TREND MICRO

10.6 OfficeScan™ SP3

Administrator's 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 products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

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

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

Copyright © 2013. Trend Micro Incorporated. All rights reserved.

Document Part No. OSEM105883_130313

Release Date: July 2013

Document Version No.: 1.0

Product Name and Version No.: OfficeScan™ 10.6 Service Pack 3

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

The user documentation for Trend Micro OfficeScan 10.6 Service Pack 3 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Table of Contents

Preface

Preface ix
OfficeScan Documentation x
Audience x
Document Conventions xi
Terminology xii

Part I: Introduction and Getting Started

Chapter 1: Introducing OfficeScan

About OfficeScan 1-2
New in this Release 1-2
Key Features and Benefits 1-14
The OfficeScan Server 1-17
The OfficeScan Client 1-18
Integration with Trend Micro Products and Services 1-19

Chapter 2: Getting Started with OfficeScan

The Web Console 2-2
The Summary Dashboard 2-5
The Server Migration Tool 2-30
Active Directory Integration 2-32
The OfficeScan Client Tree 2-35
OfficeScan Domains 2-48

Chapter 3: Getting Started with Data Protection

Data Protection Installation 3-2
Data Protection License 3-4
Deployment of Data Protection to Clients 3-5
Forensic Folder and DLP Database 3-8
Uninstalling Data Protection 3-14

Part II: Protecting Networked Computers

Chapter 4: Using Trend Micro Smart Protection

About Trend Micro Smart Protection 4-2
Smart Protection Services 4-3
Smart Protection Sources 4-5
Smart Protection Pattern Files 4-7
Setting Up Smart Protection Services 4-12
Using Smart Protection Services 4-30

Chapter 5: Installing the OfficeScan Client

OfficeScan Client Fresh Installations 5-2
Installation Considerations 5-2
Deployment Considerations 5-10
Migrating to the OfficeScan Client 5-61
Post-installation 5-65
OfficeScan Client Uninstallation 5-68

Chapter 6: Keeping Protection Up-to-Date

OfficeScan Components and Programs 6-2
Update Overview 6-11

OfficeScan Server Updates 6-14
Integrated Smart Protection Server Updates 6-26
OfficeScan Client Updates 6-26
Update Agents 6-50
Component Update Summary 6-59

Chapter 7: Scanning for Security Risks

About Security Risks 7-2
Scan Methods 7-7
Scan Types 7-13
Settings Common to All Scan Types 7-26
Scan Privileges and Other Settings 7-49
Global Scan Settings 7-64
Security Risk Notifications 7-74
Security Risk Logs 7-83
Security Risk Outbreaks 7-94

Chapter 8: Using Behavior Monitoring

Behavior Monitoring 8-2
Configuring Global Behavior Monitoring Settings 8-7
Behavior Monitoring Privileges 8-10
Behavior Monitoring Notifications for OfficeScan Client Users 8-11
Behavior Monitoring Logs 8-12

Chapter 9: Using Device Control

Device Control 9-2
Permissions for Storage Devices 9-3
Permissions for Non-storage Devices 9-10
Modifying Device Control Notifications 9-16

Device Control Logs 9-17

Chapter 10: Using Data Loss Prevention

About Data Loss Prevention 10-2
Data Loss Prevention Policies 10-3
Data Identifier Types 10-4
Data Loss Prevention Templates 10-18
DLP Channels 10-23
Data Loss Prevention Actions 10-34
Data Loss Prevention Exceptions 10-35
Data Loss Prevention Policy Configuration 10-40
Data Loss Prevention Notifications 10-45
Data Loss Prevention Logs 10-49

Chapter 11: Protecting Computers from Web-based Threats

About Web Threats 11-2
Command & Control Contact Alert Services 11-2
Web Reputation 11-4
Web Reputation Policies 11-5
Configuring Global C&C Callback Settings 11-11
Web Threat Notifications for Client Users 11-11
Configuring C&C Callback Notifications for Administrators 11-13
C&C Contact Alert Notifications for Client Users 11-16
Web Reputation Logs 11-18

Chapter 12: Using the OfficeScan Firewall

About the OfficeScan Firewall 12-2
Enabling or Disabling the OfficeScan Firewall 12-6

Firewall Policies and Profiles 12-7
Firewall Privileges 12-22
Global Firewall Settings 12-24
Firewall Violation Notifications for OfficeScan Client Users 12-26
Firewall Logs 12-27
Firewall Violation Outbreaks 12-29
Testing the OfficeScan Firewall 12-30

Part III: Managing the OfficeScan Server and Clients

Chapter 13: Managing the OfficeScan Server

Role-based Administration 13-2
Trend Micro Control Manager 13-21
Reference Servers 13-27
Administrator Notification Settings 13-29
System Event Logs 13-32
Log Management 13-33
Licenses 13-36
OfficeScan Database Backup 13-39
OfficeScan Web Server Information 13-41
Web Console Password 13-42
Web Console Settings 13-42
Quarantine Manager 13-43
Server Tuner 13-44
Smart Feedback 13-47

Chapter 14: Managing the OfficeScan Client

Computer Location 14-2
OfficeScan Client Program Management 14-6
Client-Server Connection 14-24
OfficeScan Client Proxy Settings 14-46
Viewing OfficeScan Client Information 14-50
Importing and Exporting Client Settings 14-51
Security Compliance 14-52
Trend Micro Virtual Desktop Support 14-70
Global Client Settings 14-83
Configuring Client Privileges and Other Settings 14-84

Part IV: Providing Additional Protection

Chapter 15: Using Plug-In Manager

About Plug-In Manager 15-2
Plug-In Manager Installation 15-3
Native OfficeScan Feature Management 15-4
Managing Plug-in Programs 15-4
Uninstalling Plug-In Manager 15-9
Troubleshooting Plug-In Manager 15-9

Chapter 16: Using Policy Server for Cisco NAC

About Policy Server for Cisco NAC 16-2
Components and Terms 16-2
Cisco NAC Architecture 16-6
The Client Validation Sequence 16-7

The Policy Server 16-9

Policy Server System Requirements 16-19

Cisco Trust Agent (CTA) Requirements 16-21

Supported Platforms and Requirements 16-21

Policy Server for NAC Deployment 16-23

Chapter 17: Configuring OfficeScan with Third-party Software

Overview of Check Point Architecture and Configuration 17-2

Configuring the Secure Configuration Verification File for OfficeScan 17-4

SecureClient Support Installation 17-5

Chapter 18: Getting Help

Troubleshooting Resources 18-2

Contacting Technical Support 18-24

Appendix A: IPv6 Support in OfficeScan

IPv6 Support for OfficeScan Server and Clients A-2
- OfficeScan Server Requirements A-2
- OfficeScan Client Requirements A-2
- Pure IPv6 Server Limitations A-3
- Pure IPv6 OfficeScan Client Limitations A-4

Configuring IPv6 Addresses A-6

Screens That Display IP Addresses A-7

Appendix B: Windows Server Core 2008/2012 Support

Windows Server Core 2008/2012 Support B-2

Installation Methods for Windows Server Core B-2
- Installing the OfficeScan Client Using Login Script Setup B-3

Installing the OfficeScan Client Using an OfficeScan Client Package B-4

OfficeScan Client Features on Windows Server Core B-6

Windows Server Core Commands B-7

Appendix C: Windows 8 and Windows Server 2012 Support

About Windows 8 and Windows Server 2012 ..... C-2
OfficeScan in Windows UI Mode C-2
Enabling Toast Notifications C-3

Internet Explorer 10 ..... C-4
OfficeScan Feature Support in Internet Explorer 10 ..... C-5

Appendix D: OfficeScan Rollback

Rolling Back the OfficeScan Server and OfficeScan Clients D-2
Rolling Back the OfficeScan Clients D-2
Rolling Back the OfficeScan Server D-4

Appendix E: Glossary

Index

Index IN-1

Preface

Preface

Welcome to the Trend Micro™ OfficeScan™ *Administrator's Guide*. This document discusses getting started information, client installation procedures, and OfficeScan server and client management.

Topics in this chapter:

- *OfficeScan Documentation on page x*
- *Audience on page x*
- *Document Conventions on page xi*
- *Terminology on page xii*

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, and upgrading the server and clients
Administrator's Guide	A PDF document that discusses getting started information, client installation procedures, and OfficeScan server and client management
Help	HTML files compiled in WebHelp or CHM format that provide "how to's", usage advice, and field-specific information. The Help is accessible from the OfficeScan server, client, and Policy Server consoles, and from the OfficeScan Master Setup.
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following 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 OfficeScan server and OfficeScan client installation and management. These users are expected to have advanced networking and server management knowledge.

- **Cisco NAC administrators**: Responsible for designing and maintaining security systems with Cisco NAC servers and Cisco networking equipment. They are assumed to have experience with this equipment.
- **End users**: Users who have the OfficeScan client installed on their computers. The computer skill level of these individuals ranges from beginner to power user.

Document Conventions

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

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation or new technology components
Networked Computers > **Client Management**	A "breadcrumb" found at the start of procedures that helps users navigate to the relevant web console screen. Multiple breadcrumbs means that there are several ways to get to the same screen.
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, `C:\Program Files\<file_name>` can be `C:\Program Files\sample.jpg`.
Note	Provides configuration notes or recommendations
Tip	Provides best practice information and Trend Micro recommendations

Convention	Description
WARNING!	Provides warnings about activities that may harm computers on your network

Terminology

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

Table 3. OfficeScan Terminology

Terminology	Description
OfficeScan client	The OfficeScan client program
Client computer	The computer where the OfficeScan client is installed
Client user (or user)	The person managing the OfficeScan client on the client computer
Server	The OfficeScan server program
Server computer	The computer where the OfficeScan server is installed
Administrator (or OfficeScan administrator)	The person managing the OfficeScan server
Console	The user interface for configuring and managing OfficeScan server and client settings The console for the OfficeScan server program is called "web console", while the console for the OfficeScan client program is called "client console".
Security risk	The collective term for virus/malware, spyware/grayware, and web threats
License service	Includes Antivirus, Damage Cleanup Services, and Web Reputation and Anti-spyware—all of which are activated during OfficeScan server installation

Terminology	Description
OfficeScan service	Services hosted through Microsoft Management Console (MMC). For example, `ofcservice.exe`, the OfficeScan Master Service.
Program	Includes the OfficeScan client, Cisco Trust Agent, and Plug-In Manager
Components	Responsible for scanning, detecting, and taking actions against security risks

`Client installation folder`	The folder on the computer that contains the OfficeScan client files. If you accept the default settings during installation, you will find the installation folder at any of the following locations:
	`C:\Program Files\Trend Micro\OfficeScan Client`
	`C:\Program Files\Trend Micro (x86)\OfficeScan Client`

`Server installation folder`	The folder on the computer that contains the OfficeScan server files. If you accept the default settings during installation, you will find the installation folder at any of the following locations:
	`C:\Program Files\Trend Micro\OfficeScan`
	`C:\Program Files\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 client	An OfficeScan client that has been configured to use smart scan
Conventional scan client	An OfficeScan client that has been configured to use conventional scan

Terminology	Description
Dual-stack	An entity that has both IPv4 and IPv6 addresses. For example: • A dual-stack endpoint is a computer with both IPv4 and IPv6 addresses. • A dual-stack client refers to a client installed on a dual-stack endpoint. • A dual-stack Update Agent distributes updates to clients. • A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses.
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address
Plug-in solutions	Native OfficeScan features and plug-in programs delivered through Plug-In Manager

Part I

Introduction and Getting Started

Chapter 1

Introducing OfficeScan

This chapter introduces Trend Micro™ OfficeScan™ and provides an overview of its features and capabilities.

Topics in this chapter:

- *About OfficeScan on page 1-2*
- *New in this Release on page 1-2*
- *Key Features and Benefits on page 1-14*
- *The OfficeScan Server on page 1-17*
- *The OfficeScan Client on page 1-18*
- *Integration with Trend Micro Products and Services on page 1-19*

About OfficeScan

Trend Micro™ OfficeScan™ protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of the OfficeScan client program that resides at the endpoint and a server program that manages all clients. The OfficeScan client guards the computer and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every client.

OfficeScan is powered by the Trend Micro Smart Protection Network™, a next generation cloud-client infrastructure that delivers security that is smarter than conventional approaches. Unique in-the-cloud technology and a lighter-weight client reduce reliance on conventional pattern downloads and eliminate the delays commonly associated with desktop updates. Businesses benefit from increased network bandwidth, reduced processing power, and associated cost savings. Users get immediate access to the latest protection wherever they connect—within the company network, from home, or on the go.

New in this Release

Trend Micro OfficeScan includes the following new features and enhancements.

Data Protection Enhancements

The Data Protection enhancements in the release include the following features.

TABLE 1-1. Data Protection Enhancements

FEATURE	DESCRIPTION
Forensic data quarantine	OfficeScan clients create and upload encrypted forensic data files to the server allowing companies to track and record the specific Data Loss Prevention incidents that occur on the network. OfficeScan generates a hash value for each forensic file for verification and integrity purposes. Through integration with Control Manager, security officers can view the exact digital asset that caused each incident and take appropriate measures. For details, see *Forensic Folder and DLP Database on page 3-8*.
Multi-rule DLP policies	Administrators can create multiple rules for a single policy. Each rule can contain multiple templates and administrators can assign specific actions depending on the type of digital asset identified or the channel through which the transmission occurred. Global exceptions apply to all rules in a given policy, avoiding the need to copy settings. For details, see *Data Loss Prevention Policies on page 10-3*.
Enhanced DLP log details	Logs display more detailed records about each Data Loss Prevention incident. Details not only include the rules that triggered the incident, but also the exact template that identified the digital asset. For details, see *Data Loss Prevention Logs on page 10-49*.
Extended non-storage device support	Device Control can now monitor Bluetooth adaptors and Wireless NICs. For details, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/officescan.aspx.

FEATURE	DESCRIPTION
Extended DLP channel support	Data Loss Prevention can now monitor the following: • 126.com Webmail • 139 Webmail • 163.com Webmail • Tencent QQ (files sent using instant messaging) • Tencent QQ Webmail • SINA Webmail • Sohu Webmail For details, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/officescan.aspx.

Command & Control Contact Alert Services

This version of OfficeScan provides administrators with heightened detection capabilities for Command & Control servers.

TABLE 1-2. C&C Contact Services

FEATURE	DESCRIPTION
Global Intelligence and Virtual Analyzer C&C server lists	OfficeScan can automatically detect any known C&C server through use of the Trend Micro Smart Protection Network Global Intelligence list. Web Reputation Services checks all URLs against both the traditional malicious list, and the new Global Intelligence C&C server list. Administrators that have integrated a Smart Protection Server with Deep Discovery Advisor can also check the risk level of suspicious network connections using the Virtual Analyzer C&C server list. The Virtual Analyzer generates this list based on data received from connected Trend Micro products ensuring very company-specific protection. For details, see *Command & Control Contact Alert Services on page 11-2*.

Feature	Description
C&C IP list	The C&C IP list works in conjunction with the Network Content Inspection Engine (NCIE) to detect network connections with known C&C servers. NCIE detects C&C server contact through any network channel. For details, see *Command & Control Contact Alert Services on page 11-2*.
Notifications for administrators and users	OfficeScan C&C Contact Alert Services provides standard and outbreak notifications that keep administrators and users informed about any known or potential advanced persistent threat or C&C callbacks originating from the network.
C&C Callback Events widget	The **C&C Callback Events** widget provides administrators with a quick view of all callbacks from the network, the targets of the attacks, the risk level of the attack, and the callback address. For details, see *C&C Callback Events Widget on page 2-24*.

Scan Enhancements

This OfficeScan version also provides the following scan enhancements.

Table 1-3. Scan Enhancements

Scan Type	Description
Behavior Monitoring	Behavior Monitoring works in conjunction with Web Reputation Services to verify the prevalence of files downloaded through HTTP channels or email applications. After detecting a "newly encountered" file, administrators can choose to prompt users before executing the file. Trend Micro classifies a program as newly encountered based on the number of file detections or historical age of the file as determined by the Smart Protection Network. For details, see *Configuring Global Behavior Monitoring Settings on page 8-7*.

Scan Type	Description
Virus Scan Performance	The OfficeScan Virus Scan Engine (VSAPI 9.713 or later) has been updated with a deferred scanning feature to improve file copying performance. For details, see *Enable Deferred Scanning on File Operations on page 7-67*.

Web Reputation Pattern Enhancement

This version of OfficeScan enhances the integrated Smart Protection Server's Web Reputation Pattern. The Web Reputation Pattern has been redesigned to provide the following benefits:

- Reduced memory consumption
- Incremental pattern updates, which greatly reduce bandwidth consumption

Rollback Enhancements

The version of OfficeScan simplifies the procedure required to rollback the OfficeScan server and clients. During OfficeScan installation, administrators can choose to back up the server files which can then be used to roll back the server and clients to the previously installed version.

For detailed rollback instructions, refer to *OfficeScan Rollback on page D-1*.

New in Version 10.6 SP2

Trend Micro OfficeScan SP2 included the following new features and enhancements.

Platform and Browser Support

This version of OfficeScan provides support for client installations on Windows 8™ and Windows Server™ 2012 / Server Core 2012.

This version of OfficeScan also provides support for server installations on Windows Server™ 2012.

This version of OfficeScan provides support for Internet Explorer™ 10.

Note

Clients operating using the Windows UI mode receive limited support. For details, see *Windows 8 and Windows Server 2012 Support on page C-1*.

Detection and Performance Enhancement

This version of OfficeScan provides the following detection and performance enhancement.

TABLE 1-4. Detection and Performance Enhancement

ENHANCEMENT	DESCRIPTION
MSI installation	Real-time scanning now verifies the file signature of an MSI installation package before proceeding with an installation. Once OfficeScan receives verification that the file signature is trusted, real-time scan allows the installation to proceed without further file scanning.

VDI Enhancement

This version of OfficeScan enhances the smart scan update feature for virtual environments. When a large number of smart scan clients request a pattern update, the server now places the client requests in a queue until the server can send a response. As each client completes the update, the server prompts the next client in the queue to begin updating.

Data Loss Prevention Enhancements

This version of OfficeScan enhances the Data Loss Prevention feature to provide:

- Windows 8, Windows Server 2012, Windows Server Core 2012 support

  - Windows Store App support on the Windows UI and desktop application support
  - HTTPS support using Internet Explorer 10
- HTTPS support using Chrome™ versions 19, 20, 21, and 22
- Updated Gmail support
- Microsoft Office™ 2013 support

New in Version 10.6 SP1

Trend Micro OfficeScan SP1 included the following new features and enhancements.

Policy Management from Control Manager

Control Manager 6.0 allows administrators to create and deploy policies to OfficeScan servers that Control Manager manages. For details, see the Control Manager Administrator's Guide.

Behavior Monitoring 64-bit Support

The Behavior Monitoring capabilities of OfficeScan now support 64-bit versions of the following platforms:

- Windows Server 2008™
- Windows 7™
- Windows Vista™ with SP1 (or later)

Client Self-protection 64-bit Support

Client Self-protection now supports 64-bit versions of the following platforms:

- Windows Server 2008™
- Windows 7™

- Windows Vista™ with SP1 (or later)

Device Control 64-bit Support for Unauthorized Change Prevention

The Device Control capabilities of OfficeScan now support 64-bit versions of the following platforms during Unauthorized Change Prevention monitoring:

- Windows 2008™
- Windows 7™
- Windows Vista™ with SP1 (or later)

Note

Device Control for Data Protection provides support for all 64-bit versions of Windows platforms. For details about configuring 64-bit permissions, see *Permissions for Storage Devices on page 9-3*.

Data Protection Enhancements

The Data Protection enhancements in OfficeScan 10.6 SP1 include the following support and upgrades:

- Data Loss Prevention and Device Control support for 64-bit versions of Windows platforms
- Over 100 new pre-configured Data Loss Prevention templates and data identifiers

Virtual Desktop Infrastructure Enhancements

This version of OfficeScan enhances Virtual Desktop Infrastructure (VDI) support and capabilities.

- **Microsoft Hyper-V™ Support**: Administrators can now manage virtual clients using the Microsoft Hyper-V™ Server in addition to VMware vCenter™ server and the Citrix XenServer™.

- **Non-persistent Environment Enhancement**: OfficeScan now identifies virtual clients by Media Access Control (MAC) address. This prevents OfficeScan from assigning multiple globally unique identifiers (GUIDs) to the same client in non-persistent environments.

For details, see *Trend Micro Virtual Desktop Support on page 14-70*.

Extended Web Reputation Port Scanning

OfficeScan can now scan HTTP traffic on all ports for web reputation policy violations. If administrators do not want to scan traffic on all ports, OfficeScan provides the option of scanning traffic on the default 80, 81, and 8080 HTTP ports.

For details, see *Configuring a Web Reputation Policy on page 11-5*.

New in Version 10.6

Trend Micro OfficeScan 10.6 included the following new features and enhancements.

- **Data Protection**

  The Data Protection module provides Data Loss Prevention and expands the range of devices monitored by Device Control.

  Plug-in Manager manages the installation and licensing of the Data Protection module. For more information, see *Data Protection Installation on page 3-2*.

TABLE 1-5. OfficeScan Data Protection Features

DATA PROTECTION FEATURES	DETAILS
Data Loss Prevention	Data Loss Prevention safeguards an organization's digital assets against accidental or deliberate leakage. Data Loss Prevention allows you to: • Identify the digital assets to protect • Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email and external devices • Enforce compliance to established privacy standards For more information, see *About Data Loss Prevention on page 10-2*.
Device Control	OfficeScan out-of-the-box has a Device Control feature that regulates access to USB storage devices, CD/DVD, floppy disks, and network drives. Device Control that is part of the Data Protection module expands the range of devices by regulating access to the following devices: • Imaging devices • Modems • Ports (COM and LPT) • Infrared devices • PCMCIA cards • Print screen key • IEEE 1394 interface For more information, see *Device Control on page 9-2*.

- **Plug-in Manager 2.0**

  Plug-in Manager 2.0 installs with the OfficeScan server. This Plug-in Manager version delivers widgets.

  Widgets provide a quick visual reference for the OfficeScan features and plug-in solutions that you deem most vital to your business. Widgets are available in the

OfficeScan server's Summary dashboard, which replaces the Summary screen in previous OfficeScan versions. For more information, see *The Summary Dashboard on page 2-5*.

- **IPv6 Support**

  The OfficeScan server and clients can now be installed on IPv6 computers.

  In addition, new versions of Control Manager and Smart Protection Server now support IPv6 to provide seamless integration with the OfficeScan server and clients.

  For more information, see *IPv6 Support for OfficeScan Server and Clients on page A-2*.

- **Cache Files for Scans**

  The OfficeScan client now builds cache files, which contain information about safe files that have been scanned previously and files that Trend Micro deems trustworthy. Cache files provide a quick reference during on-demand scans, thus reducing the usage of system resources. On-demand scans (Manual Scan, Scheduled Scan, and Scan Now) are now more efficient, providing up to 40% improvement to speed performance.

  For more information, see *Cache Settings for Scans on page 7-60*.

- **Startup Enhancement**

  When a computer starts, the OfficeScan client will postpone the loading of some client services if CPU usage is more than 20%. When CPU usage is below the limit, the client starts to load the services.

  Services include:

  - OfficeScan NT Firewall
  - OfficeScan Data Protection Service
  - Trend Micro Unauthorized Change Prevention Service

- **Damage Cleanup Services Enhancement**

  Damage Cleanup Services can now run in advanced cleanup mode to stop activities by rogue security software, also known as FakeAV. The client also uses advanced

cleanup rules to proactively detect and stop applications that exhibit FakeAV behavior.

You can choose the cleanup mode when you configure virus/malware scan actions for Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now. For more information, see *Damage Cleanup Services on page 7-40*.

- **Web Reputation HTTPS Support**

  Clients can now scan HTTPS traffic for web threats. You can configure this feature when you create a web reputation policy. For more information, see *Web Reputation Policies on page 11-5*.

  Important

  - HTTPS scanning only supports Windows 8 or Windows 2012 platforms operating in desktop mode.
  - After enabling HTTPS scanning for the first time on OfficeScan clients running Internet Explorer 9 or 10, users must enable the `TmIEPlugInBHO Class` add-on in the browser pop-up window before HTTPS scanning is operational.

- **Windows Server Core 2008 Support**

  The OfficeScan client can now be installed on Windows Server Core 2008. Users can use the command line interface to launch the client console and check the endpoint's protection status.

  For more information, see *Windows Server Core 2008/2012 Support on page B-2*.

- **Other Enhancements**

  This release includes the following enhancements:

  - Smart scan clients now run Outlook Mail Scan in smart scan mode. In previous versions, smart scan clients run Outlook Mail Scan in conventional scan mode.
  - Logs and notifications for spyware/grayware detections now show the user name logged on to the computer at the time of detection.

- In the spyware/grayware logs, if the second level scan result is "Passed", the first level scan result is now "Further action required" instead of "No action required". With this enhancement, you can now take additional measures such as cleaning spyware/grayware that you consider harmful.
- Client Self-protection is now a granular setting that you can configure in the client tree.
- You can now configure all clients to send heartbeat messages to the OfficeScan server. In the previous version, only clients in unreachable networks send heartbeat messages. For more information, see *Unreachable Clients on page 14-41*.
- When exporting client tree settings to a `.dat` file, all settings, will now be exported. In previous versions, only scan settings and client privileges/other settings are exported. For more information on exporting settings, see *Importing and Exporting Client Settings on page 14-51*.
- When using the Client Mover tool, you can now specify the client tree subdomain to which the client will be grouped after it moves to its new parent server. For more information, see *Client Mover on page 14-21*.

Key Features and Benefits

OfficeScan provides the following features and benefits:

- **Plug-In Manager and Plug-in Solutions**

  Plug-In Manager facilitates the installation, deployment, and management of plug-in solutions.

  Administrators can install two kinds of plug-in solutions:

  - Plug-in programs
  - Native OfficeScan features

- **Centralized Management**

  A web-based management console gives administrators transparent access to all clients and servers on the network. The web console coordinates automatic

deployment of security policies, pattern files, and software updates on every client and server. And with Outbreak Prevention Services, it shuts down infection vectors and rapidly deploys attack-specific security policies to prevent or contain outbreaks before pattern files are available. OfficeScan also performs real-time monitoring, provides event notification, and delivers comprehensive reporting. Administrators can perform remote administration, set customized policies for individual desktops or groups, and lock client security settings.

- **Security Risk Protection**

  OfficeScan protects computers from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak. To contain outbreaks, OfficeScan enforces outbreak prevention policies and isolates infected computers until they are completely risk-free.

  OfficeScan uses smart scan to make the scanning process more efficient. This technology works by off-loading a large number of signatures previously stored on the local computer to Smart Protection Sources. Using this approach, the system and network impact of the ever-increasing volume of signature updates to endpoint systems is significantly reduced.

  For information about smart scan and how to deploy it to clients, see *Scan Methods on page 7-7*.

- **Damage Cleanup Services**

  Damage Cleanup Services™ cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, viral files) through a fully-automated process. To address the threats and nuisances posed by Trojans, Damage Cleanup Services does the following:

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

  Because Damage Cleanup Services runs automatically in the background, it is not necessary to configure it. Users are not even aware when it runs. However,

OfficeScan may sometimes notify the user to restart their computer to complete the process of removing a Trojan.

- **Web Reputation**

  Web reputation technology proactively protects client computers within or outside the corporate network from malicious and potentially dangerous websites. Web reputation breaks the infection chain and prevents downloading of malicious code.

  Verify the credibility of websites and pages by integrating OfficeScan with the Smart Protection Server or the Trend Micro Smart Protection Network.

- **OfficeScan Firewall**

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

- **Data Loss Prevention**

  Data Loss Prevention safeguards an organization's digital assets against accidental or deliberate leakage. Data Loss Prevention allows administrators to:

  - Identify the digital assets to protect
  - Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email messages and external devices
  - Enforce compliance to established privacy standards

- **Device Control**

  Device Control regulates access to external storage devices and network resources connected to computers. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

- **Behavior Monitoring**

  Behavior Monitoring constantly monitors clients for unusual modifications to the operating system or on installed software.

- **Security and Policy Enforcement**

OfficeScan provides seamless integration of the Cisco™ Trust Agent, enabling the most effective policy enforcement within a Cisco Self-Defending Network. OfficeScan also includes a Policy Server for automated communication with Cisco Access Control Servers. When integrated with Trend Micro™ Network VirusWall™ or any Network Admission Control (NAC) device, OfficeScan can check clients trying to enter the network and then remedy, redirect, restrict, deny, or permit access. If a computer is vulnerable or becomes infected, OfficeScan can automatically isolate it and its network segments until all computers update or cleanup is complete.

