agent endpoints 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.

For details, see the Control Manager documentation.

Third-Party Security Software

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

Note

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

Active Directory

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

Web Server

The OfficeScan web server's functions are as follows:

- Allows users to access the web console
- Accepts commands from agents
- Allows agents 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 agents:

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

IPv6 Support

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

- The OfficeScan server to be upgraded must be installed on Windows Server 2008 or 2012. OfficeScan servers on Windows Server 2003 cannot be upgraded because Windows Server 2003 only supports IPv6 addressing partially.
- The OfficeScan server to be upgraded must be version 10.x.

- The server must already be using an IIS web server. Apache web server does not support IPv6 addressing.
- Assign an IPv6 address to the server. In addition, the server must be identified by its host name, preferably its fully qualified domain name (FQDN). If the server is identified by its IPv6 address, all agents currently managed by the server lose connection with the server. If the server is identified by its IPv4 address, it cannot deploy the agent to pure IPv6 endpoints.
- Verify that the host machine’s IPv6 or IPv4 address can be retrieved using, for example, the **`ping`** or **`nslookup`** command.

Unsupported Operating Systems

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

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

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

If you have upgraded the OfficeScan server but did not move unsupported agents, use a tool called Client Mover for Legacy Platforms to move the agents to a parent server that can manage them. For details about the tool, see *Using Client Mover for Legacy Platforms on page 4-5*.

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.

Tip

This version of OfficeScan provides a backup mechanism for rollback purposes. Perform a manual database back up if you do not plan on using the automated back up during installation.

Backing up and Restoring the OfficeScan Database and Configuration Files

Procedure

1. Back up the database from the OfficeScan 10.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 agent settings
- `ous.ini`: Contains the update source table for antivirus component deployment
- `Private` folder: Contains firewall and update source settings
- `Web\tmOPP` folder: Contains Outbreak Prevention settings
- `Pccnt\Common\OfcPfw*.dat`: Contains firewall settings
- `Download\OfcPfw*.dat`: Contains firewall deployment settings
- `Log` folder: Contains system events and the connection verification logs
- `Virus` folder: Contains quarantined files
- `HTTPDB` folder: Contains the OfficeScan database

4. Upgrade the OfficeScan server.

Note

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

Scan Method Deployment During Upgrade

In this OfficeScan version, administrators can configure agents to use either Smart Scan or Conventional Scan.

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

- When planning to upgrade the OfficeScan 10.x server directly on the server computer, it is not necessary to make scan method changes from the web console because agents retain their scan method settings after they upgrade.
- When planning to upgrade OfficeScan 10.x agents by moving them to the OfficeScan 11.0 server:
  - In the OfficeScan 11.0 server, choose manual agent grouping. This agent grouping method allows for the creation of new domains.

    Note

    When using automatic agent grouping, enable it only after all agents have upgraded to ensure that all scan method settings are retained during agent upgrade.

  - Duplicate the domain structure and scan method settings in the OfficeScan 10.x server into the OfficeScan 11.0 server. If the domain structure and scan method settings on the two servers are not identical, some agents that move to the OfficeScan 11.0 server may not apply their original scan method settings.

Installation and Upgrade Checklist

Setup prompts for the following information when installing or upgrading the OfficeScan server.

TABLE 1-2. Installation and Upgrade Checklist

INSTALLATION INFORMATION	INFORMATION NEEDED DURING			
	LOCAL/ SILENT FRESH INSTALL	REMOTE FRESH INSTALL	LOCAL/ SILENT UPGRADE	REMOTE UPGRADE
OfficeScan 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 or use the default path. If the path does not exist, Setup creates it automatically.	Yes	Yes	No	Yes
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

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 agents. 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 the default port numbers are currently in use. If enabling secure connections: • SSL certificate validity period • SSL port (Default: 4343)	Yes	Yes	No	Yes

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. The following information is necessary to register the product: • 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 Protection Server installation When installing the integrated server, specify the following: • SSL certificate validity period • SSL port	Yes	Yes	Yes	Yes

Installation Information	Information needed during			
	Local/ Silent Fresh Install	Remote Fresh Install	Local/ Silent Upgrade	Remote Upgrade

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

Remote installation endpoint analysis Setup prompts for the following information before performing target endpoint analysis: • User name and password for an administrator account with "logon as a service" privilege on the target endpoint	No	Yes	No	Yes
Install the OfficeScan agent	Yes	No	No	No

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 agent by specifying the following: • OfficeScan agent uninstallation/ unloading password	Yes	Yes	No	No
OfficeScan Agent installation path Specify the directory on the agent endpoint where the OfficeScan agent installation occurs. Specify the following: • Installation path: The default agent installation path is `$ProgramFiles\Trend Micro\OfficeScan Client`. Identify the installation path or use the default path. If the path does not exist, Setup creates it during agent installation. • OfficeScan Agent communication port number: OfficeScan generates the port number randomly. Accept the generated port number or specify a new one.	Yes	Yes	No	No

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 or use the default name.	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 needed after full deployment. It gives your installation team a chance to rehearse and refine the deployment process. It also allows administrators to test if the deployment plan meets the 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 when installing OfficeScan server on the same endpoint with certain third-party applications. Refer to the documentation of third-party applications for details.

Microsoft Lockdown Tools and URLScan

When using the Microsoft IIS Lockdown Tool or URLScan, lockdown of the following OfficeScan files may block OfficeScan agent and server communication:

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

Preventing URLScan Interference in Agent-Server Communication

Procedure

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

When installing the OfficeScan agent during server installation, OfficeScan needs access to all files that the agent scans. Since Microsoft Exchange Server queues messages in local directories, it is necessary to exclude these directories from scanning which allows the Exchange Server to process email messages.

OfficeScan automatically excludes all Microsoft Exchange 2000/2003 directories from scanning. Configure this setting on the web console (**Agents** > **Global Agent Settings > Scan Settings**). For Microsoft Exchange 2007 scan exclusion details, refer to:

http://technet.microsoft.com/en-us/library/bb332342(EXCHG.80).aspx

Database Servers

Administrators can scan database servers, however, this may decrease the performance of applications that access the databases. Consider excluding databases and their backup folders from Real-Time Scan. Perform a Manual Scan during off-peak hours to minimize the impact of the database scans.

Internet Connection Firewall (ICF)

Windows Server 2003 provides a built-in firewall called Internet Connection Firewall (ICF). When running 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 OfficeScan

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

Topics in this chapter:

Performing a Fresh Installation of the OfficeScan Server

To perform fresh installations, run Setup on endpoints that meet the OfficeScan server installation and upgrade requirements (for details, see *Fresh Installation and Upgrade Requirements on page 1-2*). Setup installs the OfficeScan server and Plug-in Manager 2.1. This Plug-in Manager version provides the widget functionality in OfficeScan. For information on the installation screens and configuration options, see the *The Setup Installation Screens on page 2-4*.

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

Silent Installation

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

When silent installation runs on the target endpoint, Setup installs OfficeScan 11.0 and Plug-in Manager 2.1. Plug-in Manager 2.1 provides the widget functionality in OfficeScan.

Preparing for Silent Installation

Procedure

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 use the settings.

   Important

   - Setup only shows screens for local installation.
   - For fresh installations, create a response file from any endpoint without the 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.

Recording Setup Configuration to a Response File

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

Procedure

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%`.

Running Silent Installation

Procedure

1. Copy the installation package and `setup.iss` to the target endpoint.

2. In the target endpoint, 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 endpoint.

5. To determine if installation was successful:

- Check the OfficeScan program shortcuts on the target endpoint. If the shortcuts are not available, retry the installation.
- Log on to the OfficeScan web console.

The Setup Installation Screens

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

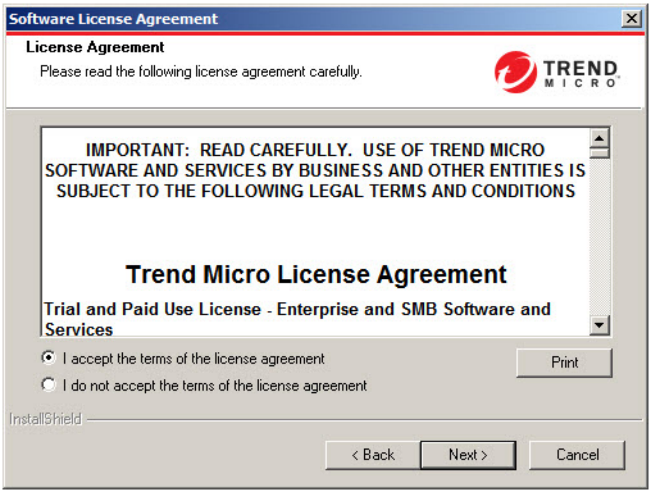
Table 2-1. Installation Screens and Tasks

Screens	Local/ Silent Fresh Install	Remote Fresh Install
OfficeScan Setup Prerequisites	✓	✓
Welcome	✓	✓

Screens	Local/ Silent Fresh Install	Remote Fresh Install
License Agreement on page 2-7	✓	✓
Installation Destination on page 2-8	✓	✓
Endpoint Prescan on page 2-9	✓	✓
Setup Status (Endpoint Analysis) **Note** Analysis may take some time to complete, especially during HTTP server initialization.	✓	
Installation Path on page 2-10	✓	✓
Proxy Server on page 2-11	✓	✓
Web Server on page 2-12	✓	✓
Server Identification on page 2-16	✓	✓
Registration and Activation on page 2-18	✓	✓
OfficeScan Agent Deployment on page 2-20	✓	✓
Install Integrated Smart Protection Server on page 2-20	✓	✓
Enable Web Reputation Services on page 2-23	✓	✓
Installation Destination on page 2-25		✓

Screens	Local/ Silent Fresh Install	Remote Fresh Install
Target Endpoint Analysis on page 2-26		✓
Install OfficeScan Agent on page 2-27	✓	✓
Smart Protection Network on page 2-28	✓	✓
Administrator Account Password on page 2-30	✓	✓
OfficeScan Agent Installation on page 2-31	✓	✓
OfficeScan Firewall on page 2-33	✓	✓
Anti-spyware Feature on page 2-34	✓	✓
Web Reputation Feature on page 2-35	✓	✓
Server Authentication Certificate on page 2-36	✓	✓
OfficeScan Program Shortcuts on page 2-39	✓	
Installation Information on page 2-40	✓	✓
OfficeScan Server Installation	✓	✓
InstallShield Wizard Complete on page 2-41	✓	✓

License Agreement



Software License Agreement

License Agreement

Please read the following license agreement carefully.

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

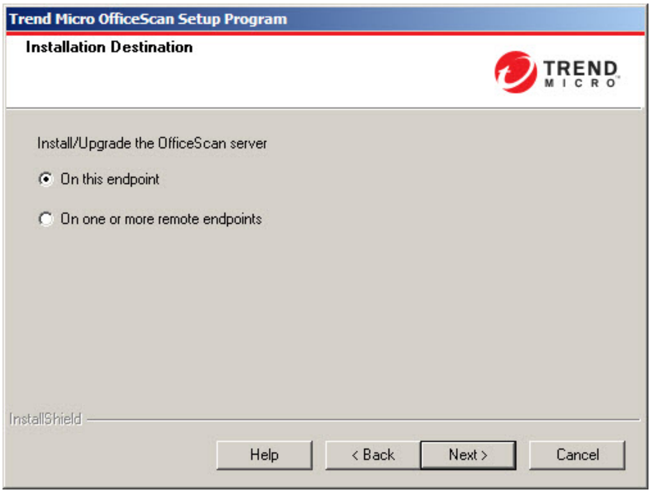
● I accept the terms of the license agreement

○ I do not accept the terms of the 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 without accepting the license agreement terms.

Installation Destination


Trend Micro OfficeScan Setup Program

Installation Destination

Install/Upgrade the OfficeScan server

● On this endpoint

○ On one or more remote endpoints

FIGURE 2-2. Installation Destination screen

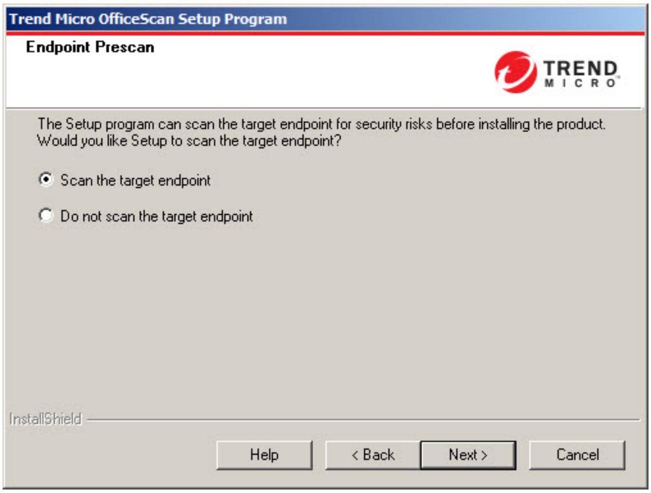
Run Setup and install the OfficeScan server on the current endpoint or other endpoint(s) on the network.

Remote Installation Notes

When installing remotely, Setup checks if the target endpoint meets the requirements for server installation. Before proceeding:

- Obtain administrator rights to the target endpoint.
- Record the endpoint's host name and logon credentials (user name and password).
- Verify that the target endpoints meet the requirements for installing the OfficeScan server.
- Ensure the endpoint has Microsoft IIS server 6.0 or later if using this as the web server. When using Apache web server, Setup automatically installs this server if not present on the target endpoint.

Endpoint Prescan



Trend Micro OfficeScan Setup Program

Endpoint Prescan

The Setup program can scan the target endpoint for security risks before installing the product. Would you like Setup to scan the target endpoint?

● Scan the target endpoint

○ Do not scan the target endpoint

FIGURE 2-3. Endpoint Prescan screen

Before the OfficeScan server installation commences, Setup can scan the target endpoint for viruses and malware. Setup scans the most vulnerable areas of the endpoint, which include the following:

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

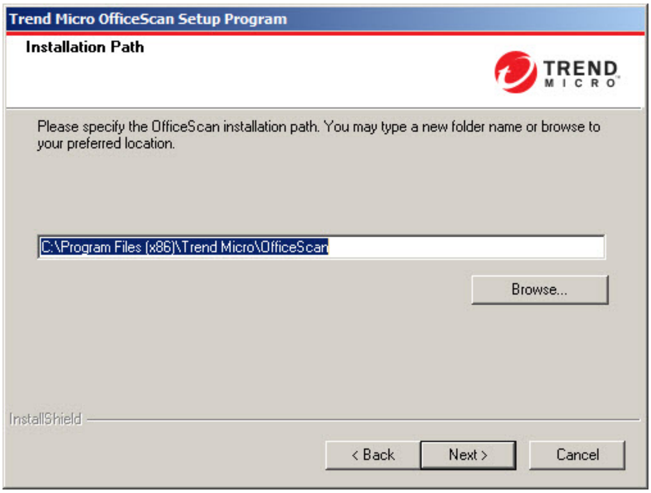
Setup can perform the following actions against detected virus/malware and Trojan horse programs:

- **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.

When performing a local installation, scanning occurs by clicking **Next**. When performing a remote installation, scanning occurs right before the actual installation.

Installation Path



Please specify the OfficeScan installation path. You may type a new folder name or browse to your preferred location.

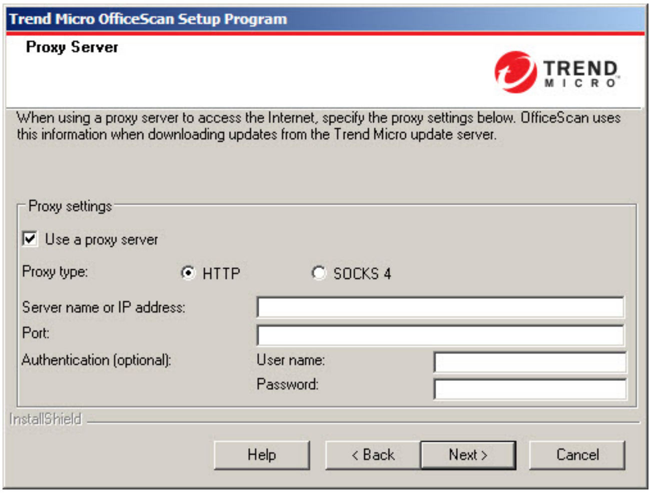
C:\Program Files (x86)\Trend Micro\OfficeScan

FIGURE 2-4. Installation Path screen

Accept the default installation path or specify a new one.

The specified installation path applies only when performing a remote fresh installation. For remote upgrades, OfficeScan uses the previous version's settings

Proxy Server



Trend Micro OfficeScan Setup Program

Proxy Server

When using a proxy server to access the Internet, specify the proxy settings below. OfficeScan uses this information when downloading updates from the Trend Micro update server.

Proxy settings

☑ Use a proxy server

Proxy type: ● HTTP ○ SOCKS 4

Server name or IP address:

Port:

Authentication (optional): User name: Password:

FIGURE 2-5. Proxy Server screen

The OfficeScan server uses the HTTP protocol for agent-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.

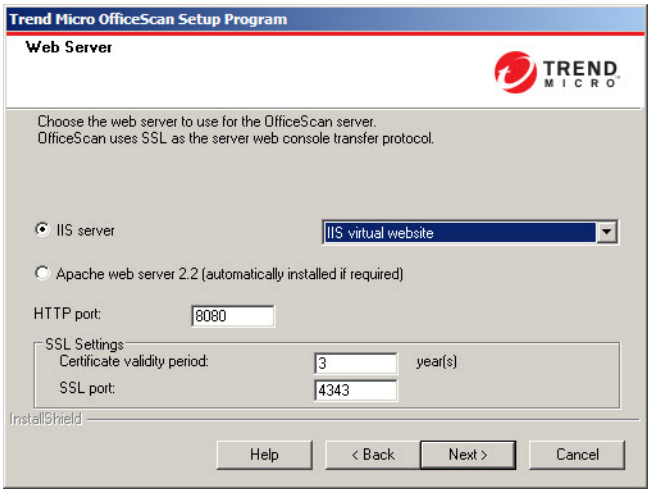
Administrators can skip specifying proxy settings during installation and do so after installation from the OfficeScan web console.

Proxy settings apply only when performing a remote fresh installation. For remote upgrade, OfficeScan uses the previous version's settings.

Note

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

Web Server



Trend Micro OfficeScan Setup Program

Web Server

Choose the web server to use for the OfficeScan server.
OfficeScan uses SSL as the server web console transfer protocol.

● IIS server — IIS virtual website

○ Apache web server 2.2 (automatically installed if required)

HTTP port: 8080

SSL Settings

Certificate validity period: 3 year(s)

SSL port: 4343

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 agents. The web server converts these commands to agent CGIs and forwards them to the OfficeScan Master Service.

Web server settings only apply when performing a remote fresh installation. When performing a remote upgrade, OfficeScan uses the previous version's settings.

IPv6 Support

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

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

Web Server

If Setup detects both IIS and Apache web servers installed on the target endpoint, administrators can choose either of the two web servers. If neither exists on the target endpoint, administrators cannot choose IIS and OfficeScan installs Apache web server 2.2 automatically.

If using an Apache web server:

- Apache web server 2.2 is required. If Apache web server exists on the endpoint but the version is not 2.2, OfficeScan installs and uses version 2.2. OfficeScan does not remove the existing Apache web server.
- If enabling SSL, and Apache web server 2.2 exists, the Apache web server must have SSL settings pre-configured.
- By default, the administrator account is the only account created on the Apache web server.

Tip

Trend Micro recommends creating another account from which to run the web server. Otherwise, the OfficeScan server may become compromised if a malicious hacker takes control of the Apache server.

- Before installing the Apache web server, refer to the Apache website for the latest information on upgrades, patches, and security issues.

If using an IIS web server:

- The following Microsoft Internet Information Server (IIS) versions are required:
    - Version 6.0 on Windows Server 2003
    - Version 7.0 on Windows Server 2008
    - Version 7.5 on Windows Server 2008 R2

- Version 8.0 on Windows Server 2012

Do not install the web server on endpoints running IIS-locking applications because this could prevent successful installation. See the IIS documentation for more information.

HTTP Port

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

SSL Support

OfficeScan uses Secure Sockets Layer (SSL) for 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 selecting SSL, Setup automatically creates an SSL certificate, which is a requirement for SSL connections. The certificate contains server information, public key, and private key.

The SSL certificate should have a validity period between 1 and 20 years. The administrator can still use the certificate after it expires. However, a warning message appears every time SSL connection is invoked using the same certificate.

How communication through SSL works:

1. The administrator sends information from the web console to the web server through SSL connection.

2. The web server responds to the web console with the required certificate.

3. The browser performs key exchange using RSA encryption.

4. The web console sends data to the web server using RC4 encryption.

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

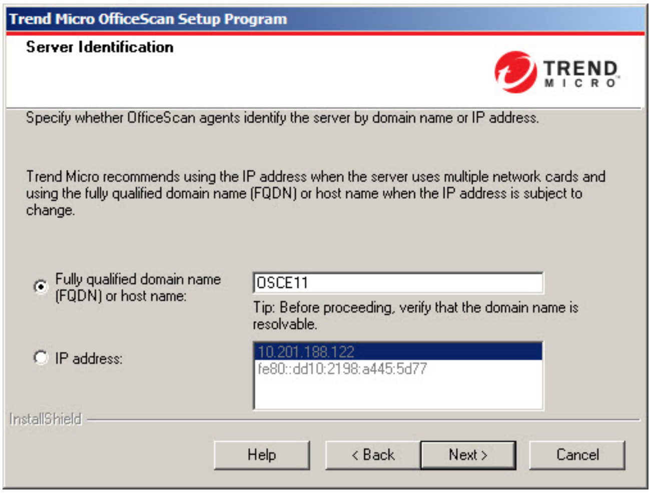
Web Server Ports

The following table lists the default port numbers for the web server

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

WEB SERVER AND SETTINGS	PORTS	
	HTTP	HTTPS (SSL)
Apache web server with SSL enabled	8080 (configurable)	4343 (configurable)
IIS default website with SSL enabled	80 (not configurable)	443 (not configurable)
IIS virtual website with SSL enabled	8080 (configurable)	4343 (configurable)

Server Identification



Trend Micro OfficeScan Setup Program

Server Identification

Specify whether OfficeScan agents identify the server by domain name or IP address.