The OfficeScan Server

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

The server performs two important functions:

- Installs, monitors, and manages OfficeScan clients
- Downloads most of the components needed by clients. The OfficeScan server downloads components from the Trend Micro ActiveUpdate server and then distributes them to clients.

Note

Some components are downloaded by smart protection sources. See *Smart Protection Sources on page 4-5* for details.

FIGURE 1-1. How the OfficeScan server works

The OfficeScan server is capable of providing real-time, bidirectional communication between the server and clients. Manage the clients from a browser-based web console, which administrators can access from virtually anywhere on the network. The server communicates with the client (and the client with the server) through Hypertext Transfer Protocol (HTTP).

The OfficeScan Client

Protect Windows computers from security risks by installing the OfficeScan client on each computer.

The OfficeScan client reports to the parent server from which it was installed. Configure clients to report to another server by using the Client Mover tool. The client sends events and status information to the server in real time. Examples of events are virus/

malware detection, client startup, client shutdown, start of a scan, and completion of an update.

Integration with Trend Micro Products and Services

OfficeScan integrates with the Trend Micro products and services listed in the following table. For seamless integration, ensure that the products run the required or recommended versions.

TABLE 1-6. Products and Services that Integrate with OfficeScan

PRODUCT/ SERVICE	DESCRIPTION	VERSION
ActiveUpdate server	Provides all the components that the OfficeScan client needs to protect clients from security threats	Not applicable
Smart Protection Network	Provides File Reputation Services and Web Reputation Services to clients. Smart Protection Network is hosted by Trend Micro.	Not applicable
Standalone Smart Protection Server	Provides the same File Reputation Services and Web Reputation Services offered by Smart Protection Network. A standalone Smart Protection Server is intended to localize the service to the corporate network to optimize efficiency. **Note** An integrated Smart Protection Server is installed with the OfficeScan server. It has the same functions as its standalone counterpart but has limited capacity.	• 2.5 (recommended) • 2.0

Product/ Service	Description	Version
Control Manager	A software management solution that provides the ability to control antivirus and content security programs from a central location—regardless of the platform or the physical location of the program.	• 6.0 (recommended) • 5.5 SP1 • 5.5 • 5.0
Deep Discovery Advisor	Deep Discovery provides network-wide monitoring powered by custom sandboxing and relevant real-time intelligence to enable early attack detection, enable rapid containment, and deliver custom security updates that immediately improve protection against further attack.	3.0 and later

Chapter 2

Getting Started with OfficeScan

This chapter describes how to get started with Trend Micro™ OfficeScan™ and initial configuration settings.

Topics in this chapter:

- *The Web Console on page 2-2*
- *The Summary Dashboard on page 2-5*
- *Active Directory Integration on page 2-32*
- *The OfficeScan Client Tree on page 2-35*
- *OfficeScan Domains on page 2-48*

The Web Console

The web console is the central point for monitoring throughout the corporate network. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console uses standard Internet technologies, such as Java, CGI, HTML, and HTTP.

Note

Configure the timeout settings from the web console. See *Web Console Settings on page 13-42*.

Use the web console to do the following:

- Manage clients installed on networked computers
- Group clients into logical domains for simultaneous configuration and management
- Set scan configurations and initiate manual scan on a single or multiple networked computers
- Configure notifications about security risks on the network and view logs sent by clients
- Configure outbreak criteria and notifications
- Delegate web console administration tasks to other OfficeScan administrators by configuring roles and user accounts
- Ensure that clients comply with security guidelines

Note

The web console does not support Windows 8 or Windows Server 2012 in Windows UI mode.

Requirements for Opening the Web Console

Open the web console from any computer on the network that has the following resources:

- 300MHz Intel™ Pentium™ processor or equivalent
- 128MB of RAM
- At least 30MB of available disk space
- Monitor that supports 1024 x 768 resolution at 256 colors or higher
- Microsoft Internet Explorer™ 7.0 or higher

On the web browser, type one of the following in the address bar based on the type of OfficeScan server installation:

TABLE 2-1. OfficeScan Web Console URLs

INSTALLATION TYPE	URL
Without SSL on a default site	`http://<OfficeScan server FQDN or IP address>/OfficeScan`
Without SSL on a virtual site	`http://<OfficeScan server FQDN or IP address>:<HTTP port number>/OfficeScan`
With SSL on a default site	`https://<OfficeScan server FQDN or IP address>/OfficeScan`
With SSL on a virtual site	`https://<OfficeScan server FQDN or IP address>/OfficeScan`

Note

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

Logon Account

During OfficeScan server installation, Setup creates a root account and prompts you to type the password for this account. When opening the web console for the first time, type "root" as the user name and the root account password. If you forget the password, contact your support provider for help in resetting the password.

Define user roles and set up user accounts to allow other users to access the web console without using the root account. When users log on to the console, they can use the user accounts you have set up for them. For more information, see *Role-based Administration on page 13-2*.

The Web Console Banner

The banner area of the web console provides you the following options:

FIGURE 2-1. Web console banner area

- **<account name>**: Click the account name (for example, root) to modify details for the account, such as the password.
- **Log Off**: Logs you off from the web console
- **Help** ( )
  - **What's New**: Opens a page with a list of new features included in the current product release
  - **Contents and Index**: Opens the OfficeScan Server Help
  - **Knowledge Base**: Opens the Trend Micro Knowledge Base, where you can view FAQs and updated product information, access customer support, and register OfficeScan
  - **Security Info**: Displays the Trend Micro Security Information page, where you can read about the latest security risks

- **Sales**: Displays the Trend Micro sales web page, where you can contact your regional sales representative
- **Support**: Displays the Trend Micro support web page, where you can submit questions and find answers to common questions about Trend Micro products
- **About**: Provides an overview of the product, instructions to check component version details, and a link to the Support Intelligence System. For details, see *Support Intelligence System on page 18-2*.

The Summary Dashboard

The **Summary** dashboard appears when you open the OfficeScan web console or click **Summary** in the main menu.

Each web console user account has a completely independent dashboard. Any changes to a user account's dashboard will not affect the dashboards of the other user accounts.

If a dashboard contains OfficeScan client data, the data that displays depends on the client domain permissions for the user account. For example, if you grant a user account permissions to manage domains A and B, the user account's dashboard will only show data from clients belonging to domains A and B.

For details about user accounts, see *Role-based Administration on page 13-2*.

The **Summary** dashboard contains the following:

- Product License Status section
- Widgets
- Tabs

Product License Status Section

This section is found on top of the dashboard and shows the status of the OfficeScan licenses.

FIGURE 2-2. Product License Status section

Reminders about the license status display during the following instances:

- If you have a full version license:
  - 60 days before a license expires
  - During the product's grace period. The duration of the grace period varies by region. Please verify the grace period with your Trend Micro representative.
  - When the license expires and grace period elapses. During this time, you will not be able to obtain technical support or perform component updates. The scan engines will still scan computers using out-of-date components. These out-of-date components may not be able to protect you completely from the latest security risks.
- If you have an evaluation version license:
  - 14 days before a license expires
  - When the license expires. During this time, OfficeScan disables component updates, scanning, and all client features.

If you have obtained an Activation Code, renew a license by going to **Administration** > **Product License**.

Tabs and Widgets

Widgets are the core components of the dashboard. Widgets provide specific information about various security-related events. Some widgets allow you to perform certain tasks, such as updating outdated components.

The information that a widget displays comes from:

- OfficeScan server and clients
- Plug-in solutions and their client-side agents
- Trend Micro Smart Protection Network

Note

Enable Smart Feedback to display data from Smart Protection Network. For details about Smart Feedback, see *Smart Feedback on page 13-47*.

Tabs provide a container for widgets. The Summary dashboard supports up to 30 tabs.

Working with Tabs

Manage tabs by performing the following tasks:

TABLE 2-2. Tab Tasks

TASK	STEPS
Add a new tab	1. Click the add icon on top of the dashboard. A new screen displays. 2. Specify the following: • **Title**: The name of the tab • **Layout**: Choose from the available layouts • **Auto-fit**: Enable auto-fit if you selected a layout with several boxes (such as " ") and each box will contain only one widget. Auto-fit adjusts a widget to fit the size of a box. 3. Click **Save**.
Modify tab settings	1. Click **Tab Settings** on the top right corner of the tab. A new screen displays. 2. Modify the tab name, layout, and auto-fit settings. 3. Click **Save**.
Move a tab	Use drag-and-drop to change a tab's position.
Delete a tab	Click the delete icon next to the tab title. Deleting a tab deletes all widgets in the tab.

Working with Widgets

Manage widgets by performing the following tasks:

TABLE 2-3. Widget Tasks

TASK	STEPS
Add a new widget	1. Click a tab. 2. Click **Add Widgets** on the top right corner of the tab. A new screen displays. 3. Select the widgets to add. For a list of available widgets, see *Available Widgets on page 2-10*. • Click the display icons ( ) on the top right section of the screen to switch between the Detailed view and Summary view. • To the left of the screen are widget categories. Select a category to narrow down the selections. • Use the search text box on top of the screen to search for a specific widget. 4. Click **Add**.
Move a widget	Use drag-and-drop to move a widget to a different location within the tab.
Resize a widget	Resize a widget on a multi-column tab by pointing the cursor to the right edge of the widget and then moving the cursor to the left or right.
Edit the widget title	1. Click the edit icon ( ). A new screen appears. 2. Type the new title. **Note** For some widgets, such as OfficeScan and Plug-ins Mashup, widget-related items can be modified. 3. Click **Save**.
Refresh widget data	Click the refresh icon ( ).
Delete a widget	Click the delete icon ( ).

Predefined Tabs and Widgets

The **Summary** dashboard comes with a set of predefined tabs and widgets. You can rename or delete these tabs and widgets.

TABLE 2-4. Default Tabs in the Summary Dashboard

TAB	DESCRIPTION	WIDGETS
OfficeScan	This tab contains the same information found in the **Summary** screen in previous OfficeScan versions. In this tab, you can view the overall security risk protection of the OfficeScan network. You can also take action on items that require immediate intervention, such as outbreaks or outdated components.	• *Client Connectivity Widget on page 2-13* • *Security Risk Detections Widget on page 2-16* • *Outbreaks Widget on page 2-17* • *Client Updates Widget on page 2-19*
OfficeScan and Plug-ins	This tab shows which clients are running the OfficeScan client and plug-in solutions. Use this tab to assess the overall security status of clients.	*OfficeScan and Plug-ins Mashup Widget on page 2-20*
Smart Protection Network	This tab contains information from Trend Micro Smart Protection Network, which provides File Reputation Services and Web Reputation Services to OfficeScan clients.	• *Web Reputation Top Threat Sources Widget on page 2-27* • *Web Reputation Top Threatened Users Widget on page 2-28* • *File Reputation Threat Map Widget on page 2-29*

Available Widgets

The following widgets are available in this release:

TABLE 2-5. Available Widgets

WIDGET NAME	AVAILABILITY
Client Connectivity	Available out-of-the-box For details, see *Client Connectivity Widget on page 2-13*.
Security Risk Detections	Available out-of-the-box For details, see *Security Risk Detections Widget on page 2-16*.
Outbreaks	Available out-of-the-box For details, see *Outbreaks Widget on page 2-17*.
Client Updates	Available out-of-the-box For details, see *Client Updates Widget on page 2-19*.
OfficeScan and Plug-ins Mashup	Available out-of-the-box but only shows data from OfficeScan clients Data from the following plug-in solutions are available after activating each solution: • Intrusion Defense Firewall • Trend Micro Virtual Desktop Support For details, see *OfficeScan and Plug-ins Mashup Widget on page 2-20*.
Top Data Loss Preventions Incidents	Available after activating OfficeScan Data Protection For details, see *Top Data Loss Preventions Incidents Widget on page 2-21*.
Data Loss Prevention Incidents Over Time	Available after activating OfficeScan Data Protection For details, see *Data Loss Prevention Incidents Over Time Widget on page 2-23*.
Web Reputation Top Threat Sources	Available out-of-the-box For details, see *Web Reputation Top Threat Sources Widget on page 2-27*.

Widget Name	Availability
Web Reputation Top Threatened Users	Available out-of-the-box For details, see *Web Reputation Top Threatened Users Widget on page 2-28*.
File Reputation Threat Map	Available out-of-the-box For details, see *File Reputation Threat Map Widget on page 2-29*.
C&C Callback Events	Available out-of-the-box For details, see *C&C Callback Events Widget on page 2-24*.
IDF - Alert Status	Available after activating Intrusion Defense Firewall. See the IDF documentation for details about these widgets.
IDF - Computer Status	
IDF - Network Events History	
IDF - System Events History	

Client Connectivity Widget

The **Client Connectivity** widget shows the connection status of antivirus clients with the OfficeScan server. Data displays in a table and pie chart. You can switch between the table and pie chart by clicking the display icons ( ).

Client Connectivity

Latest data refresh: 05/09/2012 01:49 pm

All

Display:

Status	Smart Scan	Conventional Scan	Total
Online	71	6	77
Offline	13	0	13
Roaming	0	0	0
Total	84	6	90

FIGURE 2-3. Client Connectivity widget displaying a table

Client Connectivity Widget Presented as a Table

The table breaks down clients by scan methods.

If the number of clients for a particular status is 1 or more, you can click the number to view the clients in a client tree. You can initiate tasks on these clients or change their settings.

To display only clients using a particular scan method, click **All** and then select the scan method.

FIGURE 2-4. Connection status of conventional scan clients

FIGURE 2-5. Connection status of smart scan clients

If you selected **Smart Scan**:

- The table breaks down online smart scan clients by connection status with Smart Protection Servers.

Note

Only online clients can report their connection status with Smart Protection Servers.

If clients are disconnected from a Smart Protection Server, restore the connection by performing the steps in *Smart Protection Sources are Unavailable on page 14-38*.

- Each Smart Protection Server is a clickable URL that, when clicked, launches the server's console.
- If there are several Smart Protection Servers, click **MORE**. A new screen opens, showing all the Smart Protection Servers.

FIGURE 2-6. Smart Protection Servers list

In the screen, you can:

- View all the Smart Protection Servers to which clients connect and the number of clients connected to each server. Clicking the number opens the client tree where you can manage client settings.
- Launch a server's console by clicking the link for the server

Client Connectivity Widget Presented as a Pie Chart

The pie chart only shows the number of clients for each status and does not break down clients by scan methods. Clicking a status separates it from, or re-connects it to, the rest of the pie.

FIGURE 2-7. Client Connectivity widget displaying a pie chart

Security Risk Detections Widget

The **Security Risk Detections** widget shows the number of security risks and infected computers.

Type	Detections	Infected Computers
Virus/Malware	176	16
Spyware/Grayware	8	4

FIGURE 2-8. Security Risk Detections widget

If the number of infected computers is 1 or more, you can click the number to view the infected computers in a client tree. You can initiate tasks on the clients on these computers or change their settings.

Outbreaks Widget

The **Outbreaks** widget provides the status of any current security risk outbreaks and the last outbreak alert.

FIGURE 2-9. Outbreaks widget

In this widget, you can:

- View outbreak details by clicking the date/time link of the alert.
- Reset the status of the outbreak alert information and immediately enforce outbreak prevention measures when OfficeScan detects an outbreak. For details on enforcing outbreak prevention measures, see *Outbreak Prevention Policies on page 7-99*.

- Click **View Top 10 Security Risk Statistics** to view the most prevalent security risks, the computers with the most number of security risks, and the top infection sources. A new screen appears.

FIGURE 2-10. Top 10 Security Risk Statistics screen

In the **Top 10 Security Risk Statistics** screen, you can:

- View detailed information about a security risk by clicking the security risk name.
- View the overall status of a particular computer by clicking the computer name.
- View security risk logs for the computer by clicking **View** corresponding to a computer name.

- Reset the statistics in each table by clicking **Reset Count**.

Client Updates Widget

The **Client Updates** widget shows components and programs that protect networked computers from security risks.

Client Updates

Online Clients: 77, Smart Scan: 71, Conventional Scan: 6 — Latest data refresh: 05/09/2012 02:14 pm

Expand All | Collapse All

Antivirus	Current Version	Upgraded	Not Upgraded	Upgrade Rate
Smart Scan Agent Pattern	8.979.00	71	0	100%
Virus Pattern	8.979.00	6	0	100%
IntelliTrap Pattern	0.165.00	77	0	100%
IntelliTrap Exception Pattern	0.761.00	77	0	100%
Virus Scan Engine (32-bit)	9.500.1005	34	0	100%
Virus Scan Engine (64-bit)	9.500.1005	43	0	100%
Anti-spyware				
Damage Cleanup Services	Current Version	Upgraded	Not Upgraded	Upgrade Rate
Virus Cleanup Template	1186	77	0	100%
Virus Cleanup Engine (32-bit)	6.5.1055	34	0	100%
Virus Cleanup Engine (64-bit)	6.5.1055	43	0	100%
Firewall				
Behavior Monitoring Components				
Program				

FIGURE 2-11. Client Updates widget

In this widget, you can:

- View the current version for each component.
- View the number of clients with outdated components under the **Outdated** column. If there are clients that need to be updated, click the number link to start the update.
- For each program, view the clients that have not been upgraded by clicking the number link corresponding to the program.

> **Note**
>
> To upgrade Cisco Trust Agent, go to **Cisco NAC** > **Agent Deployment**.

OfficeScan and Plug-ins Mashup Widget

The **OfficeScan and Plug-ins Mashup** widget combines data from OfficeScan clients and installed plug-in programs and then presents the data in a client tree. This widget helps you quickly assess the protection coverage on clients and reduces the overhead required to manage the individual plug-in programs.

FIGURE 2-12. OfficeScan and Plug-ins Mashup widget

This widget shows data for the following plug-in programs:

- Intrusion Defense Firewall
- Trend Micro Virtual Desktop Support

These plug-in programs must be activated for the mashup widget to display data. Upgrade the plug-in programs if newer versions are available.

In this widget, you can:

- Choose the columns that display in the client tree. Click the edit icon ( ) on the top right corner of the widget and then select the columns in the screen that displays.

TABLE 2-6. OfficeScan and Plug-ins Mashup Columns

COLUMN NAME	DESCRIPTION
Computer Name	The endpoint name This column is always available and cannot be removed.
Domain Hierarchy	The endpoint's domain in the OfficeScan client tree
Connection Status	The OfficeScan clients connectivity with its parent OfficeScan server
Virus/Malware	The number of viruses and malware detected by the OfficeScan client
Spyware/Grayware	The number of spyware and grayware detected by the OfficeScan client
VDI Support	Indicates whether the endpoint is a virtual machine
IDF Security Profile	See the IDF documentation for details about these columns and the data that they show.
IDF Firewall	
IDF Status	
IDF DPI	

- Double-click data in the table. If you double-click OfficeScan data, the OfficeScan client tree displays. If you double-click plug-in program data (except data in the **VDI Support** column), the plug-in program's main screen displays.
- Use the search feature to find individual endpoints. You can type a full or partial host name.

Top Data Loss Preventions Incidents Widget

This widget is available only if you activate OfficeScan Data Protection.

This widget shows the number of digital asset transmissions, regardless of the action (block or pass).

FIGURE 2-13. Top Data Loss Preventions Incidents widget

To view data:

1. Select a time period for the detections. Choose from:
   - **Today**: Detections in the last 24 hours, including the current hour
   - **1 Week**: Detections in the last 7 days, including the current day
   - **2 Weeks**: Detections in the last 14 days, including the current day
   - **1 Month**: Detections in the last 30 days, including the current day
2. After selecting the time period, choose from:
   - **User**: Users that transmitted digital assets the most number of times
   - **Channel**: Channels most often used to transmit digital assets
   - **Template**: Digital asset templates that triggered the most detections

- **Computer**: Computers that transmitted digital assets the most number of times

> **Note**
> This widget shows a maximum of 10 users, channels, templates, or computers.

Data Loss Prevention Incidents Over Time Widget

This widget is available only if you activate OfficeScan Data Protection.

This widget plots the number of digital asset transmissions over a period of time. Transmissions include those that are blocked or passed (allowed).

FIGURE 2-14. Data Loss Prevention Incidents Over Time widget

To view data, select a time period for the detections. Choose from:

- **Today**: Detections in the last 24 hours, including the current hour
- **1 Week**: Detections in the last 7 days, including the current day

- **2 Weeks**: Detections in the last 14 days, including the current day
- **1 Month**: Detections in the last 30 days, including the current day

C&C Callback Events Widget

The **C&C Callback Events** widget displays all C&C callback event information including the target of the attack and the source callback address.

Administrators can choose to view C&C callback information from a specific C&C server list. To select the list source (Global Intelligence, Virtual Analyzer), click the edit icon ( ) and select the list from the **C&C list source** drop-down.

View C&C callback data by selecting the following:

- **Compromised host**: Displays the most recent C&C information per targeted endpoint

FIGURE 2-15. C&C Callback Events widget displaying target information

TABLE 2-7. Compromised Host Information

COLUMN	DESCRIPTION
Compromised Host	The name of the endpoint targeted by the C&C attack
Callback Addresses	The number of callback addresses that the endpoint attempted to contact
Latest Callback Address	The last callback address that the endpoint attempted to contact
Callback Attempts	The number of times the targeted endpoint attempted to contact the callback address **Note** Click the hyperlink to open the **C&C Callback Logs** screen and view more detailed information.

- Callback address: Displays the most recent C&C information per C&C callback address

FIGURE 2-16. C&C Callback Events widget displaying callback address information

TABLE 2-8. C&C Address Information

COLUMN	DESCRIPTION
Callback Address	The address of C&C callbacks originating from the network

Column	Description
C&C Risk Level	The risk level of the callback address determined by either the Global Intelligence or Virtual Analyzer list
Compromised Hosts	The number of endpoints that the callback address targeted
Latest Compromised Host	The name of the endpoint that last attempted to contact the C&C callback address
Callbacks Attempts	The number of attempted callbacks made to the address from the network **Note** Click the hyperlink to open the **C&C Callback Logs** screen and view more detailed information.

Web Reputation Top Threat Sources Widget

This widget displays the total number of security threat detections made by Web Reputation Services. The information is displayed in a world map by geographic location. For help using this widget, click the Help button ( ) on top of the widget.

FIGURE 2-17. Web Reputation Top Threat Sources widget

Web Reputation Top Threatened Users Widget

This widget displays the number of users affected by malicious URLs detected by Web Reputation Services. The information is displayed in a world map by geographic location. For help using this widget, click the Help button (?) on top of the widget.

FIGURE 2-18. Web Reputation Top Threatened Users widget

File Reputation Threat Map Widget

This widget displays the total number of security threat detections made by File Reputation Services. The information is displayed in a world map by geographic location. For help using this widget, click the Help button ( ) on top of the widget.

FIGURE 2-19. File Reputation Threat Map widget

The Server Migration Tool

OfficeScan provides the Server Migration Tool, which allows administrators to copy OfficeScan settings from previous OfficeScan versions to the current version. The Server Migration Tool migrates the following settings:

- Domain structures
- Manual Scan settings*
- Scheduled Scan settings*
- Real-time Scan settings*
- Scan now settings*
- Web Reputation settings*
- Approved URL list*
- Behavior Monitoring settings*
- Device Control settings*
- Data Loss Prevention settings*
- Privileges and other settings*
- Additional service settings*
- Spyware/Grayware approved list*
- Global client settings
- Computer location
- Firewall policies and profiles
- Smart protection sources
- Server update schedule
- Client update source and schedule
- Notifications
- Proxy settings
- OfficeScan Client Port and Client_LocalServer_Port in the `ofcscan.ini` file

Note

- Settings with an asterisk (*) retain the configurations at both the root and domain level.
- The tool does not back up the OfficeScan client listings of the OfficeScan server; only the domain structures.
- OfficeScan client only migrates features available on the older version of the OfficeScan client server. For features that are not available on the older server, OfficeScan client applies the default settings.

Using the Server Migration Tool

Note

This version of OfficeScan supports migrations from OfficeScan version 8.0 and later.

Older OfficeScan versions may not contain all the settings available in the latest version. OfficeScan automatically applies the default settings for any feature not migrated in the previous OfficeScan server version.

Procedure

1. On the OfficeScan server computer, navigate to <*Server installation folder*> `\PCCSRV\Admin\Utility\ServerMigrationTool`.
2. Double-click `ServerMigrationTool.exe` to start the Server Migration Tool.

   The Server Migration Tool opens.
3. To export the settings from the source OfficeScan server:
   a. Specify the destination folder using the **Browse** button.

      Note

      The default name of the export package is `OsceMigrate.zip`.

   b. Click **Export**.

      A confirmation message appears.

   c. Copy the export package to the destination OfficeScan server.
4. To import the settings to the destination OfficeScan server:
   a. Locate the export package using the **Browse** button.
   b. Click **Import**.

      A warning message appears.

   c. Click **Yes** to proceed.

A confirmation message appears.

5. Verify that the server contains all the previous OfficeScan version settings.

6. Move the old OfficeScan clients to the new server.

   For details about moving OfficeScan clients, see *Moving an OfficeScan Client to Another Domain or OfficeScan Server on page 2-57* or *Client Mover on page 14-21*.

Active Directory Integration

Integrate OfficeScan with your Microsoft™ Active Directory™ structure to manage OfficeScan clients more efficiently, assign web console permissions using Active Directory accounts, and determine which clients do not have security software installed. All users in the network domain can have secure access to the OfficeScan console. You can also configure limited access to specific users, even those in another domain. The authentication process and the encryption key provide validation of credentials for users.

Active Directory integration allows you to take full advantage of the following features:

- **Role-based administration**: Assign specific administrative responsibilities to users by granting them access to the product console using their Active Directory accounts. For details, see *Role-based Administration on page 13-2*.

- **Custom client groups**: Use Active Directory or IP addresses to manually group clients and map them to domains in the OfficeScan client tree. For details, see *Automatic Client Grouping on page 2-50*.

- **Outside server management**: Ensure that computers in the network that are not managed by the OfficeScan server comply with your company's security guidelines. For details, see *Security Compliance for Unmanaged Endpoints on page 14-65*.

Manually or periodically synchronize the Active Directory structure with the OfficeScan server to ensure data consistency. For details, see *Synchronizing Data with Active Directory Domains on page 2-34*.

Integrating Active Directory with OfficeScan

Procedure

1. Navigate to **Administration** > **Active Directory** > **Active Directory Integration**.
2. Under **Active Directory Domains**, specify the Active Directory domain name.
3. Specify credentials that the OfficeScan server will use when synchronizing data with the specified Active Directory domain. The credentials are required if the server is not part of the domain. Otherwise, the credentials are optional. Be sure that these credentials do not expire or the server will not be able to synchronize data.
   a. Click **Enter domain credentials**.
   b. In the popup window that opens, type the username and password. The username can be specified using any of the following formats:
      - `domain\username`
      - `username@domain`
   c. Click **Save**.
4. Click the (+) button to add more domains. If necessary, specify domain credentials for any of the added domains.
5. Click the (-) button to delete domains.
6. Specify encryption settings if you specified domain credentials. As a security measure, OfficeScan encrypts the domain credentials you specified before saving them to the database. When OfficeScan synchronizes data with any of the specified domains, it will use an encryption key to decrypt the domain credentials.
   a. Go to the **Encryption Settings for Domain Credentials** section.
   b. Type an encryption key that does not exceed 128 characters.
   c. Specify a file to which to save the encryption key. You can choose a popular file format, such as `.txt`. Type the file's full path and name, such as `C:\AD_Encryption\EncryptionKey.txt`.

WARNING!

If the file is removed or the file path changes, OfficeScan will not be able to synchronize data with all of the specified domains.

7. Click one of the following:
   - **Save**: Save the settings only. Because synchronizing data may strain network resources, you can choose to save the settings only and synchronize at a later time, such as during non-critical business hours.
   - **Save and Synchronize**: Save the settings and synchronize data with the Active Directory domains.
8. Schedule periodic synchronizations. For details, see *Synchronizing Data with Active Directory Domains on page 2-34*.

Synchronizing Data with Active Directory Domains

Synchronize data with Active Directory domains regularly to keep the OfficeScan client tree structure up-to-date and to query unmanaged clients.

Manually Synchronizing Data with Active Directory Domains

Procedure

1. Navigate to **Administration** > **Active Directory** > **Active Directory Integration**.
2. Verify that the domain credentials and encryption settings have not changed.
3. Click **Save and Synchronize**.

Automatically Synchronizing Data with Active Directory Domains

Procedure

1. Navigate to **Administration** > **Active Directory** > **Scheduled Synchronization**.
2. Select **Enable scheduled Active Directory synchronization**.
3. Specify the synchronization schedule.

   Note

   For daily, weekly, and monthly synchronizations, the period of time is the number of hours during which OfficeScan synchronizes Active Directory with the OfficeScan server.

4. Click **Save**.

The OfficeScan Client Tree

The OfficeScan client tree displays all the clients (grouped into *OfficeScan Domains on page 2-48*) that the server currently manages. Clients are grouped into domains so you can simultaneously configure, manage, and apply the same configuration to all domain members.