Trend Micro recommends using the IP address when the server uses multiple network cards and using the fully qualified domain name (FQDN) or host name when the IP address is subject to change.

● Fully qualified domain name (FQDN) or host name: OSCE11

Tip: Before proceeding, verify that the domain name is resolvable.

○ IP address: 10.201.188.122
fe80::dd10:2198:a445:5d77

FIGURE 2-7. Server Identification screen

The selected option on this screen applies only when performing a remote fresh installation.

Specify if OfficeScan agents identify the server computer by its fully qualified domain name (FQDN), host (domain) name, or IP address.

Communication between the server computer and agents is dependent on the specified IP address. Changing the IP address results in agents not being able to communicate with the OfficeScan server. The only way to restore communication is to redeploy all the agents. The same situation applies if the server computer is identified by a host name that changes.

In most networks, the server computer's IP address is more likely to change than its host name, thus it is usually preferable to identify the server computer by a host name.

Tip

For administrators using the IP address instead of the host name, Trend Micro does not recommend changing the IP address (obtained from the DHCP server) after the installation. Administrators can avoid further communication issues with OfficeScan agents by setting the IP address configuration to Static (on the DHCP server) using the same IP address information obtained from the DHCP server.

Another way to preserve the IP address configuration is to reserve the IP address for the OfficeScan server only. This forces the DHCP server to assign OfficeScan the same IP address even when DHCP-enabled.

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

IPV6 Support

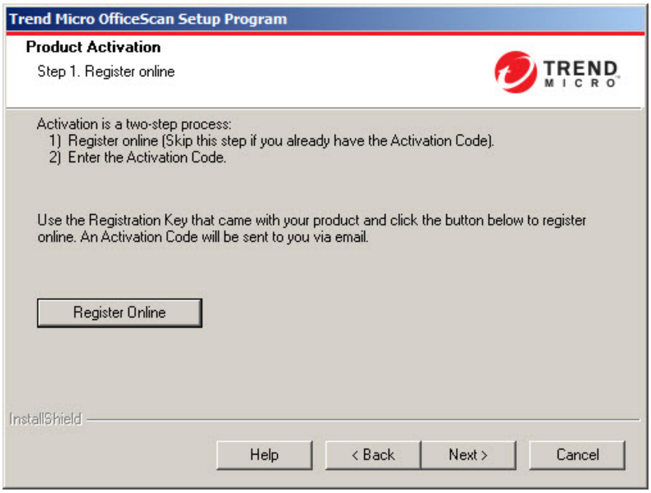
If the server manages IPv4 and IPv6 agents, it must have both IPv4 and IPv6 addresses and administrators must identify the server by its host name. If administrators identify the server by its IPv4 address, IPv6 agents cannot connect to the server. The same issue occurs if pure IPv4 agents connect to a server identified by its IPv6 address.

If the server manages only IPv6 agents, the minimum requirement is an IPv6 address. Server identification can be by its host name or IPv6 address. When administrators identify the server by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.

Note

Specify the FQDN only when performing a local installation of the server. There is no FQDN support for remote installations.

Registration and Activation



Trend Micro OfficeScan Setup Program

Product Activation

Step 1. Register online

Activation is a two-step process:

1) Register online (Skip this step if you already have the Activation Code).
2) Enter the Activation Code.

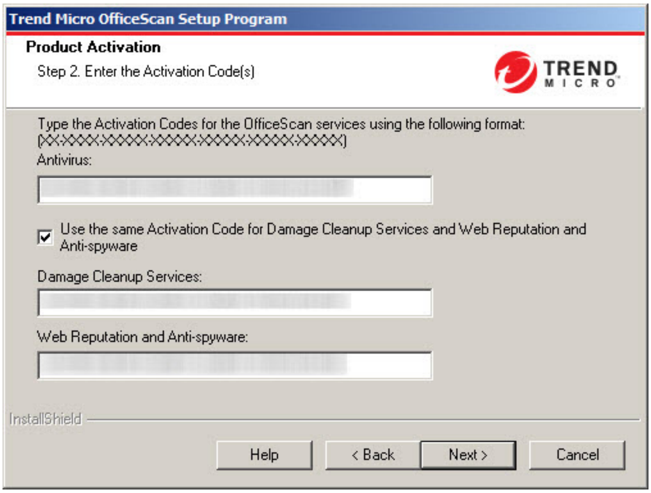
Use the Registration Key that came with your product and click the button below to register online. An Activation Code will be sent to you via email.

FIGURE 2-8. Product Activation - Step 1 screen

Register OfficeScan using the Registration Key that came with the product and then obtain the Activation Codes. Skip this step if the Activation Codes are already available.

To obtain the Activation Codes, click **Register Online**. Setup opens the Trend Micro registration website. After completing the registration form, Trend Micro sends an email with the Activation Codes. After receiving the codes, continue with the installation process.

When installing the OfficeScan server on a pure IPv6 endpoint, set up a dual-stack proxy server that can convert between IP addresses. This allows the server to connect to the Trend Micro registration website successfully.



Trend Micro OfficeScan Setup Program

Product Activation

Step 2. Enter the Activation Code(s)

Type the Activation Codes for the OfficeScan services using the following format: (XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

Antivirus:

☑ Use the same Activation Code for Damage Cleanup Services and Web Reputation and Anti-spyware

Damage Cleanup Services:

Web Reputation and Anti-spyware:

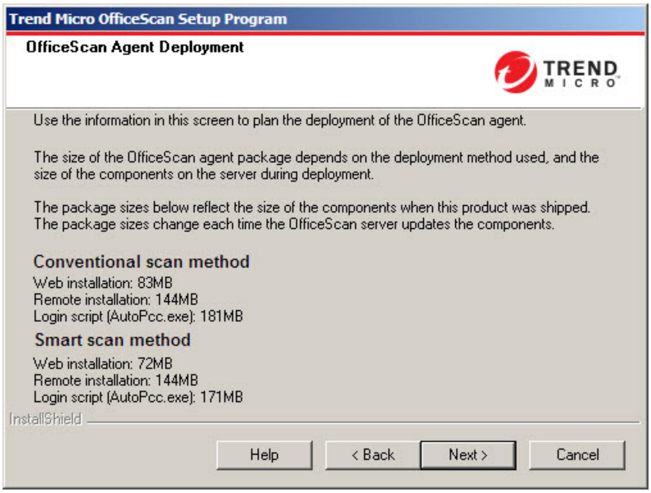
FIGURE 2-9. Product Activation - Step 2 screen

Specify the Activation Codes. The Activation Codes are case-sensitive.

If the Activation Code is valid for all services:

1. Type the Activation Code in the **Antivirus** text box.
2. Select **Use the same Activation Code for Damage Cleanup Services and Web Reputation and Anti-spyware**.
3. Click **Next** and verify the licensing information.

OfficeScan Agent Deployment



Trend Micro OfficeScan Setup Program

OfficeScan Agent Deployment

Use the information in this screen to plan the deployment of the OfficeScan agent.

The size of the OfficeScan agent package depends on the deployment method used, and the size of the components on the server during deployment.

The package sizes below reflect the size of the components when this product was shipped. The package sizes change each time the OfficeScan server updates the components.

Conventional scan method

Web installation: 83MB
Remote installation: 144MB
Login script (AutoPcc.exe): 181MB

Smart scan method

Web installation: 72MB
Remote installation: 144MB
Login script (AutoPcc.exe): 171MB

FIGURE 2-10. OfficeScan Agent Deployment screen

There are several methods for installing or upgrading OfficeScan agents. This screen lists the different deployment methods and approximate network bandwidth needed.

Use this screen to estimate the size required on the servers and the bandwidth consumption when deploying agents to the target endpoints.

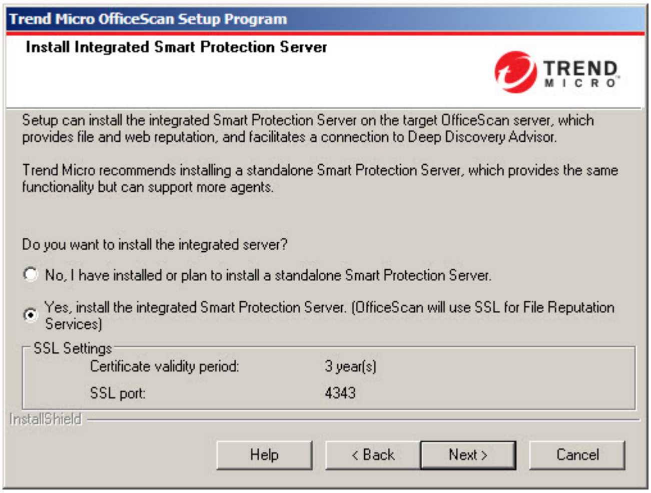
Note

All these installation methods require local administrator or domain administrator rights on the target endpoints.

Install Integrated Smart Protection Server

Note

This screen does not display when using an IIS virtual website during local upgrade installations.



Trend Micro OfficeScan Setup Program

Install Integrated Smart Protection Server

Setup can install the integrated Smart Protection Server on the target OfficeScan server, which provides file and web reputation, and facilitates a connection to Deep Discovery Advisor.

Trend Micro recommends installing a standalone Smart Protection Server, which provides the same functionality but can support more agents.

Do you want to install the integrated server?

○ No, I have installed or plan to install a standalone Smart Protection Server.

● Yes, install the integrated Smart Protection Server. (OfficeScan will use SSL for File Reputation Services)

SSL Settings

Certificate validity period:	3 year(s)
SSL port:	4343

FIGURE 2-11. Install Integrated Smart Protection Server screen

Setup can install the integrated Smart Protection Server on the target endpoint. The integrated server provides File Reputation Services to agents that use smart scan and Web Reputation Services to agents subject to web reputation policies. Manage the integrated server from the OfficeScan web console.

Trend Micro recommends installing the standalone Smart Protection Server, which has the same functions as the integrated server but can serve more agents. The standalone server is installed separately and has its own management console. See the *Trend Micro Smart Protection Server Administrator's Guide* for information on the standalone server.

Tip

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

Agent Connection Protocols for File Reputation Services

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

Note

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

The port numbers used for File Reputation Services depend on the web server (Apache or IIS) the OfficeScan server uses. See *Web Server on page 2-12* for more information.

The HTTP port does not display on the installation screen. The HTTPS port displays, but configuration is optional.

TABLE 2-3. Ports for the Integrated Smart Protection Server's File Reputation Services

WEB SERVER AND SETTINGS	PORTS FOR FILE REPUTATION SERVICES	
	HTTP	HTTPS (SSL)
Apache web server	8082	4345
IIS default website	80	443
IIS virtual website	8080	4343

Integrated Server Not Installed

When performing a fresh installation and not choosing to install the integrated server:

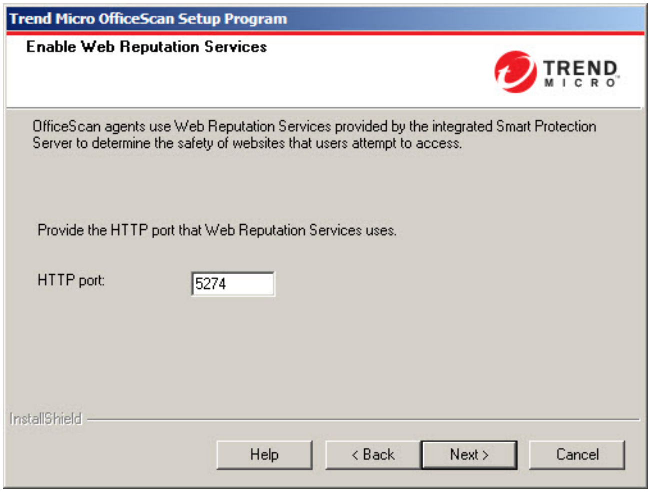
- Conventional scan becomes the default scan method.
- When enabling web reputation policies in a separate installation screen (for details, see *Web Reputation Feature on page 2-35*), agents cannot send web reputation queries because OfficeScan assumes that no Smart Protection Server installation occurred.

If a standalone server is available after installing OfficeScan, perform the following tasks from the OfficeScan web console:

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

When upgrading from OfficeScan 10.x servers where the integrated server has been disabled, the integrated server is not installed. OfficeScan agents retain their scan methods and the smart protection sources to which they send queries.

Enable Web Reputation Services


Trend Micro OfficeScan Setup Program

Enable Web Reputation Services

OfficeScan agents use Web Reputation Services provided by the integrated Smart Protection Server to determine the safety of websites that users attempt to access.

Provide the HTTP port that Web Reputation Services uses.

HTTP port: 5274

FIGURE 2-12. Enable Web Reputation Services screen

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

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

Agent Connection Protocols for Web Reputation Services

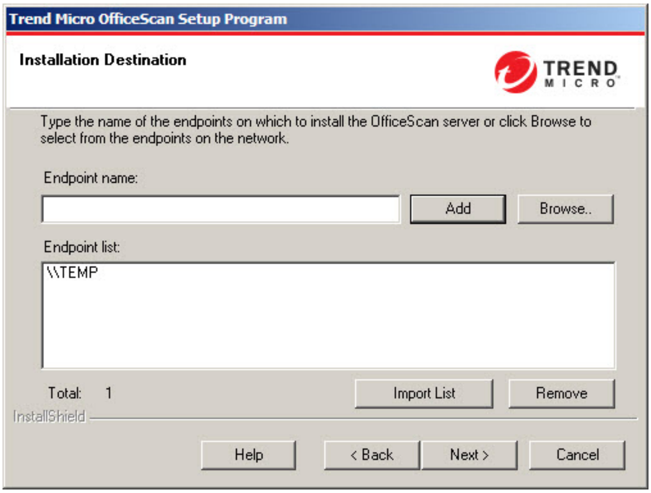
OfficeScan agents can connect to the integrated Smart Protection Server's Web Reputation Services using HTTP.

The HTTP port number used for Web Reputation Services depends on the web server (Apache or IIS) the OfficeScan server uses. See *Web Server on page 2-12* for more information.

Table 2-4. Ports for the Integrated Smart Protection Server's Web Reputation Services

Web Server and Settings	HTTP Port for Web Reputation Services
Apache web server with SSL enabled	5274
IIS default website with SSL enabled	80 (not configurable)
IIS virtual website with SSL enabled	8080 (not configurable)

Installation Destination



Trend Micro OfficeScan Setup Program

Installation Destination

Type the name of the endpoints on which to install the OfficeScan server or click Browse to select from the endpoints on the network.

Endpoint name:

Endpoint list:

\\TEMP

Total: 1

FIGURE 2-13. Installation Destination screen

Specify the target endpoint to which OfficeScan installs. Manually type the endpoint's host name or IP address. Click **Browse** to search for endpoint(s) in the network.

Import endpoint name(s) from a text file by clicking **Import List**. When installing to multiple endpoints simultaneously and all endpoints pass the analysis, Setup installs the OfficeScan server in the listed order in the text file.

In the text file:

- Specify one endpoint 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 (-).

For example:

```
\\domain1\test-abc
```

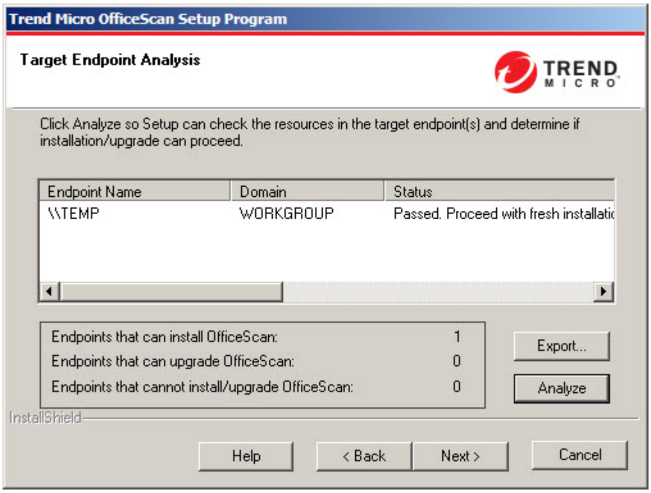
```
\\domain2\test-123
```

Tips to ensure that remote installation can proceed:

- Obtain administrator rights to the target endpoint.
- Record the endpoint's host name and logon credentials (user name and password).
- Verify that the target endpoints meet the system requirements for installing the OfficeScan server.
- Ensure the endpoint has Microsoft IIS server 6.0 or later if using this as the web server. When choosing to use the Apache web server, Setup automatically installs this server if not present in the target endpoint.
- Do not specify the endpoint launching Setup as a target endpoint. Run local installation on the endpoint instead.

After specifying the target endpoint(s), click **Next.** Setup checks if the endpoint(s) meet the OfficeScan installation requirements.

Target Endpoint Analysis



Trend Micro OfficeScan Setup Program

Target Endpoint Analysis

Click Analyze so Setup can check the resources in the target endpoint(s) and determine if installation/upgrade can proceed.

Endpoint Name	Domain	Status
\\TEMP	WORKGROUP	Passed. Proceed with fresh installatic

Endpoints that can install OfficeScan:	1
Endpoints that can upgrade OfficeScan:	0
Endpoints that cannot install/upgrade OfficeScan:	0

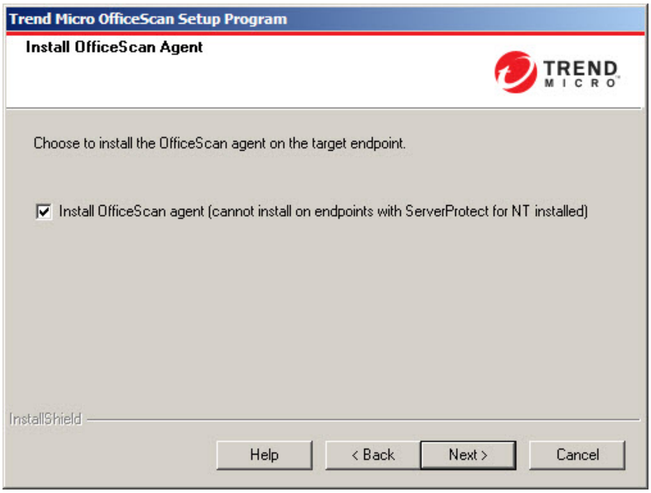
FIGURE 2-14. Target Endpoint Analysis screen

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

When installing to multiple endpoints, installation proceeds if at least one of the endpoints pass the analysis. Setup installs the OfficeScan server to that endpoint and ignores the endpoints that did not pass the analysis.

During remote installation, the installation progress only displays in the endpoint from which Setup launched and not on the target endpoint(s).

Install OfficeScan Agent


Trend Micro OfficeScan Setup Program

Install OfficeScan Agent

Choose to install the OfficeScan agent on the target endpoint.

☑ Install OfficeScan agent (cannot install on endpoints with ServerProtect for NT installed)

FIGURE 2-15. Install OfficeScan Agent screen

Choose to install the OfficeScan agent on the target server.

OfficeScan Agent

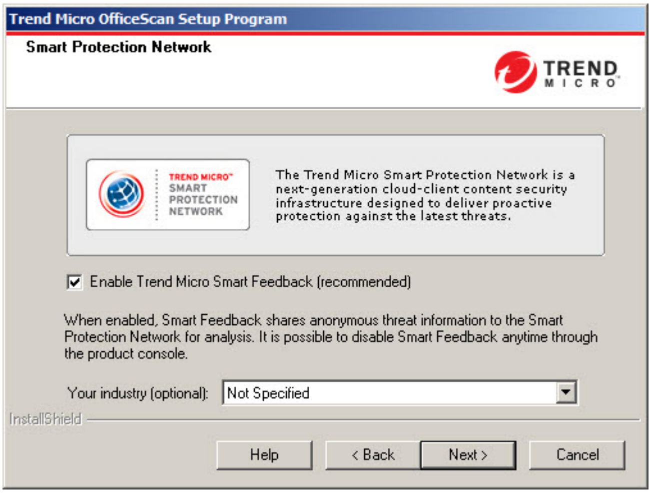
The OfficeScan agent program provides the actual protection against security risks. Therefore, to protect the OfficeScan server endpoint against security risks, it needs to also have the OfficeScan agent program. Choosing to install the OfficeScan agent during server installation is a convenient way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

Note

Install the OfficeScan agent to other endpoints on the network after server installation. See the *Administrator's Guide* for the OfficeScan agent installation methods.

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

Smart Protection Network



Trend Micro OfficeScan Setup Program

Smart Protection Network

The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to deliver proactive protection against the latest threats.

☑ Enable Trend Micro Smart Feedback (recommended)

When enabled, Smart Feedback shares anonymous threat information to the Smart Protection Network for analysis. It is possible to disable Smart Feedback anytime through the product console.

Your industry (optional): Not Specified

FIGURE 2-16. Smart Protection Network screen

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

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and its 24/7 threat research centers and technologies. Each new threat identified through every single customer's routine reputation check automatically updates all Trend Micro threat databases, blocking any subsequent customer encounters of a given threat.

By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in the protection of others. Because the gathered threat information is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected.

Samples of information sent to Trend Micro:

- File checksums
- Websites accessed
- File information, including sizes and paths
- Names of executable files

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

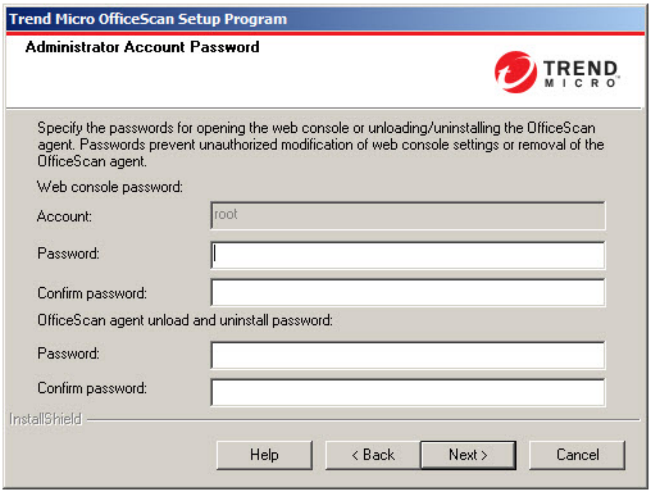
Tip

You do not need to participate in Smart Feedback to protect your endpoints. Your participation is optional and you may opt out at any time. Trend Micro recommends that you participate in Smart Feedback to help provide better overall protection for all Trend Micro customers.

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Administrator Account Password



Trend Micro OfficeScan Setup Program

Administrator Account Password

Specify the passwords for opening the web console or unloading/uninstalling the OfficeScan agent. Passwords prevent unauthorized modification of web console settings or removal of the OfficeScan agent.

Web console password:

Account: root

Password:

Confirm password:

OfficeScan agent unload and uninstall password:

Password:

Confirm password:

FIGURE 2-17. Administration Account Password screen

Specify passwords to access the web console and unload and uninstall the OfficeScan agent.

Access the Web Console

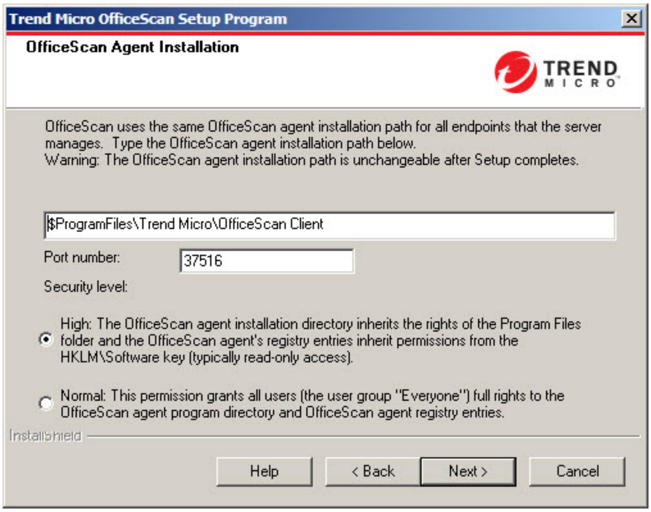
Setup creates a root account during installation. The root account has full access to all OfficeScan web console functions. Logging on using this account also allows the administrator to create custom user accounts that other users can use to log on to the web console. Users can configure or view one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

Specify a password known only to the OfficeScan administrators. For help resetting a forgotten password, contact your support provider.

Unload and Uninstall the OfficeScan Agent

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

OfficeScan Agent Installation



OfficeScan Agent Installation

OfficeScan uses the same OfficeScan agent installation path for all endpoints that the server manages. Type the OfficeScan agent installation path below.
Warning: The OfficeScan agent installation path is unchangeable after Setup completes.

$ProgramFiles\Trend Micro\OfficeScan Client

Port number: 37516

Security level:

● High: The OfficeScan agent installation directory inherits the rights of the Program Files folder and the OfficeScan agent's registry entries inherit permissions from the HKLM\Software key (typically read-only access).

○ Normal: This permission grants all users (the user group "Everyone") full rights to the OfficeScan agent program directory and OfficeScan agent registry entries.

FIGURE 2-18. OfficeScan Agent Installation screen

Accept the default agent installation settings or specify a different OfficeScan agent 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 specified path includes a directory that does not exist on the agent, Setup creates the directory automatically during agent installation.

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

Note

Modification of the OfficeScan agent installation path is not possible after installation of the OfficeScan server completes. All installed OfficeScan agents use the same installation path.

When specifying variables for the OfficeScan agent installation path, use the following:

- `$BOOTDISK`: The drive letter of the hard disk that the endpoint boots from, by default `C:\`
- `$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:

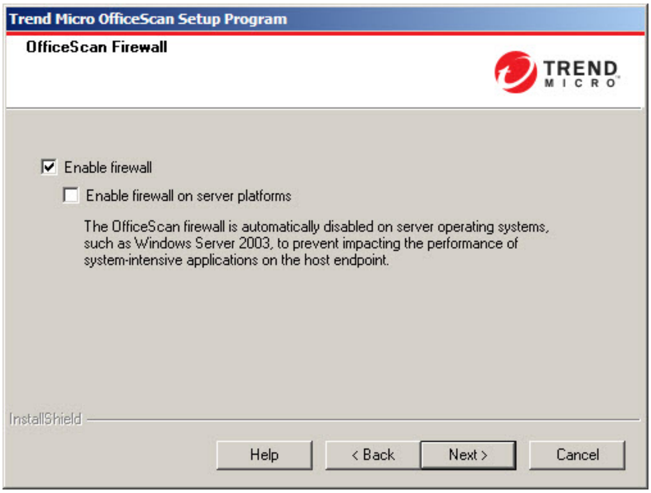
- **Port number**: Setup randomly generates this port number, which the OfficeScan server uses to communicate with agents. Accept the default or type a new value.
- **Security level**: After installing OfficeScan, change the security level from the OfficeScan console.

  Go to **Agents** > **Agent Management**. Click **Settings** > **Privileges and Other Settings** > **Other Settings**.

  - **Normal**: This permission grants all users (the user group “Everyone”) full rights to the agent program directory and agent registry entries.

- **High**: The agent installation directory inherits the rights of the `Program Files` folder and the agent's registry entries inherit permissions from the `HKLM\Software` key. For most Active Directory configurations, this automatically limits "normal" users (those without administrator privileges) to read-only access.

OfficeScan Firewall



Trend Micro OfficeScan Setup Program

OfficeScan Firewall

☑ Enable firewall

□ Enable firewall on server platforms

The OfficeScan firewall is automatically disabled on server operating systems, such as Windows Server 2003, to prevent impacting the performance of system-intensive applications on the host endpoint.

FIGURE 2-19. OfficeScan Firewall screen

This screen displays only after activating the Antivirus service.

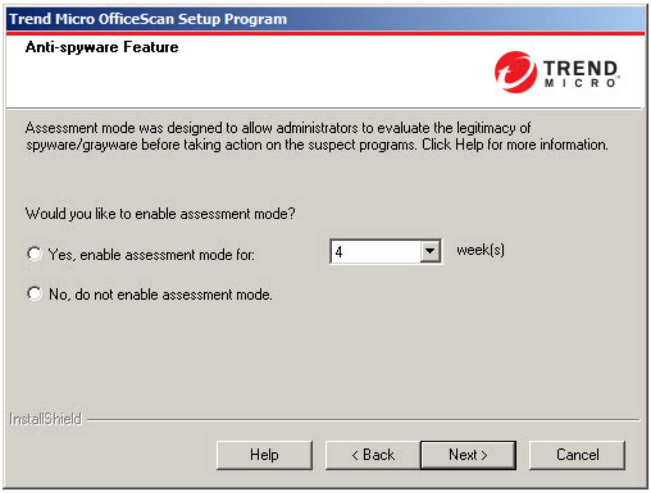
OfficeScan Firewall

The OfficeScan Firewall protects agents 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.

Optionally choose to disable the Firewall and enable it later from the OfficeScan server web console.

Optionally enable the Firewall on server platforms. When upgrading and the Firewall service is already enabled on server platforms, select **Enable firewall on server platforms** so that OfficeScan does not disable the Firewall service after the upgrade.

Anti-spyware Feature



Assessment mode was designed to allow administrators to evaluate the legitimacy of spyware/grayware before taking action on the suspect programs. Click Help for more information.

Would you like to enable assessment mode?

○ Yes, enable assessment mode for: 4 week(s)

○ No, do not enable assessment mode.

FIGURE 2-20. Anti-spyware Feature screen

This screen displays only after activating the Web Reputation and Anti-spyware service.

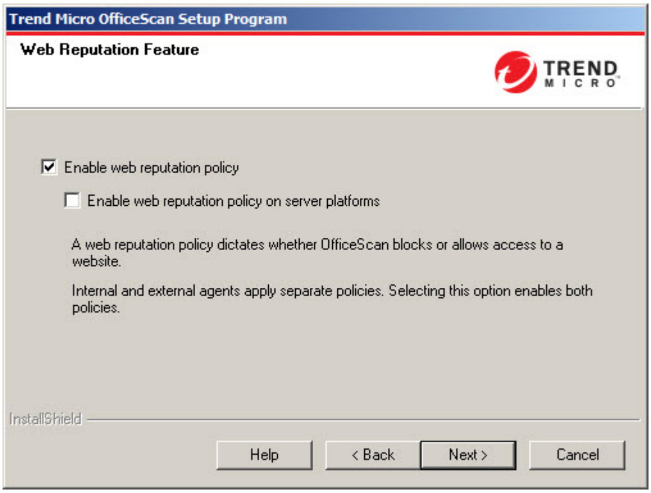
When in assessment mode, all agents managed by the server log spyware/grayware detected during Manual Scan, Scheduled Scan, Real-Time Scan, and Scan Now but do not clean spyware/grayware components. Cleaning terminates processes or deletes registries, files, cookies, and shortcuts.

Trend Micro provides assessment mode to allow for the evaluation of items that Trend Micro detects as spyware/grayware. Administrators can then configure the appropriate action. For example, add spyware/grayware detected as a security risk 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, change assessment mode settings from the web console (**Agents** > **Global Agent Settings**, **Spyware/Grayware Settings** section).

Web Reputation Feature



Trend Micro OfficeScan Setup Program

Web Reputation Feature

☑ Enable web reputation policy

□ Enable web reputation policy on server platforms

A web reputation policy dictates whether OfficeScan blocks or allows access to a website.

Internal and external agents apply separate policies. Selecting this option enables both policies.

FIGURE 2-21. Web Reputation Feature screen

Web Reputation policies dictate whether OfficeScan blocks or allows access to a website. For details about policies, see the *Administrator's Guide*.

Selecting **Enable web reputation policy** enables policies for internal and external agents installed on desktop platforms, such as Windows XP, Vista, Windows 7, Windows 8, and Windows 8.1. Select **Enable web reputation policy on server platforms** if server platforms, such as Windows Server 2003, Windows Server 2008, and Windows Server 2012, require the same level of web threat protection as desktop platforms.

OfficeScan agents use the location criteria configured in the web console's **Endpoint Location** screen to determine their location and the policy to apply. OfficeScan agents switch policies each time the location changes.

Configure web reputation policy settings from the web console after installation. OfficeScan administrators typically configure a stricter policy for external agents.

Web reputation policies are granular settings in the OfficeScan agent tree. Enforce specific policies to all agents, agent groups, or individual agents.

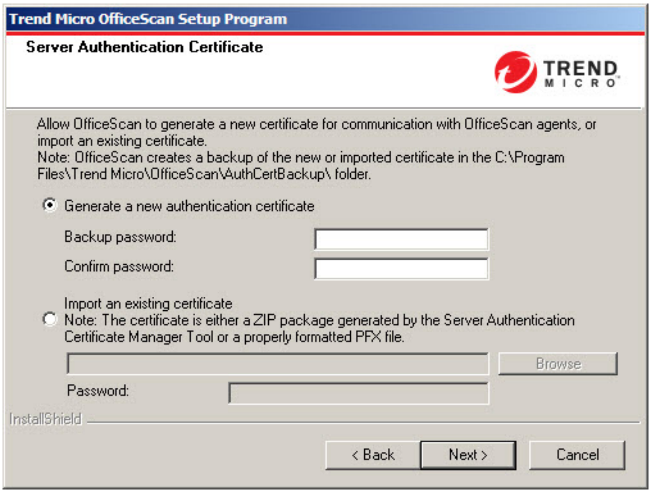
When enabling web reputation policies, be sure to install Smart Protection Servers (integrated or standalone) and add them to the smart protection source list on the OfficeScan web console. OfficeScan agents send web reputation queries to the servers to verify the safety of websites that users are accessing.

Note

The integrated server installs with the OfficeScan server. For details, see *Install Integrated Smart Protection Server on page 2-20*. The standalone server installs separately.

Server Authentication Certificate

The Setup program attempts to detect preexisting authentication certificates during installation. If a preexisting certificate exists, OfficeScan automatically maps the file on the **Server Authentication Certificate** screen. If no preexisting certificate exists, OfficeScan defaults to the **Generate a new authentication certificate** option.



Server Authentication Certificate

Allow OfficeScan to generate a new certificate for communication with OfficeScan agents, or import an existing certificate.
Note: OfficeScan creates a backup of the new or imported certificate in the C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\ folder.

● Generate a new authentication certificate

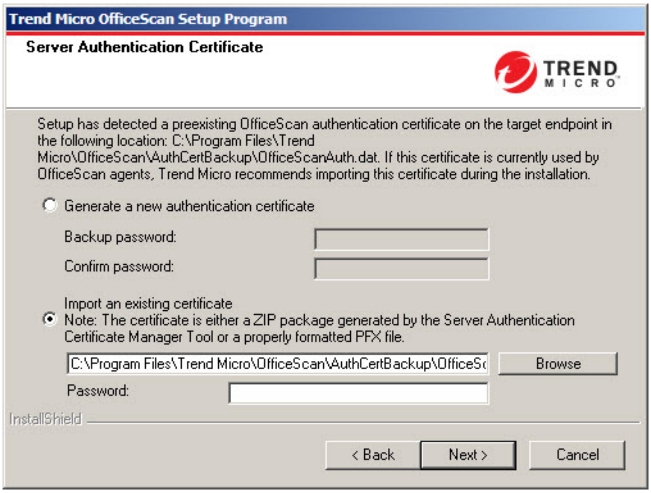
Backup password:

Confirm password:

○ Import an existing certificate
Note: The certificate is either a ZIP package generated by the Server Authentication Certificate Manager Tool or a properly formatted PFX file.

Password:

FIGURE 2-22. Server Authentication Certificate screen for new certificates



Server Authentication Certificate

Setup has detected a preexisting OfficeScan authentication certificate on the target endpoint in the following location: C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\OfficeScanAuth.dat. If this certificate is currently used by OfficeScan agents, Trend Micro recommends importing this certificate during the installation.

○ Generate a new authentication certificate

Backup password:

Confirm password:

● Import an existing certificate
Note: The certificate is either a ZIP package generated by the Server Authentication Certificate Manager Tool or a properly formatted PFX file.

C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\OfficeSc

Password:

FIGURE 2-23. Server Authentication Certificate screen for preexisting certificates

OfficeScan uses public-key cryptography to authenticate communications that the OfficeScan server initiates on agents. With public-key cryptography, the server keeps a private key and deploys a public key to all agents. The agents use the public key to verify that incoming communications are server-initiated and valid. The agents respond if the verification is successful.

Note

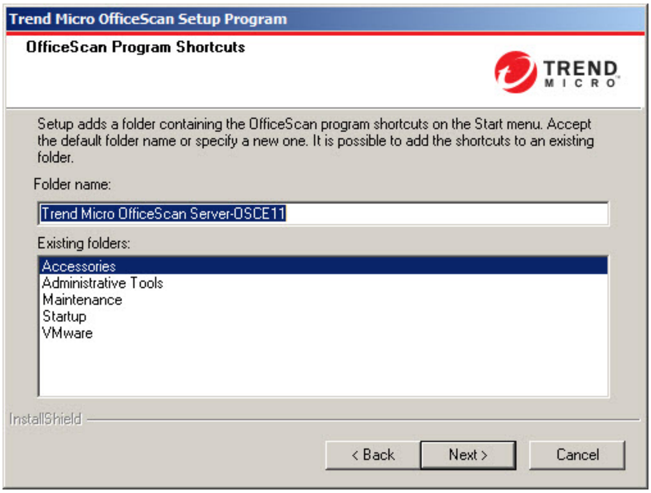
OfficeScan does not authenticate communications that agents initiate on the server.

OfficeScan can generate the authentication certificate during the installation or administrators can import a preexisting authentication certificate from another OfficeScan server.

Tip

When backing up the certificate, Trend Micro recommends encrypting the certificate with a password.

OfficeScan Program Shortcuts



Trend Micro OfficeScan Setup Program

OfficeScan Program Shortcuts

Setup adds a folder containing the OfficeScan program shortcuts on the Start menu. Accept the default folder name or specify a new one. It is possible to add the shortcuts to an existing folder.

Folder name:

Trend Micro OfficeScan Server-OSCE11

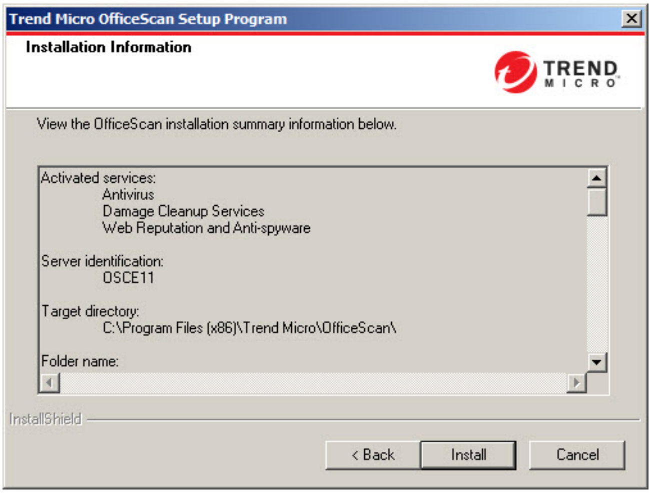
Existing folders:

Accessories
Administrative Tools
Maintenance
Startup
VMware

FIGURE 2-24. OfficeScan Program Shortcuts screen

Accept the default folder name, specify a new one, or select an existing folder to which Setup adds the program shortcuts.

Installation Information



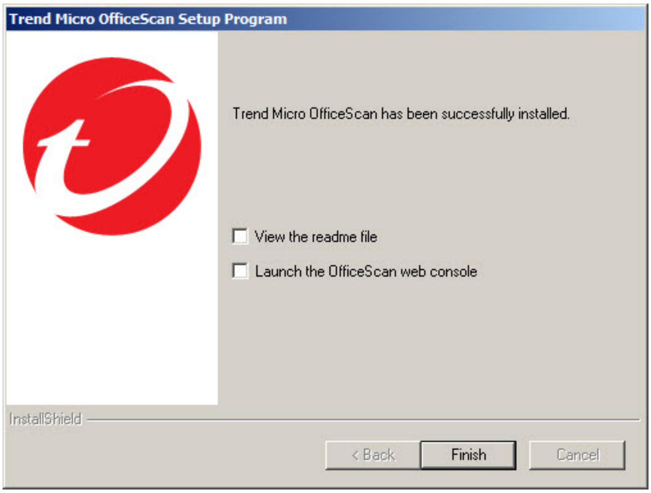
View the OfficeScan installation summary information below.

```
Activated services:
        Antivirus
        Damage Cleanup Services
        Web Reputation and Anti-spyware

Server identification:
        OSCE11

Target directory:
        C:\Program Files (x86)\Trend Micro\OfficeScan\

Folder name:
```

FIGURE 2-25. 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.**

InstallShield Wizard Complete



Trend Micro OfficeScan has been successfully installed.

□ View the readme file

□ Launch the OfficeScan web console

FIGURE 2-26. InstallShield Wizard Complete screen

When the installation is complete, view the readme file for basic information about the product and known issues.

Administrators can launch the web console to start configuring OfficeScan settings.

Chapter 3

Upgrading OfficeScan

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

Topics in this chapter:

Upgrading the OfficeScan Server and Agents

Running Setup on a previously configured OfficeScan 10.x server upgrades the server. If Plug-in Manager is installed on the endpoint, Setup also upgrades Plug-in Manager to version 2.1. If Plug-in Manager is not installed, version 2.1 will automatically be installed. This Plug-in Manager version provides the widget functionality in OfficeScan.

If the OfficeScan server allows agents to upgrade the OfficeScan agent program, the installation package immediately upgrades all agents after the server installation completes.

If the OfficeScan server blocks agent upgrades, depending on network bandwidth and the number of agents the OfficeScan server manages, stagger the agent upgrade in groups.

Tip

Trend Micro highly recommends restarting the OfficeScan agents after upgrading to ensure that all OfficeScan components have been updated.

Before Upgrading the OfficeScan Server and Agents

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

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

    - When Common Firewall Driver update starts, agent endpoints are temporarily disconnected from the network. Users are not notified before disconnection.

      An option on the OfficeScan 10 SP1 or later web console, which is enabled by default, postpones the Common Firewall Driver update until the agent endpoint is restarted. To avoid the disconnection issue, ensure that this option is enabled. To check the status of this option, go to **Networked Computers** > **Global Client Settings** and go to the **Firewall Settings** section. The option is **Update the OfficeScan firewall driver only after a system reboot**.

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

  If the option to display the restart notification message is enabled on the web console, users are 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, go to **Networked Computers** > **Global Client Settings** and go to the **Alert Settings** section. The option is **Display a notification message if the client computer needs to restart to load a kernel mode driver**.