The client tree displays in the main frame when you access certain functions from the main menu.

FIGURE 2-20. OfficeScan Client Tree

Client Tree Icons

The OfficeScan client tree icons provide visual hints that indicate the type of computer and the status of OfficeScan clients that OfficeScan manages.

TABLE 2-9. OfficeScan Client Tree Icons

ICON	DESCRIPTION
	Domain
	Root

Icon	Description
	Update agent
	Smart scan available OfficeScan client
	Smart scan unavailable OfficeScan client
	Smart scan available update agent
	Smart scan unavailable update agent

Client Tree General Tasks

Below are the general tasks you can perform when the client tree displays:

Procedure

- Click the root domain icon ( ) to select all domains and clients. When you select the root domain icon and then choose a task above the client tree, a screen for configuring settings displays. On the screen, choose from the following general options:
  - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configure the settings.
  - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.
- To select multiple, adjacent domains or clients:
  - From the right panel, select the first domain, press and hold the SHIFT key, and then click the last domain or client in the range.

- To select a range of non-contiguous domains or clients, from the right panel, press and hold the CTRL key and then click the domains or clients that you want to select.
- Search for a client to manage by specifying the client name in the **Search for computers** text box. The domain with a list of all the clients in that domain displays, with the specified client name highlighted. To go to the next client, click **Search** again. For more search options, click **Advanced Search**.

Note

IPv6 or IPv4 addresses cannot be specified when searching for specific clients. Use Advanced Search to search by IPv4 or IPv6 address. For details, see *Advanced Search Options on page 2-39*.

- After selecting a domain, the client tree table expands to show the clients belonging to the domain and all the columns containing relevant information for each client. To view only a set of related columns, select an item in the client tree view.
  - **View all**: Shows all columns
  - **Update view**: Shows all the components and programs
  - **Antivirus view**: Shows antivirus components
  - **Anti-spyware view**: Shows anti-spyware components
  - **Data protection view**: Shows the status of the Data Protection module on clients
  - **Firewall view**: Shows firewall components
  - **Smart protection view**: Shows the scan method used by clients (conventional or smart scan) and smart protection components
  - **Update Agent view**: Shows information for all Update Agents managed by the OfficeScan server
- Rearrange columns by dragging the column titles to different positions in the client tree. OfficeScan automatically saves the new column positions.
- Sort clients based on column information by clicking the column name.

- Refresh the client tree by clicking the refresh icon ( ).
- View client statistics below the client tree, such as the total number of clients, number of smart scan clients, and number of conventional scan clients.

Advanced Search Options

Search for clients based on the following criteria:

Procedure

- **Basic**: Includes basic information about computers such as IP address, operating system, domain, MAC address, scan method, and web reputation status
  - Searching by IPv4 address range requires a portion of an IP address starting with the first octet. The search returns all computers with IP addresses containing that entry. For example, typing 10.5 returns all computers in the IP address range 10.5.0.0 to 10.5.255.255.
  - Searching by IPv6 address range requires a prefix and length.
  - Searching by MAC address requires a MAC address range in hexadecimal notation, for example, 000A1B123C12.
- **Component versions**: Select the check box next to the component name, narrow down the criteria by selecting **Earlier than** or **Earlier than and including**, and type a version number. The current version number displays by default.
- **Status**: Includes client settings

Click **Search** after specifying the search criteria. A list of computer names that meet the criteria appears in the client tree.

Client Tree Specific Tasks

The client tree displays when you access certain screens on the web console. Above the client tree are menu items specific to the screen you have accessed. These menu items

allow you to perform specific tasks, such as configuring client settings or initiating client tasks. To perform any of the tasks, first select the task target (either the root domain which will apply settings to all clients, one or several domains, or one or several clients) and then select a menu item.

The following screens display the client tree:

- *Client Management Screen on page 2-40*
- *Outbreak Prevention Screen on page 2-43*
- *Component Update for Networked Computers Screen on page 2-44*
- *Rollback Screen on page 2-45*
- *Security Risk Logs for Networked Computers Screen on page 2-46*
- *Agent Deployment Screen on page 2-48*

Client Management Screen

To view this screen, navigate to **Networked Computers** > **Client Management**.

Manage general client settings in the **Client Management** screen.

FIGURE 2-21. Client Management screen

The following table lists the tasks you can perform:

TABLE 2-10. Client Management Tasks

MENU BUTTON	TASK
Status	View detailed client information. For details, see *Viewing OfficeScan Client Information on page 14-50*.
Tasks	• Run Scan Now on client computers. For details, see *Initiating Scan Now on page 7-23*. • Uninstall the client. For details, see *Uninstalling the OfficeScan Client from the Web Console on page 5-68*. • Restore spyware/grayware components. For details, see *Restoring Spyware/Grayware on page 7-48*.

Menu Button	Task

Settings	• Configure scan settings. For details, see the following topics:
	  • *Scan Methods on page 7-7*
	  • *Manual Scan on page 7-17*
	  • *Real-time Scan on page 7-14*
	  • *Scheduled Scan on page 7-19*
	  • *Scan Now on page 7-21*
	• Configure web reputation settings. For details, see *Web Reputation Policies on page 11-5*.
	• Configure Behavior Monitoring settings. For details, see *Behavior Monitoring on page 8-2*.
	• Configure Device Control settings. For details, see *Device Control on page 9-2*.
	• Configure Data Loss Prevention policies. For details, see *Data Loss Prevention Policy Configuration on page 10-40*.
	• Assign clients as Update Agents. For details, see *Update Agent Configuration on page 6-51*.
	• Configure client privileges and other settings. For details, see *Configuring Client Privileges and Other Settings on page 14-84*.
	• Enable or disable OfficeScan client services. For details, see *OfficeScan Client Services on page 14-6*.
	• Configure the spyware/grayware approved list. For details, see *Spyware/Grayware Approved List on page 7-46*.
	• Import and export client settings. For details, see *Importing and Exporting Client Settings on page 14-51*.

MENU BUTTON	TASK
Logs	View the following logs: • Virus/Malware logs (for details, see *Viewing Virus/Malware Logs on page 7-83*) • Spyware/Grayware logs (for details, see *Viewing Spyware/ Grayware Logs on page 7-90*) • Firewall logs (for details, see *Firewall Logs on page 12-27*) • Web reputation logs (for details, see *Web Reputation Logs on page 11-18*) • C&C Callback logs (for details, see *Viewing C&C Callback Logs on page 11-19*.) • Behavior Monitoring logs (for details, see *Behavior Monitoring Logs on page 8-12*) • Device Control logs (for details, see *Device Control Logs on page 9-17*) Delete logs. For details, see *Log Management on page 13-33*.
Manage Client Tree	Manage the client tree. For details, see *Client Grouping Tasks on page 2-55*.
Export	Export a list of clients to a comma-separated value (`.csv`) file.

Outbreak Prevention Screen

To view this screen, navigate to **Networked Computers** > **Outbreak Prevention**.

Specify and activate outbreak prevention settings in the **Outbreak Prevention** screen. For details, see *Configuring Security Risk Outbreak Prevention on page 7-98*.

FIGURE 2-22. Outbreak Prevention screen

Component Update for Networked Computers Screen

To view this screen, navigate to **Updates** > **Networked Computers** > **Manual Update**. Select **Manually select clients** and click **Select**.

Initiate manual update in the **Component Update for Networked Computers** screen. For details, see *OfficeScan Client Manual Updates on page 6-41*.

FIGURE 2-23. Component Update for Networked Computers screen

Rollback Screen

To view this screen, navigate to **Updates** > **Rollback**. Click **Synchronize with Server**.

Roll back client components in the **Rollback** screen. For details, see *Rolling Back Components for OfficeScan Clients on page 6-48*.

FIGURE 2-24. Rollback screen

Security Risk Logs for Networked Computers Screen

To view this screen, navigate to **Logs** > **Networked Computer Logs** > **Security Risks**.

View and manage logs in the **Security Risk Logs for Networked Computers** screen.

FIGURE 2-25. Security Risk Logs for Networked Computers screen

Perform the following tasks:

1. View logs that clients send to the server. For details, see:
   - *Viewing Virus/Malware Logs on page 7-83*
   - *Viewing Spyware/Grayware Logs on page 7-90*
   - *Viewing Firewall Logs on page 12-28*
   - *Viewing Web Reputation Logs on page 11-18*
   - *Viewing C&C Callback Logs on page 11-19*
   - *Viewing Behavior Monitoring Logs on page 8-13*
   - *Viewing Device Control Logs on page 9-17*

- *Viewing Data Loss Prevention Logs on page 10-50*

2. Delete logs. For details, see *Log Management on page 13-33*.

Agent Deployment Screen

To view this screen, navigate to **Cisco NAC** > **Agent Deployment**.

If you have set up Policy Server for Cisco NAC, deploy the Cisco Trust Agent (CTA) to clients in the **Agent Deployment** screen. For details, see *Cisco Trust Agent Deployment on page 16-27*.

FIGURE 2-26. Agent Deployment screen

OfficeScan Domains

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

the same configuration to all domain members. For more information on client grouping, see *Client Grouping on page 2-49*.

Client Grouping

Use Client Grouping to manually or automatically create and manage domains on the OfficeScan client tree.

There are two ways to group clients into domains.

TABLE 2-11. Client Grouping Methods

METHOD	CLIENT GROUPING	DESCRIPTIONS
Manual	• NetBIOS domain • Active Directory domain • DNS domain	Manual client grouping defines the domain to which a newly installed client should belong. When the client appears in the client tree, you can move it to another domain or to another OfficeScan server. Manual client grouping also allows you to create, manage, and remove domains in the client tree. For details, see *Manual Client Grouping on page 2-49*.
Automatic	Custom client groups	Automatic client grouping uses rules to sort clients in the client tree. After you define the rules, you can access the client tree to manually sort the clients or allow OfficeScan to automatically sort them when specific events occur or at scheduled intervals. For details, see *Automatic Client Grouping on page 2-50*.

Manual Client Grouping

OfficeScan uses this setting only during fresh client installations. The installation program checks the network domain to which a target computer belongs. If the domain name already exists in the client tree, OfficeScan groups the client on the target computer under that domain and will apply the settings configured for the domain. If

the domain name does not exist, OfficeScan adds the domain to the client tree, groups the client under that domain, and then applies the root settings to the domain and client.

Configuring Manual Client Grouping

Procedure

1. Navigate to **Networked Computers** > **Client Grouping**.
2. Specify client grouping method:
   - NetBIOS domain
   - Active Directory domain
   - DNS domain
3. Click **Save**.

What to do next

Manage domains and the clients grouped under them by performing the following tasks:

- Add a domain
- Delete a domain or client
- Rename a domain
- Move a client to another domain

For details, see *Client Grouping Tasks on page 2-55*.

Automatic Client Grouping

Automatic client grouping uses rules defined by IP addresses or Active Directory domains. If a rule defines an IP address or an IP address range, the OfficeScan server will group a client with a matching IP address to a specific domain in the client tree. Similarly, if a rule defines one or several Active Directory domains, the OfficeScan server will group a client belonging to a particular Active Directory domain to a specific domain in the client tree.

Clients apply only one rule at a time. Prioritize rules so that if a client satisfies more than one rule, the rule with the highest priority applies.

Configuring Automatic Client Grouping

Procedure

1. Navigate to **Networked Computers** > **Client Grouping**
2. Go to the **Client Grouping** section and select **Custom client groups**.
3. Go to the **Automatic Client Grouping** section.
4. To start creating rules, click **Add** and then select either **Active Directory** or **IP Address**.
   - If you selected **Active Directory**, see the configuration instructions in *Defining a Client Grouping Rule by Active Directory Domains on page 2-52*.
   - If you selected **IP Address**, see the configuration instructions in *Defining a Client Grouping Rule by IP Addresses on page 2-54*.
5. If you created more than one rule, prioritize the rules by performing these steps:
   a. Select a rule.
   b. Click an arrow under the **Grouping Priority** column to move the rule up or down the list. The ID number of the rule changes to reflect the new position.
6. To use the rules during client sorting:
   a. Select the check boxes for the rules that you want to use.
   b. Ensure that the rules are enabled. Under the Status column, a green check mark icon ( ) should appear. If a red "x" mark icon ( ) appears, clicking the icon enables the rule and changes the icon to green.

Note

If you do not select the check box for a rule or if you disable a rule, the rule will not be used when sorting clients in the client tree. For example, if the rule dictates that a client should move to a new domain, the client will not move and stays in its current domain.

7. Specify a sorting schedule in the **Scheduled Domain Creation** section.

   a. Select **Enable scheduled domain creation**.

   b. Specify the schedule under **Schedule-based Domain Creation**.

8. Choose from the following options:

   - **Save and Create Domain Now**: Choose this option if you specified new domains in *Defining a Client Grouping Rule by IP Addresses on page 2-54*, step 7 or in *Defining a Client Grouping Rule by Active Directory Domains on page 2-52*, step 7.
   - **Save**: Choose this option if you did not specify new domains or want to create the new domains only when client sorting runs.

Note

Client sorting will not start after completing this step.

Defining a Client Grouping Rule by Active Directory Domains

Ensure that you have configured Active Directory integration settings before performing the steps in the procedure below. For details, see *Active Directory Integration on page 2-32*.

Procedure

1. Navigate to **Networked Computers** > **Client Grouping**.
2. Go to the **Client Grouping** section and select **Custom client groups**.

3. Go to the **Automatic Client Grouping** section.
4. Click **Add** and then select **Active Directory**.

   A new screen appears.
5. Select **Enable grouping**.
6. Specify a name for the rule.
7. Under **Active Directory source**, select the Active Directory domain(s) or subdomains.
8. Under **Client tree**, select an existing OfficeScan domain to which the Active Directory domains map. If the desired OfficeScan domain does not exist, perform the following steps:

   a. Mouseover on a particular OfficeScan domain and click the add domain icon. In the example below, the new domain will be added under the root OfficeScan domain.

FIGURE 2-27. Add domain icon

   b. Type the domain name in the text box provided.

   c. Click the check mark next to the text box. The new domain is added and is automatically selected.
9. (Optional) Select **Duplicate Active Directory structure into OfficeScan client tree**. This option duplicates the hierarchy of the selected Active Directory domains to the selected OfficeScan domain.
10. Click **Save**.

Defining a Client Grouping Rule by IP Addresses

Create custom client groups using network IP addresses to sort clients in the OfficeScan client tree. The feature can help administrators arrange the OfficeScan client tree structure before the client registers to the OfficeScan server.

Procedure

1. Navigate to **Networked Computers** > **Client Grouping**.
2. Go to the **Client Grouping** section and select **Custom client groups**.
3. Go to the **Automatic Client Grouping** section.
4. Click **Add** and then select **IP Address**.

   A new screen appears.
5. Select **Enable grouping**.
6. Specify a name for the grouping.
7. Specify one of the following:
   - A single IPv4 or IPv6 address
   - An IPv4 address range
   - An IPv6 prefix and length

   Note

   If a dual-stack client's IPv4 and IPv6 addresses belong to two separate client groups, the client will be grouped under the IPv6 group. If IPv6 is disabled on the client's host machine, the client will move to the IPv4 group.
8. Select the OfficeScan domain to which the IP address or IP address ranges maps. If the domain does not exist, do the following:

   a. Mouseover anywhere on the client tree and click the add domain icon.

FIGURE 2-28. Add domain icon

b. Type the domain in the text box provided.

c. Click the check mark next to the text box. The new domain is added and is automatically selected.

9. Click **Save**.

Client Grouping Tasks

You can perform the following tasks when grouping clients in domains:

- Add a domain. See *Adding a Domain on page 2-55* for details.
- Delete a domain or client. See *Deleting a Domain or Client on page 2-56* for details.
- Rename a domain. See *Renaming a Domain on page 2-57* for details.
- Move a client to another domain or another OfficeScan server. See *Moving an OfficeScan Client to Another Domain or OfficeScan Server on page 2-57* for details.
- Delete a domain or a client. See *Deleting a Domain or Client on page 2-56* for details.

Adding a Domain

Procedure

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

2. Click **Manage Client Tree** > **Add Domain**.
3. Type a name for the domain you want to add.
4. Click **Add**.

   The new domain appears in the client tree.
5. (Optional) Create subdomains.
   a. Select the parent domain.
   b. Click **Manage Client Tree** > **Add domain**.
   c. Type the subdomain name.

Deleting a Domain or Client

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, select:
   - One or several domains
   - One, several, or all clients belonging to a domain
3. Click **Manage Client Tree** > **Remove Domain/Client**.
4. To delete an empty domain, click **Remove Domain/Client**. If the domain has clients and you click **Remove Domain/Client**, the OfficeScan server will re-create the domain and group all clients under that domain the next time clients connect to the OfficeScan server. You can perform the following tasks before deleting the domain:
   a. Move clients to other domains. To move clients to other domains, drag and drop clients to the destination domains.
   b. Delete all clients.
5. To delete a client, click **Remove Domain/Client**.

Note

Deleting a client from the client tree does not remove the OfficeScan client from the client computer. The OfficeScan client can still perform server-independent tasks, such as updating components. However, the server is unaware of the existence of the client and will therefore not deploy configurations or send notifications to the client.

Renaming a Domain

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. Select a domain in the client tree.
3. Click **Manage Client Tree** > **Rename Domain**.
4. Type a new name for the domain.
5. Click **Rename**.

   The new domain name appears in the client tree.

Moving an OfficeScan Client to Another Domain or OfficeScan Server

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, open a domain and select one, several, or all clients.
3. Click **Manage Client Tree** > **Move Client**.
4. To move clients to another domain:
   - Select **Move selected client(s) to another domain**.
   - Select the domain.

- (Optional) Apply the settings of the new domain to the clients.

Tip

You can also drag and drop clients to another domain in the client tree.

5. To move clients to another OfficeScan server:
   - Select **Move selected client(s) to another OfficeScan Server**.
   - Type the server name or IPv4/IPv6 address and HTTP port number.
6. Click **Move**.

Chapter 3

Getting Started with Data Protection

This chapter discusses how to install and activate the Data Protection module.

Topics in this chapter:

- *Data Protection Installation on page 3-2*
- *Data Protection License on page 3-4*
- *Deployment of Data Protection to Clients on page 3-5*
- *Forensic Folder and DLP Database on page 3-8*
- *Uninstalling Data Protection on page 3-14*

Data Protection Installation

The Data Protection module includes the following features:

- **Data Loss Prevention (DLP)**: Prevents unauthorized transmission of digital assets
- **Device Control**: Regulates access to external devices

Note

OfficeScan out-of-the-box has a Device Control feature that regulates access to commonly used devices such as USB storage devices. Device Control that is part of the Data Protection module expands the range of monitored devices. For a list of monitored devices, see *Device Control on page 9-2*.

Data Loss Prevention and Device Control are native OfficeScan features but are licensed separately. After you install the OfficeScan server, these features are available but are not functional and cannot be deployed to clients. Installing Data Protection means downloading a file from the ActiveUpdate server or a custom update source, if one has been set up. When the file has been incorporated into the OfficeScan server, you can activate the Data Protection license to enable the full functionality of its features. Installation and activation are performed from **Plug-in Manager**.

Important

- You do not need to install the Data Protection module if the standalone Trend Micro Data Loss Prevention software is already installed and running on endpoints.
- The Data Protection module can be installed on a pure IPv6 Plug-In Manager. However, only the Device Control feature can be deployed to pure IPv6 clients. The Data Loss Prevention feature does not work on pure IPv6 clients.

Installing Data Protection

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.

2. On the **Plug-in Manager** screen, go to the **OfficeScan Data Protection** section and click **Download**.

   The size of the file to be downloaded displays beside the **Download** button.

   Plug-In Manager stores the downloaded file to <*Server installation folder*> `\PCCSRV\Download\Product`.

   Note

   If Plug-In Manager is unable to download the file, it automatically re-downloads after 24 hours. To manually trigger Plug-In Manager to download the file, restart the OfficeScan Plug-In Manager service from the Microsoft Management Console.

3. Monitor the download progress.

   You can navigate away from the screen during the download.

   If you encounter problems downloading the file, check the server update logs on the OfficeScan web console. On the main menu, click **Logs** > **Server Update Logs**.

   After Plug-In Manager downloads the file, OfficeScan Data Protection displays in a new screen.

   Note

   If OfficeScan Data Protection does not display, see the reasons and solutions in *Troubleshooting Plug-In Manager on page 15-9*.

4. To install OfficeScan Data Protection immediately, click **Install Now**, or to install at a later time, perform the following:

   a. Click **Install Later**.

   b. Open the **Plug-in Manager** screen.

   c. Go to the **OfficeScan Data Protection** section and click **Install**.

5. Read the license agreement and accept the terms by clicking **Agree**.

   The installation starts.

6. Monitor the installation progress. After the installation, the OfficeScan Data Protection version displays.

Data Protection License

View, activate, and renew the Data Protection license from Plug-In Manager.

Obtain an Activation Code from Trend Micro and then use it to activate the license.

Activating or Renewing the Data Protection License

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the OfficeScan Data Protection section and click **Manage Program**.
3. Click **New Activation Code**.
4. Type the Activation Code.

   You can also copy the Activation Code and then paste it on any of the text boxes.
5. Click **Save**.

Viewing the Data Protection License Information

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the OfficeScan Data Protection section and click **Manage Program**.
3. Click **View License Information**.

4. View the following license details in the screen that opens.
   - **Status**: Displays either "Activated", "Not Activated" or "Expired".
   - **Version**: Displays either "Full" or "Evaluation" version. Activation of both the full and evaluation versions displays only as "Full".
   - **Seats**: Displays how many OfficeScan clients can install the Data Protection module
   - **License expires on**: If Data Protection has multiple licenses, the latest expiration date displays. For example, if the license expiration dates are 12/31/2011 and 06/30/2011, 12/31/2011 displays.
   - **Activation code**: Displays the Activation Code
   - Reminders: Depending on your current license version, Data Protection displays reminders about the license expiration date either during the grace period (full versions only), or when the license expires.

   Note

   The duration of the grace period varies by region. Please verify the grace period with your Trend Micro representative.

   If you do not renew the license, Data Loss Prevention and Device Control still work but you will no longer be eligible for technical support.

5. Click **View detailed license online** to view information about your license on the Trend Micro website.
6. To update the screen with the latest license information, click **Update Information**.

Deployment of Data Protection to Clients

Deploy the Data Protection module to OfficeScan clients after activating its license. After the deployment, OfficeScan clients will start to use Data Loss Prevention and Device Control.

Important

- By default, the module is disabled on Windows Server 2003, Windows Server 2008, and Windows Server 2012 to prevent impacting the performance of the host machine. If you want to enable the module, monitor the system's performance constantly and take the necessary action when you notice a drop in performance.

  Note

  You can enable or disable the module from the web console. For details, see *OfficeScan Client Services on page 14-6*.

- If the Trend Micro Data Loss Prevention software already exists on the endpoint, OfficeScan will not replace it with the Data Protection module.
- Only Device Control can be deployed to pure IPv6 clients. Data Loss Prevention does not work on pure IPv6 clients.
- Online clients install the Data Protection module immediately. Offline and roaming clients install the module when they become online.
- Users must restart their computers to finish installing Data Loss Prevention drivers. Inform users about the restart ahead of time.
- Trend Micro recommends enabling debug logging to help you troubleshoot deployment issues. For details, see *Data Protection Debug Logs on page 10-55*.

Deploying the Data Protection Module to Clients

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, you can:
   - Click the root domain icon ( ) to deploy the module to all existing and future clients.
   - Select a specific domain to deploy the module to all existing and future clients under the domain.
   - Select a specific client to deploy the module only to that client.

3. Deploy the module in two different ways:
   - Click **Settings** > **DLP Settings**.
   - Click **Settings** > **Device Control Settings**.

   Note

   If you deploy from **Settings** > **DLP Settings** and the Data Protection module was deployed successfully, Data Loss Prevention drivers will be installed. If the drivers are installed successfully, a message displays, informing users to restart their computers to finish installing the drivers.

   If the message does not display, there might be problems installing the drivers. If you enabled debug logging, check the debug logs for details about driver installation problems.

4. A message displays, indicating the number of client that have not installed the module. Click **Yes** to start the deployment.

   Note

   If you click **No** (or if the module was not deployed to one or several client for some reason), the same message displays when you click **Settings** > **DLP Settings** or **Settings** > **Device Control Settings** again.

   Clients start to download the module from the server.

5. Check if the module was deployed to clients.
   a. In the client tree, select a domain.
   b. In the client tree view, select **Data protection view** or **View all**.
   c. Check the **Data Protection Status** column. The deployment status can be any of the following:
      - **Running**: The module was deployed successfully and its features have been enabled.
      - **Requires restart**: Data Loss Prevention drivers have not been installed because users have not restarted their computers. If the drivers are not installed, Data Loss Prevention will not be functional.

- **Stopped**: The service for the module has not been started or the target computer has been shut down normally. To start the Data Protection service, navigate to **Networked Computers** > **Client Management** > **Settings** > **Additional Service Settings** and enable Data Protection Services.
- **Cannot install**: There was a problem deploying the module to the client. You will need to re-deploy the module from the client tree.
- **Cannot install (Data Loss Prevention already exists)**: The Trend Micro Data Loss Prevention software already exists on the endpoint. OfficeScan will not replace it with the Data Protection module.
- **Not installed**: The module has not been deployed to the client. This status displays if you chose not to deploy the module to the client or if the client's status is offline or roaming during deployment.

Forensic Folder and DLP Database

After a Data Loss Prevention incident occurs, OfficeScan logs the incident details in a specialized forensic database. OfficeScan also creates an encrypted file containing a copy of the sensitive data which triggered the incident and generates a hash value for verification purposes and to ensure the integrity of the sensitive data. OfficeScan creates the encrypted forensic files on the client machine and then uploads the files to a specified location on the server.

Important

- The encrypted forensic files contain highly sensitive data and administrators should exercise caution when granting access to these files.
- OfficeScan integrates with Control Manager to provide Control Manager users with the DLP Incident Reviewer or DLP Compliance Officer roles the ability to access the data within the encrypted files. For details about the DLP roles and access to the forensic file data in Control Manager, see the *Control Manager Administrator's Guide 6.0 Patch 2* or later.

Modifying the Forensic Folder and Database Settings

Administrators can change the location and deletion schedule of the forensic folder, and the maximum size of files that clients upload by modifying OfficeScan's INI files.

WARNING!

Changing the location of the forensic folder after logging Data Loss Prevention incidents can cause a disconnect between the database data and the location of existing forensic files. Trend Micro recommends manually migrating any existing forensic files to the new forensic folder after modifying the forensic folder location.

The following table outlines the server settings available in the <*Server installation folder*>`\PCCSRV\Private\ofcserver.ini` file located on the OfficeScan server.

TABLE 3-1. Forensic Folder Server Settings in `PCCSRV\Private\ofcserver.ini`

OBJECTIVE	INI SETTING	VALUES
Enabling the user-defined forensic folder location	[INI_IDLP_SECTION] `EnableUserDefinedUploadFolder`	0: Disable (default) 1: Enable

OBJECTIVE	INI SETTING	VALUES
Configuring the user-defined forensic folder location	[INI_IDLP_SECTION] `UserDefinedUploadFolder` **Note** • Administrators must enable the `EnableUserDefinedUploadFolder` setting before OfficeScan applies this setting. • The default location of the forensic folder is: <*Server installation folder*>`\PCCSRV\Private\DLPForensicData` • The user-defined forensic folder location must be a physical drive (internal or external) on the server machine. OfficeScan does not support mapping a network drive location.	Default value: <Please replace this value with customer defined folder path. For example: C:\VolumeData\OfficeScanDlpForensicData> User-defined value: Must be the physical location of a drive on the server machine
Enabling the purging of forensic data files	[INI_IDLP_SECTION] `ForensicDataPurgeEnable`	0: Disable 1: Enable (default)

Objective	INI Setting	Values
Configuring the time frequency of the forensic data file purge check	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` **Note** • Administrators must enable the `ForensicDataPurgeEnable` setting before OfficeScan applies this setting. • OfficeScan only deletes data files that have passed the expiry date specified in the `ForensicDataExpiredPeriodInDays` setting.	1: Monthly, on the first day of the month at 00:00 2: Weekly (default), every Sunday at 00:00 3: Daily, every day at 00:00 4: Hourly, every hour at HH:00
Configuring the length of time to store forensic data files on the server	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	Default value (in days): 180 Minimum value: 1 Maximum value: 3650
Configuring the time frequency of the forensic file disk space check	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` **Note** If the available disk space in the forensic data folder is less than the value configured for the `InformUploadOnDiskFreeSpaceInGb` setting, OfficeScan records an event log on the web console.	Default value (in seconds): 5

OBJECTIVE	INI SETTING	VALUES
Configuring the upload frequency of the forensic file disk space check	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` **Note** If the available disk space in the forensic data folder is less than the value configured for the `InformUploadOnDiskFreeSpaceInGb` setting, OfficeScan records an event log on the web console.	Default value (in number of files): 200
Configuring the minimum disk space value that triggers a limited disk space notification	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` **Note** If the available disk space in the forensic data folder is less than the value configured, OfficeScan records an event log on the web console.	Default value (in GB): 10
Configuring the minimum space available to upload forensic data files from clients	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **Note** If the available disk space in the forensic data folder is less than the value configured, OfficeScan clients do not upload forensic data files to the server and OfficeScan records an event log on the web console.	Default value (in GB): 1

The following table outlines the OfficeScan client settings available in the <*Server installation folder*>`\PCCSRV\ofcscan.ini` file located on the OfficeScan server.