2. The OfficeScan server cannot upgrade to this version if:

   - The agent is running Login Script (`AutoPcc.exe`) at the time of server upgrade. Ensure that no agent is running Login Script before upgrading the server.

   - The server is performing database-related tasks. Before upgrading, check the status of the OfficeScan database (`DbServer.exe`). For example, open Windows Task Manager and verify that CPU usage for `DbServer.exe` is 00. If CPU usage is higher, wait until usage is 00, which signals that database-related tasks have been completed. If you run an upgrade and encounter upgrade problems, it is possible that database files have been locked. In this case, restart the server computer to unlock the files and then run another upgrade.

Use one of following upgrade methods:

- *Upgrade Method 1: Disable Automatic Agent Upgrade on page 3-4*
- *Upgrade Method 2: Upgrade Update Agents on page 3-6*
- *Upgrade Method 3: Move Agents to the OfficeScan 11.0 Server on page 3-12*
- *Upgrade Method 4: Enable Automatic Agent Upgrade on page 3-14*

Upgrade Method 1: Disable Automatic Agent Upgrade

By disabling automatic agent upgrade, it is possible to upgrade the server first and then upgrade agents in groups. Use this upgrade method when upgrading a large number of agents.

Part 1: Configure Update Settings on the OfficeScan 10.x Server

Procedure

1. Go to **Networked Computers** > **Client Management**.

2. On the client tree, click the root domain icon (🌐) to select all clients.

3. Click **Settings** > **Privileges and Other Settings** and go to the **Other Settings** tab.

4. Select **Clients can update components but not upgrade the client program or deploy hot fixes**.

5. Click **Apply to All Clients**.

Tip

It may take a while to deploy the settings to online clients on a complex network environment and a large number of clients. Before the upgrade, allocate sufficient time for settings to deploy to all clients. OfficeScan clients that do not apply the settings automatically upgrade.

Part 2: Upgrade the OfficeScan Server

See *Performing a Local Upgrade on page 3-16* or *Performing a Remote Upgrade on page 3-29* for details on upgrading the OfficeScan server.

Note

To speed up the upgrade process, unload the OfficeScan agent before upgrading any OfficeScan server running Windows Server 2008 Standard 64-bit.

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

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

Part 3: Upgrade OfficeScan Agents

Procedure

1. Go to **Updates** > **Agents** > **Automatic Update**, and ensure that the following options are enabled:

    - **Initiate component update on agents immediately after the OfficeScan server downloads a new component**

    - **Let agents initiate component update after restarting and connecting to the OfficeScan server (roaming agents excluded)**

2. Go to **Agents** > **Agent Management**.

3. On the agent tree, select the agents that you want to upgrade. You can select one or several domains, or individual/all agents within a domain.

4. Click **Settings** > **Privileges and Other Settings** and go to the **Other Settings** tab.

5. Disable **OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes**.

6. Click **Save**.

7. Check the upgrade results.

    - *Online Agents on page 3-10*

    - *Offline Agents on page 3-11*

    - *Roaming Agents on page 3-11*

8. Restart the agent endpoints to finish upgrading the agents.

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

Upgrade Method 2: Upgrade Update Agents

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

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

Part 1: Configure Update Settings on the OfficeScan 10.x Server

Procedure

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

> **Tip**
>
> It may take a while to deploy the settings to online clients on a complex network environment and a large number of clients. Before the upgrade, allocate sufficient time for settings to deploy to all clients. OfficeScan clients that do not apply the settings automatically upgrade.

Part 2: Upgrade the OfficeScan Server

See *Performing a Local Upgrade on page 3-16* or *Performing a Remote Upgrade on page 3-29* for details on upgrading the OfficeScan server.

Note

To speed up the upgrade process, unload the OfficeScan agent before upgrading any OfficeScan server running Windows Server 2008 Standard 64-bit.

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

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

Part 3: Upgrade Update Agents

Procedure

1. Go to **Agents** > **Agent Management**.
2. On the agent tree, select the Update Agents to upgrade.

   Tip

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

3. Click **Settings** > **Privileges and Other Settings** and go to the **Other Settings** tab.
4. Disable **OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes**.
5. Click **Save**.
6. Go to **Updates** > **Agents** > **Manual Update**.
7. Select the **Manually select agents** option and click **Select**.
8. In the agent tree that opens, choose the Update Agents to upgrade.

Tip

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

9. Click **Initiate Update** on top of the agent tree.

10. Check the upgrade results.

    - Online Update Agents upgrade immediately after initiating component update.

    - Offline Update Agents upgrade when they become online.

    - Roaming Update Agents upgrade when they become online or, if the Update Agent has scheduled update privileges, when scheduled update runs.

11. Restart the Update Agents' endpoints to finish upgrading the agents.

12. Repeat step 1to step 11 until all Update Agents have been upgraded.

Part 4: Configure Update Agent Settings

Procedure

1. Go to **Agents** > **Agent Management**.

2. On the agent tree, select the Update Agents to upgrade.

Tip

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

3. Ensure that Update Agents have the latest components.

4. Click **Settings** > **Update Agent Settings**.

5. Select the following options:

    - **Component updates**

- **Domain settings**
- **OfficeScan agent programs and hot fixes**

6. Click **Save**.

   Wait for the Update Agent to finish downloading the agent program before proceeding to Part 5.

7. Repeat step 1 to step 6 until all Update Agents have applied the necessary settings.

Part 5: Upgrade OfficeScan Agents

Procedure

1. Go to **Updates** > **Agents** > **Automatic Update**, and ensure that the following options are enabled:

   - **Initiate component update on agents immediately after the OfficeScan server downloads a new component**
   - **Let agents initiate component update after restarting and connecting to the OfficeScan server (roaming agents excluded)**

2. Go to **Agents** > **Agent Management**.

3. On the agent tree, select the agents that you want to upgrade. You can select one or several domains, or individual/all agents within a domain.

4. Click **Settings** > **Privileges and Other Settings** and go to the **Other Settings** tab.

5. Disable **OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes**.

6. Click **Save**.

7. Check the upgrade results.

   - *Online Agents on page 3-10*
   - *Offline Agents on page 3-11*

- *Roaming Agents on page 3-11*

8. Restart the agent endpoints to finish upgrading the agents.

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

Upgrade Results

Online Agents

Note

Restart the agent endpoints after the upgrade.

- Automatic Upgrade

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

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

- Manual Upgrade

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

  - Create and deploy an EXE or MSI OfficeScan agent package.

Note

See the *Administrator's Guide* for instructions on creating the agent package.

- Instruct agent users to run **Update Now** on the agent endpoint.
- If the agent endpoint runs Windows Server 2003, XP Professional, Server 2008, Vista™ (all editions except Vista Home), 7™ (all editions except 7 Home), Windows 8 (Pro/Enterprise), or Windows Server 2012, instruct the user to perform the following steps:
  - Connect to the server computer.
  - Navigate to `\\<server computer name>\ofcscan`.
  - Launch `AutoPcc.exe`.
- If the agent endpoint runs Windows XP Home, Vista Home, Windows 7 Home, or Windows 8, instruct the user to right-click `AutoPcc.exe`, and select **Run as administrator**.
- Initiate manual agent update.

To initiate manual agent update:

1. Navigate to **Updates** > **Agents** > **Manual Update**.
2. Select the **Manually select agents** option and click **Select**.
3. In the agent tree that opens, choose the agents to upgrade.
4. Click **Initiate Component Update** on top of the agent tree.

Offline Agents

Offline agents upgrade when they become online.

Roaming Agents

Roaming agents upgrade when they become online or, if the agent has scheduled update privileges, when scheduled update runs.

Upgrade Method 3: Move Agents to the OfficeScan 11.0 Server

Perform a fresh installation of the OfficeScan 11.0 server and then move agents to this server. When you move the agents, they automatically upgrade to OfficeScan 11.0.

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

Procedure

1. Perform a fresh installation of the OfficeScan 11.0 server. For details, see *The Setup Installation Screens on page 2-4*.
2. Log on to the web console.
3. Go to **Updates** > **Agents** > **Automatic Update**, and ensure that the following options are enabled:
   - **Initiate component update on agents immediately after the OfficeScan server downloads a new component**
   - **Let agents initiate component update after restarting and connecting to the OfficeScan server (roaming agents excluded)**
4. Go to **Agents** > **Agent Management**.
5. On the agent tree, click the root domain icon (🌐) to select all agents.
6. Click **Settings** > **Privileges and Other Settings** and go to the **Other Settings** tab.
7. Disable **OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes**.
8. Click **Apply to All Agents**.
9. Record the following OfficeScan 11.0 server information. Specify this information on the OfficeScan 10.x/8.0 SP1 server when moving agents:
   - Endpoint name or IP address

- Server listening port

  To view the server listening port navigate to **Administration** > **Settings** > **Agent Connection**. The port number displays on the screen.

Part 2: Upgrade OfficeScan Agents

Procedure

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

2. Click **Cancel Notification**. This function clears the server notification queue, which will prevent problems moving clients to the OfficeScan 11.0 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. On the client tree, select the clients that you want to upgrade. Select only online clients because offline and roaming clients cannot be moved.

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

6. Specify the OfficeScan 11.0 server computer name/IP address and server listening port under **Move selected client(s) online to another OfficeScan Server**.

7. Click **Move**.

Upgrade Results

- Online agents start to move and upgrade.

- Tips for managing offline and roaming agents:

  - Disable roaming mode on agents in order to upgrade them.

- For offline agents, instruct users to connect to the network so that the agent can become online. For agents that are offline for an extended period of time, instruct users to uninstall the agent from the endpoint and then use a suitable agent installation method (such as agent packager) discussed in the *Administrator's Guide* to install the OfficeScan agent.

Note

Restart the agent endpoints to finish upgrading the agents.

Upgrade Method 4: Enable Automatic Agent Upgrade

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

If the server manages a small number of agents, consider allowing agents to upgrade immediately. It is possible to use the upgrade methods discussed previously.

Part 1: Configure Update Settings on the OfficeScan 10.x Server

Procedure

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

6. Click **Apply to All Clients**.

> **Tip**
>
> It may take a while to deploy the settings to online clients on a complex network environment and a large number of clients. Before the upgrade, allocate sufficient time for settings to deploy to all clients. OfficeScan clients that do not apply the settings automatically upgrade.

Part 2: Upgrade the OfficeScan Server

See *Performing a Local Upgrade on page 3-16* or *Performing a Remote Upgrade on page 3-29* for details on upgrading the OfficeScan server.

> **Note**
>
> To speed up the upgrade process, unload the OfficeScan agent before upgrading any OfficeScan server running Windows Server 2008 Standard 64-bit.

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

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

Upgrade Results

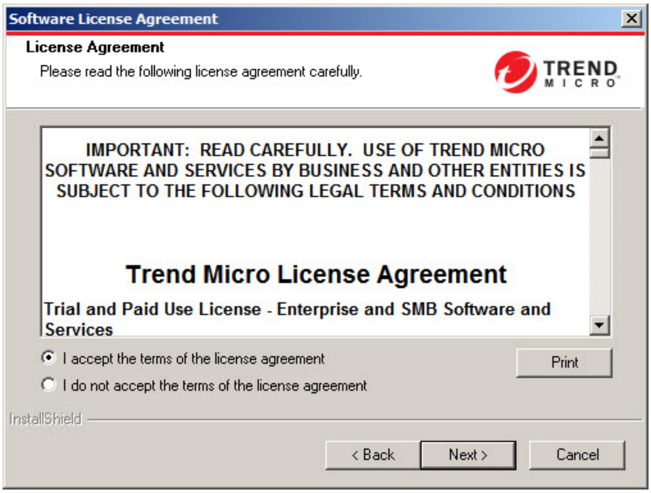
- Online agents upgrade immediately after server upgrade is complete.
- Offline agents upgrade when they become online.
- Roaming agents upgrade when they become online or, if the agent has scheduled update privileges, when scheduled update runs.

> **Note**
>
> Restart the agent endpoints to finish upgrading the agents.

Performing a Local Upgrade

During a local upgrade, OfficeScan applies the settings used by the previous OfficeScan server version. A limited subset of screens display that allow you to configure the new features offered by OfficeScan 11.0.

License Agreement



Software License Agreement

License Agreement

Please read the following license agreement carefully.

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

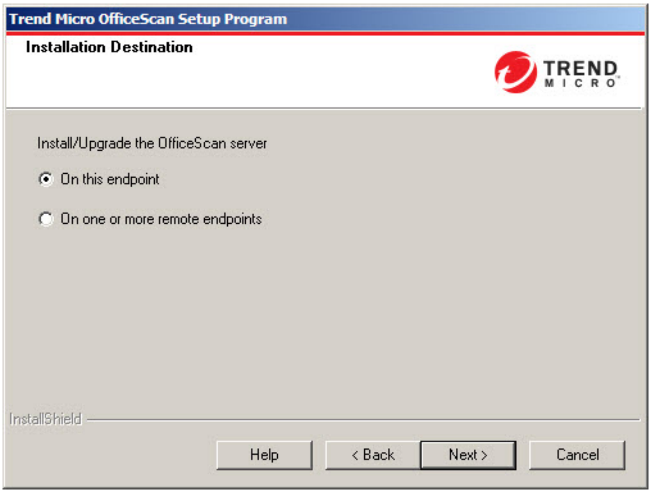
● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

FIGURE 3-1. License Agreement screen

Read the license agreement carefully and accept the license agreement terms to proceed with installation. Installation cannot proceed without accepting the license agreement terms.

Installation Destination



Trend Micro OfficeScan Setup Program

Installation Destination

Install/Upgrade the OfficeScan server

● On this endpoint

○ On one or more remote endpoints

FIGURE 3-2. Installation Destination screen

Run Setup and install the OfficeScan server on the current endpoint or other endpoint(s) on the network.

Remote Upgrade Notes

When upgrading remotely, Setup checks if the target endpoint meets the requirements for a server upgrade. Before proceeding:

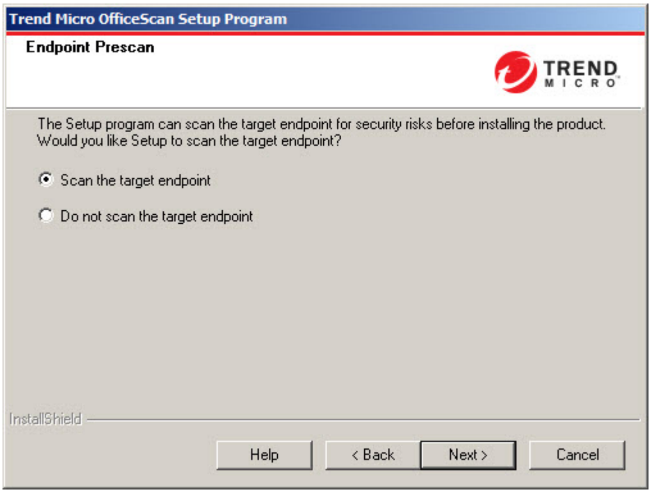
- Obtain administrator rights to the target endpoint.
- Record the endpoint's host name and logon credentials (user name and password).
- Verify that the target endpoints meet the requirements for installing the OfficeScan server.
- Ensure the endpoint has Microsoft IIS server 6.0 or later if using this as the web server. When using Apache web server, Setup automatically installs this server if not present on the target endpoint.

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

Important

For remote upgrades, re-enter all the settings. However, these settings are disregarded after the server upgrades because the server will use the previous version's settings.

Endpoint Prescan



The Setup program can scan the target endpoint for security risks before installing the product. Would you like Setup to scan the target endpoint?

● Scan the target endpoint

○ Do not scan the target endpoint

FIGURE 3-3. Endpoint Prescan screen

Before the OfficeScan server installation commences, Setup can scan the target endpoint for viruses and malware. Setup scans the most vulnerable areas of the endpoint, which include the following:

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

- Program Files folder

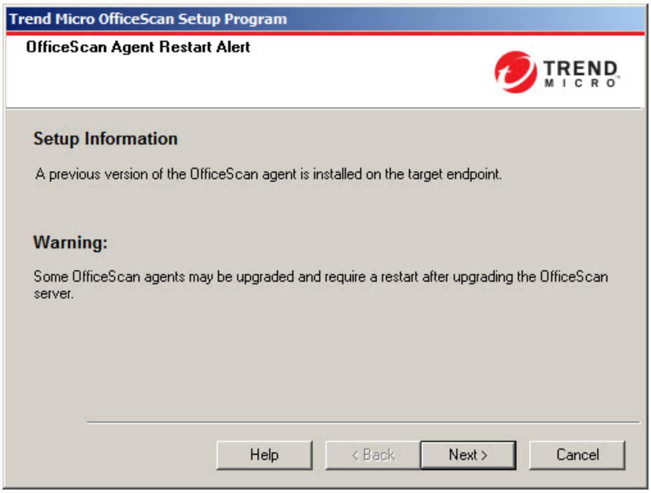
Setup can perform the following actions against detected virus/malware and Trojan horse programs:

- **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.

When performing a local installation, scanning occurs by clicking **Next**. When performing a remote installation, scanning occurs right before the actual installation.

OfficeScan Agent Restart Alert

The Setup program assesses the target endpoint resources. During upgrade scenarios, a warning screen appears if the OfficeScan agent program exists on the target endpoint.


Trend Micro OfficeScan Setup Program
OfficeScan Agent Restart Alert
TREND MICRO

Setup Information

A previous version of the OfficeScan agent is installed on the target endpoint.

Warning:

Some OfficeScan agents may be upgraded and require a restart after upgrading the OfficeScan server.

Help
< Back
Next >
Cancel

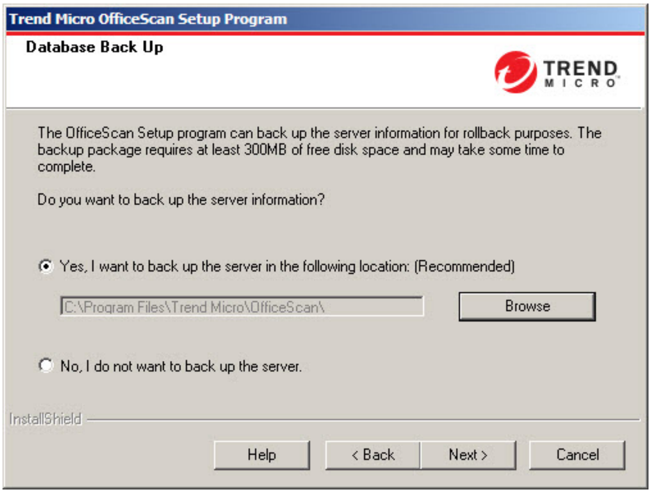
FIGURE 3-4. OfficeScan Agent Restart Alert

Database Back Up

During upgrades, the Setup program provides the option to back up the OfficeScan database before upgrading to the latest version. You can use this backup information for rollback purposes.

Note

The backup package may require more than 300MB of free disk space.



The OfficeScan Setup program can back up the server information for rollback purposes. The backup package requires at least 300MB of free disk space and may take some time to complete.

Do you want to back up the server information?

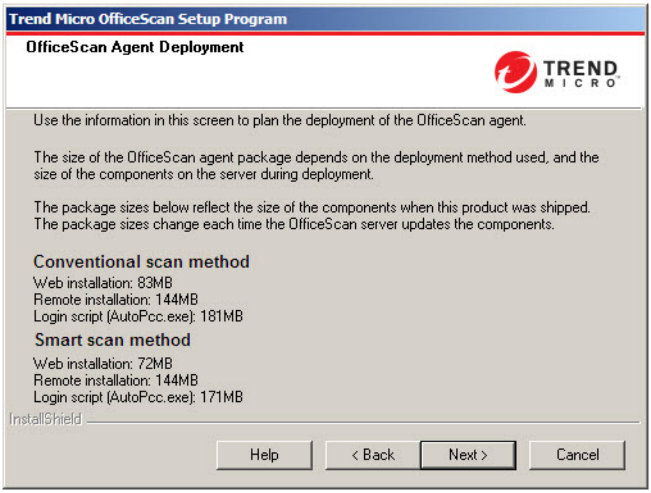
● Yes, I want to back up the server in the following location: (Recommended)

C:\Program Files\Trend Micro\OfficeScan\

○ No, I do not want to back up the server.

FIGURE 3-5. Database Back Up screen

OfficeScan Agent Deployment



Trend Micro OfficeScan Setup Program
OfficeScan Agent Deployment
TREND MICRO

Use the information in this screen to plan the deployment of the OfficeScan agent.

The size of the OfficeScan agent package depends on the deployment method used, and the size of the components on the server during deployment.

The package sizes below reflect the size of the components when this product was shipped. The package sizes change each time the OfficeScan server updates the components.

Conventional scan method

Web installation: 83MB
Remote installation: 144MB
Login script (AutoPcc.exe): 181MB

Smart scan method

Web installation: 72MB
Remote installation: 144MB
Login script (AutoPcc.exe): 171MB

FIGURE 3-6. OfficeScan Agent Deployment screen

There are several methods for installing or upgrading OfficeScan agents. This screen lists the different deployment methods and approximate network bandwidth needed.

Use this screen to estimate the size required on the servers and the bandwidth consumption when deploying agents to the target endpoints.

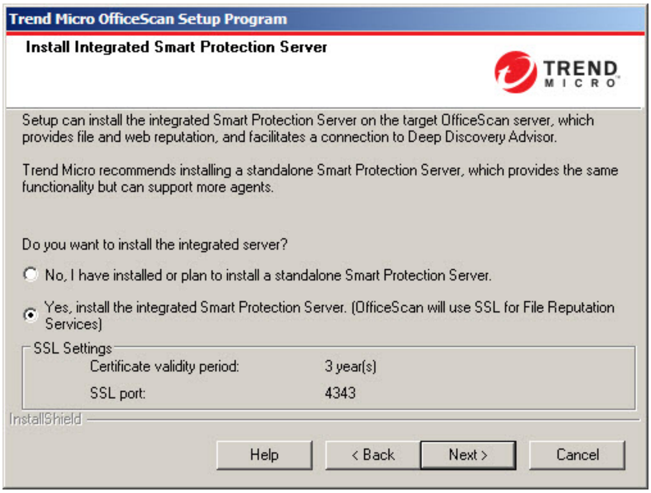
Note

All these installation methods require local administrator or domain administrator rights on the target endpoints.

Install Integrated Smart Protection Server

Note

This screen does not display when using an IIS virtual website during local upgrade installations.



Install Integrated Smart Protection Server

Setup can install the integrated Smart Protection Server on the target OfficeScan server, which provides file and web reputation, and facilitates a connection to Deep Discovery Advisor.

Trend Micro recommends installing a standalone Smart Protection Server, which provides the same functionality but can support more agents.

Do you want to install the integrated server?

○ No, I have installed or plan to install a standalone Smart Protection Server.

● Yes, install the integrated Smart Protection Server. (OfficeScan will use SSL for File Reputation Services)

SSL Settings

Certificate validity period: 3 year(s)

SSL port: 4343

FIGURE 3-7. Install Integrated Smart Protection Server screen

Setup can install the integrated Smart Protection Server on the target endpoint. The integrated server provides File Reputation Services to agents that use smart scan and

Web Reputation Services to agents subject to web reputation policies. Manage the integrated server from the OfficeScan web console.

Trend Micro recommends installing the standalone Smart Protection Server, which has the same functions as the integrated server but can serve more agents. The standalone server is installed separately and has its own management console. See the *Trend Micro Smart Protection Server Administrator's Guide* for information on the standalone server.

Tip

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

Agent Connection Protocols for File Reputation Services

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

Note

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

The port numbers used for File Reputation Services depend on the web server (Apache or IIS) the OfficeScan server uses. See *Web Server on page 2-12* for more information.

The HTTP port does not display on the installation screen. The HTTPS port displays, but configuration is optional.

Table 3-1. Ports for the Integrated Smart Protection Server's File Reputation Services

Web Server and Settings	Ports for File Reputation Services	
	HTTP	HTTPS (SSL)
Apache web server	8082	4345
IIS default website	80	443
IIS virtual website	8080	4343

Integrated Server Not Installed

When performing a fresh installation and not choosing to install the integrated server:

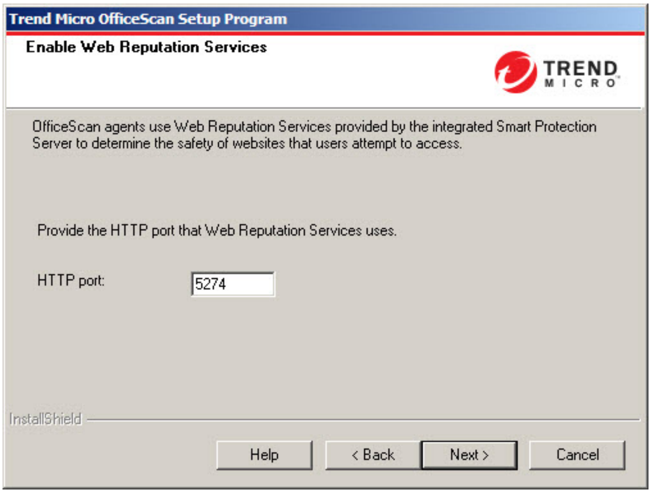
- Conventional scan becomes the default scan method.
- When enabling web reputation policies in a separate installation screen (for details, see *Web Reputation Feature on page 2-35*), agents cannot send web reputation queries because OfficeScan assumes that no Smart Protection Server installation occurred.

If a standalone server is available after installing OfficeScan, perform the following tasks from the OfficeScan web console:

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

When upgrading from OfficeScan 10.x servers where the integrated server has been disabled, the integrated server is not installed. OfficeScan agents retain their scan methods and the smart protection sources to which they send queries.

Enable Web Reputation Services



Trend Micro OfficeScan Setup Program

Enable Web Reputation Services

OfficeScan agents use Web Reputation Services provided by the integrated Smart Protection Server to determine the safety of websites that users attempt to access.

Provide the HTTP port that Web Reputation Services uses.

HTTP port: 5274

FIGURE 3-8. Enable Web Reputation Services screen

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

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

Agent Connection Protocols for Web Reputation Services

OfficeScan agents can connect to the integrated Smart Protection Server's Web Reputation Services using HTTP.

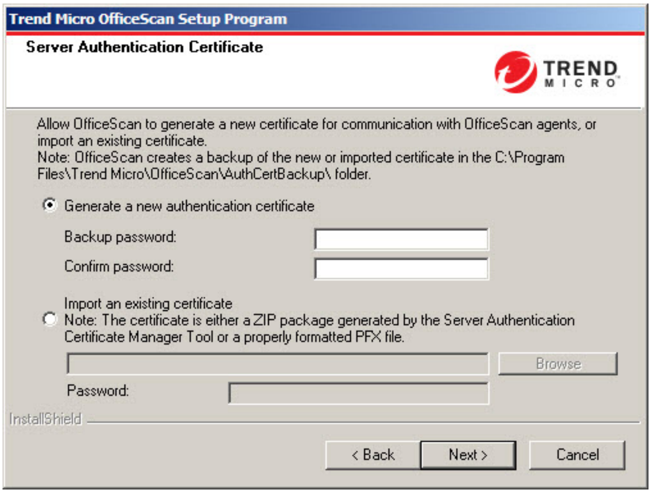
The HTTP port number used for Web Reputation Services depends on the web server (Apache or IIS) the OfficeScan server uses. See *Web Server on page 2-12* for more information.

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

WEB SERVER AND SETTINGS	HTTP PORT FOR WEB REPUTATION SERVICES
Apache web server with SSL enabled	5274
IIS default website with SSL enabled	80 (not configurable)
IIS virtual website with SSL enabled	8080 (not configurable)

Server Authentication Certificate

The Setup program attempts to detect preexisting authentication certificates during installation. If a preexisting certificate exists, OfficeScan automatically maps the file on the **Server Authentication Certificate** screen. If no preexisting certificate exists, OfficeScan defaults to the **Generate a new authentication certificate** option.



Trend Micro OfficeScan Setup Program

Server Authentication Certificate

Allow OfficeScan to generate a new certificate for communication with OfficeScan agents, or import an existing certificate.
Note: OfficeScan creates a backup of the new or imported certificate in the C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\ folder.

● Generate a new authentication certificate

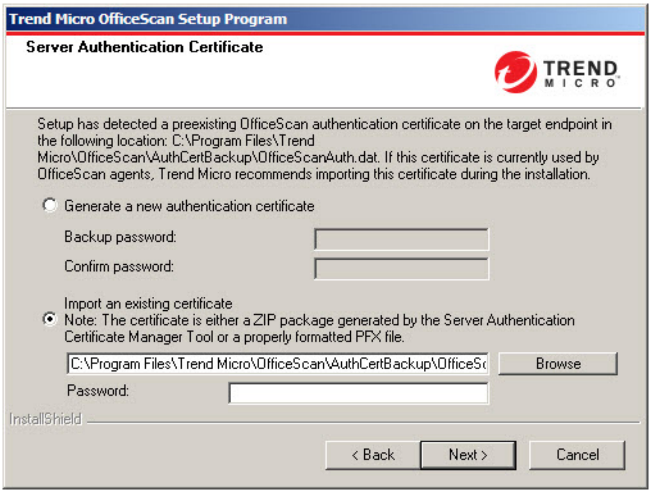
Backup password:

Confirm password:

○ Import an existing certificate
Note: The certificate is either a ZIP package generated by the Server Authentication Certificate Manager Tool or a properly formatted PFX file.

Password:

FIGURE 3-9. Server Authentication Certificate screen for new certificates



Trend Micro OfficeScan Setup Program

Server Authentication Certificate

Setup has detected a preexisting OfficeScan authentication certificate on the target endpoint in the following location: C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\OfficeScanAuth.dat. If this certificate is currently used by OfficeScan agents, Trend Micro recommends importing this certificate during the installation.

○ Generate a new authentication certificate

Backup password:

Confirm password:

● Import an existing certificate
Note: The certificate is either a ZIP package generated by the Server Authentication Certificate Manager Tool or a properly formatted PFX file.

C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\OfficeSc

Password:

FIGURE 3-10. Server Authentication Certificate screen for preexisting certificates

OfficeScan uses public-key cryptography to authenticate communications that the OfficeScan server initiates on agents. With public-key cryptography, the server keeps a private key and deploys a public key to all agents. The agents use the public key to verify that incoming communications are server-initiated and valid. The agents respond if the verification is successful.

Note

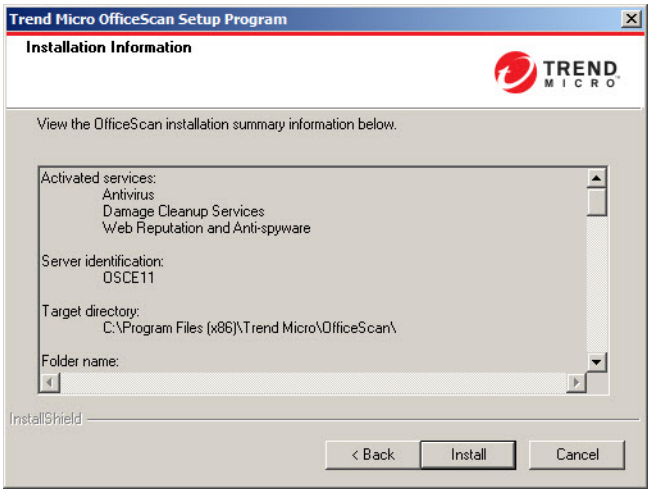
OfficeScan does not authenticate communications that agents initiate on the server.

OfficeScan can generate the authentication certificate during the installation or administrators can import a preexisting authentication certificate from another OfficeScan server.

Tip

When backing up the certificate, Trend Micro recommends encrypting the certificate with a password.

Installation Information



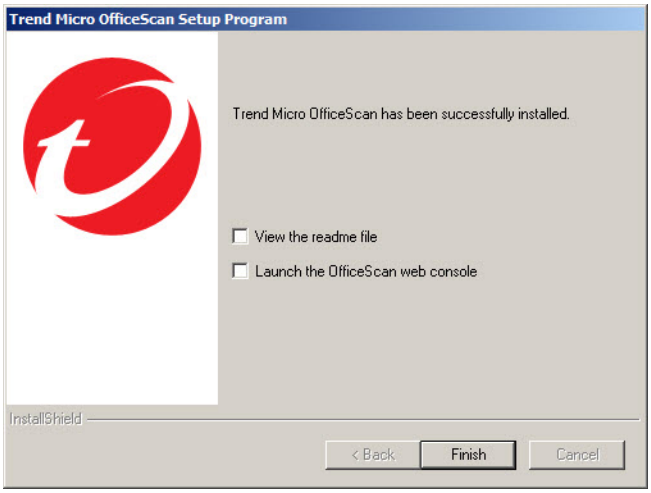
View the OfficeScan installation summary information below.

```
Activated services:
        Antivirus
        Damage Cleanup Services
        Web Reputation and Anti-spyware

Server identification:
        OSCE11

Target directory:
        C:\Program Files (x86)\Trend Micro\OfficeScan\

Folder name:
```

FIGURE 3-11. 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.**

InstallShield Wizard Complete


Trend Micro OfficeScan Setup Program

Trend Micro OfficeScan has been successfully installed.

□ View the readme file

□ Launch the OfficeScan web console

FIGURE 3-12. InstallShield Wizard Complete screen

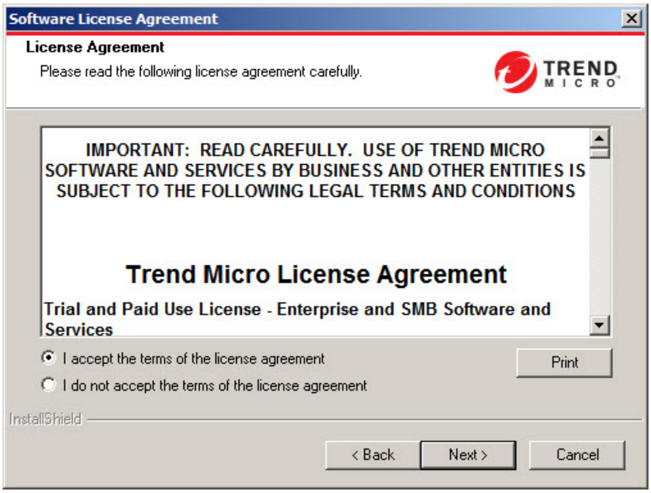
When the installation is complete, view the readme file for basic information about the product and known issues.

Administrators can launch the web console to start configuring OfficeScan settings.

Performing a Remote Upgrade

When performing a remote upgrade, OfficeScan provides more configuration options since it cannot ascertain all the previously configured settings on the previous OfficeScan server version before the upgrade begins. During the upgrade, OfficeScan uses the configuration settings of the previous OfficeScan version server as overrides to the settings you configure during the upgrade setup. For any settings that do not exist in the previous OfficeScan server version, OfficeScan applies the settings you configure during the upgrade setup.

License Agreement


Software License Agreement
License Agreement
Please read the following license agreement carefully.
TREND MICRO

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

● I accept the terms of the license agreement

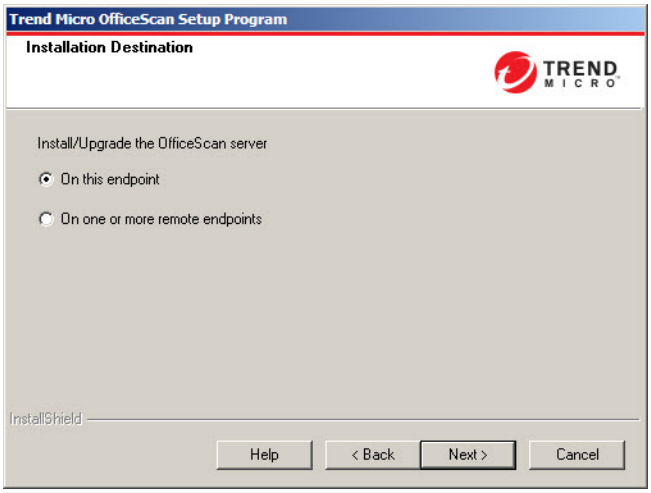
○ I do not accept the terms of the license agreement

Print
InstallShield
< Back
Next >
Cancel

FIGURE 3-13. License Agreement screen

Read the license agreement carefully and accept the license agreement terms to proceed with installation. Installation cannot proceed without accepting the license agreement terms.

Installation Destination


Trend Micro OfficeScan Setup Program

Installation Destination

Install/Upgrade the OfficeScan server

● On this endpoint

○ On one or more remote endpoints

FIGURE 3-14. Installation Destination screen

Run Setup and install the OfficeScan server on the current endpoint or other endpoint(s) on the network.

Remote Upgrade Notes

When upgrading remotely, Setup checks if the target endpoint meets the requirements for a server upgrade. Before proceeding:

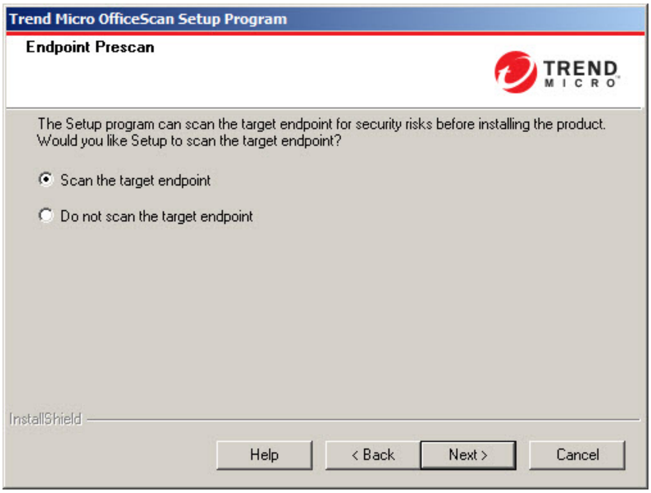
- Obtain administrator rights to the target endpoint.
- Record the endpoint's host name and logon credentials (user name and password).
- Verify that the target endpoints meet the requirements for installing the OfficeScan server.
- Ensure the endpoint has Microsoft IIS server 6.0 or later if using this as the web server. When using Apache web server, Setup automatically installs this server if not present on the target endpoint.

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

Important

For remote upgrades, re-enter all the settings. However, these settings are disregarded after the server upgrades because the server will use the previous version's settings.

Endpoint Prescan


Trend Micro OfficeScan Setup Program

Endpoint Prescan

The Setup program can scan the target endpoint for security risks before installing the product. Would you like Setup to scan the target endpoint?

● Scan the target endpoint

○ Do not scan the target endpoint

FIGURE 3-15. Endpoint Prescan screen

Before the OfficeScan server installation commences, Setup can scan the target endpoint for viruses and malware. Setup scans the most vulnerable areas of the endpoint, which include the following:

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

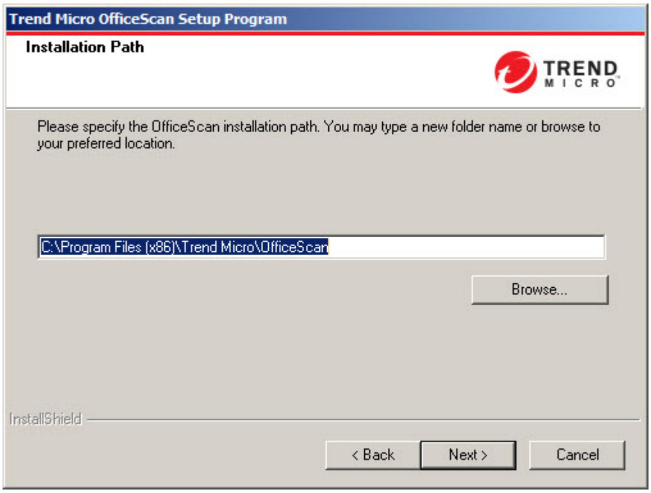
- Program Files folder

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.

When performing a local installation, scanning occurs by clicking **Next**. When performing a remote installation, scanning occurs right before the actual installation.

Installation Path


Trend Micro OfficeScan Setup Program

Installation Path

Please specify the OfficeScan installation path. You may type a new folder name or browse to your preferred location.

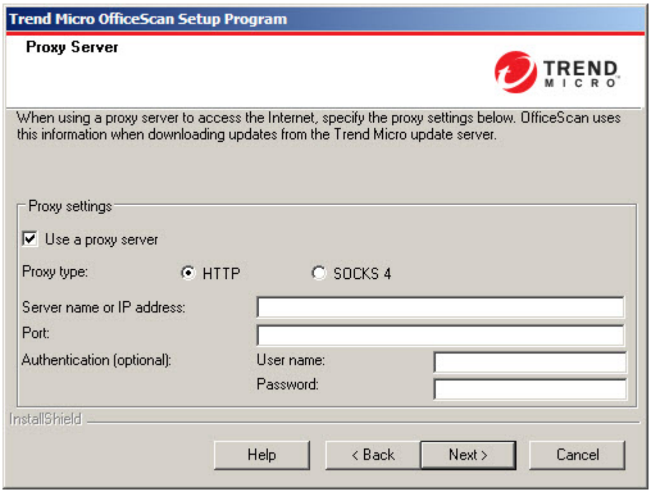
C:\Program Files (x86)\Trend Micro\OfficeScan

FIGURE 3-16. Installation Path screen

Accept the default installation path or specify a new one.

The specified installation path applies only when performing a remote fresh installation. For remote upgrades, OfficeScan uses the previous version's settings

Proxy Server


Trend Micro OfficeScan Setup Program

Proxy Server

When using a proxy server to access the Internet, specify the proxy settings below. OfficeScan uses this information when downloading updates from the Trend Micro update server.

Proxy settings

☑ Use a proxy server

Proxy type: ● HTTP ○ SOCKS 4

Server name or IP address:

Port:

Authentication (optional): User name: Password:

Figure 3-17. Proxy Server screen

The OfficeScan server uses the HTTP protocol for agent-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.

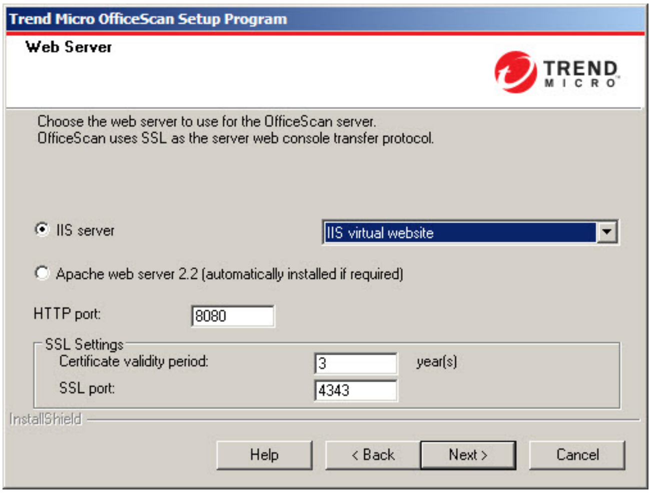
Administrators can skip specifying proxy settings during installation and do so after installation from the OfficeScan web console.

Proxy settings apply only when performing a remote fresh installation. For remote upgrade, OfficeScan uses the previous version's settings.

Note

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

Web Server



Trend Micro OfficeScan Setup Program

Web Server

Choose the web server to use for the OfficeScan server.
OfficeScan uses SSL as the server web console transfer protocol.