TABLE 3-2. Forensic File OfficeScan Client Settings in `PCCSRV\ofcscan.ini`

OBJECTIVE	INI SETTING	VALUES
Enabling the uploading of forensic data files to the server	`UploadForensicDataEnable`	0: Disable 1: Enable (default)
Configuring the maximum size of files that the OfficeScan client uploads to the server	`UploadForensicDataSizeLimitInMb` **Note** The OfficeScan client only sends files that are less than this size to the server.	Default value (in MB): 10 Minimum value: 1 Maximum value: 2048
Configuring the length of time to store forensic data files on the OfficeScan client	`ForensicDataKeepDays` **Note** The OfficeScan client deletes forensic data files that have passed the expiry date specified every day at 11:00 am.	Default value (in days): 180 Minimum value: 1 Maximum value: 3650
Configuring the frequency in which the OfficeScan client checks for server connectivity	`ForensicDataDelayUploadFrequenceInMinutes` **Note** OfficeScan clients that are unable to upload forensic files to the server automatically try to resend the files using the specified time interval.	Default value (in minutes): 5 Minimum value: 5 Maximum value: 60

Creating a Backup of Forensic Data

Depending on the company's security policy, the length of time necessary to store the forensic data information may vary greatly. In order to free disk space on the server, Trend Micro recommends performing a manual backup of the forensic folder data and forensic database.

Procedure

1. Navigate to the forensic data folder location on the server.
   - Default location: <*Server installation folder*>`\PCCSRV\Private\DLPForensicData`
   - To locate the customized forensic folder location, see *Configuring the user-defined forensic folder location on page 3-10*.
2. Copy the folder to a new location.
3. To manually backup the forensic data database, navigate to <*Server installation folder*>`\PCCSRV\Private`.
4. Copy the `DLPForensicDataTracker.db` file to a new location.

Uninstalling Data Protection

If you uninstall the Data Protection module from Plug-In Manager:

- All Data Loss Prevention configurations, settings, and logs are removed from the OfficeScan server.
- All Device Control configurations and settings provided by the Data Protection module are removed from the server.
- The Data Protection module is removed from clients. Client computers must be restarted to remove Data Protection completely.
- Data Loss Prevention policies will no longer be enforced on clients.
- Device Control will no longer monitor access to the following devices:
  - Bluetooth adapters
  - COM and LPT ports
  - IEEE 1394 interface
  - Imaging devices

- Infrared devices
- Modems
- PCMCIA card
- Print screen key
- Wireless NICs

Reinstall the Data Protection module anytime. After reinstallation, activate the license using a valid Activation Code.

Uninstalling Data Protection from Plug-In Manager

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the **OfficeScan Data Protection** section and click **Uninstall**.
3. Monitor the uninstallation progress. You can navigate away from the screen during the uninstallation.
4. Refresh the **Plug-in Manager** screen after the uninstallation. OfficeScan Data Protection is again available for installation.

Part II

Protecting Networked Computers

Chapter 4

Using Trend Micro Smart Protection

This chapter discusses Trend Micro™ smart protection solutions and describes how to set up the environment required to use the solutions.

Topics in this chapter:

- *About Trend Micro Smart Protection on page 4-2*
- *Smart Protection Services on page 4-3*
- *Smart Protection Sources on page 4-5*
- *Smart Protection Pattern Files on page 4-7*
- *Setting Up Smart Protection Services on page 4-12*
- *Using Smart Protection Services on page 4-30*

About Trend Micro Smart Protection

Trend Micro™ smart protection is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both local and hosted solutions to protect users whether they are on the network, at home, or on the go, using light-weight clients to access its unique in-the-cloud correlation of email, web and file reputation technologies, as well as 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.

By incorporating in-the-cloud reputation, scanning, and correlation technologies, the Trend Micro smart protection solutions reduce reliance on conventional pattern file downloads and eliminate the delays commonly associated with desktop updates.

The Need for a New Solution

In the current approach to file-based threat handling, patterns (or definitions) required to protect a client are, for the most part, delivered on a scheduled basis. Patterns are delivered in batches from Trend Micro to clients. When a new update is received, the virus/malware prevention software on the client reloads this batch of pattern definitions for new virus/malware risks into memory. If a new virus/malware risk emerges, this pattern once again needs to be updated partially or fully and reloaded on the client to ensure continued protection.

Over time, there has been a significant increase in the volume of unique emerging threats. The increase in the volume of threats is projected to grow at a near-exponential rate over the coming years. This amounts to a growth rate that far outnumbers the volume of currently known security risks. Going forward, the volume of security risks represents a new type of security risk. The volume of security risks can impact server and workstation performance, network bandwidth usage, and, in general, the overall time it takes to deliver quality protection - or "time to protect".

A new approach to handling the volume of threats has been pioneered by Trend Micro that aims to make Trend Micro customers immune to the threat of virus/malware volume. The technology and architecture used in this pioneering effort leverages technology that off-loads the storage of virus/malware signatures and patterns to the cloud. By off-loading the storage of these virus/malware signatures to the cloud, Trend

Micro is able to provide better protection to customers against the future volume of emerging security risks.

Smart Protection Services

Smart protection includes services that provide anti-malware signatures, web reputations, and threat databases that are stored in-the-cloud.

Smart protection services include:

- **File Reputation Services**: File Reputation Services off-loads a large number of anti-malware signatures that were previously stored on client computers to smart protection sources. For details, see *File Reputation Services on page 4-3*.
- **Web Reputation Services**: Web Reputation Services allows local smart protection sources to host URL reputation data that were previously hosted solely by Trend Micro. Both technologies ensure smaller bandwidth consumption when updating patterns or checking a URL's validity. For details, see *Web Reputation Services on page 4-4*.
- **Smart Feedback**: Trend Micro continues to harvest information anonymously sent from Trend Micro products worldwide to proactively determine each new threat. For details, see *Smart Feedback on page 4-4*.

File Reputation Services

File Reputation Services checks the reputation of each file against an extensive in-the-cloud database. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall client footprint.

Clients must be in smart scan mode to use File Reputation Services. These clients are referred to as **smart scan clients** in this document. Clients that are not in smart scan mode do not use File Reputation Services and are called **conventional scan clients**. OfficeScan administrators can configure all or several clients to be in smart scan mode.

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. Web reputation then continues to scan sites and block users from accessing infected ones. Web reputation features help ensure that the pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web reputation technology assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

OfficeScan clients subject to web reputation policies use Web Reputation Services. OfficeScan administrators can subject all or several clients to web reputation policies.

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 computers. 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

Smart Protection Sources

Trend Micro delivers File Reputation Services and Web Reputation Services to OfficeScan and smart protection sources.

Smart protection sources provide File Reputation Services by hosting the majority of the virus/malware pattern definitions. OfficeScan clients host the remaining definitions. A client sends scan queries to smart protection sources if its own pattern definitions cannot determine the risk of the file. Smart protection sources determine the risk using identification information.

Smart protection sources provide Web Reputation Services by hosting web reputation data previously available only through Trend Micro hosted servers. A client sends web reputation queries to smart protection sources to check the reputation of websites that a user is attempting to access. The client correlates a website's reputation with the specific web reputation policy enforced on the computer to determine whether access to the site will be allowed or blocked.

The smart protection source to which a client connects depends on the client's location. Clients can connect to either Trend Micro Smart Protection Network or Smart Protection Server.

Trend Micro™ Smart Protection Network™

The Trend Micro™ Smart Protection Network™ is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. Smart Protection Network uses lighter-weight clients to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as 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.

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Smart Protection Server

Smart Protection Servers are for users who have access to their local corporate network. Local servers localize smart protection services to the corporate network to optimize efficiency.

There are two types of Smart Protection Servers:

- **Integrated Smart Protection Server**: The OfficeScan Setup program includes an integrated Smart Protection Server that installs on the same computer where the OfficeScan server is installed. After the installation, manage settings for this server from the OfficeScan web console. The integrated server is intended for small-scale deployments of OfficeScan, in which the number of clients does not exceed 3,000. For larger deployments, the standalone Smart Protection Server is required.
- **Standalone Smart Protection Server**: A standalone Smart Protection Server installs on a VMware or Hyper-V server. The standalone server has a separate management console and is not managed from the OfficeScan web console.

Smart Protection Sources Compared

The following table highlights the differences between Smart Protection Network and Smart Protection Server.

TABLE 4-1. Smart Protection Sources Compared

BASIS OF COMPARISON	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Availability	Available for internal clients, which are clients that meet the location criteria specified on the OfficeScan web console	Available mainly for external clients, which are clients that do not meet the location criteria specified on the OfficeScan web console
Purpose	Designed and intended to localize smart protection services to the corporate network to optimize efficiency	A globally scaled, Internet-based infrastructure that provides smart protection services to clients who do not have immediate access to their corporate network
Administration	OfficeScan administrators install and manage these smart protection sources	Trend Micro maintains this source
Pattern update source	Trend Micro ActiveUpdate server	Trend Micro ActiveUpdate server
Client connection protocols	HTTP and HTTPS	HTTPS

Smart Protection Pattern Files

Smart protection pattern files are used for File Reputation Services and Web Reputation Services. Trend Micro releases these pattern files through the Trend Micro ActiveUpdate server.

Smart Scan Agent Pattern

The Smart Scan Agent Pattern is updated daily and is downloaded by the OfficeScan clients' update source (the OfficeScan server or a custom update source). The update source then deploys the pattern to smart scan clients.

Note

Smart scan clients are OfficeScan clients that administrators have configured to use File Reputation Services. Clients that do not use File Reputation Services are called conventional scan clients.

Smart scan clients use the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, another pattern, called Smart Scan Pattern, is leveraged.

Smart Scan Pattern

The Smart Scan Pattern is updated hourly and is downloaded by smart protection sources. Smart scan clients do not download the Smart Scan Pattern. Clients verify potential threats against the Smart Scan Pattern by sending scan queries to smart protection sources.

Web Blocking List

The Web Blocking List is downloaded by smart protection sources. OfficeScan clients that are subject to web reputation policies do not download the Web Blocking List.

Note

Administrators can subject all or several clients to web reputation policies.

Clients subject to web reputation policies verify a website's reputation against the Web Blocking List by sending web reputation queries to a smart protection source. The client correlates the reputation data received from the smart protection source with the web reputation policy enforced on the computer. Depending on the policy, the client will either allow or block access to the site.

Smart Protection Pattern Update Process

Smart protection pattern updates originate from the Trend Micro ActiveUpdate server.

FIGURE 4-1. Pattern update process

Usage of Smart Protection Patterns

An OfficeScan client uses the Smart Scan Agent Pattern to scan for security risks and only queries the Smart Scan Pattern if the Smart Scan Agent Pattern cannot determine the risk of a file. The client queries the Web Blocking List when a user attempts to

access a website. Advanced filtering technology enables the client to "cache" the query results. This eliminates the need to send the same query more than once.

Clients that are currently in your intranet can connect to a Smart Protection Server to query the Smart Scan Pattern or Web Blocking List. Network connection is required to connect to the Smart Protection Server. If more than one Smart Protection Server has been set up, administrators can determine the connection priority.

Tip

Install several Smart Protection Servers to ensure the continuity of protection in the event that connection to a Smart Protection Server is unavailable.

Clients that are currently not in your intranet can connect to Trend Micro Smart Protection Network for queries. Internet connection is required to connect to the Smart Protection Network.

FIGURE 4-2. Query process

Clients without access to the network or the Internet still benefit from protection provided by the Smart Scan Agent Pattern and the cache containing previous query results. The protection is reduced only when a new query is necessary and the client, after repeated attempts, is still unable to reach any smart protection source. In this case, a client flags the file for verification and temporarily allows access to the file. When connection to a smart protection source is restored, all the files that have been flagged are re-scanned. Then, the appropriate scan action is performed on files that have been confirmed as a threat.

The following table summarizes the extent of protection based on the client's location.

TABLE 4-2. Protection Behaviors Based on Location

LOCATION	PATTERN FILE AND QUERY BEHAVIOR
Access to the intranet	• **Pattern file**: Clients download the Smart Scan Agent Pattern file from the OfficeScan server or a custom update source. • **File and web reputation queries**: Clients connect to the Smart Protection Server for queries.
Without access to the intranet but with connection to Smart Protection Network	• **Pattern file**: Clients do not download the latest Smart Scan Agent Pattern file unless connection to an OfficeScan server or a custom update source is available. • **File and web reputation queries**: Clients connect to Smart Protection Network for queries.
Without access to the intranet and without connection to Smart Protection Network	• **Pattern file**: Clients do not download the latest Smart Scan Agent Pattern file unless connection to an OfficeScan server or a custom update source is available. • **File and web reputation queries**: Clients do not receive query results and must rely on the Smart Scan Agent Pattern and the cache containing previous query results.

Setting Up Smart Protection Services

Before clients can leverage File Reputation Services and Web Reputation Services, ensure that the smart protection environment has been properly set up. Check the following:

- *Smart Protection Server Installation on page 4-12*
- *Integrated Smart Protection Server Management on page 4-17*
- *Smart Protection Source List on page 4-23*
- *Client Connection Proxy Settings on page 4-30*
- *Trend Micro Network VirusWall Installations on page 4-30*

Smart Protection Server Installation

You can install the integrated or standalone Smart Protection Server if the number of clients is 1,000 or less. Install a standalone Smart Protection Server if there are more than 1,000 clients.

Trend Micro recommends installing several Smart Protection Servers for failover purposes. Clients that are unable to connect to a particular server will try to connect to the other servers you have set up.

Because the integrated server and the OfficeScan server run on the same computer, the computer's performance may reduce significantly during peak traffic for the two servers. Consider using a standalone Smart Protection Server as the primary smart protection source for clients and the integrated server as a backup.

Standalone Smart Protection Server Installation

For instructions on installing and managing the standalone Smart Protection Server, see the *Smart Protection Server Installation and Upgrade Guide*.

Integrated Smart Protection Server Installation

If you installed the integrated server during OfficeScan server installation:

- Enable the integrated server and configure settings for the server. For details, see *Integrated Smart Protection Server Management on page 4-17*.
- If the integrated server and OfficeScan client exist on the same server computer, consider disabling the OfficeScan firewall. The OfficeScan firewall is intended for client computer use and may affect performance when enabled on server computers. For instructions on disabling the firewall, see *Enabling or Disabling the OfficeScan Firewall on page 12-6*.

Note

Consider the effects of disabling the firewall and ensure that it adheres to your security plans.

Tip

Install the integrated Smart Protection Server after completing the OfficeScan installation by using the *Integrated Smart Protection Server Tool on page 4-13*.

Integrated Smart Protection Server Tool

The Trend Micro OfficeScan Integrated Smart Protection Tool helps administrators to install or uninstall an Integrated Smart Protection Server after the OfficeScan server installation is completed. The current OfficeScan version does not permit administrators to install/remove an Integrated Smart Protection Server once the OfficeScan server installation is complete. This tool enhances the flexibility of installation features from previous versions of OfficeScan.

Before installing the integrated Smart Protection Server, import the following to your upgraded OfficeScan 10.6 SP3 server:

- Domain structures
- The following root and domain level settings:
  - Scan configurations for all scan types (Manual, Real-time, Scheduled, Scan Now)
  - Web reputation settings
  - Behavior Monitoring settings

  - Device Control settings
  - Data Loss Prevention settings
  - Privileges and other settings
  - Additional service settings
  - Spyware/grayware approved list
- Global client settings
- Computer location
- Firewall policies and profiles
- Smart protection sources
- Server update schedule
- Client update source and schedule
- Notifications
- Proxy settings

Procedure

1. Open a command prompt and navigate to the <*Server installation folder*> `\PCCSRV`\Admin\Utility\ISPSInstaller directory where `ISPSInstaller.exe` is located.

2. Run `ISPSInstaller.exe` using one of the following commands:

TABLE 4-3. Installer Options

COMMAND	DESCRIPTION
`ISPSInstaller.exe /i`	Installs the integrated Smart Protection Server using default port settings. For details on the default port settings, see the table below.

Command	Description
`ISPSInstaller.exe /i /f:[port number] /s:[port number] /w:[port number]`	Installs the integrated Smart Protection Server using the ports specified, where: • `/f:[port number]` represents the HTTP file reputation port • `/s:[port number]` represents the HTTPS file reputation port • `/w:[port number]` represents the web reputation port **Note** An unspecified port is automatically assigned the default value.
`ISPSInstaller.exe /u`	Uninstalls the integrated Smart Protection Server

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

Web Server and Settings	Ports for File Reputation Services		HTTP Port for Web Reputation Services
	HTTP	HTTPS (SSL)	
Apache web server with SSL enabled	8080	4343 (not configurable)	8080 (not configurable)
Apache web server with SSL disabled	8080	4345 (not configurable)	8080 (not configurable)
IIS default website with SSL enabled	80	443 (not configurable)	80 (not configurable)
IIS default website with SSL disabled	80	443 (not configurable)	80 (not configurable)
IIS virtual website with SSL enabled	8082	4345 (configurable)	5274 (configurable)

Web Server and Settings	Ports for File Reputation Services		HTTP Port for Web Reputation Services
	HTTP	HTTPS (SSL)	
IIS virtual website with SSL disabled	8082	4345 (configurable)	5274 (configurable)

3. After the installation completes, open the OfficeScan web console and verify the following:
   - Open the **Microsoft Management Console** (by typing `services.msc` in the **Start** menu) and check that the Trend Micro Local Web Classification Server and Trend Micro Smart Scan Server are listed with a "Started" status.
   - Open **Windows Task Manager**. In the **Processes** tab, check that `iCRCService.exe` and `LWCSService.exe` are running,
   - On the OfficeScan web console, check that the menu item **Smart Protection** > **Integrated Server** appears.

Smart Protection Server Best Practices

Optimize the performance of Smart Protection Servers by doing the following:

- Avoid performing Manual Scans and Scheduled Scans simultaneously. Stagger the scans in groups.
- Avoid configuring all clients from performing Scan Now simultaneously.
- Customize Smart Protection Servers for slower network connections, about 512Kbps, by making changes to the `ptngrowth.ini` file.

Customizing ptngrowth.ini for the Standalone Server

Procedure

1. Open the `ptngrowth.ini` file in `/var/tmcss/conf/`.
2. Modify the `ptngrowth.ini` file using the recommended values below:

- `[COOLDOWN]`
- `ENABLE=1`
- `MAX_UPDATE_CONNECTION=1`
- `UPDATE_WAIT_SECOND=360`

3. Save the `ptngrowth.ini` file.
4. Restart the `lighttpd` service by typing the following command from the Command Line Interface (CLI):
   - `service lighttpd restart`

Customizing ptngrowth.ini for the Integrated Server

Procedure

1. Open the `ptngrowth.ini` file in <*Server installation folder*>`\PCCSRV\WSS\`.
2. Modify the `ptngrowth.ini` file using the recommended values below:
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Save the `ptngrowth.ini` file.
4. Restart the `Trend Micro Smart Protection Server` service.

Integrated Smart Protection Server Management

Manage the integrated Smart Protection Server by performing the following tasks:

- Enabling the integrated server's File Reputation Services and Web Reputation Services

- Recording the integrated server's addresses
- Updating the integrated server's components
- Configuring the integrated server's Approved/Blocked URL List
- Configuring the Virtual Analyzer C&C List settings

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-20*.

Enabling the Integrated Server's File Reputation Services and Web Reputation Services

For clients to send scan and web reputation queries to the integrated server, File Reputation Services and Web Reputation Services must be enabled. Enabling these services also allows the integrated server to update components from the ActiveUpdate server.

These services are automatically enabled if you chose to install the integrated server during the OfficeScan server installation.

If you disable the services, be sure that you have installed standalone Smart Protection Servers to which clients can send queries.

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-20*.

Recording the Integrated Server's Addresses

You will need the integrated server's addresses when configuring the smart protection source list for internal clients. For details about the list, see *Smart Protection Source List on page 4-23*.

When clients send scan queries to the integrated server, they identify the server by one of two File Reputation Services addresses - HTTP or HTTPS address. Connection through the HTTPS address allows for a more secure connection while HTTP connection uses less bandwidth.

When clients send web reputation queries, they identify the integrated server by its Web Reputation Services address.

Tip

Clients managed by another OfficeScan server can also connect to this integrated server. On the other OfficeScan server's web console, add the integrated server's address to the Smart Protection Source list.

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-20*.

Updating the Integrated Server's Components

The integrated server updates the following components:

- **Smart Scan Pattern**: Clients verify potential threats against the Smart Scan Pattern by sending scan queries to the integrated server.
- **Web Blocking List**: Clients subject to web reputation policies verify a website's reputation against the Web Blocking List by sending web reputation queries to the integrated server.

You can manually update these components or configure an update schedule. The integrated server downloads the components from the ActiveUpdate server.

Note

A pure IPv6 integrated server cannot update directly from Trend Micro ActiveUpdate Server. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the integrated server to connect to the ActiveUpdate server.

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-20*.

Integrated Server's Approved/Blocked URL List Configuration

Clients maintain their own approved/blocked URL list. Configure the list for clients when you set up web reputation policies (see *Web Reputation Policies on page 11-5* for details). Any URL in the client's list will automatically be allowed or blocked.

The integrated server has its own approved/blocked URL list. If a URL is not in the client's list, the client sends a web reputation query to the integrated server (if the

integrated server has been assigned as a smart protection source). If the URL is found in the integrated server's approved/blocked URL list, the integrated server notifies the client to allow or block the URL.

Note

The blocked URL list has a higher priority than the Web Blocking List.

To add URLs to the integrated server's approved/blocked list, import a list from a standalone Smart Protection Server. It is not possible to add URLs manually.

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-20*.

Deep Discovery Advisor and Virtual Analyzer Connection Settings

Configure the Virtual Analyzer C&C list settings to establish a connection between the integrated Smart Protection Server and the Deep Discovery Advisor server. The Deep Discovery Advisor's virtual analyzer creates the Virtual Analyzer C&C list which the Smart Protection Server stores for use by OfficeScan.

After establishing a successful connection to the Deep Discovery Advisor server, enable the Virtual Analyzer C&C list to monitor C&C callbacks made to servers previously identified by other clients on the network.

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-20*.

Configuring Integrated Smart Protection Server Settings

Procedure

1. Navigate to **Smart Protection** > **Integrated Server**.
2. Select **Enable File Reputation Services**.
3. Select the protocol (HTTP or HTTPS) that clients will use when sending scan queries to the integrated server.
4. Select **Enable Web Reputation Services**.

5. Record the integrated server's addresses found under the Server Address column.

6. To update the integrated server's components:

   - View the current versions of the Smart Scan Pattern and Web Blocking List. If an update is available, click **Update Now**. The update result displays on top of the screen.

   - To update the pattern automatically:

     a. Select **Enable scheduled updates**.

     b. Choose whether to update hourly or every 15 minutes.

     c. Select an update source under **File Reputation Services**. The Smart Scan Pattern will be updated from this source.

     d. Select an update source under **Web Reputation Services**. The Web Blocking List will be updated from this source.

Note

- If you choose the ActiveUpdate server as the update source, ensure that the server has Internet connection and, if you are using a proxy server, test if Internet connection can be established using the proxy settings. See *Proxy for OfficeScan Server Updates on page 6-17* for details.

- If you choose a custom update source, set up the appropriate environment and update resources for this update source. Also ensure that there is a functional connection between the server computer and this update source. If you need assistance setting up an update source, contact your support provider.

7. To configure the integrated server's Approved/Blocked List:

   a. Click **Import** to populate the list with URLs from a pre-formatted `.csv` file. You can obtain the `.csv` file from a standalone Smart Protection Server.

   b. If you have an existing list, click **Export** to save the list to a `.csv` file.

8.

Note

- Contact the Deep Discovery Advisor administrator to obtain the server name or IP address, port number, and a valid API key.
- This version of OfficeScan only supports Deep Discovery Advisor 3.0 and later.

To configure the Deep Discovery Advisor server's Virtual Analyzer connection:

a. Type the server name or IP address of the Deep Discovery Advisor server.

Note

The server name supports FQDN formats and the IP address supports IPv4 format. The server address only supports HTTPS protocol.

b. Type the API key.

c. Click **Register** to connect to the Deep Discovery Advisor server.

Note

Administrators can test the connection to the server before registering to the server.

d. Select **Enable Virtual Analyzer C&C list** to allow OfficeScan to use the custom C&C list analyzed by the local Deep Discovery Advisor server.

Note

The **Enable Virtual Analyzer C&C list** option is only available after establishing a successful connection to the Deep Discovery Advisor server.

Administrators can manually synchronize with the Deep Discovery Advisor at any time by clicking the **Sync Now** button.

9. Click **Save**.

Smart Protection Source List

Clients send queries to smart protection sources when scanning for security risks and determining a website's reputation.

IPv6 Support for Smart Protection Sources

A pure IPv6 client cannot send queries directly to pure IPv4 sources, such as:

- Smart Protection Server 2.0 (integrated or standalone)

  Note

  IPv6 support for Smart Protection Server starts in version 2.5.

- Trend Micro Smart Protection Network

Similarly, a pure IPv4 client cannot send queries to pure IPv6 Smart Protection Servers.

A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow clients to connect to the sources.

Smart Protection Sources and Computer Location

The smart protection source to which the client connects depends on the client computer's location.

For details on configuring location settings, see *Computer Location on page 14-2*.

TABLE 4-5. Smart Protection Sources by Location

LOCATION	SMART PROTECTION SOURCES
External	External clients send scan and web reputation queries to Trend Micro Smart Protection Network.

LOCATION	SMART PROTECTION SOURCES
Internal	Internal clients send scan and web reputation queries to Smart Protection Servers or Trend Micro Smart Protection Network. If you have installed Smart Protection Servers, configure the smart protection source list on the OfficeScan web console. An internal client picks a server from the list if it needs to make a query. If a client is unable to connect to the first server, it picks another server on the list. **Tip** Assign a standalone Smart Protection Server as the primary scan source and the integrated server as a backup. This reduces the traffic directed to the computer that hosts the OfficeScan server and integrated server. The standalone server can also process more queries. You can configure either the standard or custom list of smart protection sources. The standard list is used by all internal clients. A custom list defines an IP address range. If an internal client's IP address is within the range, the client uses the custom list.

Configuring the Standard List of Smart Protection Sources

Procedure

1. Navigate to **Smart Protection** > **Smart Protection Sources**.
2. Click the **Internal Clients** tab.
3. Select **Use the standard list (list will be used by all internal clients)**.
4. Click the **standard list** link.

   A new screen opens.
5. Click **Add**.

   A new screen opens.
6. Specify the Smart Protection Server's host name or IPv4/IPv6 address. If you specify an IPv6 address, enclose it in parentheses.

Note

Specify the host name if there are IPv4 and IPv6 clients connecting to the Smart Protection Server.

7. Select File Reputation Services. Clients send scan queries using the HTTP or HTTPS protocol. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

   a. If you want clients to use HTTP, type the server's listening port for HTTP requests. If you want clients to use HTTPS, select SSL and type the server's listening port for HTTPS requests.

   b. Click **Test Connection** to check if connection to the server can be established.

Tip

The listening ports form part of the server address. To obtain the server address:

For the integrated server, open the OfficeScan web console and go to **Smart Protection** > **Integrated Server**.

For the standalone server, open the standalone server's console and go to the **Summary** screen.

8. Select **Web Reputation Services**. Clients send web reputation queries using the HTTP protocol. HTTPS is not supported.

   a. Type the server's listening port for HTTP requests.

   b. Click **Test Connection** to check if connection to the server can be established.

9. Click **Save**.

   The screen closes.

10. Add more servers by repeating the previous steps.

11. On top of the screen, select **Order** or **Random**.

    - **Order**: Clients pick servers in the order in which they appear on the list. If you select **Order**, use the arrows under the **Order** column to move servers up and down the list.

- **Random**: Clients pick servers randomly.

Tip

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

12. Perform miscellaneous tasks on the screen.
    - If you have exported a list from another server and want to import it to this screen, click **Import** and locate the `.dat` file. The list loads on the screen.
    - To export the list to a `.dat` file, click **Export** and then click **Save**.
    - To refresh the service status of servers, click **Refresh**.
    - Click the server name to do one of the following:
      - To view or edit server information.
      - View the full server address for Web Reputation Services or File Reputation Services.
    - To open the console of a Smart Protection Server, click **Launch console**.
      - For the integrated Smart Protection Server, the server's configuration screen displays.
      - For standalone Smart Protection Servers and the integrated Smart Protection Server of another OfficeScan server, the console logon screen displays.
    - To delete an entry, select the check box for the server and click **Delete**.
13. Click **Save**.

    The screen closes.
14. Click **Notify All Clients**.

Configuring Custom Lists of Smart Protection Sources

Procedure

1. Navigate to **Smart Protection** > **Smart Protection Sources**.
2. Click the **Internal Clients** tab.
3. Select **Use custom lists based on client IP addresses**.
4. (Optional) Select U**se the standard list when all servers on the custom lists are unavailable**.
5. Click **Add**.

   A new screen opens.
6. In the **IP range** section, specify an IPv4 or IPv6 address range, or both.

   Note

   Clients with an IPv4 address can connect to pure IPv4 or dual-stack Smart Protection Servers. Clients with an IPv6 address can connect to pure IPv6 or dual-stack Smart Protection Servers. Clients with both IPv4 and IPv6 addresses can connect to any Smart Protection Server.
7. In the **Proxy Setting** section, specify proxy settings clients will use to connect to the Smart Protection Servers.
   a. Select **Use a proxy server for client and Smart Protection Server communication**.
   b. Specify the proxy server name or IPv4/IPv6 address, and port number.
   c. If the proxy server requires authentication, type the user name and password.
8. In the **Custom Smart Protection Server List**, add the Smart Protection Servers.
   a. Specify the Smart Protection Server's host name or IPv4/IPv6 address. If you specify an IPv6 address, enclose it in parentheses.

Note

Specify the host name if there are IPv4 and IPv6 clients connecting to the Smart Protection Server.

b. Select **File Reputation Services**. Clients send scan queries using the HTTP or HTTPS protocol. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

   i. If you want clients to use HTTP, type the server's listening port for HTTP requests. If you want clients to use HTTPS, select **SSL** and type the server's listening port for HTTPS requests.

   ii. Click **Test Connection** to check if connection to the server can be established.

Tip

The listening ports form part of the server address. To obtain the server address:

For the integrated server, open the OfficeScan web console and go to **Smart Protection** > **Integrated Server**.

For the standalone server, open the standalone server's console and go to the Summary screen.

c. Select **Web Reputation Services**. Clients send web reputation queries using the HTTP protocol. HTTPS is not supported.

   i. Type the server's listening port for HTTP requests.

   ii. Click **Test Connection** to check if connection to the server can be established.

d. Click **Add to the List**.

e. Add more servers by repeating the previous steps.

f. Select **Order** or **Random**.

   - **Order**: Clients pick servers in the order in which they appear on the list. If you select **Order**, use the arrows under the **Order** column to move servers up and down the list.

- **Random**: Clients pick servers randomly.

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

g. Perform miscellaneous tasks in the screen.

- To refresh the service status of servers, click **Refresh**.
- To open the console of a Smart Protection Server, click **Launch console**.
  - For the integrated Smart Protection Server, the server's configuration screen displays.
  - For standalone Smart Protection Servers and the integrated Smart Protection Server of another OfficeScan server, the console logon screen displays.
- To delete an entry, click **Delete** (Delete).

9. Click **Save**.

   The screen closes. The list you just added appears as an IP range link under the **IP Range** table.

10. Repeat step 4 to step 8 to add more custom lists.

11. Perform miscellaneous tasks in the screen.

    - To modify a list, click the IP range link and then modify the settings in the screen that opens.
    - To export the list to a .dat file, click **Export** and then click **Save**.
    - If you have exported a list from another server and want to import it to this screen, click **Import** and locate the `.dat` file. The list loads on the screen.

12. Click **Notify All Clients**.

Client Connection Proxy Settings

If connection to the Smart Protection Network requires proxy authentication, specify authentication credentials. For details, see *External Proxy for OfficeScan Clients on page 14-47*.

Configure internal proxy settings that clients will use when connecting to a Smart Protection Server. For details, see *Internal Proxy for OfficeScan Clients on page 14-46*.

Computer Location Settings

OfficeScan includes a location awareness feature that identifies the client computer's location and determines whether the client connects to the Smart Protection Network or Smart Protection Server. This ensures that clients remain protected regardless of their location.

To configure location settings, see *Computer Location on page 14-2*.

Trend Micro Network VirusWall Installations

If you have Trend Micro™ Network VirusWall™ Enforcer installed:

- Install a hot fix (build 1047 for Network VirusWall Enforcer 2500 and build 1013 for Network VirusWall Enforcer 1200).
- Update the OPSWAT engine to version 2.5.1017 to enable the product to detect a client's scan method.

Using Smart Protection Services

After the smart protection environment has been properly set up, clients are ready to use File Reputation Services and Web Reputation Services. You can also begin to configure Smart Feedback settings.

Note

For instructions on setting up the smart protection environment, see *Setting Up Smart Protection Services on page 4-12*.

To benefit from protection provided by File Reputation Services, clients must use the scan method called smart scan. For details about smart scan and how to enable smart scan on clients, see *Scan Methods on page 7-7*.

To allow OfficeScan clients to use Web Reputation Services, configure web reputation policies. For details, see *Web Reputation Policies on page 11-5*.

Note

Settings for scan methods and web reputation policies are granular. Depending on your requirements, you can configure settings that will apply to all clients or configure separate settings for individual clients or client groups.

For instructions on configuring Smart Feedback, see *Smart Feedback on page 13-47*.

Chapter 5

Installing the OfficeScan Client

This chapter describes Trend Micro™ OfficeScan™ system requirements and OfficeScan client installation procedures.

For details on upgrading OfficeScan client, see the *OfficeScan Installation and Upgrade Guide*.

Topics in this chapter:

- *OfficeScan Client Fresh Installations on page 5-2*
- *Installation Considerations on page 5-2*
- *Deployment Considerations on page 5-10*
- *Migrating to the OfficeScan Client on page 5-61*
- *Post-installation on page 5-65*
- *OfficeScan Client Uninstallation on page 5-68*

OfficeScan Client Fresh Installations

The OfficeScan client can be installed on computers running Microsoft Windows platforms. OfficeScan is also compatible with various third-party products.

Visit the following website for a complete list of system requirements and compatible third-party products:

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

Installation Considerations

Before installing clients, consider the following:

- **OfficeScan client features**: Some client features are not available on certain Windows platforms.
- **IPv6 support**: The OfficeScan client can be installed on dual-stack or pure IPv6 clients. However:
  - Some of the Windows operating systems to which the OfficeScan client can be installed do not support IPv6 addressing.
  - For some of the installation methods, there are special requirements to install the OfficeScan client successfully.
- **OfficeScan client IP addresses**: For clients with both IPv4 and IPv6 addresses, you can choose which IP address will be used when the client registers to the server.
- **Exception lists**: Ensure that exception lists for the following features have been configured properly:
  - **Behavior Monitoring**: Add critical computer applications to the Approved Programs list to prevent the OfficeScan client from blocking these applications. For more information, see *Behavior Monitoring Exception List on page 8-5*.

- **Web Reputation**: Add websites that you consider safe to the Approved URL List to prevent the OfficeScan client from blocking access to the websites. For more information, see *Web Reputation Policies on page 11-5*.

OfficeScan Client Features

The OfficeScan client features available on a computer depend on the computer's operating system.

TABLE 5-1. OfficeScan client Features on Server Platforms

FEATURE	WINDOWS OPERATING SYSTEM		
	SERVER 2003	SERVER 2008/ SERVER CORE 2008	SERVER 2012/ SERVER CORE 2012
Manual Scan, Real-time Scan, and Scheduled Scan	Yes	Yes	Yes
Component update (manual and scheduled update)	Yes	Yes	Yes
Update Agent	Yes	Yes	Yes
Web reputation	Yes but disabled by default during server installation	Yes but disabled by default during server installation	Yes but disabled by default during server installation and limited support for Windows UI mode
Damage Cleanup Services	Yes	Yes	Yes
OfficeScan firewall	Yes but disabled by default during server installation	Yes but disabled by default during server installation	Yes but disabled by default during server installation and Application Filtering not supported

Feature	Windows Operating System		
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012
Behavior Monitoring	Yes (32-bit) but disabled by default	Yes (32-bit) but disabled by default	Yes (64-bit) but disabled by default
	No (64-bit)	Yes (64-bit) but disabled by default	
Client Self-protection for: • Registry keys • Processes	Yes (32-bit) but disabled by default	Yes (32-bit) but disabled by default	Yes (64-bit) but disabled by default
	No (64-bit)	Yes (64-bit) but disabled by default	
Client Self-protection for: • Services • File protection	Yes	Yes	Yes
Device Control (Unauthorized Change Prevention service)	Yes (32-bit) but disabled by default	Yes (32-bit) but disabled by default	Yes (64-bit) but disabled by default
	No (64-bit)	Yes (64-bit) but disabled by default	
Data Protection (including Data Protection for Device Control)	Yes (32-bit) but disabled by default	Yes (32-bit) but disabled by default	Yes (64-bit) but disabled by default
	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	
Microsoft Outlook mail scan	Yes (32-bit)	No	No
	No (64-bit)		
POP3 mail scan	Yes	Yes	Yes
Support for Cisco NAC	No	No	No
Client Plug-in Manager	Yes	Yes	Yes

Feature	Windows Operating System		
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012
Roaming mode	Yes	Yes (Server) No (Server Core)	Yes
SecureClient support	Yes (32-bit)	No	No
	No (64-bit)		
Smart Feedback	Yes	Yes	Yes

Table 5-2. OfficeScan client Features on Desktop Platforms

Feature	Windows Operating System			
	XP	Vista	Windows 7	Windows 8
Manual Scan, Real-time Scan, and Scheduled Scan	Yes	Yes	Yes	Yes
Component update (manual and scheduled update)	Yes	Yes	Yes	Yes
Update Agent	Yes	Yes	Yes	Yes
Web reputation	Yes	Yes	Yes	Yes but only limited support for Windows UI mode
Damage Cleanup Services	Yes	Yes	Yes	Yes
OfficeScan firewall	Yes	Yes	Yes	Yes but Application Filtering not supported

Feature	Windows Operating System			
	XP	Vista	Windows 7	Windows 8
Behavior Monitoring	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)
	No (64-bit)	Yes (64-bit) Vista 64-bit support requires SP1 or SP2	Yes (64-bit)	Yes (64-bit)
Client Self-protection for: • Registry keys • Processes	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)
	No (64-bit)	Yes (64-bit) Vista 64-bit support requires SP1 or SP2	Yes (64-bit)	Yes (64-bit)
Client Self-protection for: • Services • File protection	Yes	Yes	Yes	Yes
Device Control (Unauthorized Change Prevention service)	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)
	No (64-bit)	Yes (64-bit) Vista 64-bit support requires SP1 or SP2	Yes (64-bit)	Yes (64-bit)
Data Protection (including Data Protection for Device Control)	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)	Yes (32-bit) in desktop mode
	Yes (64-bit)	Yes (64-bit)	Yes (64-bit)	Yes (64-bit) in desktop mode
Microsoft Outlook mail scan	Yes (32-bit)	No	No	No
	No (64-bit)			

Feature	Windows Operating System			
	XP	Vista	Windows 7	Windows 8
POP3 mail scan	Yes	Yes	Yes	Yes
Support for Cisco NAC	Yes	No	No	No
Client Plug-in Manager	Yes	Yes	Yes	Yes
Roaming mode	Yes	Yes	Yes	Yes
SecureClient support	Yes (32-bit)	No	No	No
	No (64-bit)			
Smart Feedback	Yes	Yes	Yes	Yes

OfficeScan Client Installation and IPv6 Support

This topic discusses considerations when installing the OfficeScan client to dual-stack or pure IPv6 clients.

Operating System

The OfficeScan client can only be installed on the following operating systems that support IPv6 addressing:

- Windows Vista™ (all editions)
- Windows Server 2008 (all editions)
- Windows 7 (all editions)
- Windows Server 2012 (all editions)
- Windows 8 (all editions)

Visit the following website for a complete list of system requirements:

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

Installation Methods

All of the OfficeScan client installation methods can be used to install the OfficeScan client on pure IPv6 or dual-stack clients. For some installation methods, there are special requirements to install the OfficeScan client successfully.

It is not possible to migrate ServerProtect™ to the OfficeScan client using the ServerProtect Normal Server Migration Tool because the tool does not support IPv6 addressing.

TABLE 5-3. Installation Methods and IPv6 Support

INSTALLATION METHOD	REQUIREMENTS/CONSIDERATIONS
Web install page and browser-based installation	The URL to the installation page includes the OfficeScan server's host name or its IP address. If you are installing to a pure IPv6 client, the server must be dual-stack or pure IPv6 and its host name or IPv6 address must be part of the URL. For dual-stack clients, the IPv6 address that displays in the installation status screen depends on the option selected in the **Preferred IP Address** section of **Networked Computers** > **Global Client Settings**.
Client Packager	When running the packager tool, you will need to choose whether to assign Update Agent privileges to the client. Remember that a pure IPv6 Update Agent can distribute updates only to pure IPv6 or dual-stack clients.
Security Compliance, Vulnerability Scanner, and remote installation	A pure IPv6 server cannot install the OfficeScan client on pure IPv4 endpoints. Similarly, a pure IPv4 server cannot install the OfficeScan client on pure IPv6 endpoints.

Client IP Addresses

An OfficeScan server installed in an environment that supports IPv6 addressing can manage the following OfficeScan clients:

- An OfficeScan server installed on a pure IPv6 host machine can manage pure IPv6 clients.
- An OfficeScan server installed on a dual-stack host machine and has been assigned both IPv4 and IPv6 addresses can manage pure IPv6, dual-stack, and pure IPv4 clients.

After you install or upgrade clients, the clients register to the server using an IP address.

- Pure IPv6 clients register using their IPv6 address.
- Pure IPv4 clients register using their IPv4 address.
- Dual-stack clients register using either their IPv4 or IPv6 address. You can choose the IP address that these clients will use.

Configuring the IP Address that Dual-stack Clients Use When Registering to the Server

This setting is only available on dual-stack OfficeScan servers and is applied only by dual-stack clients.

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Go to the **Preferred IP Address** section.
3. Choose from the following options:
   - **IPv4 only**: Clients use their IPv4 address.
   - **IPv4 first, then IPv6**: Clients use their IPv4 address first. If the client cannot register using its IPv4 address, it uses its IPv6 address. If registration is unsuccessful using both IP addresses, the client retries using the IP address priority for this selection.

- **IPv6 first, then IPv4**: Clients use their IPv6 address first. If the client cannot register using its IPv6 address, it uses its IPv4 address. If registration is unsuccessful using both IP addresses, the client retries using the IP address priority for this selection.

4. Click **Save**.

Deployment Considerations

This section provides a summary of the different OfficeScan client installation methods to perform a fresh installation of the OfficeScan client. All installation methods require local administrator rights on the target computers.

If you are installing clients and want to enable IPv6 support, read the guidelines in *OfficeScan Client Installation and IPv6 Support on page 5-7*.

TABLE 5-4. Deployment Considerations for Installation

Installation Method/ Operating System Support	Deployment Considerations					
	WAN Deployment	Centrally Managed	Requires User Intervention	Requires IT Resource	Mass deployment	Bandwidth Consumed
Web install page Supported on all operating systems except Windows Server Core 2008 and Windows 8/ Server 2012/ Server Core 2012 in Windows UI mode	No	No	Yes	No	No	High

Installation Method/ Operating System Support	Deployment Considerations					
	WAN Deployment	Centrally Managed	Requires User Intervention	Requires IT Resource	Mass deployment	Bandwidth Consumed
From the Initiate Browser-based Installation page Supported on all operating systems **Note** Not supported on Windows 8 or Windows Server 2012 operating in Windows UI mode.	No	No	Yes	Yes	No	High, if installations start at the same time
UNC-based Installations Supported on all operating systems	No	No	Yes	Yes	No	High, if installations start at the same time

Installation Method/ Operating System Support	Deployment Considerations					
	WAN Deployment	Centrally Managed	Requires User Intervention	Requires IT Resource	Mass deployment	Bandwidth Consumed
From the Remote Installation page Supported on all operating systems except: • Windows Vista Home Basic and Home Premium Editions • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8 (basic versions)	No	Yes	No	Yes	No	High
Login Script Setup Supported on all operating systems	No	No	Yes	Yes	No	High, if installations start at the same time
Client Packager Supported on all operating systems	No	No	Yes	Yes	No	Low, if scheduled

Installation Method/ Operating System Support	Deployment Considerations					
	WAN Deployment	Centrally Managed	Requires User Intervention	Requires IT Resource	Mass deployment	Bandwidth Consumed
Client Packager (MSI package deployed through Microsoft SMS) Supported on all operating systems	Yes	Yes	Yes/No	Yes	Yes	Low, if scheduled
Client Packager (MSI package deployed through Active Directory) Supported on all operating systems	Yes	Yes	Yes/No	Yes	Yes	High, if installations start at the same time
Client disk image Supported on all operating systems	No	No	No	Yes	No	Low

Installation Method/ Operating System Support	Deployment Considerations					
	WAN Deployment	Centrally Managed	Requires User Intervention	Requires IT Resource	Mass deployment	Bandwidth Consumed
Trend Micro Vulnerability Scanner (TMVS) Supported on all operating systems except: • Windows Vista Home Basic and Home Premium Editions • Windows XP Home Edition • Windows 8 (basic versions)	No	Yes	No	Yes	No	High

Installation Method/ Operating System Support	Deployment Considerations					
	WAN Deployment	Centrally Managed	Requires User Intervention	Requires IT Resource	Mass deployment	Bandwidth Consumed
Security Compliance Installations Supported on all operating systems except: • Windows Vista Home Basic and Home Premium Editions • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8 (basic versions)	No	Yes	No	Yes	No	High

Web Install Page Installations

Users can install the OfficeScan client program from the web install page if you installed the OfficeScan server to a computer running the following platforms:

- Windows Server 2003 with Internet Information Server (IIS) 6.0 or Apache 2.0.x
- Windows Server 2008 with Internet Information Server (IIS) 7.0
- Windows Server 2008 R2 with Internet Information Server (IIS) 7.5
- Windows Server 2012 with Internet Information Server (IIS) 8.0

To install from the web install page, you need the following:

- Internet Explorer with the security level set to allow ActiveX™ controls. The required versions are as follows:
  - 6.0 on Windows XP and Windows Server 2003
  - 7.0 on Windows Vista and Windows Server 2008
  - 8.0 on Windows 7
  - 10.0 on Windows 8 and Windows Server 2012
- Administrator privileges on the computer

Send the following instructions to users to install the OfficeScan client from the web install page. To send an OfficeScan client installation notification through email, see *Initiating a Browser-based Installation on page 5-18*.

Installing from the Web Install Page

Procedure

1. Log on to the computer using a built-in administrator account.

   Note

   For Windows 7 or 8 platforms, you have to enable the built-in administrator account first. Windows 7 and 8 disable the built-in administrator account by default. For more information, refer to the Microsoft support site (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).

2. If installing to a computer running Windows XP, Vista, Server 2008, 7, 8, or Server 2012, perform the following steps:

   a. Launch Internet Explorer and add the OfficeScan server URL (such as `https://<OfficeScan server name>:4343/officescan`) to the list of trusted sites. In Windows XP Home, access the list by going to **Tools** > **Internet Options** > **Security** tab, selecting the **Trusted Sites** icon, and clicking **Sites**.

b. Modify the Internet Explorer security setting to enable **Automatic prompting for ActiveX controls**. On Windows XP, go to **Tools** > **Internet Options** > **Security** tab, and click **Custom level**.

3. Open an Internet Explorer window and type one of the following:

   - OfficeScan server with SSL:

     ```
     https://<OfficeScan server name>:<port>/officescan
     ```

   - OfficeScan server without SSL:

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

4. Click the link on the logon page.

5. In the new screen that displays, click **Install Now** to start installing the OfficeScan client. The OfficeScan client installation starts. Allow ActiveX control installation when prompted. The OfficeScan client icon appears in the Windows system tray after installation.

Note

For a list of icons that display on the system tray, see *OfficeScan Client Icons on page 14-24*.

Browser-based Installation

Set up an email message that instructs users on the network to install the OfficeScan client. Users click the OfficeScan client installer link provided in the email to start the installation.

Before you install OfficeScan clients:

- Check the OfficeScan client installation requirements.
- Identify which computers on the network currently do not have protection against security risks. Perform the following tasks:

- Run the Trend Micro Vulnerability Scanner. This tool analyzes computers for installed antivirus software based on an IP address range you specify. For details, see *Vulnerability Scanner Usage on page 5-37*.
- Run Security Compliance. For details, see *Security Compliance for Unmanaged Endpoints on page 14-65*.

Initiating a Browser-based Installation

Procedure

1. Navigate to **Networked Computers** > **Client Installation** > **Browser-based**.
2. Modify the subject line of the email message if necessary.
3. Click **Create Email.**

   The default mail program opens.
4. Send the email to the intended recipients.

Performing a UNC-based Installation

`AutoPcc.exe` is a standalone program that installs the OfficeScan client to unprotected computers and updates program files and components. Computers must be part of the domain to be able to use AutoPcc using a Uniform Naming Convention (UNC) path.

Procedure

1. Navigate to **Networked Computers** > **Client Installation** > **UNC-based**.
   - To install the OfficeScan client to an unprotected computer using `AutoPcc.exe`:
     a. Connect to the server computer. Navigate to the UNC path:

     ```
     \\<server computer name>\ofscan
     ```

b. Right-click `AutoPcc.exe` and select **Run as administrator**.

- For remote desktop installations using `AutoPcc.exe`:

  a. Open a Remote Desktop Connection (Mstsc.exe) in console mode. This forces the `AutoPcc.exe` installation to run in session 0.

  b. Navigate to the `\\<server computer name>\ofscan` directory and execute `AutoPcc.exe`.

Installing Remotely from the OfficeScan Web Console

Install the OfficeScan client remotely to one or several computers connected to the network. Ensure you have administrator rights to the target computers to perform remote installation. Remote installation does not install the OfficeScan client on a computer already running the OfficeScan server.

Note

This installation method cannot be used on computers running Windows XP Home, Windows Vista Home Basic and Home Premium Editions, Windows 7 Home Basic and Home Premium Editions (32-bit and 64-bit versions), and Windows 8 (32-bit and 64-bit basic versions). A pure IPv6 server cannot install the OfficeScan client on pure IPv4 clients. Similarly, a pure IPv4 server cannot install the OfficeScan client on pure IPv6 clients.

Procedure

1. If running Windows Vista, Windows 7, Windows 8 (Pro, Enterprise), or Windows Server 2012, perform the following steps:

   a. Enable a built-in administrator account and set the password for the account.

   b. Disable simple file sharing on the endpoint.

   c. Click **Start** > **Programs** > **Administrative Tools** > **Windows Firewall with Advanced Security**.

   d. For Domain Profile, Private Profile, and Public Profile, set the firewall state to "Off".

e. Open Microsoft Management Console (click **Start** > **Run** and type `services.msc`) and start the **Remote Registry** and **Remote Procedure Call** services. When installing the OfficeScan client, use the built-in administrator account and password.

2. In the web console, go to **Networked Computers** > **Client Installation** > **Remote**.

3. Select the target computers.

   - The **Domains and Computers** list displays all the Windows domains on the network. To display computers under a domain, double-click the domain name. Select a computer, and then click **Add**.

   - If you have a specific computer name in mind, type the computer name in the field on top of the page and click **Search**.

   OfficeScan prompts you for the target computer's user name and password. Use an administrator account user name and password to continue.

4. Type the user name and password, and then click **Log in**.

   The target computer appears in the **Selected Computers** table.

5. Repeat steps 3 and 4 to add more computers.

6. Click **Install** when you are ready to install the OfficeScan client to target computers.

   A confirmation box appears.

7. Click **Yes** to confirm that you want to install the OfficeScan client to the target computers.

   A progress screen appears as the program files copy to each target computer.

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

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

Note

If you install to multiple computers, OfficeScan records any unsuccessful installation in the logs (for details, see *Fresh Installation Logs on page 18-16*), but it will not postpone the other installations. You do not have to supervise the installation after you click **Install**. Check the logs later to see the installation results.

Installing with Login Script Setup

Login Script Setup automates the installation of the OfficeScan client to unprotected computers when they log on to the network. Login Script Setup adds a program called `AutoPcc.exe` to the server login script.

`AutoPcc.exe` installs the OfficeScan client to unprotected computers and updates program files and components. Computers must be part of the domain to be able to use AutoPcc through the login script.

OfficeScan Client Installation

`AutoPcc.exe` automatically installs the OfficeScan client to an unprotected Windows Server 2003 computer when the computer logs on to the server whose login scripts you modified. However, `AutoPcc.exe` does not automatically install the OfficeScan client to Windows Vista, 7, 8, Server 2008, and Server 2012 computers. Users need to connect to the server computer, navigate to `\\<server computer name>\ofcscan`, right-click `AutoPcc.exe`, and select **Run as administrator**.

For remote desktop installation using `AutoPcc.exe`:

- The computer must be run in `Mstsc.exe /console mode`. This forces the `AutoPcc.exe` installation to run in session 0.
- Map a drive to the "ofcscan" folder and execute `AutoPcc.exe` from that point.

Program and Component Updates

`AutoPcc.exe` updates the program files and the antivirus, anti-spyware, and Damage Cleanup Services components.

The Windows Server 2003, 2008, and 2012 Scripts

If you already have an existing login script, Login Script Setup appends a command that executes `AutoPcc.exe`. Otherwise, OfficeScan creates a batch file called `ofcscan.bat` that contains the command to run `AutoPcc.exe`.

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

```
\\<Server_name>\ofcscan\autopcc
```

Where:

- `<Server_name>` is the computer name or IP address of the OfficeScan server computer.
- "`ofcscan`" is the OfficeScan shared folder name on the server.
- "`autopcc`" is the link to the autopcc executable file that installs the OfficeScan client.

Login script location (through a net logon shared directory):

- `Windows Server 2003: \\Windows 2003 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2008: \\Windows 2008 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2012: \\Windows 2012 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

Adding Autopcc.exe to the Login Script Using Login Script Setup

---

Procedure

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

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

2. Locate the server whose login script you want to modify, select it, and then click **Select**. Ensure that the server is a primary domain controller and that you have administrator access to the server.

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

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

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

4. To modify the login script for a user profile, select the user profile from the Users list, and then click **Add**.

5. To modify the login script of all users, click **Add All**.

6. To exclude a user profile that you previously selected, select the name from the **Selected users** list, and click **Delete**.

7. To reset your choices, click **Delete All**.

8. Click **Apply** when all target user profiles are in the **Selected users** list.

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

9. Click **OK**.

   Login Script Setup returns to its initial screen.

10. To modify the login scripts of other servers, repeat steps 2 to 4.

11. To close Login Script Setup, click **Exit**.

Installing with Client Packager

Client Packager creates an installation package that you can send to users using conventional media such as CD-ROM. Users run the package on the client computer to install or upgrade the OfficeScan client and update components.

Client Packager is especially useful when deploying the OfficeScan client or components to clients in low-bandwidth remote offices. OfficeScan clients installed using Client Packager report to the server where the package was created.

Client Packager requires the following:

- 350MB free disk space
- Windows Installer 2.0 (to run an MSI package)

Creating an Installation Package Using Client Packager

Procedure

1. On the OfficeScan server computer, browse to <*Server installation folder*> `\PCCSRV\Admin\Utility\ClientPackager`.
2. Double-click `ClnPack.exe` to run the tool. The Client Packager console opens.
3. Select the type of package you want to create.

TABLE 5-5. Client Package Types

PACKAGE TYPE	DESCRIPTION
Setup	Select **Setup** to create the package as an executable file. The package installs the OfficeScan client program with the components currently available on the server. If the target computer has an earlier OfficeScan client version installed, running the executable file upgrades the client.
Update	Select **Update** to create a package that contains the components currently available on the server. The package will be created as an executable file. Use this package if there are issues updating components on a client computer.

Package Type	Description
MSI	Select **MSI** to create a package that conforms to the Microsoft Installer Package format. The package also installs the OfficeScan client program with the components currently available on the server. If the target computer has an earlier OfficeScan client version installed, running the MSI file upgrades the client.