● IIS server — IIS virtual website

○ Apache web server 2.2 (automatically installed if required)

HTTP port: 8080

SSL Settings

Certificate validity period: 3 year(s)

SSL port: 4343

FIGURE 3-18. 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 agents. The web server converts these commands to agent CGIs and forwards them to the OfficeScan Master Service.

Web server settings only apply when performing a remote fresh installation. When performing a remote upgrade, OfficeScan uses the previous version’s settings.

IPv6 Support

For fresh installations, select IIS server to enable IPv6 support. Apache web server does not support IPv6 addressing. If the target endpoint only has an IPv6 address and

Apache is the selected web server, the installation does not proceed. If the target endpoint has both IPv6 and IPv4 addresses, administrators can choose Apache, but IPv6 support is not enabled after the server installation.

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

Web Server

If Setup detects both IIS and Apache web servers installed on the target endpoint, administrators can choose either of the two web servers. If neither exists on the target endpoint, administrators cannot choose IIS and OfficeScan installs Apache web server 2.2 automatically.

If using an Apache web server:

- Apache web server 2.2 is required. If Apache web server exists on the endpoint but the version is not 2.2, OfficeScan installs and uses version 2.2. OfficeScan does not remove the existing Apache web server.
- If enabling SSL, and Apache web server 2.2 exists, the Apache web server must have SSL settings pre-configured.
- By default, the administrator account is the only account created on the Apache web server.

Tip

Trend Micro recommends creating another account from which to run the web server. Otherwise, the OfficeScan server may become compromised if a malicious hacker takes control of the Apache server.

- Before installing the Apache web server, refer to the Apache website for the latest information on upgrades, patches, and security issues.

If using an IIS web server:

- The following Microsoft Internet Information Server (IIS) versions are required:
    - Version 6.0 on Windows Server 2003

- Version 7.0 on Windows Server 2008
- Version 7.5 on Windows Server 2008 R2
- Version 8.0 on Windows Server 2012

Do not install the web server on endpoints running IIS-locking applications because this could prevent successful installation. See the IIS documentation for more information.

HTTP Port

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

SSL Support

OfficeScan uses Secure Sockets Layer (SSL) for 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 selecting SSL, Setup automatically creates an SSL certificate, which is a requirement for SSL connections. The certificate contains server information, public key, and private key.

The SSL certificate should have a validity period between 1 and 20 years. The administrator can still use the certificate after it expires. However, a warning message appears every time SSL connection is invoked using the same certificate.

How communication through SSL works:

1. The administrator sends information from the web console to the web server through SSL connection.

2. The web server responds to the web console with the required certificate.
3. The browser performs key exchange using RSA encryption.
4. The web console sends data to the web server using RC4 encryption.

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

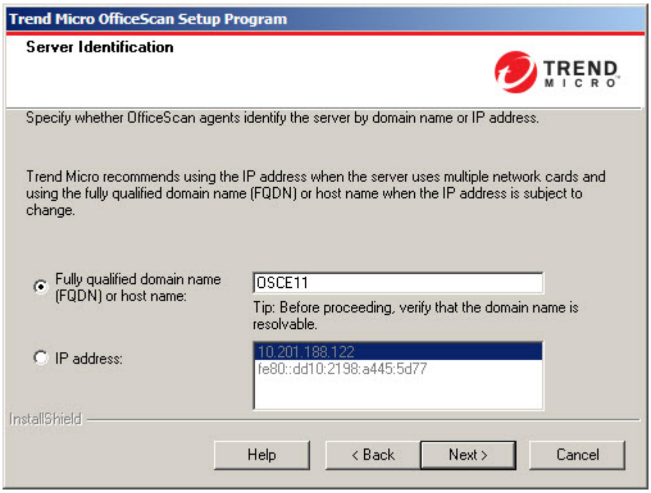
Web Server Ports

The following table lists the default port numbers for the web server

TABLE 3-3. Port Numbers for the OfficeScan Web Server

WEB SERVER AND SETTINGS	PORTS	
	HTTP	HTTPS (SSL)
Apache web server with SSL enabled	8080 (configurable)	4343 (configurable)
IIS default website with SSL enabled	80 (not configurable)	443 (not configurable)
IIS virtual website with SSL enabled	8080 (configurable)	4343 (configurable)

Server Identification


Trend Micro OfficeScan Setup Program

Server Identification

Specify whether OfficeScan agents identify the server by domain name or IP address.

Trend Micro recommends using the IP address when the server uses multiple network cards and using the fully qualified domain name (FQDN) or host name when the IP address is subject to change.

● Fully qualified domain name (FQDN) or host name: OSCE11

Tip: Before proceeding, verify that the domain name is resolvable.

○ IP address: 10.201.188.122 / fe80::dd10:2198:a445:5d77

FIGURE 3-19. Server Identification screen

The selected option on this screen applies only when performing a remote fresh installation.

Specify if OfficeScan agents identify the server computer by its fully qualified domain name (FQDN), host (domain) name, or IP address.

Communication between the server computer and agents is dependent on the specified IP address. Changing the IP address results in agents not being able to communicate with the OfficeScan server. The only way to restore communication is to redeploy all the agents. The same situation applies if the server computer is identified by a host name that changes.

In most networks, the server computer's IP address is more likely to change than its host name, thus it is usually preferable to identify the server computer by a host name.

Tip

For administrators using the IP address instead of the host name, Trend Micro does not recommend changing the IP address (obtained from the DHCP server) after the installation. Administrators can avoid further communication issues with OfficeScan agents by setting the IP address configuration to Static (on the DHCP server) using the same IP address information obtained from the DHCP server.

Another way to preserve the IP address configuration is to reserve the IP address for the OfficeScan server only. This forces the DHCP server to assign OfficeScan the same IP address even when DHCP-enabled.

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

IPV6 Support

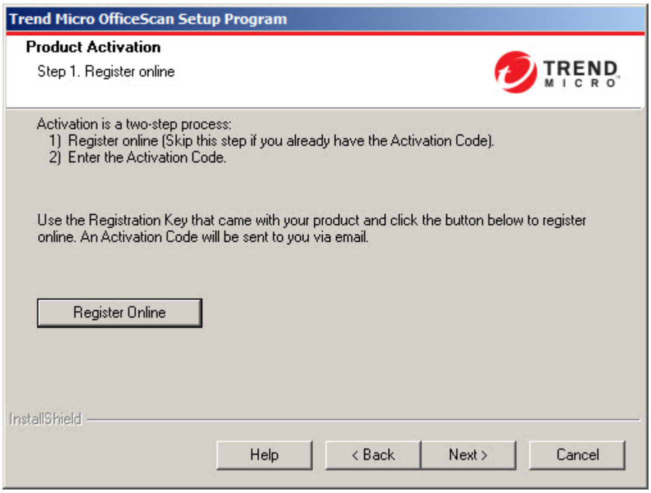
If the server manages IPv4 and IPv6 agents, it must have both IPv4 and IPv6 addresses and administrators must identify the server by its host name. If administrators identify the server by its IPv4 address, IPv6 agents cannot connect to the server. The same issue occurs if pure IPv4 agents connect to a server identified by its IPv6 address.

If the server manages only IPv6 agents, the minimum requirement is an IPv6 address. Server identification can be by its host name or IPv6 address. When administrators identify the server by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.

Note

Specify the FQDN only when performing a local installation of the server. There is no FQDN support for remote installations.

Registration and Activation


Trend Micro OfficeScan Setup Program

Product Activation

Step 1. Register online

Activation is a two-step process:

1) Register online (Skip this step if you already have the Activation Code).
2) Enter the Activation Code.

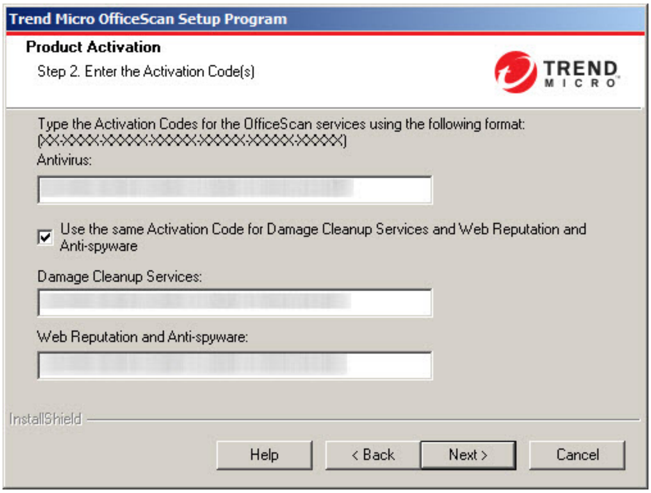
Use the Registration Key that came with your product and click the button below to register online. An Activation Code will be sent to you via email.

FIGURE 3-20. Product Activation - Step 1 screen

Register OfficeScan using the Registration Key that came with the product and then obtain the Activation Codes. Skip this step if the Activation Codes are already available.

To obtain the Activation Codes, click **Register Online**. Setup opens the Trend Micro registration website. After completing the registration form, Trend Micro sends an email with the Activation Codes. After receiving the codes, continue with the installation process.

When installing the OfficeScan server on a pure IPv6 endpoint, set up a dual-stack proxy server that can convert between IP addresses. This allows the server to connect to the Trend Micro registration website successfully.



Trend Micro OfficeScan Setup Program

Product Activation

Step 2. Enter the Activation Code(s)

Type the Activation Codes for the OfficeScan services using the following format: (XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

Antivirus:

☑ Use the same Activation Code for Damage Cleanup Services and Web Reputation and Anti-spyware

Damage Cleanup Services:

Web Reputation and Anti-spyware:

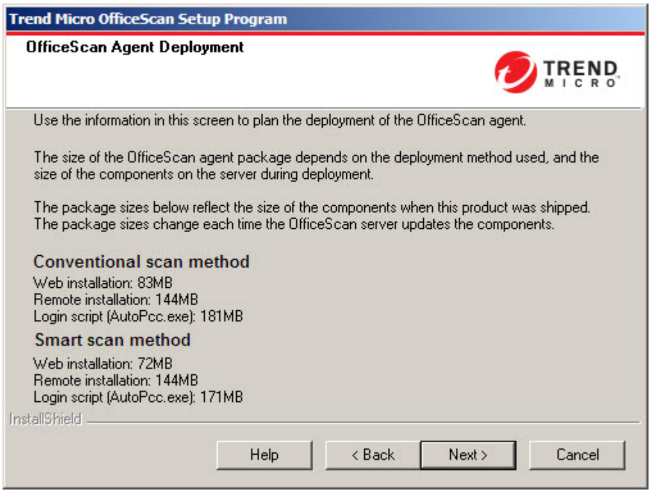
FIGURE 3-21. Product Activation - Step 2 screen

Specify the Activation Codes. The Activation Codes are case-sensitive.

If the Activation Code is valid for all services:

1. Type the Activation Code in the **Antivirus** text box.
2. Select **Use the same Activation Code for Damage Cleanup Services and Web Reputation and Anti-spyware**.
3. Click **Next** and verify the licensing information.

OfficeScan Agent Deployment



OfficeScan Agent Deployment

Use the information in this screen to plan the deployment of the OfficeScan agent.

The size of the OfficeScan agent package depends on the deployment method used, and the size of the components on the server during deployment.

The package sizes below reflect the size of the components when this product was shipped. The package sizes change each time the OfficeScan server updates the components.

Conventional scan method

Web installation: 83MB
Remote installation: 144MB
Login script (AutoPcc.exe): 181MB

Smart scan method

Web installation: 72MB
Remote installation: 144MB
Login script (AutoPcc.exe): 171MB

FIGURE 3-22. OfficeScan Agent Deployment screen

There are several methods for installing or upgrading OfficeScan agents. This screen lists the different deployment methods and approximate network bandwidth needed.

Use this screen to estimate the size required on the servers and the bandwidth consumption when deploying agents to the target endpoints.

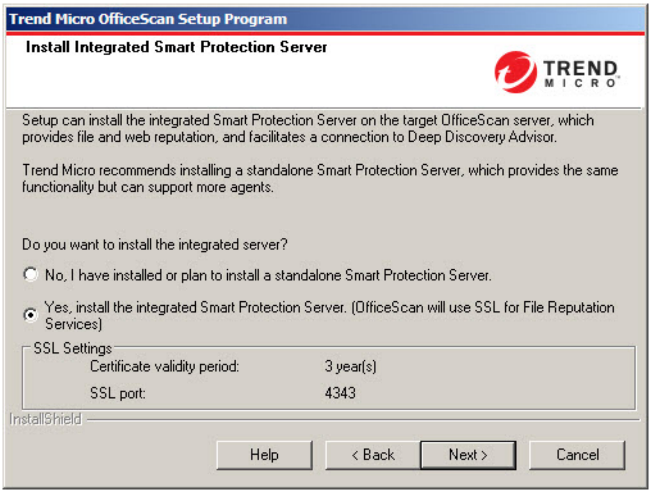
Note

All these installation methods require local administrator or domain administrator rights on the target endpoints.

Install Integrated Smart Protection Server

Note

This screen does not display when using an IIS virtual website during local upgrade installations.



Trend Micro OfficeScan Setup Program

Install Integrated Smart Protection Server

Setup can install the integrated Smart Protection Server on the target OfficeScan server, which provides file and web reputation, and facilitates a connection to Deep Discovery Advisor.

Trend Micro recommends installing a standalone Smart Protection Server, which provides the same functionality but can support more agents.

Do you want to install the integrated server?

○ No, I have installed or plan to install a standalone Smart Protection Server.

● Yes, install the integrated Smart Protection Server. (OfficeScan will use SSL for File Reputation Services)

SSL Settings

Certificate validity period: 3 year(s)

SSL port: 4343

FIGURE 3-23. Install Integrated Smart Protection Server screen

Setup can install the integrated Smart Protection Server on the target endpoint. The integrated server provides File Reputation Services to agents that use smart scan and Web Reputation Services to agents subject to web reputation policies. Manage the integrated server from the OfficeScan web console.

Trend Micro recommends installing the standalone Smart Protection Server, which has the same functions as the integrated server but can serve more agents. The standalone server is installed separately and has its own management console. See the *Trend Micro Smart Protection Server Administrator's Guide* for information on the standalone server.

Tip

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

Agent Connection Protocols for File Reputation Services

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

Note

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

The port numbers used for File Reputation Services depend on the web server (Apache or IIS) the OfficeScan server uses. See *Web Server on page 2-12* for more information.

The HTTP port does not display on the installation screen. The HTTPS port displays, but configuration is optional.

Table 3-4. Ports for the Integrated Smart Protection Server's File Reputation Services

Web Server and Settings	Ports for File Reputation Services	
	HTTP	HTTPS (SSL)
Apache web server	8082	4345
IIS default website	80	443
IIS virtual website	8080	4343

Integrated Server Not Installed

When performing a fresh installation and not choosing to install the integrated server:

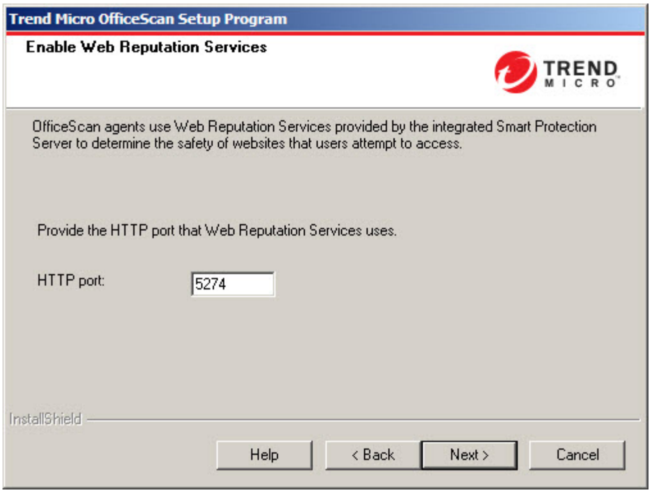
- Conventional scan becomes the default scan method.
- When enabling web reputation policies in a separate installation screen (for details, see *Web Reputation Feature on page 2-35*), agents cannot send web reputation queries because OfficeScan assumes that no Smart Protection Server installation occurred.

If a standalone server is available after installing OfficeScan, perform the following tasks from the OfficeScan web console:

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

When upgrading from OfficeScan 10.x servers where the integrated server has been disabled, the integrated server is not installed. OfficeScan agents retain their scan methods and the smart protection sources to which they send queries.

Enable Web Reputation Services


Trend Micro OfficeScan Setup Program
Enable Web Reputation Services
TREND MICRO
InstallShield
Help
< Back
Next >
Cancel

OfficeScan agents use Web Reputation Services provided by the integrated Smart Protection Server to determine the safety of websites that users attempt to access.

Provide the HTTP port that Web Reputation Services uses.

HTTP port: 5274

FIGURE 3-24. Enable Web Reputation Services screen

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

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

Agent Connection Protocols for Web Reputation Services

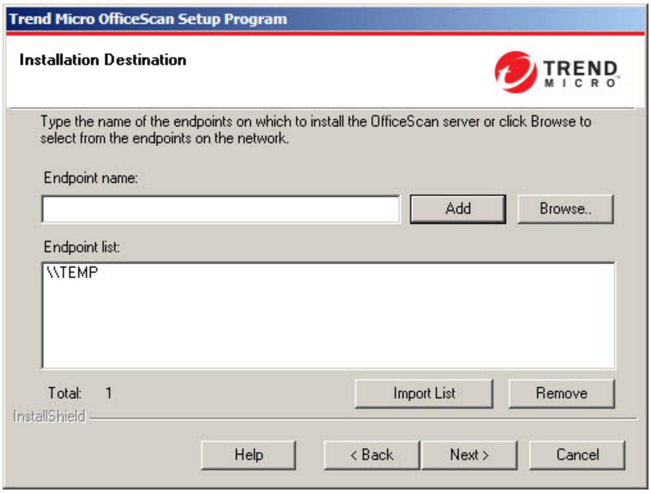
OfficeScan agents can connect to the integrated Smart Protection Server's Web Reputation Services using HTTP.

The HTTP port number used for Web Reputation Services depends on the web server (Apache or IIS) the OfficeScan server uses. See *Web Server on page 2-12* for more information.

TABLE 3-5. Ports for the Integrated Smart Protection Server's Web Reputation Services

WEB SERVER AND SETTINGS	HTTP PORT FOR WEB REPUTATION SERVICES
Apache web server with SSL enabled	5274
IIS default website with SSL enabled	80 (not configurable)
IIS virtual website with SSL enabled	8080 (not configurable)

Installation Destination



Type the name of the endpoints on which to install the OfficeScan server or click Browse to select from the endpoints on the network.

Endpoint name:

Endpoint list:

\\TEMP

Total: 1

FIGURE 3-25. Installation Destination screen

Specify the target endpoint to which OfficeScan installs. Manually type the endpoint's host name or IP address. Click **Browse** to search for endpoint(s) in the network.

Import endpoint name(s) from a text file by clicking **Import List**. When installing to multiple endpoints simultaneously and all endpoints pass the analysis, Setup installs the OfficeScan server in the listed order in the text file.

In the text file:

- Specify one endpoint 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 (-).

For example:

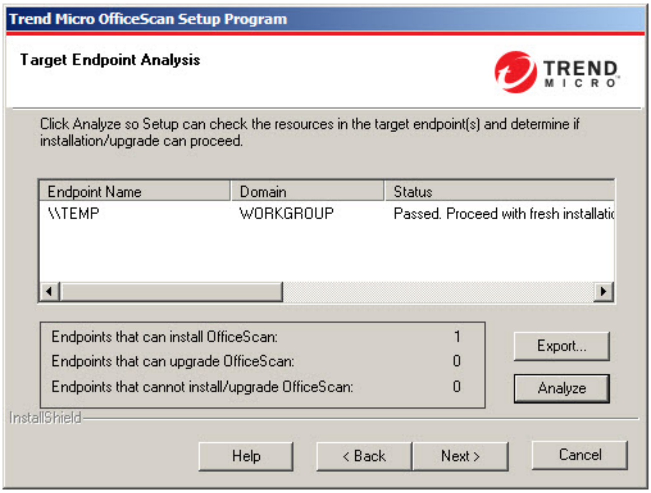
```
\\domain1\test-abc

\\domain2\test-123
```

Tips to ensure that remote installation can proceed:

- Obtain administrator rights to the target endpoint.
- Record the endpoint's host name and logon credentials (user name and password).
- Verify that the target endpoints meet the system requirements for installing the OfficeScan server.
- Ensure the endpoint has Microsoft IIS server 6.0 or later if using this as the web server. When choosing to use the Apache web server, Setup automatically installs this server if not present in the target endpoint.
- Do not specify the endpoint launching Setup as a target endpoint. Run local installation on the endpoint instead.

After specifying the target endpoint(s), click **Next.** Setup checks if the endpoint(s) meet the OfficeScan installation requirements.

Target Endpoint Analysis



Trend Micro OfficeScan Setup Program

Target Endpoint Analysis

Click Analyze so Setup can check the resources in the target endpoint(s) and determine if installation/upgrade can proceed.