4. Configure the following settings (some settings are only available if you select a particular package type):

   - *Windows Operating System Type on page 5-26*
   - *Scan Method on page 5-26*
   - *Silent Mode on page 5-28*
   - *Disable Prescan on page 5-28*
   - *Force Overwrite with Latest Version on page 5-28*
   - *Update Agent Capabilities on page 5-28*
   - *Outlook Mail Scan on page 5-29*
   - *Check Point SecureClient Support on page 5-30*
   - *Components on page 5-30*

5. Next to **Source file**, ensure that the location of the `ofcscan.ini` file is correct. To modify the path, click (...) to browse for the `ofcscan.ini` file. By default, this file is in the `<Server installation folder>\PCCSRV` folder of the OfficeScan server.

6. In Output file, click (...), specify where you want to create the OfficeScan client package, and type the package file name (for example, `ClientSetup.exe`).

7. Click **Create**.

   After Client Packager creates the package, the message "Package created successfully" appears. Locate the package in the directory that you specified in the previous step.

8. Deploy the package.

Package Deployment Guidelines

1. Send the package to users and ask them to run the OfficeScan client package on their computers by double-clicking the `.exe` or `.msi` file.

   Note

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

2. If you have users who will install the `.exe` package on computers running Windows Vista, Server 2008, 7, 8, or Server 2012, instruct them to right-click the `.exe` file and select **Run as administrator**.

3. If you created an `.msi` file, deploy the package by performing the following tasks:

   - Use Active Directory or Microsoft SMS. See *Deploying an MSI Package Using Active Directory on page 5-30* or *Deploying an MSI Package Using Microsoft SMS on page 5-32*.

4. Launch the MSI package from a command prompt window to install the OfficeScan client silently to a remote computer running Windows XP, Vista, Server 2008, 7, 8, or Server 2012.

Windows Operating System Type

Select the operating system for which you want to create the package. Deploy the package only to computers that run the operating system type. Create another package to deploy to another operating system type.

Scan Method

Select the scan method for the package. See *Scan Methods on page 7-7* for details.

The components included in the package depend on the scan method you have selected. For details on the components available for each scan method, see *OfficeScan Client Updates on page 6-26*.

Before selecting the scan method, take note of the following guidelines to help you deploy the package efficiently:

- If you will use the package to upgrade a client to this OfficeScan version, check the domain level scan method on the web console. On the console, go to **Networked Computers** > **Client Management**, select the client tree domain to which the client belongs, and click **Settings** > **Scan Settings** > **Scan Methods**. The domain level scan method should be consistent with the scan method for the package.

- If you will use the package to perform a fresh installation of the OfficeScan client, check the client grouping setting. On the web console, go to **Networked Computers** > **Client Grouping**.

- If the client grouping is by NetBIOS, Active Directory, or DNS domain, check the domain to which the target computer belongs. If the domain exists, check the scan method configured for the domain. If the domain does not exist, check the root level scan method (select the root domain icon ( ) in the client tree and click **Settings** > **Scan Settings** > **Scan Methods**). The domain or root level scan method should be consistent with the scan method for the package.

- If the client grouping is by custom client groups, check the **Grouping Priority** and **Source**.

FIGURE 5-1. Automatic Client Grouping preview pane

If the target computer belongs to a particular source, check the corresponding **Destination**. The destination is the domain name that appears in the client tree. The client will apply the scan method for that domain after the installation.

- If you will use the package to update components on a client using this OfficeScan version, check the scan method configured for the client tree domain to which the client belongs. The domain level scan method should be consistent with the scan method for the package.

Silent Mode

This option creates a package that installs on the client computer in the background, unnoticeable to the client and without showing an installation status window. Enable this option if you plan to deploy the package remotely to the target computer.

Disable Prescan

This option applies only for fresh installations.

If the target computer does not have the OfficeScan client installed, the package first scans the computer for security risks before installing the OfficeScan client. If you are certain that the target computer is not infected with security risks, disable prescan.

If prescan is enabled, Setup scans for virus/malware in the most vulnerable areas of the computer, which include the following:

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

Force Overwrite with Latest Version

This option overwrites component versions on the client with the versions currently available on the server. Enable this option to ensure that components on the server and client are synchronized.

Update Agent Capabilities

This option assigns Update Agent privileges to the OfficeScan client on the target computer. Update Agents help the OfficeScan server deploy components to clients. For details, see *Update Agents on page 6-50*.

You can allow the Update Agent to perform the following tasks:

- Deploy components
- Deploy settings
- Deploy programs

If you assign Update Agent privileges to an OfficeScan client:

1. Keep in mind that if the package will be deployed to a pure IPv6 client, the Update Agent can distribute updates only to pure IPv6 or dual-stack clients.
2. Use the Scheduled Update Configuration Tool to enable and configure scheduled updates for the agent. For details, see *Update Methods for Update Agents on page 6-57*.
3. The OfficeScan server that manages the Update Agent will not be able to synchronize or deploy the following settings to the agent:

   - Update Agent privilege
   - Client scheduled update
   - Updates from Trend Micro ActiveUpdate server
   - Updates from other update sources

   Therefore, deploy the OfficeScan client package only to computers that will not be managed by an OfficeScan server. Afterwards, configure the Update Agent to get its updates from an update source other than an OfficeScan server, such as a custom update source. If you want the OfficeScan server to synchronize settings with the Update Agent, do not use Client Packager and choose a different OfficeScan client installation method instead.

Outlook Mail Scan

This option installs the Outlook Mail Scan program, which scans Microsoft Outlook™ mailboxes for security risks. For details, see *Mail Scan Privileges and Other Settings on page 7-58*.

Check Point SecureClient Support

This tool adds support for Check Point™ SecureClient™ for Windows XP and Windows Server 2003. SecureClient verifies the Virus Pattern version before allowing connection to the network. For details, see *Overview of Check Point Architecture and Configuration on page 17-2*.

Note

SecureClient does not verify the virus pattern versions on clients using smart scan.

Components

Select the components and features to include in the package.

- For details about components, see *OfficeScan Components and Programs on page 6-2*.
- The Data Protection module will only be available if you install and activate Data Protection. For details about Data Protection, see *Using Data Loss Prevention on page 10-1*.

Deploying an MSI Package Using Active Directory

Take advantage of Active Directory features to deploy the MSI package simultaneously to multiple client computers. For instructions on creating an MSI file, see *Installing with Client Packager on page 5-23*.

Procedure

1. Perform the following:
   - For Windows Server 2003 and lower versions:
     a. Open the Active Directory console.
     b. Right-click the Organizational Unit (OU) where you want to deploy the MSI package and click **Properties**.
     c. In the **Group Policy** tab, click **New**.

- For Windows Server 2008 and Windows Server 2008 R2:

  a. Open the Group Policy Management Console. Click **Start** > **Control Panel** > **Administrative Tools** > **Group Policy Management**.

  b. In the console tree, expand **Group Policy Objects** in the forest and domain containing the GPO that you want to edit.

  c. Right-click the GPO that you want to edit, and then click **Edit**. This opens the Group Policy Object Editor.

- For Windows Server 2012:

  a. Open the Group Policy Management Console. Click **Server Management** > **Tools** > **Group Policy Management**.

  b. In the console tree, expand **Group Policy Objects** in the forest and domain containing the GPO that you want to edit.

  c. Right-click the GPO that you want to edit, and then click **Edit**. This opens the Group Policy Object Editor.

2. Choose between Computer Configuration and User Configuration, and open **Software Settings** below it.

Tip

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

---

3. Below Software Settings, right-click **Software installation**, and then select **New** and **Package**.

4. Locate and select the MSI package.

5. Select a deployment method and then click **OK**.

   - **Assigned**: The MSI package is automatically deployed the next time a user logs on to the computer (if you selected User Configuration) or when the computer restarts (if you selected Computer Configuration). This method does not require any user intervention.

- **Published**: To run the MSI package, inform users to go to Control Panel, open the Add/Remove Programs screen, and select the option to add/install programs on the network. When the OfficeScan client MSI package displays, users can proceed to install the OfficeScan client.

Deploying an MSI Package Using Microsoft SMS

Deploy the MSI package using Microsoft System Management Server (SMS) if you have Microsoft BackOffice SMS installed on the server. For instructions on creating an MSI file, see *Installing with Client Packager on page 5-23*.

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

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

Known issues when installing with Microsoft SMS:

- "Unknown" appears in the Run Time column of the SMS console.
- If the installation was unsuccessful, the installation status may still show that the installation is complete on the SMS program monitor. For instructions on how to check if the installation was successful, see *Post-installation on page 5-65*.

The following instructions apply if you use Microsoft SMS 2.0 and 2003.

Obtaining the Package Locally

Procedure

1. Open the SMS Administrator console.
2. On the **Tree** tab, click **Packages**.
3. On the **Action** menu, click **New** > **Package From Definition**.

   The **Welcome** screen of the Create Package From Definition Wizard appears.
4. Click **Next**.

The **Package Definition** screen appears.

5. Click **Browse**.

   The **Open** screen appears.

6. Browse and select the MSI package file created by Client Packager, and then click **Open**.

   The MSI package name appears on the **Package Definition** screen. The package shows "OfficeScan client" and the program version.

7. Click **Next**.

   The **Source Files** screen appears.

8. Click **Always obtain files from a source directory**, and then click **Next**.

   The **Source Directory** screen appears, displaying the name of the package you want to create and the source directory.

9. Click **Local drive on site server**.

10. Click **Browse** and select the source directory containing the MSI file.

11. Click **Next**.

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

Obtaining the Package Remotely

Procedure

1. On the OfficeScan server, use Client Packager to create a Setup package with an `.exe` extension (you cannot create an `.msi` package). See *Installing with Client Packager on page 5-23* for details.

2. On the computer where you want to store the source, create a shared folder.

3. Open the SMS Administrator console.

4. On the **Tree** tab, click **Packages**.
5. On the **Action** menu, click **New** > **Package From Definition**.

   The **Welcome** screen of the Create Package From Definition Wizard appears.
6. Click **Next**.

   The **Package Definition** screen appears.
7. Click **Browse**.

   The **Open** screen appears.
8. Browse for the MSI package file. The file is on the shared folder you created.
9. Click **Next**.

   The **Source Files** screen appears.
10. Click **Always obtain files from a source directory**, and then click **Next**.

    The **Source Directory** screen appears.
11. Click **Network path (UNC name)**.
12. Click **Browse** and select the source directory containing the MSI file (the shared folder you created).
13. Click **Next**.

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

Distributing the Package to Target Computers

Procedure

1. On the **Tree** tab, click **Advertisements**.
2. On the **Action** menu, click **All Tasks** > **Distribute Software**.

   The **Welcome** screen of the **Distribute Software Wizard** appears.

3. Click **Next**.

   The **Package** screen appears.

4. Click **Distribute an existing package**, and then click the name of the Setup package you created.

5. Click **Next**.

   The **Distribution Points** screen appears.

6. Select a distribution point to which you want to copy the package, and then click **Next**.

   The **Advertise a Program** screen appears.

7. Click **Yes** to advertise the OfficeScan client Setup package, and then click **Next**.

   The **Advertisement Target** screen appears.

8. Click **Browse** to select the target computers.

   The **Browse Collection** screen appears.

9. Click **All Windows NT Systems**.

10. Click **OK**.

    The **Advertisement Target** screen appears again.

11. Click **Next**.

    The **Advertisement Name** screen appears.

12. In the text boxes, type a name and your comments for the advertisement, and then click **Next**.

    The **Advertise to Subcollections** screen appears.

13. Choose whether to advertise the package to subcollections. Choose to advertise the program only to members of the specified collection or to members of subcollections.

14. Click **Next**.

    The **Advertisement Schedule** screen appears.

15. Specify when to advertise the OfficeScan client Setup package by typing or selecting the date and time.

Note

If you want Microsoft SMS to stop advertising the package on a specific date, click **Yes. This advertisement should expire**, and then specify the date and time in the **Expiration date and time** list boxes.

16. Click **Next**.

    The **Assign Program** screen appears.

17. Click **Yes, assign the program**, and then click **Next**.

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

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

Installations Using a Client Disk Image

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

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

Creating a Disk Image of an OfficeScan Client

Procedure

1. Install the OfficeScan client on a computer.

2. Copy `ImgSetup.exe` from <*Server installation folder*>`\PCCSRV\Admin\Utility\ImgSetup` to this computer.

3. Run `ImgSetup.exe` on this computer.

   This creates a `RUN` registry key under `HKEY_LOCAL_MACHINE`.

4. Create a disk image of the OfficeScan client using the disk imaging software.

5. Restart the clone.

   `ImgSetup.exe` automatically starts and creates one new GUID value. The OfficeScan client reports this new GUID to the server and the server creates a new record for the new OfficeScan client.

WARNING!

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

Vulnerability Scanner Usage

Use Vulnerability Scanner to detect installed antivirus solutions, search for unprotected computers on the network, and install OfficeScan clients to computers.

Considerations When Using Vulnerability Scanner

To help you decide whether to use Vulnerability Scanner, consider the following:

- *Network Administration on page 5-38*
- *Network Topology and Architecture on page 5-38*
- *Software/Hardware Specifications on page 5-39*
- *Domain Structure on page 5-39*
- *Network Traffic on page 5-40*
- *Network Size on page 5-40*

Network Administration

TABLE 5-6. Network Administration

SETUP	EFFECTIVENESS OF VULNERABILITY SCANNER
Administration with strict security policy	Very effective. Vulnerability Scanner reports whether all computers have antivirus software installed.
Administrative responsibility distributed across different sites	Moderately effective
Centralized administration	Moderately effective
Outsource service	Moderately effective
Users administer their own computers	Not effective. Because Vulnerability Scanner scans the network for antivirus installations, it is not feasible to have users scan their own computers.

Network Topology and Architecture

TABLE 5-7. Network Topology and Architecture

SETUP	EFFECTIVENESS OF VULNERABILITY SCANNER
Single location	Very effective. Vulnerability Scanner allows you to scan an entire IP segment and install the OfficeScan client easily on the LAN.
Multiple locations with high speed connection	Moderately effective
Multiple locations with low speed connection	Not effective. You need to run Vulnerability Scanner on each location and OfficeScan client installation must be directed to a local OfficeScan server.
Remote and isolated computers	Moderately effective

Software/Hardware Specifications

TABLE 5-8. Software/Hardware Specifications

SETUP	EFFECTIVENESS OF VULNERABILITY SCANNER
Windows NT-based operating systems	Very effective. Vulnerability Scanner can easily install the OfficeScan client remotely to computers running NT-based operating systems.
Mixed operating systems	Moderately effective. Vulnerability Scanner can only install to computers running Windows NT-based operating systems.
Desktop management software	Not effective. Vulnerability Scanner cannot be used with desktop management software. However, it can help track the progress of the OfficeScan client installation.

Domain Structure

TABLE 5-9. Domain Structure

SETUP	EFFECTIVENESS OF VULNERABILITY SCANNER
Microsoft Active Directory	Very effective. Specify the domain administrator account in Vulnerability Scanner to allow remote installation of the OfficeScan client.
Workgroup	Not effective. Vulnerability Scanner may have difficulty installing to computers using different administrative accounts and passwords.
Novell™ Directory Service	Not effective. Vulnerability Scanner requires a Windows Domain account to install the OfficeScan client.
Peer-to-peer	Not effective. Vulnerability Scanner may have difficulty installing to computers using different administrative accounts and passwords.

Network Traffic

TABLE 5-10. Network Traffic

SETUP	EFFECTIVENESS OF VULNERABILITY SCANNER
LAN connection	Very effective
512 Kbps	Moderately effective
T1 connection and higher	Moderately effective
Dialup	Not effective. It will take a long time to finish installing the OfficeScan client.

Network Size

TABLE 5-11. Network Size

SETUP	EFFECTIVENESS OF VULNERABILITY SCANNER
Very large enterprise	Very effective. The bigger the network, the more Vulnerability Scanner is needed for checking OfficeScan client installations.
Small and medium business	Moderately effective. For small networks, Vulnerability Scanner can be an option to install the OfficeScan client. Other OfficeScan client installation methods may prove much easier to implement.

Guidelines When Installing the OfficeScan Client Using Vulnerability Scanner

Vulnerability Scanner will not install the OfficeScan client if:

- The OfficeScan server or another security software is installed on the target host machine.
- The remote computer runs Windows XP Home, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7 Home Basic, Windows 7 Home Premium, or Windows 8 (basic versions).

Note

You can install the OfficeScan client to the target host machine using the other installation methods discussed in *Deployment Considerations on page 5-10*.

Before using Vulnerability Scanner to install the OfficeScan client, perform the following steps:

- For Windows Vista (Business, Enterprise, or Ultimate Edition) or Windows 7 (Professional, Enterprise, Ultimate Edition), Windows 8 (Pro, Enterprise), Windows Server 2012 (Standard):

  1. Enable a built-in administrator account and set the password for the account.
  2. Click **Start** > **Programs** > **Administrative Tools** > **Windows Firewall with Advanced Security**.
  3. For Domain Profile, Private Profile, and Public Profile, set the firewall state to "Off".
  4. Open Microsoft Management Console (click **Start** > **Run** and type `services.msc`) and start the **Remote Registry** service. When installing the OfficeScan client, use the built-in administrator account and password.

- For Windows XP Professional (32-bit or 64-bit version):

  1. Open Windows Explorer and click **Tools** > **Folder Options**.
  2. Click the **View** tab and disable **Use simple file sharing (Recommended)**.

Vulnerability Scan Methods

Vulnerability scan checks the presence of security software on host machines and can install the OfficeScan client to unprotected host machines.

There are several ways to run vulnerability scan.

TABLE 5-12. Vulnerability Scan Methods

METHOD	DETAILS
Manual vulnerability scan	Administrators can run vulnerability scans on demand.
DHCP scan	Administrators can run vulnerability scans on host machines requesting IP addresses from a DHCP server. Vulnerability Scanner listens on port 67, which is the DHCP server's listening port for DHCP requests. If it detects a DHCP request from a host machine, vulnerability scan runs on the machine. **Note** Vulnerability Scanner is unable to detect DHCP requests if you launched it on Windows Server 2008, Windows 7, Windows 8, or Windows Server 2012.
Scheduled vulnerability scan	Vulnerability scans automatically run according to the schedule configured by administrators.

After Vulnerability Scanner runs, it displays the status of the OfficeScan client on the target host machines. The status can be any of the following:

- **Normal**: The OfficeScan client is up and running and is working properly
- **Abnormal**: The OfficeScan client services are not running or the client does not have real-time protection
- **Not installed**: The TMListen service is missing or the OfficeScan client has not been installed
- **Unreachable**: Vulnerability Scanner was unable to establish connection with the host machine and determine the status of the OfficeScan client

Running a Manual Vulnerability Scan

Procedure

1. To run a vulnerability scan on the OfficeScan server computer, navigate to <*Server installation folder*>`\PCCSRV\Admin\Utility\TMVS` and double-click

`TMVS.exe`. The Trend Micro Vulnerability Scanner console appears. To run vulnerability scan on another computer running Windows Server 2003, Server 2008, Vista, 7, 8 , or Server 2012:

a. On the OfficeScan server computer, navigate to `<Server installation folder>\PCCSRV\Admin\Utility`.

b. Copy the `TMVS` folder to the other computer.

c. On the other computer, open the `TMVS` folder and then double-click `TMVS.exe`.

The **Trend Micro Vulnerability Scanner** console appears.

Note

You cannot launch the tool from Terminal Server.

2. Go to the **Manual Scan** section.

3. Type the IP address range of the computers you want to check.

a. Type an IPv4 address range.

Note

Vulnerability Scanner can only query an IPv4 address range if it runs on a pure IPv4 or dual-stack host machine. Vulnerability Scanner only supports a class B IP address range, for example, 168.212.1.1 to 168.212.254.254.

b. For an IPv6 address range, type the IPv6 prefix and length.

Note

Vulnerability Scanner can only query an IPv6 address range if it runs on a pure IPv6 or dual-stack host machine.

4. Click **Settings**.

The **Settings** screen appears.

5. Configure the following settings:

a. **Ping settings**: Vulnerability Scan can "ping" the IP addresses specified in the previous step to check if they are currently in use. If a target host machine is using an IP address, Vulnerability Scanner can determine the host machine's operating system. For details, see *Ping Settings on page 5-56*.

b. **Method for retrieving computer descriptions**: For host machines that respond to the "ping" command, Vulnerability Scanner can retrieve additional information about the host machines. For details, see *Method for Retrieving Computer Descriptions on page 5-53*.

c. **Product query**: Vulnerability Scanner can check for the presence of security software on the target host machines. For details, see *Product Query on page 5-50*.

d. **OfficeScan server settings**: Configure these settings if you want Vulnerability Scanner to automatically install OfficeScan client to unprotected host machines. These settings identify the OfficeScan client's parent server and the administrative credentials used to log on to the host machines. For details, see *OfficeScan Server Settings on page 5-58*.

Note

Certain conditions may prevent the installation of the OfficeScan client to the target host machines. For details, see *Guidelines When Installing the OfficeScan Client Using Vulnerability Scanner on page 5-40*.

---

e. **Notifications**: Vulnerability Scanner can send the vulnerability scan results to OfficeScan administrators. It can also display notifications on unprotected host machines. For details, see *Notifications on page 5-54*.

f. **Save results**: In addition to sending the vulnerability scan results to administrators, Vulnerability Scan can also save the results to a `.csv` file. For details, see *Vulnerability Scan Results on page 5-56*.

6. Click **OK**.

   The Settings screen closes.

7. Click **Start**.

   The vulnerability scan results appear in the **Results** table under the **Manual Scan** tab.

Note

MAC address information does not display in the **Results** table if the computer runs Windows Server 2008 or Windows Server 2012.

8. To save the results to a comma-separated value (CSV) file, click **Export**, locate the folder where you want to save the file, type the file name, and click **Save**.

Running a DHCP Scan

Procedure

1. Configure DHCP settings in the `TMVS.ini` file found under the following folder: <*Server installation folder*>`\PCCSRV\Admin\Utility\TMVS`.

TABLE 5-13. DHCP Settings in the `TMVS.ini` File

SETTING	DESCRIPTION
DhcpThreadNum=x	Specify the thread number for DHCP mode. The minimum is 3, the maximum is 100. The default value is 3.
DhcpDelayScan=x	This is the delay time in seconds before checking the requesting computer for installed antivirus software. The minimum is 0 (do not wait) and the maximum is 600. The default value is 60.
LogReport=x	0 disables logging, 1 enables logging. Vulnerability Scanner sends the results of the scan to the OfficeScan server. Logs display in the **System Event Logs** screen on the web console.
OsceServer=x	This is the OfficeScan server's IP address or DNS name.
OsceServerPort=x	This is the web server port on the OfficeScan server.

2. To run a vulnerability scan on the OfficeScan server computer, navigate to `<Server installation folder>\PCCSRV\Admin\Utility\TMVS` and double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears.

a. On the OfficeScan server computer, navigate to `<Server installation folder>\PCCSRV\Admin\Utility`.

b. Copy the `TMVS` folder to the other computer.

c. On the other computer, open the `TMVS` folder and then double-click `TMVS.exe`.

The **Trend Micro Vulnerability Scanner** console appears.

Note

You cannot launch the tool from Terminal Server.

---

3. Under the **Manual Scan** section, click **Settings**.

The **Settings** screen appears.

4. Configure the following settings:

a. **Product query**: Vulnerability Scanner can check for the presence of security software on the target host machines. For details, see *Product Query on page 5-50*.

b. **OfficeScan server settings**: Configure these settings if you want Vulnerability Scanner to automatically install the OfficeScan client to unprotected host machines. These settings identify the OfficeScan client's parent server and the administrative credentials used to log on to the host machines. For details, see *OfficeScan Server Settings on page 5-58*.

Note

Certain conditions may prevent the installation of the OfficeScan client to the target host machines. For details, see *Guidelines When Installing the OfficeScan Client Using Vulnerability Scanner on page 5-40*.

---

c. **Notifications**: Vulnerability Scanner can send the vulnerability scan results to OfficeScan administrators. It can also display notifications on unprotected host machines. For details, see *Notifications on page 5-54*.

d. **Save results**: In addition to sending the vulnerability scan results to administrators, Vulnerability Scan can also save the results to a `.csv` file. For details, see *Vulnerability Scan Results on page 5-56*.

5. Click **OK**.

   The Settings screen closes.

6. In the **Results** table, click the **DHCP Scan** tab.

   Note

   The **DHCP Scan** tab is not available on computers running Windows Server 2008,Windows 7, Windows 8, and Windows Server 2012.

7. Click **Start**.

   Vulnerability Scanner begins listening for DHCP requests and performing vulnerability checks on computers as they log on to the network.

8. To save the results to a comma-separated value (CSV) file, click **Export**, locate the folder where you want to save the file, type the file name, and click **Save**.

Configuring a Scheduled Vulnerability Scan

Procedure

1. To run a vulnerability scan on the OfficeScan server computer, navigate to <*Server installation folder*>`\PCCSRV\Admin\Utility\TMVS` and double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears. To run a vulnerability scan on another computer running Windows Server 2003, Server 2008, Vista, 7, 8, or Server 2012:

   a. On the OfficeScan server computer, navigate to `<Server installation folder>\PCCSRV\Admin\Utility`.

   b. Copy the `TMVS` folder to the other computer.

   c. On the other computer, open the `TMVS` folder and then double-click `TMVS.exe`.

The **Trend Micro Vulnerability Scanner** console appears.

> **Note**
> You cannot launch the tool from Terminal Server.

2. Go to the **Scheduled Scan** section.
3. Click **Add/Edit**.

   The **Scheduled Scan** screen appears.
4. Configure the following settings:

   a. **Name**: Type a name for the scheduled vulnerability scan.

   b. **IP address range**: Type the IP address range of the computers you want to check.

      i. Type an IPv4 address range.

      > **Note**
      > Vulnerability Scanner can only query an IPv4 address range if it runs on a pure IPv4 or dual-stack host machine that has an available IPv4 address. Vulnerability Scanner only supports a class B IP address range, for example, 168.212.1.1 to 168.212.254.254.

      ii. For an IPv6 address range, type the IPv6 prefix and length.

      > **Note**
      > Vulnerability Scanner can only query an IPv6 address range if it runs on a pure IPv6 or dual-stack host machine that has an available IPv6 address.

   c. **Schedule**: Specify the start time using the 24-hour clock format and then select how often the scan will run. Choose from daily, weekly, or monthly.

   d. **Settings**: Select which set of vulnerability scan settings to use.

      - Select **Use current settings** if you have configured and want to use manual vulnerability scan settings. For details about manual vulnerability scan settings, see *Running a Manual Vulnerability Scan on page 5-42*.

- If you did not specify manual vulnerability scan settings or if you want to use another set of settings, select **Modify settings** and then click **Settings**. The **Settings** screen appears.

  You can configure the following settings and then click **OK**:

  - **Ping settings**: Vulnerability Scan can "ping" the IP addresses specified in step 4b to check if they are currently in use. If a target host machine is using an IP address, Vulnerability Scanner can determine the host machine's operating system. For details, see *Ping Settings on page 5-56*.

  - **Method for retrieving computer descriptions**: For host machines that respond to the "ping" command, Vulnerability Scanner can retrieve additional information about the host machines. For details, see *Method for Retrieving Computer Descriptions on page 5-53*.

  - **Product query**: Vulnerability Scanner can check for the presence of security software on the target host machines. For details, see *Product Query on page 5-50*.

  - **OfficeScan server settings**: Configure these settings if you want Vulnerability Scanner to automatically install the OfficeScan client to unprotected host machines. These settings identify the OfficeScan client's parent server and the administrative credentials used to log on to the host machines. For details, see *OfficeScan Server Settings on page 5-58*.

  Note

  Certain conditions may prevent the installation of the OfficeScan client to the target host machines. For details, see *Guidelines When Installing the OfficeScan Client Using Vulnerability Scanner on page 5-40*.

  - **Notifications**: Vulnerability Scanner can send the vulnerability scan results to OfficeScan administrators. It can also display notifications on unprotected host machines. For details, see *Notifications on page 5-54*.

- **Save results**: In addition to sending the vulnerability scan results to administrators, Vulnerability Scan can also save the results to a .csv file. For details, see *Vulnerability Scan Results on page 5-56*.

5. Click **OK**.

   The **Scheduled Scan** screen closes.The scheduled vulnerability scan you created appears under the **Scheduled Scan** section. If you enabled notifications, Vulnerability Scanner sends you the scheduled vulnerability scan results.

6. To execute the scheduled vulnerability scan immediately, click **Run Now**.

   The vulnerability scan results appear in the **Results** table under the **Scheduled Scan** tab.

   Note

   MAC address information does not display in the **Results table** if the computer runs Windows Server 2008 or Windows Server 2012.

7. To save the results to a comma-separated value (`CSV`) file, click **Export**, locate the folder where you want to save the file, type the file name, and click **Save**.

Vulnerability Scan Settings

Vulnerability scan settings are configured from Trend Micro Vulnerability Scanner (`TMVS.exe`) or from the `TMVS.ini` file.

Note

See *Server Debug Logs Using LogServer.exe on page 18-3* for information on how to collect debug logs for Vulnerability Scanner.

Product Query

Vulnerability Scanner can check for the presence of security software on clients. The following table discusses how Vulnerability Scanner checks security products:

TABLE 5-14. Security Products Checked by Vulnerability Scanner

PRODUCT	DESCRIPTION
ServerProtect for Windows	Vulnerability Scanner uses RPC endpoint to check if `SPNTSVC.exe` is running. It returns information including operating system, and Virus Scan Engine, Virus Pattern and product versions. Vulnerability Scanner cannot detect the ServerProtect Information Server or the ServerProtect Management Console.
ServerProtect for Linux	If the target computer does not run Windows, Vulnerability Scanner checks if it has ServerProtect for Linux installed by trying to connect to port 14942.
OfficeScan client	Vulnerability Scanner uses the OfficeScan client port to check if the OfficeScan client is installed. It also checks if the `TmListen.exe` process is running. It retrieves the port number automatically if executed from its default location. If you launched Vulnerability Scanner on a computer other than the OfficeScan server, check and then use the other computer's communication port.
PortalProtect™	Vulnerability Scanner loads the web page `http://localhost:port/PortalProtect/index.html` to check for product installation.
ScanMail™ for Microsoft Exchange™	Vulnerability Scanner loads the web page `http://ipaddress:port/scanmail.html` to check for ScanMail installation. By default, ScanMail uses port 16372. If ScanMail uses a different port number, specify the port number. Otherwise, Vulnerability Scanner cannot detect ScanMail.
InterScan™ family	Vulnerability Scanner loads each web page for different products to check for product installation. • InterScan Messaging Security Suite 5.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x: `http://localhost:port/InterScan/cgi-bin/interscan.dll`

PRODUCT	DESCRIPTION
Trend Micro Internet Security™ (PC-cillin)	Vulnerability Scanner uses port 40116 to check if Trend Micro Internet Security is installed.
McAfee VirusScan ePolicy Orchestrator	Vulnerability Scanner sends a special token to TCP port 8081, the default port of ePolicy Orchestrator for providing connection between the server and client. The computer with this antivirus product replies using a special token type. Vulnerability Scanner cannot detect the standalone McAfee VirusScan.
Norton Antivirus™ Corporate Edition	Vulnerability Scanner sends a special token to UDP port 2967, the default port of Norton Antivirus Corporate Edition RTVScan. The computer with this antivirus product replies using a special token type. Since Norton Antivirus Corporate Edition communicates by UDP, the accuracy rate is not guaranteed. Furthermore, network traffic may influence UDP waiting time.

Vulnerability Scanner detects products and computers using the following protocols:

- **RPC**: Detects ServerProtect for NT
- **UDP**: Detects Norton AntiVirus Corporate Edition clients
- **TCP**: Detects McAfee VirusScan ePolicy Orchestrator
- **ICMP**: Detects computers by sending ICMP packets
- **HTTP**: Detects OfficeScan clients
- **DHCP**: If it detects a DHCP request, Vulnerability Scanner checks if antivirus software has already been installed on the requesting computer.

Configuring Product Query Settings

Product query settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-41*.

Procedure

1. To specify product query settings from Vulnerability Scanner (`TMVS.exe`):

a. Launch `TMVS.exe`.

b. Click **Settings**.

The **Settings** screen appears.

c. Go to the **Product query** section.

d. Select the products to check.

e. Click **Settings** next to a product name and then specify the port number that Vulnerability Scanner will check.

f. Click **OK**.

The **Settings** screen closes.

2. To set the number of computers that Vulnerability Scanner simultaneously checks for security software:

a. Navigate to <*Server installation folder*>`\PCCSRV\Admin\Utility\TMVS` and open `TMVS.ini` using a text editor such as Notepad.

b. To set the number of computers checked during manual vulnerability scans, change the value for `ThreadNumManual`. Specify a value between 8 and 64.

For example, type `ThreadNumManual=60` if you want Vulnerability Scanner to check 60 computers at the same time.

c. To set the number of computers checked during scheduled vulnerability scans, change the value for `ThreadNumSchedule`. Specify a value between 8 and 64.

For example, type `ThreadNumSchedule=50` if you want Vulnerability Scanner to check 50 computers at the same time.

d. Save `TMVS.ini`.

Method for Retrieving Computer Descriptions

When Vulnerability Scanner is able to "ping" host machines, it can retrieve additional information about the host machines. There are two methods for retrieving information:

- **Quick retrieval**: Retrieves only the computer name
- **Normal retrieval**: Retrieves both domain and computer information

Configuring Retrieval Settings

Retrieval settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-41*.

Procedure

1. Launch `TMVS.exe`.
2. Click **Settings**.

   The **Settings** screen appears.
3. Go to the **Method for retrieving computer descriptions** section.
4. Select **Normal** or **Quick**.
5. If you selected **Normal**, select **Retrieve computer descriptions when available**.
6. Click **OK**.

   The **Settings** screen closes.

Notifications

Vulnerability Scanner can send the vulnerability scan results to OfficeScan administrators. It can also display notifications on unprotected host machines.

Configuring Notification Settings

Notification settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-41*.

Procedure

1. Launch `TMVS.exe`.

2. Click **Settings**.

   The **Settings** screen appears.

3. Go to the **Notifications** section.

4. To automatically send the Vulnerability Scan results to yourself or to other administrators in your organization:

   a. Select **Email results to the system administrator**.

   b. Click **Configure** to specify email settings.

   c. In **To**, type the email address of the recipient.

   d. In **From**, type the email address of the sender.

   e. In **SMTP server**, type the SMTP server address.

      For example, type `smtp.company.com`. The SMTP server information is required.

   f. In **Subject**, type a new subject for the message or accept the default subject.

   g. Click **OK**.

5. To inform users that their computers do not have security software installed:

   a. Select **Display a notification on unprotected computers**.

   b. Click **Customize** to configure the notification message.

   c. In the **Notification Message** screen, type a new message or accept the default message.

   d. Click **OK**.

6. Click **OK**.

   The **Settings** screen closes.

Vulnerability Scan Results

You can configure Vulnerability Scanner to save the vulnerability scan results to a comma-separated value (CSV) file.

Configuring Scan Results

Vulnerability scan results settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-41*.

Procedure

1. Launch `TMVS.exe`.
2. Click **Settings**.

   The **Settings** screen appears.
3. Go to the **Save results** section.
4. Select **Automatically save the results to a CSV file**.
5. To change the default folder for saving the `CSV` file:
   a. Click **Browse**.
   b. Select a target folder on the computer or on the network.
   c. Click **OK**.
6. Click **OK**.

   The **Settings** screen closes.

Ping Settings

Use "ping" settings to validate the existence of a target machine and determine its operating system. If these settings are disabled, Vulnerability Scanner scans all the IP addresses in the specified IP address range – even those that are not used on any host machine – thereby making the scanning attempt longer than it should be.

Configuring Ping Settings

Ping settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-41*.

Procedure

1. To specify ping settings from Vulnerability Scanner (`TMVS.exe`):
   a. Launch `TMVS.exe`.
   b. Click **Settings**.

      The **Settings** screen appears.
   c. Go to the **Ping** settings section.
   d. Select **Allow Vulnerability Scanner to ping computers on your network to check their status**.
   e. In the **Packet size** and **Timeout** fields, accept or modify the default values.
   f. Select **Detect the type of operating system using ICMP OS fingerprinting**.

      If you select this option, Vulnerability Scanner determines if a host machine runs Windows or another operating system. For host machines running Windows, Vulnerability Scanner can identify the version of Windows.
   g. Click **OK**.

      The **Settings** screen closes.
2. To set the number of computers that Vulnerability Scanner simultaneously pings:
   a. Navigate to <*Server installation folder*>`\PCCSRV\Admin\Utility\TMVS` and open `TMVS.ini` using a text editor such as Notepad.
   b. Change the value for `EchoNum`. Specify a value between 1 and 64.

      For example, type `EchoNum=60` if you want Vulnerability Scanner to ping 60 computers at the same time.
   c. Save `TMVS.ini`.

OfficeScan Server Settings

OfficeScan server settings are used when:

- Vulnerability Scanner installs the OfficeScan client to unprotected target machines. Server settings allow Vulnerability Scanner to identify the OfficeScan client's parent server and the administrative credentials to use when logging on to the target machines.

  Note

  Certain conditions may prevent the installation of the OfficeScan client to the target host machines. For details, see *Guidelines When Installing the OfficeScan Client Using Vulnerability Scanner on page 5-40*.

- Vulnerability Scanner sends client installation logs to the OfficeScan server.

Configuring OfficeScan Server Settings

OfficeScan server settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-41*.

Procedure

1. Launch `TMVS.exe`.
2. Click **Settings**.

   The **Settings** screen appears.
3. Go to the **OfficeScan server settings** section.
4. Type the OfficeScan server name and port number.
5. Select **Auto-install OfficeScan client on unprotected computers**.
6. To configure the administrative credentials:

   a. Click **Install to Account**.

   b. In the **Account Information** screen, type a user name and password.

   c. Click **OK**.

7. Select **Send logs to the OfficeScan server**.
8. Click **OK**.

   The **Settings** screen closes.

Installing with Security Compliance

Install OfficeScan clients on computers within the network domains or install the OfficeScan client to a target computer by using its IP address.

Before installing the OfficeScan client, take note of the following:

Procedure

1. Record the logon credentials for each computer. OfficeScan will prompt you to specify the logon credentials during installation.
2. The OfficeScan client will not be installed on a computer if:
   - The OfficeScan server is installed on the computer.
   - The computer runs Windows XP Home, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7™ Starter, Windows 7 Home Basic, Windows 7 Home Premium, and Windows 8 (basic versions). If you have computers running these platforms, choose another installation method. See *Deployment Considerations on page 5-10* for details.
3. If the target computer runs Windows Vista (Business, Enterprise, or Ultimate Edition) Windows 7 (Professional, Enterprise, or Ultimate Edition), Windows 8 (Pro, Enterprise), or Windows Server 2012 (Standard), perform the following steps on the computer:
   a. Enable a built-in administrator account and set the password for the account.
   b. Disable the Windows firewall.
   c. Click **Start** > **Programs** > **Administrative Tools** > **Windows Firewall with Advanced Security**.

d. For Domain Profile, Private Profile, and Public Profile, set the firewall state to "Off".

e. Open Microsoft Management Console (click **Start** > **Run** and type `services.msc`) and start the **Remote Registry** service. When installing the OfficeScan client, use the built-in administrator account and password.

4. If there are Trend Micro or third-party endpoint security programs installed on the computer, check if OfficeScan can automatically uninstall the software and replace it with the OfficeScan client. For a list of client security software that OfficeScan automatically uninstalls, open the following files in <*Server installation folder*> `\PCCSRV\Admin`. You can open these files using a text editor such as Notepad.

   - `tmuninst.ptn`
   - `tmuninst_as.ptn`

   If the software on the target computer is not included in the list, manually uninstall it first. Depending on the uninstallation process of the software, the computer may or may not need to restart after uninstallation.

Installing the OfficeScan Client

Procedure

1. Navigate to **Security Compliance** > **Outside Server Management**.
2. Click **Install** on top of the client tree.
   - If an earlier OfficeScan client version is already installed on a computer and you click **Install**, the installation will be skipped and the client will not be upgraded to this version. To upgrade the client, a setting must be disabled.

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

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

     c. Disable the option **Clients can update components but not upgrade the client program or deploy hot fixes**.

3. Specify the administrator logon account for each computer and click **Log on**. OfficeScan starts installing the client on the target computer.
4. View the installation status.

Migrating to the OfficeScan Client

Replace client security software installed on a target computer with the OfficeScan client.

Migrating from Other Endpoint Security Software

When you install the OfficeScan client, the installation program checks for any Trend Micro or third-party endpoint security software installed on the target computer. The installation program can automatically uninstall the software and replace it with the OfficeScan client.

For a list of endpoint security software that OfficeScan automatically uninstalls, open the following files in <*Server installation folder*>`\PCCSRV\Admin`. Open these files using a text editor such as Notepad.

- `tmuninst.ptn`
- `tmuninst_as.ptn`

If the software on the target computer is not included in the list, manually uninstall it first. Depending on the uninstallation process of the software, the computer may or may not need to restart after uninstallation.

OfficeScan Client Migration Issues

- If automatic client migration is successful but a user encounters problems with the OfficeScan client right after installation, restart the computer.
- If the OfficeScan installation program proceeded to install the OfficeScan client but was unable to uninstall the other security software, there will be conflicts between the two software. Uninstall both software, and then install the OfficeScan

client using any of the installation methods discussed in *Deployment Considerations on page 5-10*.

Migrating from ServerProtect Normal Servers

The ServerProtect™ Normal Server Migration Tool is a tool that helps migrate computers running Trend Micro ServerProtect Normal Server to the OfficeScan client.

The ServerProtect Normal Server Migration Tool shares the same hardware and software specification as the OfficeScan server. Run the tool on computers running Windows Server 2003 or Windows Server 2008.

When uninstallation of the ServerProtect Normal server is successful, the tool installs the OfficeScan client. It also migrates the scan exclusion list settings (for all scan types) to the OfficeScan client.

While installing the OfficeScan client, the migration tool client installer may sometimes time out and notify you that the installation was unsuccessful. However, the OfficeScan client may have been installed successfully. Verify the installation on the client computer from the OfficeScan web console.

Migration is unsuccessful under the following circumstances:

- The remote client only has an IPv6 address. The migration tool does not support IPv6 addressing.
- The remote client cannot use the NetBIOS protocol.
- Ports 455, 337, and 339 are blocked.
- The remote client cannot use the RPC protocol.
- The Remote Registry Service stops.

Note

The ServerProtect Normal Server Migration Tool does not uninstall the Control Manager™ agent for ServerProtect. For instructions on how to uninstall the agent, refer to the ServerProtect and/or Control Manager documentation.

Using the ServerProtect Normal Server Migration Tool

Procedure

1. On the OfficeScan server computer, open <*Server installation folder*>`\PCCSRV\Admin\Utility\SPNSXfr` and copy the files `SPNSXfr.exe` and `SPNSX.ini` to `<Server installation folder>\PCCSRV\Admin`.

2. Double-click `SPNSXfr.exe` to open the tool.

   The **Server Protect Normal Server Migration Tool** console opens.

3. Select the OfficeScan server. The path of the OfficeScan server appears under OfficeScan server path. If it is incorrect, click **Browse** and select the `PCCSRV` folder in the directory where you installed OfficeScan. To enable the tool to automatically find the OfficeScan server again the next time you open the tool, select the **Auto Find Server Path** check box (selected by default).

4. Select the computers running ServerProtect Normal Server on which to perform the migration by clicking one of the following under **Target computer**:

   - **Windows Network tree**: Displays a tree of domains on the network. To select computers using this method, click the domains on which to search for client computers.

   - **Information Server name**: Search by Information Server name. To select computers by this method, type the name of an Information Server on the network in the text box. To search for multiple Information Servers, insert a semicolon ";" between server names.

   - **Certain Normal Server name**: Search by Normal Server name. To select computers by this method, type the name of a Normal Server on the network in the text box. To search for multiple Normal Servers, enter a semicolon ";" between server names.

   - **IP range search**: Search by a range of IP addresses. To select computers by this method, type a range of class B IP addresses under IP range.

Note

If a DNS server on the network does not respond when searching for clients, the search stops responding. Wait for the search to time out.

5. Select **Restart after installation** to automatically restart the target computers after migration.

   A restart is required for the migration to complete successfully. If you do not select this option, manually restart the computers after migration.

6. Click **Search**.

   The search results appear under **ServerProtect Normal Servers**.

7. Click the computers on which to perform the migration.

   a. To select all computers, click **Select All**.

   b. To clear all computers, click **Unselect All**.

   c. To export the list to a comma-separated value (CSV) file, click **Export to CSV**.

8. If logging on to the target computers requires a user name and password, do the following:

   a. Select the **Use group account/password** check box.

   b. Click **Set Logon Account**.

      The Enter Administration Information window appears.

   c. Type the user name and password.

      Note

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

   d. Click **OK**.

e. Click **Ask again if logon is unsuccessful** to be able to type the user name and password again during the migration process if you are unable to log on.

9. Click **Migrate**.

10. If you did not select the **Restart after installation** option, restart the target computers to complete the migration.

Post-installation

After completing the installation, verify the following:

- *OfficeScan Client Shortcut on page 5-65*
- *Programs List on page 5-66*
- *OfficeScan Client Services on page 5-66*
- *OfficeScan Client Installation Logs on page 5-66*

OfficeScan Client Shortcut

The OfficeScan client shortcuts appear on the Windows Start menu on the client computer.

FIGURE 5-2. OfficeScan client shortcut

Programs List

OfficeScan client is listed on the **Add/Remove Programs** list on the client computer's Control Panel.

OfficeScan Client Services

The following OfficeScan client services display on **Microsoft Management Console**:

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- OfficeScan NT Proxy Service (`TmProxy.exe`)

> **Note**
> The OfficeScan NT Proxy Service does not exist on Windows 8 or Windows Server 2012 platforms.

- OfficeScan NT Firewall (`TmPfw.exe`); if the firewall was enabled during installation
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

OfficeScan Client Installation Logs

The OfficeScan client installation log, `OFCNT.LOG`, exists on the following locations:

- `%windir%` for all installation methods except MSI package installation
- `%temp%` for the MSI package installation method

Recommended Post-installation Tasks

Trend Micro recommends performing the following post-installation tasks.

Component Updates

Update OfficeScan client components to ensure that clients have the most up-to-date protection from security risks. You can run manual client updates from the web console or instruct users to run "Update Now" from their computers.

Test Scan Using the EICAR Test Script

The European Institute for Computer Antivirus Research (EICAR) developed the EICAR test script as a safe way to confirm proper installation and configuration of antivirus software. Visit the EICAR website for more information:

http://www.eicar.org

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

WARNING!

Never use real viruses to test an antivirus product.

Performing a Test Scan

Procedure

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

Tip

Trend Micro recommends packaging the EICAR file using compression software (such as WinZip) and then performing another test scan.

OfficeScan Client Uninstallation

There are two ways to uninstall the OfficeScan client from computers:

- *Uninstalling the OfficeScan Client from the Web Console on page 5-68*
- *Running the OfficeScan Client Uninstallation Program on page 5-70*

If the OfficeScan client also has a Cisco Trust Agent (CTA) installation, uninstalling the OfficeScan client program may or may not remove the agent. This depends on the settings you configured when you deployed the agent. For more information, see *Cisco Trust Agent Deployment on page 16-27*.

If the Cisco Trust Agent exists after you uninstall the OfficeScan client, manually remove it from the **Add/Remove Programs** screen.

If the OfficeScan client cannot be uninstalled using the above methods, manually uninstall the OfficeScan client. For details, see *Manually Uninstalling the OfficeScan Client on page 5-70*.

Uninstalling the OfficeScan Client from the Web Console

Uninstall the OfficeScan client program from the web console. Perform uninstallation only if you encounter problems with the program and then reinstall it immediately to keep the computer protected from security risks.

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.

3. Click **Tasks** > **Client Uninstallation**.
4. In the **Client Uninstallation** screen, click **Initiate Uninstallation**. The server sends a notification to the clients.
5. Check the notification status and check if there are clients that did not receive the notification.
   a. Click **Select Un-notified Computers** and then **Initiate Uninstallation** to immediately resend the notification to un-notified clients.
   b. Click **Stop Uninstallation** to prompt OfficeScan to stop notifying clients currently being notified. Clients already notified and already performing uninstallation ignore this command.

The OfficeScan Client Uninstallation Program

Grant users the privilege to uninstall the OfficeScan client program and then instruct them to run the client uninstallation program from their computers.

Depending on your configuration, uninstallation may or may not require a password. If a password is required, ensure that you share the password only to users that will run the uninstallation program and then change the password immediately if it has been divulged to other users.

Granting the OfficeScan Client Uninstallation Privilege

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Uninstallation** section.

5. To allow uninstallation without a password, select **Allow the user to uninstall the OfficeScan client**. If a password is required, select **Require a password for the user to uninstall the OfficeScan client**, type the password, and then confirm it.

6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Running the OfficeScan Client Uninstallation Program

Procedure

1. On the Windows **Start** menu, click **Programs** > **Trend Micro OfficeScan Client** > **Uninstall OfficeScan Client**.

   You can also perform the following steps:

   a. Click **Control Panel** > **Add or Remove Programs**.

   b. Locate **Trend Micro OfficeScan Client** and click **Change**.

   c. Follow the on-screen instructions.

2. If prompted, type the uninstallation password. OfficeScan notifies the user of the uninstallation progress and completion. The user does not need to restart the client computer to complete the uninstallation.

Manually Uninstalling the OfficeScan Client

Perform manual uninstallation only if you encounter problems uninstalling the OfficeScan client from the web console or after running the uninstallation program.

Procedure

1. Log on to the client computer using an account with Administrator privileges.
2. Right-click the OfficeScan client icon on the system tray and select **Unload OfficeScan**. If prompted for a password, specify the unload password then click **OK**.

   Note

   - For Windows 8 and Windows Server 2012, switch to desktop mode to unload the OfficeScan client.
   - Disable the password on computers where the OfficeScan client will be unloaded. For details, see *Configuring Client Privileges and Other Settings on page 14-84*.

3. If the unload password was not specified, stop the following services from Microsoft Management Console:
   - OfficeScan NT Listener
   - OfficeScan NT Firewall
   - OfficeScan NT RealTime Scan
   - OfficeScan NT Proxy Service

     Note

     The OfficeScan NT Proxy Service does not exist on Windows 8 or Windows Server 2012 platforms.

   - Trend Micro Unauthorized Change Prevention Service
4. Remove the OfficeScan client shortcut from the Start menu.
   - On Windows 8 and Windows Server 2012:
     a. Switch to desktop mode.
     b. Move the mouse cursor to the bottom right corner of the screen and click **Start** from the menu that appears.

The **Home** screen appears.

c. Right-click **Trend Micro OfficeScan**.

d. Click **Unpin from Start**.

- On all other Windows platforms:

  Click **Start** > **Programs**, right-click **Trend Micro OfficeScan Client**, and click **Delete**.

5. Open Registry Editor (`regedit.exe`).

WARNING!

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

---

6. Delete the following registry keys:

- If there are no other Trend Micro products installed on the computer:

  - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

    For 64-bit computers:

    `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro`

- If there are other Trend Micro products installed on the computer, delete the following keys only:

  - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog`

    For 64-bit computers:

    `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog`

  - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp`

    For 64-bit computers:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro \PC-cillinNTCorp`

7. Delete the following registry keys/values:
   - For 32-bit systems:
     - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\OfficeScanNT`
     - OfficeScanNT Monitor (`REG_SZ`) under `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
   - For 64-bit systems:
     - `HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft \Windows\CurrentVersion\Uninstall\OfficeScanNT`
     - OfficeScanNT Monitor (`REG_SZ`) under `HKEY_LOCAL_MACHINE \SOFTWARE\ Wow6432Node\Microsoft\Windows \CurrentVersion\Run`
8. Delete all instances of the following registry keys in the following locations:
   - Locations:
     - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services`
   - Keys:
     - NTRtScan
     - tmcfw
     - tmcomm
     - TmFilter
     - TmListen

- tmpfw
- TmPreFilter
- TmProxy

> **Note**
> TmProxy does not exist on Windows 8 or Windows Server 2012 platforms.

- tmtdi

> **Note**
> tmtdi does not exist on Windows 8 or Windows Server 2012 platforms.

- VSApiNt
- tmlwf (for Windows Vista/Server 2008/7/8/Server 2012 computers)
- tmwfp (for Windows Vista/Server 2008/7/8/Server 2012 computers)
- tmactmon
- TMBMServer
- TMebc
- tmevtmgr
- tmeevw (for Windows 8/Server 2012)
- tmusa (for Windows 8/Server 2012)

9. Close Registry Editor.
10. Click **Start** > **Settings** > **Control Panel** and double-click **System**.

> **Note**
> For Windows 8 and Windows Server 2012 systems, skip this step.

11. Click the **Hardware** tab and then click **Device Manager**.

Note

For Windows 8 and Windows Server 2012 systems, skip this step.

12. Click **View** > **Show hidden devices**.

Note

For Windows 8 and Windows Server 2012 systems, skip this step.

13. Expand **Non-Plug and Play Drivers** and then uninstall the following devices (for Windows XP/Vista/7/Server 2003/Server 2008):

- tmcomm
- tmactmon
- tmevtmgr
- Trend Micro Filter
- Trend Micro PreFilter
- Trend Micro TDI Driver
- Trend Micro VSAPI NT
- Trend Micro Unauthorized Change Prevention Service
- Trend Micro WFP Callout Driver (For Windows Vista/Server 2008/7 computers)

14. Manually delete Trend Micro drivers using a command line editor (Windows 8/Server 2012 only) using the following commands:

- `sc delete tmcomm`
- `sc delete tmactmon`
- `sc delete tmevtmgr`
- `sc delete tmfilter`
- `sc delete tmprefilter`

- `sc delete tmwfp`
- `sc delete vsapint`
- `sc delete tmeevw`
- `sc delete tmusa`
- `sc delete tmebc`

Note

Run the command line editor using administrator privileges (for example, right-click `cmd.exe` and click **Run as administrator**) to ensure the commands execute successfully.

15. Uninstall the Common Firewall Driver.
    a. Right-click **My Network Places** and click **Properties**.
    b. Right-click **Local Area Connection** and click **Properties**.
    c. On the **General** tab, select **Trend Micro Common Firewall Driver** and click **Uninstall**.

    Note

    The following steps only apply to Windows Vista/Server 2008/7/8/Server 2012 operating systems. Clients using all other operating systems skip to step 15.

    d. Right-click **Network** and click **Properties**.
    e. Click **Manage network connections**.
    f. Right-click **Local Area Connection** and click **Properties**.
    g. On the **Networking** tab, select **Trend Micro NDIS 6.0 Filter Driver** and click **Uninstall**.
16. Restart the client computer.
17. If there are no other Trend Micro products installed on the computer, delete the `Trend Micro` installation folder (typically, `C:\Program Files\Trend`

`Micro`). For 64-bit computers, the installation folder can be found under `C:\Program Files (x86)\Trend Micro`.

18. If there are other Trend Micro products installed, delete the following folders:

    - <*Client installation folder*>
    - The `BM` folder under the Trend Micro installation folder (typically, `C:\Program Files\Trend Micro\BM` for 32-bit systems and `C:\Program Files (x86)\Trend Micro\BM` for 64-bit systems)

Chapter 6

Keeping Protection Up-to-Date

This chapter describes Trend Micro™ OfficeScan™ components and update procedures.

Topics in this chapter:

- *OfficeScan Components and Programs on page 6-2*
- *Update Overview on page 6-11*
- *OfficeScan Server Updates on page 6-14*
- *Integrated Smart Protection Server Updates on page 6-26*
- *OfficeScan Client Updates on page 6-26*
- *Update Agents on page 6-50*
- *Component Update Summary on page 6-59*

OfficeScan Components and Programs

OfficeScan makes use of components and programs to keep client computers protected from the latest security risks. Keep these components and programs up-to-date by running manual or scheduled updates.

In addition to the components, OfficeScan clients also receive updated configuration files from the OfficeScan server. Clients need the configuration files to apply new settings. Each time you modify OfficeScan settings through the web console, the configuration files change.

Components are grouped as follows:

- *Antivirus Components on page 6-2*
- *Damage Cleanup Services Components on page 6-5*
- *Anti-spyware Components on page 6-5*
- *Firewall Components on page 6-6*
- *Web Reputation Component on page 6-7*
- *Behavior Monitoring Components on page 6-7*
- *Programs on page 6-8*
- *C&C Contact Alert Service Component on page 6-11*

Antivirus Components

Antivirus components consist of the following patterns, drivers, and engines:

- *Virus Patterns on page 6-3*
- *Virus Scan Engine on page 6-3*
- *Virus Scan Driver on page 6-4*
- *IntelliTrap Pattern on page 6-5*
- *IntelliTrap Exception Pattern on page 6-5*

Virus Patterns

The virus pattern available on a client computer depends on the scan method the client is using. For information about scan methods, see *Scan Methods on page 7-7*.