Endpoint Name	Domain	Status
\\TEMP	WORKGROUP	Passed. Proceed with fresh installatic

Endpoints that can install OfficeScan:	1
Endpoints that can upgrade OfficeScan:	0
Endpoints that cannot install/upgrade OfficeScan:	0

FIGURE 3-26. Target Endpoint Analysis screen

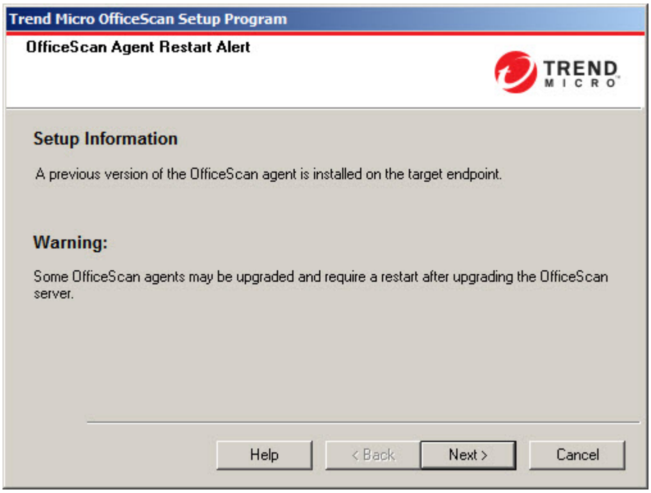
Before allowing remote installation to proceed, Setup needs to first determine if the selected target endpoint(s) can install the OfficeScan server. To start the analysis, click **Analyze**. Setup may require the administrator user name and password used to log on to the target endpoint. After the analysis,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

When installing to multiple endpoints, installation proceeds if at least one of the endpoints pass the analysis. Setup installs the OfficeScan server to that endpoint and ignores the endpoints that did not pass the analysis.

During remote installation, the installation progress only displays in the endpoint from which Setup launched and not on the target endpoint(s).

OfficeScan Agent Restart Alert

The Setup program assesses the target endpoint resources. During upgrade scenarios, a warning screen appears if the OfficeScan agent program exists on the target endpoint.


Trend Micro OfficeScan Setup Program
OfficeScan Agent Restart Alert
TREND MICRO

Setup Information

A previous version of the OfficeScan agent is installed on the target endpoint.

Warning:

Some OfficeScan agents may be upgraded and require a restart after upgrading the OfficeScan server.

Help
< Back
Next >
Cancel

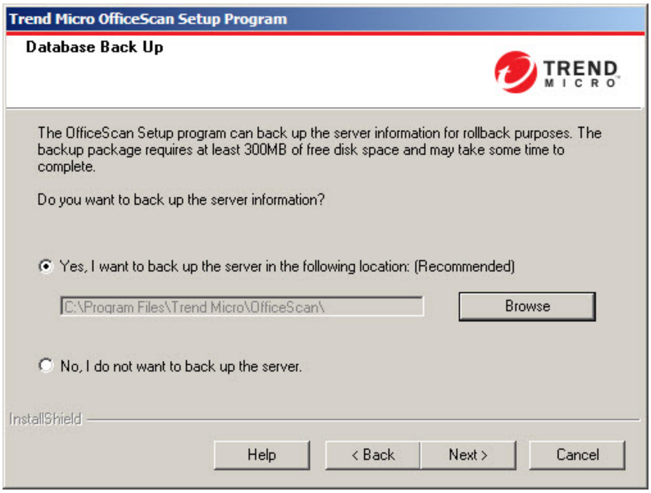
FIGURE 3-27. OfficeScan Agent Restart Alert

Database Back Up

During upgrades, the Setup program provides the option to back up the OfficeScan database before upgrading to the latest version. You can use this backup information for rollback purposes.

Note

The backup package may require more than 300MB of free disk space.



Trend Micro OfficeScan Setup Program

Database Back Up

The OfficeScan Setup program can back up the server information for rollback purposes. The backup package requires at least 300MB of free disk space and may take some time to complete.

Do you want to back up the server information?

● Yes, I want to back up the server in the following location: (Recommended)

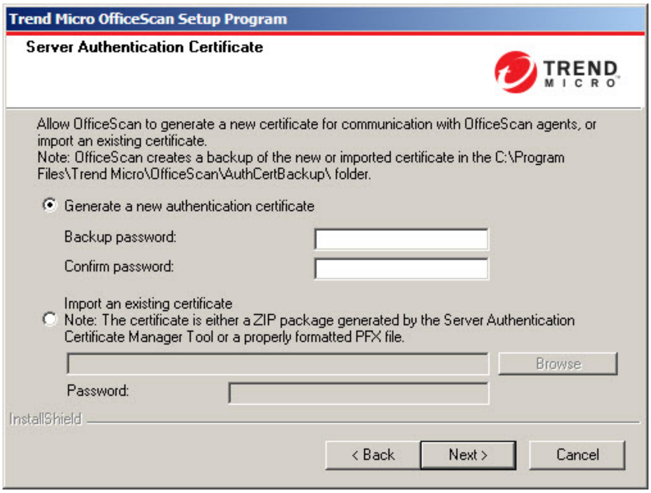
C:\Program Files\Trend Micro\OfficeScan\

○ No, I do not want to back up the server.

FIGURE 3-28. Database Back Up screen

Server Authentication Certificate

The Setup program attempts to detect preexisting authentication certificates during installation. If a preexisting certificate exists, OfficeScan automatically maps the file on the **Server Authentication Certificate** screen. If no preexisting certificate exists, OfficeScan defaults to the **Generate a new authentication certificate** option.



Trend Micro OfficeScan Setup Program

Server Authentication Certificate

Allow OfficeScan to generate a new certificate for communication with OfficeScan agents, or import an existing certificate.
Note: OfficeScan creates a backup of the new or imported certificate in the C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\ folder.

● Generate a new authentication certificate

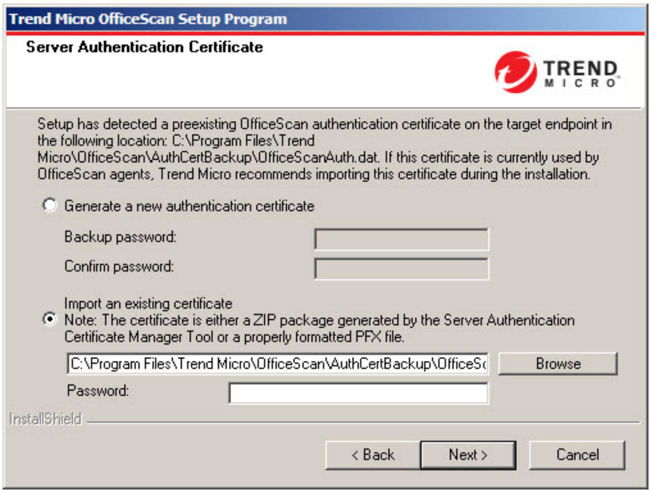
Backup password:

Confirm password:

○ Import an existing certificate
Note: The certificate is either a ZIP package generated by the Server Authentication Certificate Manager Tool or a properly formatted PFX file.

Password:

FIGURE 3-29. Server Authentication Certificate screen for new certificates



Trend Micro OfficeScan Setup Program

Server Authentication Certificate

Setup has detected a preexisting OfficeScan authentication certificate on the target endpoint in the following location: C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\OfficeScanAuth.dat. If this certificate is currently used by OfficeScan agents, Trend Micro recommends importing this certificate during the installation.

○ Generate a new authentication certificate

Backup password:

Confirm password:

● Import an existing certificate
Note: The certificate is either a ZIP package generated by the Server Authentication Certificate Manager Tool or a properly formatted PFX file.

C:\Program Files\Trend Micro\OfficeScan\AuthCertBackup\OfficeS

Password:

FIGURE 3-30. Server Authentication Certificate screen for preexisting certificates

OfficeScan uses public-key cryptography to authenticate communications that the OfficeScan server initiates on agents. With public-key cryptography, the server keeps a private key and deploys a public key to all agents. The agents use the public key to verify that incoming communications are server-initiated and valid. The agents respond if the verification is successful.

Note

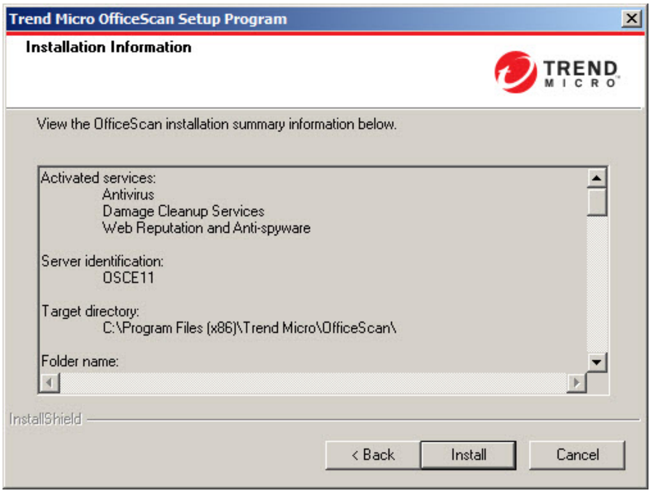
OfficeScan does not authenticate communications that agents initiate on the server.

OfficeScan can generate the authentication certificate during the installation or administrators can import a preexisting authentication certificate from another OfficeScan server.

Tip

When backing up the certificate, Trend Micro recommends encrypting the certificate with a password.

Installation Information



View the OfficeScan installation summary information below.

Activated services:
Antivirus
Damage Cleanup Services
Web Reputation and Anti-spyware

Server identification:
OSCE11

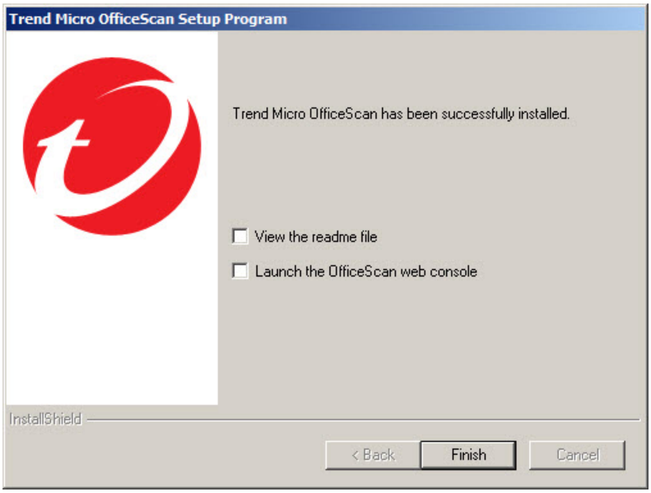
Target directory:
C:\Program Files (x86)\Trend Micro\OfficeScan\

Folder name:

FIGURE 3-31. 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.**

InstallShield Wizard Complete


Trend Micro OfficeScan Setup Program

Trend Micro OfficeScan has been successfully installed.

□ View the readme file

□ Launch the OfficeScan web console

FIGURE 3-32. InstallShield Wizard Complete screen

When the installation is complete, view the readme file for basic information about the product and known issues.

Administrators can launch the web console to start configuring OfficeScan settings.

Chapter 4

Post-installation Tasks

Perform the following tasks after the OfficeScan server installation completes.

Topics in this chapter:

Verifying the Server Installation or Upgrade

After completing the installation, verify the following:

TABLE 4-1. Items to Verify After Installing 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 URL in the Internet Explorer browser: • 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.
OfficeScan server services	The following OfficeScan server services display on the Microsoft Management Console: • OfficeScan Active Directory Integration Service: This service displays if the Active Directory integration and Role-based Administration features work properly. • OfficeScan Control Manager Agent: The status for this service should be "Started" if the OfficeScan server has been registered to Control Manager. • OfficeScan Master Service: The status for this service should be "Started". • OfficeScan Plug-in Manager: The status for this service should be "Started". • Trend Micro Smart Scan Server: The status for this service should be "Started". • Trend Micro Local Web Classification Server: The status for this service should be "Started" if Web Reputation Services was enabled during installation.

ITEM TO VERIFY	DETAILS
OfficeScan server processes	When you open Windows Task Manager, DBServer.exe is running.
Server installation log	The server installation log, OFCMAS.LOG, exists in `%windir%`.

Registry keys	The following registry key exists:
	• For 32-bit platforms:
	`HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan`
	• For 64-bit platforms:
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\TrendMicro\OfficeScan`

Program folder	The OfficeScan server files are found under the `<Server installation folder>`.

Verifying Integrated Smart Protection Server Installation

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

Procedure

1. On the server web console, go to **Administration** > **Smart Protection** > **Smart Protection Sources**.
2. Click the **standard list** link.
3. On the screen that opens, click **Integrated Smart Protection Server**.
4. On the screen that displays, click **Test Connection**.

   Connection with the integrated server should be successful.

Updating OfficeScan Components

After installing OfficeScan, update components on the server.

Note

This section describes performing a manual update. For information on scheduled update and update configurations, see the *OfficeScan Server Help*.

Updating the OfficeScan Server

Procedure

1. Log on to the 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 endpoints from security risks. Modify the scan settings from the web console by going to **Agents** > **Agent Management** and clicking **Settings** > **{Scan Type}**.

Agent Settings

OfficeScan provides several types of settings that apply to all agents registered to the server or to all agents with a certain privilege. Modify agent settings from the web console by going to **Agents** > **Global Agent Settings**.

Agent Privileges

Default agent privileges include displaying the system tray icon on the OfficeScan agent endpoint. Modify default agent privileges from the web console.

1. Go to **Agents** > **Agent Management**.

2. Click **Settings** > **Privileges and Other Settings**.

Using Client Mover for Legacy Platforms

The OfficeScan agent no longer supports the Windows 95, 98, Me, NT, or 2000 operating systems, and the Itanium architecture platform. If OfficeScan agents run any of these platforms and the administrator upgraded the server that manages them to version 11.0:

- The OfficeScan agents are not upgraded.

- The OfficeScan 11.0 server stops managing the agents. The agents' status becomes "Disconnected".

- The OfficeScan 11.0 server saves the agents’ information to a file named `unsupCln.txt`. Use this file to "move" agents to a server with the same version. Move means designating a new server to manage the agents.

- On the OfficeScan 11.0 server computer, run a tool called **Client Mover**. This tool notifies agents that they are managed by a new server and checks if agents are moved successfully. When agents receive the notification, they register to their new parent server.

Note

Perform this task only if there are agents running Windows 95, 98, Me, NT, 2000, or Itanium architecture.

Moving Agents

Procedure

1. Prepare a new parent server. This server's version should be the same as the version of the agents to be moved.

2. Record the server's endpoint name/IP address and server listening port. These details are required when you move the agents.

   Obtain the server listening port from the server's web console by going to **Administration** > **Settings** > **Agent Connection**.

3. On the OfficeScan 11.0 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 agent 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 agents to the new parent server. This command is used in conjunction with the `/V` command.

For example:

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

5. Use the `/V` command to verify that the tool successfully moved the agents. This command compares the IP addresses of the OfficeScan 11.0 server and the new parent server. If the IP addresses are the same, the tool was unable to move the agents.

   For example:

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

6. To check the result:

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

      For example: `unsupcln.txt.log.20080101_123202`

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

      Sample entry in the updated `unsupcln.txt` file:

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

      Where:

      "x12xx345-6xxx-78xx-xx91-234x567x8x91" is the client's GUID.

      "1234567891" is the agent's IP address in decimal notation.

      "23456" is the agent listening port.

      "0" is the result and it means notification was completed.

      Other possible results:

      1 = OfficeScan Agent notification successful

2 = OfficeScan Agent 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 agent's GUID.

"123.12.12.123:23456" is the agent's IP address and listening port.

Result is "Unable to send the notification. Please check the network or agent status".

7. Use the `/F` command to force the notification or verification without checking the current agent status.

Registering OfficeScan to Control Manager

When a Control Manager server manages newly installed OfficeScan servers, register OfficeScan to Control Manager after installation.

Note

Control Manager registration only applies to newly installed OfficeScan servers.

On the OfficeScan web console, go to **Administration** > **Settings** > **Control Manager**.

See the *OfficeScan Server Help* or *OfficeScan Administrator's Guide* for the procedure.

Chapter 5

Uninstalling and Rolling Back OfficeScan

This chapter describes the steps for uninstalling or rolling back Trend Micro™ OfficeScan™.

Topics in this chapter:

Uninstallation and Rollback Considerations

When experiencing problems with OfficeScan, try the following:

- Use the uninstallation program to safely remove the OfficeScan server from the endpoint. Before uninstalling the server, move the agents it manages to another OfficeScan server.
- Roll back agents to version previous OfficeScan versions instead of uninstalling the OfficeScan server. See *Rolling Back the OfficeScan Server and OfficeScan Agents Using the Server Backup Package on page 5-9*.

Before Uninstalling the OfficeScan Server

Use the uninstallation program to safely remove the OfficeScan server.

Before uninstalling the server, move the agents it manages to another OfficeScan server with the same version. Consider backing up the server database and configuration files in order to reinstall the server later.

Moving Agents to Another OfficeScan Server

The OfficeScan web console provides an option to move agents managed by the server to another OfficeScan server.

Procedure

1. Record the following information for the other OfficeScan server. This information is necessary when moving the agents.

    - Endpoint name or IP address
    - Server listening port

    To view the server listening port, go to **Administration** > **Settings** > **Agent Connection**. The port number displays on the screen.

2. On the web console of the server to uninstall, go to **Agents** > **Agent Management**.

3. On the agent tree, select the agents to upgrade and then click **Manage Agent Tree** > **Move Agent**.

4. Under **Move selected agent(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 agents 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.

Procedure

1. Back up the database from the web console by going to **Administration** > **Settings** > **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 agent 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 *Uninstalling the OfficeScan Server on page 5-4*.
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 (`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 endpoint. This overwrites the OfficeScan server database and the relevant files and folders.
9. Restart the OfficeScan Master Service.

Uninstalling the OfficeScan Server

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

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

Note

For OfficeScan agent uninstallation instructions, see the Administrator’s Guide.

Uninstalling the OfficeScan Server Using the Uninstallation Program

Procedure

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

   - Method A

   a. On the OfficeScan server endpoint, 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.

Manually Uninstalling the OfficeScan Server

Part 1: Integrated Smart Protection Server Uninstallation

Procedure

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. Go to `<Server installation folder>\PCCSRV\private` and open `ofcserver.ini`.

5. Modify the following settings:

   TABLE 5-1. ofcserver.ini Settings

SETTING	INSTRUCTION
`WSS_INSTALL`	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 Protection Server (Integrated)

IIS_VHostIdx=5
```

> **Note**
>
> The value for `IIS_VHostidx` should be the same as the "isapi" value indicated on the following line:
>
> ```
> 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 that the following items were removed:

   - Trend Micro Smart Protection Server service from the Microsoft Management Console

   - Smart Protection Server performance counters

- Smart Protection Server (Integrated) website

Part 2: OfficeScan Server Uninstallation

Procedure

1. Open Registry Editor and perform the following steps:

   WARNING!

   The next steps require the deletion of 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. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\`.

   b. Verify that the `ofcservice` hive has been deleted.

   c. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\` and delete the `OfficeScan` hive.

      For 64-bit endpoints, the path is `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\`.

   d. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\`. Delete the `OfficeScan Management Console-<Server Name>` folder.

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

3. Restart the server computer.

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

5. Delete the OfficeScan website from the Internet Information Services (IIS) console.

a. Open the IIS console.

b. Expand `ServerName`.

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

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

Rolling Back the OfficeScan Server and OfficeScan Agents Using the Server Backup Package

The OfficeScan rollback procedure involves rolling back OfficeScan agents and then rolling back the OfficeScan server.

Important

- Administrators can only roll back the OfficeScan server and agents using the following procedure if the administrator chose to back up the server during the installation process. If the server backup files are not available, refer to the previously installed OfficeScan version's *Installation and Upgrade Guide* for manual rollback procedures.
- This version of OfficeScan only supports rollbacks to the following OfficeScan versions:
  - OfficeScan 10.6 Service Pack 3
  - OfficeScan 10.6 Service Pack 2
  - OfficeScan 10.6 Service Pack 1
  - OfficeScan 10.6
  - OfficeScan 10.5
  - OfficeScan 10.0 SP1

Rolling Back the OfficeScan Agents

OfficeScan can only rollback OfficeScan agents to the same version of the server being restored. You cannot rollback OfficeScan agents to an older version than the server.

Important

Ensure that you roll back OfficeScan agents before rolling back the OfficeScan server.

Procedure

1. Ensure that OfficeScan agents can upgrade the agent program.

   a. On the OfficeScan 11.0 web console, go to **Agents** > **Agent Management**.

   b. Select the OfficeScan agents to be rolled back.

   c. Click the **Settings** > **Privileges and Other Settings** > **Other Settings** tab.

   d. Select **OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes**.

2. On the OfficeScan 11.0 web console, go to **Updates** > **Agents** > **Update Source**.

3. Select **Customized Update Source**.

4. On the **Customized Update Source List**, click **Add**.

   A new screen opens.

5. Type the IP addresses of the OfficeScan agents to be rolled back.

6. Type the update source URL.

   For example, type:

   ```
   http://<IP address of the OfficeScan server>:<port>/
   OfficeScan/download/Rollback
   ```

7. Click **Save**.

8. Click **Notify All Agents**.

When the OfficeScan agent to be rolled back updates from the update source, the OfficeScan agent is uninstalled and the previous OfficeScan agent version is installed.

9. After the previous OfficeScan agent version is installed, inform the user to restart the computer.

   After the rollback process is complete, the OfficeScan agent continues to report to the same OfficeScan server.

   Note

   After rolling back the OfficeScan agent, all components, including the Virus Pattern, also roll back to the previous version. If administrators do not roll back the OfficeScan server, the rolled-back OfficeScan agent cannot update components. Administrators must change the update source of the rolled-back OfficeScan agent to the standard update source to receive further component updates.

Restoring the Previous OfficeScan Server Version

The restoration procedure for the OfficeScan server requires that administrators uninstall the OfficeScan 11.0 server, reinstall the older server version, manually stop Windows services, update the system registry, and replace OfficeScan server files in the OfficeScan installation directory.

Important

Ensure that you roll back OfficeScan agents before restoring the OfficeScan server.

Procedure

1. Uninstall the OfficeScan 11.0.

   For details, see *Uninstalling the OfficeScan Server on page 5-4*.

2. Install the previous OfficeScan server version.

Tip

Trend Micro recommends not changing the host name or IP address when restoring the server.

To verify the previous version of the server, go to the `<Server_installation_folder>` and view the restoration folder created during the OfficeScan 11.0 server installation. The folder name (referred to as <Restore_folder_version>) is one of the following:

- OSCE106_SP3: OfficeScan 10.6 Service Pack 3
- OSCE106_SP2: OfficeScan 10.6 Service Pack 2
- OSCE106_SP1: OfficeScan 10.6 Service Pack 1
- OSCE106: OfficeScan 10.6
- OSCE105: OfficeScan 10.5
- OSCE10_SP1: OfficeScan 10.0 Service Pack 1

3. On the OfficeScan server computer, stop the following services:
   - Intrusion Defense Firewall (if installed)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - Apache 2 (if using the Apache web server)
   - World Wide Web Publishing Service (if using the IIS web server)
4. Copy and replace all files and directories from the `<Server_installation_folder>\<Restore_folder_version>\` directory to the `<Server_installation_folder>\PCCSRV\` directory.
5. Restore the OfficeScan registry.

a. Open the **Registry Editor** (`regedit.exe`).

b. In the left navigation pane, select the one of the following registry keys:

- For 32-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`
- For 64-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service`

c. Go to **File** > **Import...**.

d. Select the general OfficeScan server `.reg` file located in the `<Server_installation_folder>\<Restore_folder_version>\` directory.

The registry file name follows this format:

`RegBak_<Restore_folder_version>.reg`

e. Click **Yes** to restore all of the previous OfficeScan version keys.

6. Optionally restore the database backup schedule.

a. Open the **Registry Editor** (`regedit.exe`).

b. In the left navigation pane, select the one of the following registry keys:

- For 32-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup`
- For 64-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Database Backup`

c. Go to **File** > **Import...**.

d. Select the database `.reg` file located in the `<Server_installation_folder>\<Restore_folder_version>\` directory.

The registry file name follows this format:

`RegBak_DBBak_<Restore_folder_version>.reg`

e. Click **Yes** to restore all of the previous OfficeScan version keys.

7. Open a command line editor (`cmd.exe`) and type the following commands to reset the Local Web Classification Server performance counter:

   ```
   cd <Server installation folder>\PCCSRV\LWCS
   ```

   ```
   regsvr32.exe /u /s perfLWCSPerfMonMgr.dll
   ```

   ```
   regsvr32.exe /s perfLWCSPerfMonMgr.dll
   ```

8. Restart the following services:

   - Intrusion Defense Firewall (if installed)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - Apache 2 (if using the Apache web server)
   - World Wide Web Publishing Service (if using the IIS web server)

9. Clean the Internet Explorer cache and remove ActiveX controls manually. For details on removing ActiveX controls in Internet Explorer 9, see http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9.

   The previous OfficeScan server version settings have been restored.

   Tip

   Administrators can confirm a successful rollback by checking the OfficeScan version number on the **About** screen (**Help** > **About**).

10. Optionally register the OfficeScan server to the Control Manager server using the web console.

11. Optionally register the OfficeScan server to the Deep Discovery Advisor server using the web console.

Note

Deep Discovery Advisor integration with the OfficeScan server began in OfficeScan 10.6 Service Pack 2.

12. After confirming that OfficeScan rolled back successfully, delete all files in the `<Server_installation_folder>\<Restore_folder_version>\` directory.

Manually Rolling Back to Previous OfficeScan Versions

After encountering problems upgrading OfficeScan agents, it is possible roll back the agents to their previous version.

Note

Perform a manual rollback if you did not back up the server information during installation. If you did back up the server information during the server installation, perform the rollback procedure outlined in *Rolling Back the OfficeScan Server and OfficeScan Agents Using the Server Backup Package on page 5-9*.

To roll back successfully, prepare the following:

- The OfficeScan server to manage the rolled-back agents. The server version should be any of the following:
  - 10.6 (including all Service Packs)
  - 10.5 Patch 1
  - 10.5
  - 10.0 Service Pack 1
  - 10.0
  - 8.0 Service Pack 1

- The endpoint to act as update source. This update source contains the rollback files and components. When the agent to be rolled back updates from this source, the OfficeScan agent is uninstalled and then the previous version of the agent is installed.
- The OfficeScan 11.0 server managing the agents to be rolled back
- The OfficeScan 11.0 agents to be rolled back

Part 1: Preparing the Previous OfficeScan Server Version

Procedure

1. Prepare a server with the previous OfficeScan server version installed.
2. Apply the latest hot fixes, patches, or service packs for the previous OfficeScan server version.
3. Replicate the following OfficeScan 11.0 server settings to the previous OfficeScan server version.

    a. Agent settings

    Scan

    Update Agents

    Privileges

    Spyware/Grayware Approved List (for OfficeScan 8.0 SP1 or later)

    Behavior Monitoring Exception List (for OfficeScan 10.0 SP1 or later)

    b. Global OfficeScan agent settings

    c. Web Reputation settings (for OfficeScan 8.0 SP1 or later)

    Endpoint location

    Policies

    Proxy

d. OfficeScan firewall settings

   Policy

   Profiles

e. Connection verification schedule

f. Web Reputation settings (for OfficeScan 8.0 SP1 or later)

   Server scheduled update

   Server update source

   Agent scheduled update

   Agent update source

g. Log maintenance settings

h. Notifications - all notification settings

i. Administration settings

   Quarantine Manager

   Control Manager

   Database backup

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

   Settings on the OfficeScan agent installation package for x86 endpoints:

   - Package type: Setup
   - Windows operating system type: 32-bit
   - Output file: `InstNTPkg.exe`

   Settings on the OfficeScan agent installation package for x64 endpoints:

   - Package type: Setup

- Windows operating system type: 64-bit
- Output file: InstNTPkg.exe

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

Part 2: Preparing an Update Source for Agents to Roll Back

Procedure

1. Prepare the endpoint to act as update source.
2. On the OfficeScan 11.0 server computer, go to <Server Installation Folder>\PCCSRV and copy the Download folder (including subfolders) to the update source endpoint (the endpoint prepared in the previous step).

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

   C:\OfficeScanUpdateSource
3. On the OfficeScan 11.0 server computer:

   a. Create a temporary folder.

   b. Navigate to <Server Installation Folder>\PCCSRV\Admin and copy the following files to the temporary folder:

   RollbackAgent.dll

   RollbackAgent_64x.dll

   ClientRollback.exe

   c. In the temporary folder, compress RollbackAgent.dll as RollbackAgent.zip.

   d. In the temporary folder, compress RollbackAgent_64x.dll as RollbackAgent_64x.zip.

e. Create a subfolder in the temporary folder and name it `RollBackNTPkg`.

f. Copy the following files to the `RollBackNTPkg` subfolder:

   `ClientRollback.exe`

   The OfficeScan agent installation package for x86 endpoints (`InstPkg.exe`) created in Part 1, step 4

g. Compress the `RollbackNTPkg` subfolder as `RollbackNTPkg.zip`.

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

i. Copy the following files to the `RollBackNTPkgx64` subfolder:

   `ClientRollback.exe`

   The agent installation package for x64 endpoints (`InstPkg.exe`) created in Part 1, step 4

j. Compress the `RollbackNTPkgx64` subfolder as `RollbackNTPkgx64.zip`.

k. Copy the following compressed files from the temporary folder to the update source endpoint:

   `RollbackAgent.zip`

   `RollbackAgent_64x.zip`

   `RollbackNTPkg.zip`

   `RollbackNTPkgx64.zip`

Note

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

4. On the update source endpoint:

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

```
RollbackAgent.zip

RollbackAgent_64x.zip

RollbackNTPkg.zip

RollbackNTPkgx64.zip
```

Tip

To check the access permission, right-click each file and select Properties. In the Security tab, the permission for Internet Guest Account should be "Read".

5. In the `\Download\Product` folder, open the `server.ini` file using a text editor such as Notepad.

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

WARNING!

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

```
[All_Product]

MaxProductID=109

Product.109=OfficeScan Rollback, 3.5, <Current OfficeScan
version>

[Info_109_35000_1_5633]

Version=<Previous OfficeScan version>

Update_Path=product/RollbackAgent_64x.zip, <RollbackAgent64
file size>

Path=product/RollBackNTPkgx64.zip, <RollBackNTPkg64 file
size>
```

Where:

`<RollbackAgent file size>: File size of "RollbackAgent.zip" in bytes. For example, 90517.`

`<RollBackNTPkg file size>: File size of "RollbackNTPkg.zip" in bytes. For example, 32058256.`

`<RollbackAgent64 file size>: File size of "RollbackAgent_64x.zip" in bytes. For example, 90517.`

`<RollBackNTPkg64 file size>: File size of RollbackNTpkgx64.zip in bytes. For example, 36930773.`

Tip

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

`<Current OfficeScan version>: Current OfficeScan version (11.0)`

`<Previous OfficeScan version>: Previous OfficeScan version. For example, 10.0.`

Part 3: Rolling Back the OfficeScan Agent

Procedure

1. On the OfficeScan 11.0 web console go to **Updates** > **Agents** > **Update Source**:

   a. Select **Customized Update Source**.

   b. On the **Customized Update Source List**, click **Add**. A new screen opens.

   c. Type the IP addresses of the agents to be rolled back.

   d. Type the update source URL. For example, type:

```
http://<IP address of update source>/
OfficeScanUpdateSource/
```

e. Click **Save**.

The screen closes.

f. Click **Notify All Agents**.

When agents to be rolled back update from the update source, the OfficeScan agent is uninstalled and the previous client version is installed.

2. After the previous client version is installed, inform the user to restart the endpoint. After the restart, the OfficeScan agent reports to the OfficeScan server prepared in Part 1.

Chapter 6

Getting Help

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

Topics in this chapter:

OfficeScan Troubleshooting Resources

Use the following resources to troubleshoot possible issues with this version of OfficeScan:

- Support Intelligence System
- Case Diagnostic Tool
- Trend Micro Performance Tuning Tool
- Installation Logs
- Server Debug Logs
- Agent Debug Logs

Support Intelligence System

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

Case Diagnostic Tool

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

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

Trend Micro Performance Tuning Tool

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

Note

The Trend Micro Performance Tuning Tool only supports 32-bit platforms.

Identifying System-intensive Applications

Procedure

1. Download Trend Micro Performance Tuning Tool from:

   http://solutionfile.trendmicro.com/solutionfile/1054312/EN/TMPerfTool_2_90_1131.zip

2. Unzip `TMPerfTool.zip` to extract `TMPerfTool.exe`.

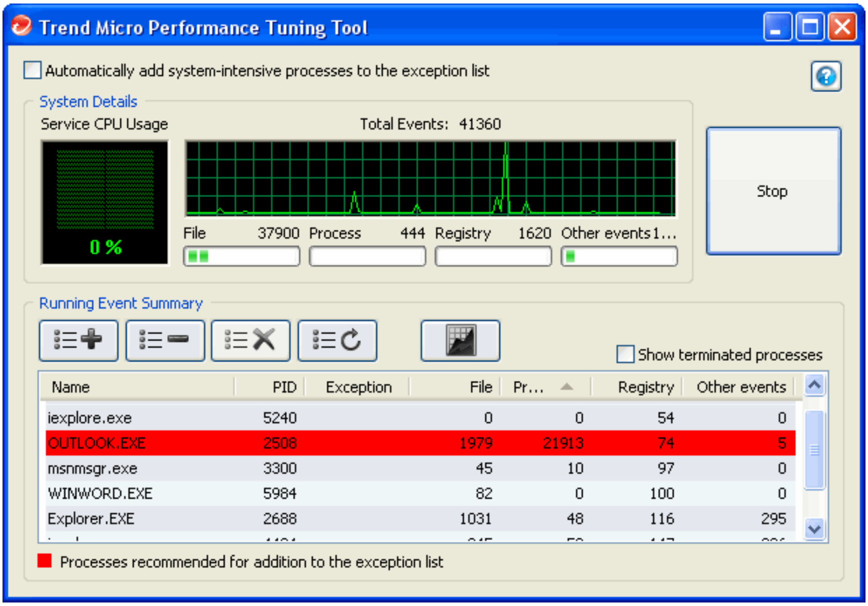
3. Place `TMPerfTool.exe` in the `<Client installation folder>` or in the same folder as `TMBMCLI.dll`.

4. Right-click `TMPerfTool.exe` and select **Run as administrator**.

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

6. Click **Analyze**. The tool starts to monitor CPU usage and event loading.

A system-intensive process is highlighted in red.



Trend Micro Performance Tuning Tool

☐ Automatically add system-intensive processes to the exception list

System Details

Service CPU Usage 0 %

Total Events: 41360

File 37900 Process 444 Registry 1620 Other events 1...

Stop

Running Event Summary

☐ Show terminated processes

Name	PID	Exception	File	Pr...	Registry	Other events
iexplore.exe	5240		0	0	54	0
OUTLOOK.EXE	2508		1979	21913	74	5
msnmsgr.exe	3300		45	10	97	0
WINWORD.EXE	5984		82	0	100	0
Explorer.EXE	2688		1031	48	116	295

🟥 Processes recommended for addition to the exception list

Figure 6-1. System-intensive process highlighted

7. Select a system-intensive process and click the **Add to the exception list (allow)** button (☰+).

8. Check if the system or application performance improves.

9. If the performance improves, select the process again and click the **Remove from the exception list** button (☰−).

10. If the performance drops again, perform the following steps:

    a. Note the name of the application.

    b. Click **Stop**.

    c. Click the **Generate report** button (📈) and then save the .xml file.

d. Review the applications that have been identified as conflicting and add them to the Behavior Monitoring exception list. For details, see the *Administrator's Guide*.

Installation Logs

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

TABLE 6-1. Installation Log Files

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

Server Debug Logs

Enable debug logging before performing the following server tasks:

- Uninstall and then install the server again.
- Perform a remote installation (Debug logging is enabled on the endpoint where you launched Setup and not on the remote endpoint.).

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.

Enabling Debug Logging on the OfficeScan Server computer

Option 1:

Procedure

1. Log on to the web console.
2. On the banner of the web console, click the "**O**" in "OfficeScan". This opens the **Debug Log Setting** screen.
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:

Procedure

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, or perform a remote installation).

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

Note

If the OfficeScan agent is present on the OfficeScan server, then the agent also outputs its debug logs in the server's debug logs.

Agent Debug Logs

Enable debug logging before installing the OfficeScan agent.

WARNING!

Debug logs may affect agent 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.

Enabling Debug Logging on the OfficeScan Agent

Procedure

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 agent users, instructing them to save the file to `C:\`. `LogServer.exe` automatically runs each time the agent endpoint starts. Instruct users NOT to close the `LogServer.exe` command window that opens when the endpoint 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 agent endpoint, check `ofcdebug.log` in `C:\`.

4. To disable debug logging for the OfficeScan agent, delete `ofcdebug.ini`.

Technical Support

This section describes how to find solutions online, use the Support Portal, and contact Trend Micro.

- *Troubleshooting Resources on page 6-8*
- *Contacting Trend Micro on page 6-10*
- *Sending Suspicious Content to Trend Micro on page 6-11*
- *Other Resources on page 6-12*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

http://community.trendmicro.com/

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Security Intelligence Community

Trend Micro cyber security experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtualization security, and data encryption.

Go to http://www.trendmicro.com/us/security-intelligence/index.html to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media

- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://www.trendmicro.com/vinfo to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports.

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Record the case number for tracking purposes.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1055473.aspx

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

http://trendedge.trendmicro.com/

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

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

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Appendix A

Sample Deployment

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

Basic Network

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

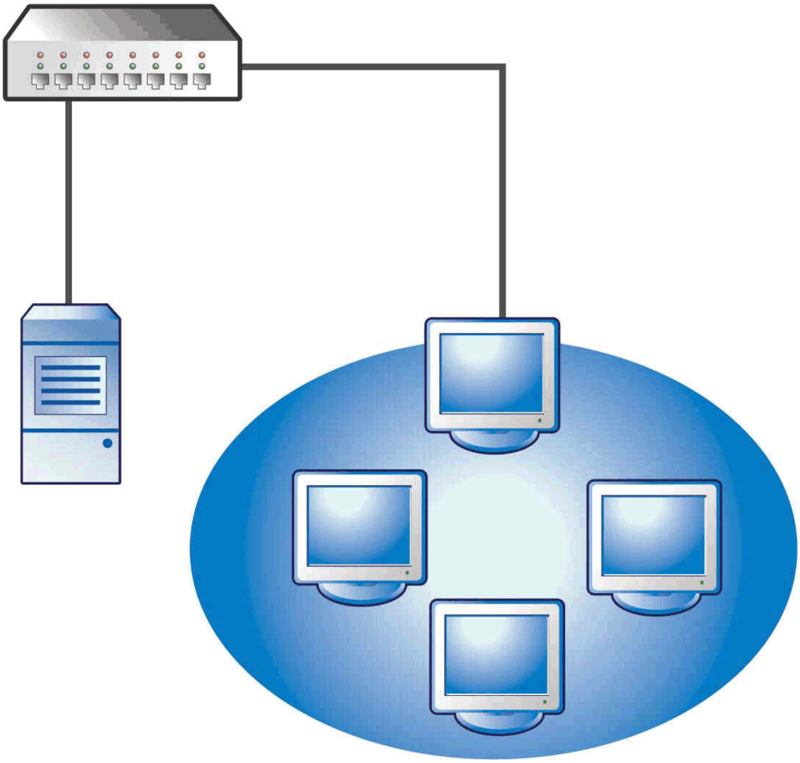


FIGURE A-1. Basic network topology

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 1 illustrates a multiple site network topology.

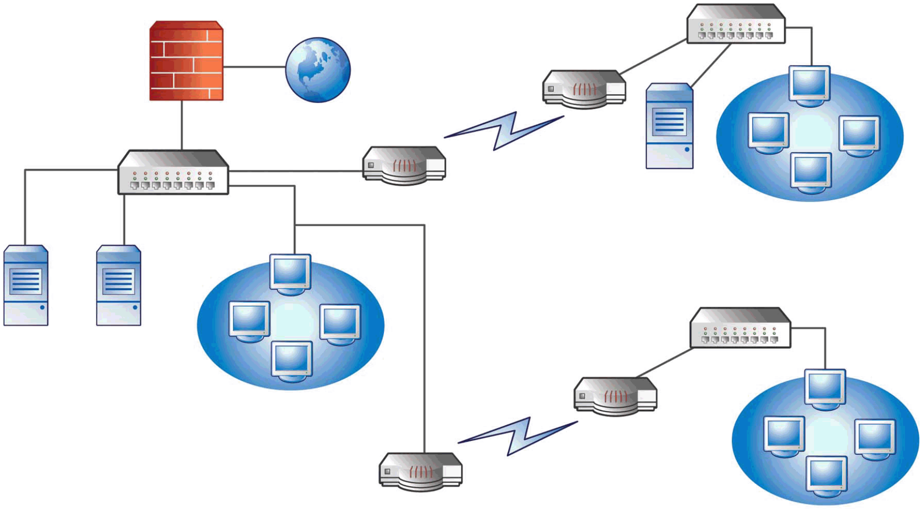


FIGURE A-2. Multiple site network topology

Network information:

- Remote Site 1 WAN link averages around 70 percent utilization during business hours. There are 35 agent endpoints on this site.
- Remote Site 2 WAN link averages around 40 percent utilization during business hours. There are 9 agent endpoints on this site.

- Server 3 only functions as a file and print server for the group at Remote Site 1. This endpoint is a possible candidate for installing the OfficeScan server, but may not be worth the extra management overhead. All servers run Windows Server 2003. The network uses Active Directory, but mainly for network authentication.
- All agent endpoints in Head Office, Remote Site 1, and Remote Site 2 run Windows Server 2003 or Windows XP.

Preparing a Multiple Site Network

Procedure

1. Identify the endpoint on which to 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 agent installation methods and eliminate methods that do not fit the requirement. See the *Administrator's Guide* for more information on the agent 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 endpoint, this option is not viable.

   - Remote installation from the web console

     This method is valid for all the LAN-connected endpoints at the head office. Because these endpoints all run Windows Server 2003, it is simple to deploy the package to the endpoints.

     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. 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 endpoints, OfficeScan deployment to these endpoints is not successful.

- OfficeScan Agent package deployment

  OfficeScan Agent 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 endpoints.

Head Office Deployment

The easiest agent 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 the agent package in Microsoft Installer Package (MSI) format and the deployment of the agent 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, agent package deployment has minimal bandwidth impact.

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

Minimizing the Impact of Component Updates Across the WAN

Procedure

1. Designate one agent to act as an Update Agent on Remote Site 1.

a. Log on to the web console and navigate to **Agents** > **Agent Management**.

b. In the agent tree, select the agent to act as the Update Agent and click **Settings** > **Update Agent Settings**.

2. Select the agents in Remote Site 1 that update components from the Update Agent.

a. Navigate to **Updates** > **Server** > **Update Source**.

b. Select **Customized Update Source** and click **Add**.

c. In the screen that displays, type the IP address range of the endpoints 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 when approximately 154 Kbits of bandwidth is available.

The best way to install the OfficeScan agent is to use the same agent 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 allows administrators to configure or create shared directories on remote endpoints without having physical access to them. After creating the shared directory on a single endpoint, copying the agent package to the directory requires less overhead than installing the agent to nine endpoints.

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, designate one agent to act as an Update Agent. See *Remote Site 1 Deployment on page A-5* for more information.

Index

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651   Fax:+1(408)257-2003   info@trendmicro.com

www.trendmicro.com

Item Code: OSEM116301/140127