TABLE 6-1. Virus Patterns

SCAN METHOD	PATTERN IN USE
Conventional Scan	The **Virus Pattern** contains information that helps OfficeScan identify the latest virus/malware and mixed threat attacks. Trend Micro creates and releases new versions of the Virus Pattern several times a week, and any time after the discovery of a particularly damaging virus/ malware. Trend Micro recommends scheduling automatic updates at least hourly, which is the default setting for all shipped products.
Smart Scan	When in smart scan mode, OfficeScan clients use two lightweight patterns that work together to provide the same protection provided by conventional anti-malware and anti-spyware patterns. A smart protection source hosts the **Smart Scan Pattern**. This pattern is updated hourly and contains majority of the pattern definitions. Smart scan clients do not download this pattern. Clients verify potential threats against the pattern by sending scan queries to the smart protection source. The client update source (the OfficeScan server or a custom update source) hosts the **Smart Scan Agent Pattern**. This pattern is updated daily and contains all the other pattern definitions not found on the Smart Scan Pattern. Clients download this pattern from the update source using the same methods for downloading other OfficeScan components. For more information about Smart Scan Pattern and Smart Scan Agent Pattern, see *Smart Protection Pattern Files on page 4-7*.

Virus Scan Engine

At the heart of all Trend Micro products lies the scan engine, which was originally developed in response to early file-based computer viruses. The scan engine today is exceptionally sophisticated and capable of detecting different types of *Viruses and*

Malware on page 7-2. The scan engine also detects controlled viruses that are developed and used for research.

Rather than scanning every byte of every file, the engine and pattern file work together to identify the following:

- Tell-tale characteristics of the virus code
- The precise location within a file where the virus resides

OfficeScan removes viruses/malware upon detection and restores the integrity of the file.

Updating the Scan Engine

By storing the most time-sensitive virus/malware information in the virus patterns, Trend Micro minimizes the number of scan engine updates while keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. Trend Micro releases new engines under the following circumstances:

- Incorporation of new scanning and detection technologies into the software
- Discovery of a new, potentially harmful virus/malware that the scan engine cannot handle
- Enhancement of the scanning performance
- Addition of file formats, scripting languages, encoding, and/or compression formats

Virus Scan Driver

The Virus Scan Driver monitors user operations on files. Operations include opening or closing a file, and executing an application. There are two versions for this driver. These are `TmXPFlt.sys` and `TmPreFlt.sys`. `TmXPFlt.sys` is used for real-time configuration of the Virus Scan Engine and `TmPreFlt.sys` for monitoring user operations.

Note

This component does not display on the console. To check its version, navigate to <*Server installation folder*>`\PCCSRV\Pccnt\Drv`. Right-click the `.sys` file, select **Properties**, and go to the **Version** tab.

IntelliTrap Pattern

The IntelliTrap pattern (for details, see *IntelliTrap on page E-6*). Pattern detects real-time compression files packed as executable files.

IntelliTrap Exception Pattern

The IntelliTrap Exception Pattern contains a list of "approved" compression files.

Damage Cleanup Services Components

Damage Cleanup Services components consist of the following engine and template.

- *Virus Cleanup Engine on page 6-5*
- *Virus Cleanup Template on page 6-5*

Virus Cleanup Engine

The Virus Cleanup Engine scans for and removes Trojans and Trojan processes. This engine supports 32-bit and 64-bit platforms.

Virus Cleanup Template

The Virus Cleanup Template is used by the Virus Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.

Anti-spyware Components

Anti-spyware components consist of the following engine and patterns:

- *Spyware Pattern on page 6-6*
- *Spyware Scan Engine on page 6-6*
- *Spyware Active-monitoring Pattern on page 6-6*

Spyware Pattern

The Spyware Pattern identifies spyware/grayware in files and programs, modules in memory, Windows registry and URL shortcuts.

Spyware Scan Engine

The Spyware Scan Engine scans for and performs the appropriate scan action on spyware/grayware. This engine supports 32-bit and 64-bit platforms.

Spyware Active-monitoring Pattern

The Spyware Active-monitoring Pattern is used for real-time spyware/grayware scanning. Only conventional scan clients use this pattern.

Smart scan clients use the Smart Scan Agent Pattern for real-time spyware/grayware scanning. Clients send scan queries to a smart protection source if the risk of the scan target cannot be determined during scanning.

Firewall Components

The Firewall components consist of the following driver and pattern:

- *Common Firewall Driver on page 6-6*
- *Common Firewall Pattern on page 6-7*

Common Firewall Driver

The Common Firewall Driver is used with the Common Firewall Pattern to scan client computers for network viruses. This driver supports 32-bit and 64-bit platforms.

Common Firewall Pattern

Like the Virus Pattern, the Common Firewall Pattern helps OfficeScan identify virus signatures, unique patterns of bits and bytes that signal the presence of a network virus.

Web Reputation Component

The Web Reputation component is the URL Filtering Engine.

URL Filtering Engine

The URL Filtering Engine facilitates communication between OfficeScan and the Trend Micro URL Filtering Service. The URL Filtering Service is a system that rates URLs and provides rating information to OfficeScan.

Behavior Monitoring Components

The Behavior Monitoring components consist of the following patterns, drivers, and services:

- *Behavior Monitoring Detection Pattern on page 6-7*
- *Behavior Monitoring Driver on page 6-8*
- *Behavior Monitoring Core Service on page 6-8*
- *Behavior Monitoring Configuration Pattern on page 6-8*
- *Digital Signature Pattern on page 6-8*
- *Policy Enforcement Pattern on page 6-8*

Behavior Monitoring Detection Pattern

This pattern contains the rules for detecting suspicious threat behavior.

Behavior Monitoring Driver

This kernel mode driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.

Behavior Monitoring Core Service

This user mode service has the following functions:

- Provides rootkit detection
- Regulates access to external devices
- Protects files, registry keys, and services

Behavior Monitoring Configuration Pattern

The Behavior Monitoring Driver uses this pattern to identify normal system events and exclude them from policy enforcement.

Digital Signature Pattern

This pattern contains a list of valid digital signatures that are used by the Behavior Monitoring Core Service to determine whether a program responsible for a system event is safe.

Policy Enforcement Pattern

The Behavior Monitoring Core Service checks system events against the policies in this pattern.

Programs

OfficeScan makes use of the following programs and product updates:

- *OfficeScan Client Program on page 6-9*
- *Cisco Trust Agent on page 6-9*

- *Hot Fixes, Patches, and Service Packs on page 6-9*

OfficeScan Client Program

The OfficeScan client program provides the actual protection from security risks.

Cisco Trust Agent

The Cisco Trust Agent enables communication between the client and routers that support Cisco NAC. This agent will only work if you install Policy Server for Cisco NAC.

Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops the following to address issues, enhance product performance, or add new features:

- *Hot Fix on page E-5*
- *Patch on page E-9*
- *Security Patch on page E-11*
- *Service Pack on page E-11*

Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix, patch, and service pack releases:

http://www.trendmicro.com/download

All releases include a readme file that contains installation, deployment, and configuration information. Read the readme file carefully before performing installation.

Hot Fix and Patch History

When the OfficeScan server deploys hot fix or patch files to OfficeScan clients, the client program records information about the hot fix or patch in Registry Editor. You

can query this information for multiple clients using logistics software such as Microsoft SMS, LANDesk™, or BigFix™.

Note

This feature does not record hot fixes and patches that are deployed only to the server.

This feature is available starting in OfficeScan 8.0 Service Pack 1 with patch 3.1.

- Clients upgraded from version 8.0 Service Pack 1 with patch 3.1 or later record installed hot fixes and patches for version 8.0 and later.
- Clients upgraded from versions earlier than 8.0 Service Pack 1 with patch 3.1 record installed hot fixes and patches for version 10.0 and later.

Information is stored in the following keys:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- For computers running x64 type platforms:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

Check for the following keys:

- **Key**: `HotFix_installed`

  Type: `REG_SZ`

  Value: `<Hot fix or patch name>`
- **Key**: `HotfixInstalledNum`

  Type: `DWORD`

  Value: `<Hot fix or patch number>`

C&C Contact Alert Service Component

The C&C Contact Alert Service component is the C&C IP List.

C&C IP List

The C&C IP list works in conjunction with the Network Content Inspection Engine (NCIE) to detect network connections with known C&C servers. NCIE detects C&C server contact through any network channel.

OfficeScan logs all connection information to servers in the C&C IP list for evaluation.

Update Overview

All component updates originate from the Trend Micro ActiveUpdate server. When updates are available, the OfficeScan server and smart protection sources (Smart Protection Server or Smart Protection Network) download the updated components. There are no component download overlaps between the OfficeScan server and smart protection sources because each one downloads a specific set of components.

Note

You can configure both the OfficeScan server and Smart Protection Server to update from a source other than the Trend Micro ActiveUpdate server. To do this, you need to set up a custom update source. If you need assistance setting up this update source, contact your support provider.

OfficeScan Server and OfficeScan Client Update

The OfficeScan server downloads most of the components that clients need. The only component it does not download is the Smart Scan Pattern, which is downloaded by smart protection sources.

If an OfficeScan server manages a large number of clients, updating may utilize a significant amount of server computer resources, affecting the server's stability and

performance. To address this issue, OfficeScan has an Update Agent feature that allows certain clients to share the task of distributing updates to other clients.

The following table describes the different component update options for the OfficeScan server and clients, and recommendations on when to use them:

TABLE 6-2. Server-Client Update Options

UPDATE OPTION	DESCRIPTION	RECOMMENDATION
ActiveUpdate server > **Server** > **Client**	The OfficeScan server receives updated components from the Trend Micro ActiveUpdate server (or other update source) and initiates component update on clients.	Use this method if there are no low-bandwidth sections between the OfficeScan server and clients.
ActiveUpdate server > **Server** > **Update Agents** > **Client**	The OfficeScan server receives updated components from the ActiveUpdate server (or other update source) and initiates component update on clients. Clients acting as Update Agents then notify clients to update components.	If there are low-bandwidth sections between the OfficeScan server and clients, use this method to balance the traffic load on the network.
ActiveUpdate server > **Update Agents** > **Client**	Update Agents receive updated components directly from the ActiveUpdate server (or other update source) and notifies clients to update components.	Use this method only if you experience problems updating Update Agents from the OfficeScan server or from other Update Agents. Under most circumstances, Update Agents receive updates faster from the OfficeScan server or from other Update Agents than from an external update source.

Update Option	Description	Recommendation
ActiveUpdate server > **Client**	OfficeScan clients receive updated components directly from the ActiveUpdate server (or other update source).	Use this method only if you experience problems updating clients from the OfficeScan server or from Update Agents. Under most circumstances, clients receive updates faster from the OfficeScan server or from Update Agents than from an external update source.

Smart Protection Source Update

A smart protection source (Smart Protection Server or Smart Protection Network) downloads the Smart Scan Pattern. Smart scan clients do not download this pattern. Clients verify potential threats against the pattern by sending scan queries to the smart protection source.

Note

See *Smart Protection Sources on page 4-5* for more information about smart protection sources.

The following table describes the update process for smart protection sources.

Table 6-3. Smart Protection Source Update Process

Update Process	Description
ActiveUpdate server > **Smart Protection Network**	The Trend Micro Smart Protection Network receives updates from the Trend Micro ActiveUpdate server. Smart scan clients that are not connected to the corporate network send queries to the Trend Micro Smart Protection Network.
ActiveUpdate server > **Smart Protection Server**	A Smart Protection Server (integrated or standalone) receives updates from the Trend Micro ActiveUpdate server. Smart protection clients that are connected to the corporate network send queries to the Smart Protection Server.

Update Process	Description
Smart Protection Network > **Smart Protection Server**	A Smart Protection Server (integrated or standalone) receives updates from the Trend Micro Smart Protection Network. Smart protection clients that are connected to the corporate network send queries to the Smart Protection Server.

OfficeScan Server Updates

The OfficeScan server downloads the following components and deploys them to clients:

Table 6-4. Components Downloaded by the OfficeScan Server

Component	Distribution	
	Conventional Scan Clients	Smart Scan Clients
Antivirus		
Smart Scan Agent Pattern	No	Yes
Virus Pattern	Yes	No
IntelliTrap Pattern	Yes	Yes
IntelliTrap Exception Pattern	Yes	Yes
Virus Scan Engine (32-bit)	Yes	Yes
Virus Scan Engine (64-bit)	Yes	Yes
Anti-spyware		
Spyware Pattern	Yes	Yes
Spyware Active-monitoring Pattern	Yes	No
Spyware Scan Engine (32-bit)	Yes	Yes
Spyware Scan Engine (64-bit)	Yes	Yes

Component	Distribution	
	Conventional Scan Clients	Smart Scan Clients
Damage Cleanup Services		
Virus Cleanup Template	Yes	Yes
Virus Cleanup Engine (32-bit)	Yes	Yes
Virus Cleanup Engine (64-bit)	Yes	Yes
Firewall		
Common Firewall Pattern	Yes	Yes
Behavior Monitoring Components		
Behavior Monitoring Detection Pattern (32-bit)	Yes	Yes
Behavior Monitoring Driver (32-bit)	Yes	Yes
Behavior Monitoring Core Service (32-bit)	Yes	Yes
Behavior Monitoring Detection Pattern (64-bit)	Yes	Yes
Behavior Monitoring Driver (64-bit)	Yes	Yes
Behavior Monitoring Core Service (64-bit)	Yes	Yes
Behavior Monitoring Configuration Pattern	Yes	Yes
Policy Enforcement Pattern	Yes	Yes
Digital Signature Pattern	Yes	Yes
C&C Contact Alert Service		
C&C IP List	Yes	Yes

Update reminders and tips:

- To allow the server to deploy the updated components to clients, enable automatic client update. For details, see *OfficeScan Client Automatic Updates on page 6-35*. If automatic client update is disabled, the server downloads the updates but does not deploy them to the clients.
- A pure IPv6 OfficeScan server cannot distribute updates directly to pure IPv4 clients. Similarly, a pure IPv4 OfficeScan server cannot distribute updates directly to pure IPv6 clients. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the OfficeScan server to distribute update to the clients.
- Trend Micro releases pattern files regularly to keep client protection current. Since pattern file updates are available regularly, OfficeScan uses a mechanism called **component duplication** that allows faster downloads of pattern files. See *OfficeScan Server Component Duplication on page 6-19* for more information.
- If you use a proxy server to connect to the Internet, use the correct proxy settings to download updates successfully.
- On the web console's Summary, add the **Client Updates** widget to view the current versions of components and determine the number of clients with updated and outdated components.

OfficeScan Server Update Sources

Configure the OfficeScan server to download components from the Trend Micro ActiveUpdate server or from another source. You may specify another source if the OfficeScan server is unable to reach the ActiveUpdate server directly. For a sample scenario, see *Isolated OfficeScan Server Updates on page 6-22*.

After the server downloads any available updates, it can automatically notify clients to update their components based on the settings you specified in **Updates** > **Networked Computers** > **Automatic Update**. If the component update is critical, let the server notify the clients at once by going to **Updates** > **Networked Computers** > **Manual Update**.

Note

If you do not specify a deployment schedule or event-triggered update settings in **Updates** > **Networked Computers** > **Automatic Update**, the server will download the updates but will not notify clients to update.

IPv6 Support for OfficeScan Server Updates

A pure IPv6 OfficeScan server cannot update directly from pure IPv4 update sources, such as:

- Trend Micro ActiveUpdate Server
- Control Manager 5.5
- Control Manager 5.0

Note

IPv6 support for Control Manager starts in version 5.5 SP1.

- Any pure IPv4 custom update source

Similarly, a pure IPv4 OfficeScan server cannot update directly from pure IPv6 custom update sources.

A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the server to connect to the update sources.

Proxy for OfficeScan Server Updates

Configure server programs hosted on the server computer to use proxy settings when downloading updates from the Trend Micro ActiveUpdate server. Server programs include the OfficeScan server and the integrated Smart Protection Server.

Configuring Proxy Settings

Procedure

1. Navigate to **Administration** > **Proxy Settings**.
2. Click the **External Proxy** tab.
3. Go to the **OfficeScan Server Computer Updates** section.
4. Select **Use a proxy server for pattern, engine, and license updates**.
5. Specify the proxy protocol, server name or IPv4/IPv6 address, and port number.
6. If the proxy server requires authentication, type the user name and password.
7. Click **Save**.

Configuring the Server Update Source

Procedure

1. Navigate to **Updates** > **Server** > **Update Source**.
2. Select the location from where you want to download component updates.

   If you choose ActiveUpdate server, ensure that the server has Internet connection and, if you are using a proxy server, test if Internet connection can be established using the proxy settings. For details, see *Proxy for OfficeScan Server Updates on page 6-17*.

   If you choose a custom update source, set up the appropriate environment and update resources for this update source. Also ensure that there is a functional connection between the server computer and this update source. If you need assistance setting up an update source, contact your support provider.

Note

The OfficeScan server uses component duplication when downloading components from the update source. See *OfficeScan Server Component Duplication on page 6-19* for details.

3. Click **Save**.

OfficeScan Server Component Duplication

When the latest version of a full pattern file is available for download from the Trend Micro ActiveUpdate server, 14 "incremental patterns" also become available. Incremental patterns are smaller versions of the full pattern file that account for the difference between the latest and previous full pattern file versions. For example, if the latest version is 175, incremental pattern v_173.175 contains signatures in version 175 not found in version 173 (version 173 is the previous full pattern version since pattern numbers are released in increments of 2. Incremental pattern v_171.175 contains signatures in version 175 not found in version 171.

To reduce network traffic generated when downloading the latest pattern, OfficeScan performs component duplication, a component update method where the OfficeScan server or Update Agent downloads only incremental patterns. See *Update Agent Component Duplication on page 6-56* for information on how Update Agents perform component duplication.

Component duplication applies to the following components:

- Virus Pattern
- Smart Scan Agent Pattern
- Virus Cleanup Template
- IntelliTrap Exception Pattern
- Spyware Pattern
- Spyware Active-monitoring pattern

Component Duplication Scenario

To explain component duplication for the server, refer to the following scenario:

TABLE 6-5. Server Component Duplication Scenario

Full patterns on the OfficeScan server	Current version: 171 Other versions available: 169	167	165	161	159	
Latest version on the ActiveUpdate server	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. The OfficeScan server compares its current full pattern version with the latest version on the ActiveUpdate server. If the difference between the two versions is 14 or less, the server only downloads the incremental pattern that accounts for the difference between the two versions.

   Note

   If the difference is more than 14, the server automatically downloads the full version of the pattern file and 14 incremental patterns.

   To illustrate based on the example:

   - The difference between versions 171 and 175 is 2. In other words, the server does not have versions 173 and 175.
   - The server downloads incremental pattern 171.175. This incremental pattern accounts for the difference between versions 171 and 175.

2. The server merges the incremental pattern with its current full pattern to generate the latest full pattern.

   To illustrate based on the example:

   - On the server, OfficeScan merges version 171 with incremental pattern 171.175 to generate version 175.

- The server has 1 incremental pattern (171.175) and the latest full pattern (version 175).

3. The server generates incremental patterns based on the other full patterns available on the server. If the server does not generate these incremental patterns, clients that missed downloading earlier incremental patterns automatically download the full pattern file, which will consequently generate more network traffic.

   To illustrate based on the example:

   - Because the server has pattern versions 169, 167, 165, 163, 161, 159, it can generate the following incremental patterns:

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - The server does not need to use version 171 because it already has the incremental pattern 171.175.

   - The server now has 7 incremental patterns:

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - The server keeps the last 7 full pattern versions (versions 175, 171, 169, 167, 165, 163, 161). It removes any older version (version 159).

4. The server compares its current incremental patterns with the incremental patterns available on the ActiveUpdate server. The server downloads the incremental patterns it does not have.

   To illustrate based on the example:

   - The ActiveUpdate server has 14 incremental patterns:

     173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - The OfficeScan server has 7 incremental patterns:

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - The OfficeScan server downloads an additional 7 incremental patterns:

     173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- The server now has all the incremental patterns available on the ActiveUpdate server.

5. The latest full pattern and the 14 incremental patterns are made available to clients.

Isolated OfficeScan Server Updates

If the OfficeScan server belongs to a network that is isolated completely from all outside sources, you can keep the server's components up-to-date by letting it update from an internal source that contains the latest components.

This topic explains the tasks that you need to perform to update an isolated OfficeScan server.

Updating an Isolated OfficeScan Server

This procedure is provided for your reference. If you are able to fulfill all the tasks in this procedure, please ask your support provider for the detailed steps for each task.

Procedure

1. Identify the update source, such as Trend Micro Control Manager or a random host machine.The update source must have:

   - A reliable Internet connection so that it can download the latest components from the Trend Micro ActiveUpdate server. Without Internet connection, the only way for the update source to have the latest components is if you obtain the components yourself from Trend Micro and then copy them into the update source.

   - A functional connection with the OfficeScan server. Configure proxy settings if there is a proxy server between the OfficeScan server and the update source. For details, see *Proxy for OfficeScan Server Updates on page 6-17*.

   - Enough disk space for downloaded components

2. Point the OfficeScan server to the new update source. For details, see *OfficeScan Server Update Sources on page 6-16*.

3. Identify the components that the server deploys to clients. For a list of deployable components, see *OfficeScan Client Updates on page 6-26*.

> **Tip**
>
> One of the ways to determine if a component is being deployed to clients is by going to the **Update Summary** screen on the web console (**Updates** > **Summary**). In this screen, the update rate for a component that is being deployed will always be larger than 0%.

4. Determine how often to download the components. Pattern files are updated frequently (some on a daily basis) so it is a good practice to update them regularly. For engines and drivers, you can ask your support provider to notify you of critical updates.

5. On the update source:

   a. Connect to the ActiveUpdate server. The server's URL depends on your OfficeScan version.

   b. Download the following items:

      - The `server.ini` file. This file contains information about the latest components.
      - The components you identified in step 3.

   c. Save the downloaded items to a directory in the update source.

6. Run a manual update of the OfficeScan server. For details, see *Manually Updating the OfficeScan Server on page 6-24*.

7. Repeat step 5 to step 6 each time you need to update components.

OfficeScan Server Update Methods

Update OfficeScan server components manually or by configuring an update schedule.

To allow the server to deploy the updated components to clients, enable automatic client update. For details, see *OfficeScan Client Automatic Updates on page 6-35*. If

automatic client update is disabled, the server downloads the updates but does not deploy them to the clients.

Update methods include:

- **Manual server update**: When an update is critical, perform manual update so the server can obtain the updates immediately. See *Manually Updating the OfficeScan Server on page 6-24* for details.
- **Scheduled server update**: The OfficeScan server connects to the update source during the scheduled day and time to obtain the latest components. See *Scheduling Updates for the OfficeScan Server on page 6-24* for details.

Manually Updating the OfficeScan Server

Manually update the components on the OfficeScan server after installing or upgrading the server and whenever there is an outbreak.

Procedure

1. Start a manual update by:
   - Navigating to **Updates** > **Server** > **Manual Update**.
   - Clicking **Update Server Now** on the web console's main menu.
2. Select the components to update.
3. Click **Update**.

   The server downloads the updated components.

Scheduling Updates for the OfficeScan Server

Configure the OfficeScan server to regularly check its update source and automatically download any available updates. Because clients normally get updates from the server, using scheduled update is an easy and effective way of ensuring that protection against security risks is always current.

Procedure

1. Navigate to **Updates** > **Server** > **Scheduled Update**.
2. Select **Enable scheduled update of the OfficeScan server**.
3. Select the components to update.
4. Specify the update schedule.

   For daily, weekly, and monthly updates, the period of time is the number of hours during which OfficeScan will perform the update. OfficeScan updates at any given time during this time period.
5. Click **Save**.

OfficeScan Server Update Logs

Check the server update logs to determine if there are problems updating certain components. Logs include component updates for the OfficeScan server.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing the Update Logs

Procedure

1. Navigate to **Logs** > **Server Update Logs**.
2. Check the **Result** column to see if there are components that were not updated.
3. To save logs to a comma-separated value (`CSV`) file, click **Export to CSV**. Open the file or save it to a specific location.

Integrated Smart Protection Server Updates

The integrated Smart Protection Server downloads two components, namely the Smart Scan Pattern and Web Blocking List. For details on these components and how to update them, see *Integrated Smart Protection Server Management on page 4-17*.

OfficeScan Client Updates

To ensure that clients stay protected from the latest security risks, update client components regularly.

Before updating clients, check if their update source (OfficeScan server or a custom update source) has the latest components. For information on how to update the OfficeScan server, see *OfficeScan Server Updates on page 6-14*.

The following table lists all components that update sources deploy to clients and the components in use when using a particular scan method.

TABLE 6-6. OfficeScan Components Deployed to Clients

COMPONENT	DISTRIBUTION	
	CONVENTIONAL SCAN CLIENTS	SMART SCAN CLIENTS
Antivirus		
Smart Scan Agent Pattern	No	Yes
Virus Pattern	Yes	No
IntelliTrap Pattern	Yes	Yes
IntelliTrap Exception Pattern	Yes	Yes
Virus Scan Engine (32-bit)	Yes	Yes
Virus Scan Engine (64-bit)	Yes	Yes
Anti-spyware		

Component	Distribution	
	Conventional Scan Clients	Smart Scan Clients
Spyware Pattern	Yes	Yes
Spyware Active-monitoring Pattern	Yes	No
Spyware Scan Engine (32-bit)	Yes	Yes
Spyware Scan Engine (64-bit)	Yes	Yes
Damage Cleanup Services		
Virus Cleanup Template	Yes	Yes
Virus Cleanup Engine (32-bit)	Yes	Yes
Virus Cleanup Engine (64-bit)	Yes	Yes
Firewall		
Common Firewall Pattern	Yes	Yes
Behavior Monitoring Components		
Behavior Monitoring Detection Pattern (32-bit)	Yes	Yes
Behavior Monitoring Driver (32-bit)	Yes	Yes
Behavior Monitoring Core Service (32-bit)	Yes	Yes
Behavior Monitoring Detection Pattern (64-bit)	Yes	Yes
Behavior Monitoring Driver (64-bit)	Yes	Yes
Behavior Monitoring Core Service (64-bit)	Yes	Yes
Behavior Monitoring Configuration Pattern	Yes	Yes

Component	Distribution	
	Conventional Scan Clients	Smart Scan Clients
Policy Enforcement Pattern	Yes	Yes
Digital Signature Pattern	Yes	Yes
C&C Contact Alert Service		
C&C IP List	Yes	Yes

OfficeScan Client Update Sources

Clients can obtain updates from the standard update source (OfficeScan server) or specific components from custom update sources such as the Trend Micro ActiveUpdate server. For details, see *Standard Update Source for OfficeScan Clients on page 6-28* and *Customized Update Sources for OfficeScan Clients on page 6-30*.

IPv6 Support for OfficeScan Client Updates

A pure IPv6 client cannot update directly from pure IPv4 update sources, such as:

- A pure IPv4 OfficeScan server
- A pure IPv4 Update Agent
- Any pure IPv4 custom update source
- Trend Micro ActiveUpdate Server

Similarly, a pure IPv4 client cannot update directly from pure IPv6 update sources, such as a pure IPv6 OfficeScan server or Update Agent.

A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the clients to connect to the update sources.

Standard Update Source for OfficeScan Clients

The OfficeScan server is the standard update source for clients.

If the OfficeScan server is unreachable, clients will not have a backup source and will therefore remain outdated. To update clients that cannot reach the OfficeScan server, Trend Micro recommends using Client Packager. Use this tool to create a package with the latest components available on the server and then run the package on clients.

Note

The client's IP address (IPv4 or IPv6) determines if connection to the OfficeScan server can be established. For details about IPv6 support for client updates, see *IPv6 Support for OfficeScan Client Updates on page 6-28*.

Configuring the Standard Update Source for OfficeScan Clients

Procedure

1. Navigate to **Updates** > **Networked Computers** > **Update Source**.
2. Select **Standard update source (update from OfficeScan server)**.
3. Click **Notify All Clients**.

OfficeScan Client Update Process

Note

This topic discusses the update process for OfficeScan clients. The update process for Update Agents is discussed in *Standard Update Source for OfficeScan Clients on page 6-28*.

If you configure OfficeScan clients to update directly from the OfficeScan server, the update process proceeds as follows:

1. The OfficeScan client obtains updates from the OfficeScan server.
2. If unable to update from the OfficeScan server, the OfficeScan client tries connecting directly to the Trend Micro ActiveUpdate server if the option **Clients download updates from the Trend Micro ActiveUpdate Server** is enabled in

Networked Computers > **Client Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings (tab)** > **Update Settings**.

Note

Only components can be updated from the ActiveUpdate server. Domain settings, programs and hot fixes can only be downloaded from the OfficeScan server or Update Agents. You can speed up the update process by configuring OfficeScan clients to only download pattern files from the ActiveUpdate server. For more information, see *ActiveUpdate Server as the OfficeScan Client Update Source on page 6-34*.

Customized Update Sources for OfficeScan Clients

Aside from the OfficeScan server, OfficeScan clients can update from custom update sources. Custom update sources help reduce OfficeScan client update traffic directed to the OfficeScan server and allow OfficeScan clients that cannot connect to the OfficeScan server to get timely updates. Specify the custom update sources on the Customized Update Source List, which can accommodate up to 1024 update sources.

Tip

Trend Micro recommends assigning some OfficeScan clients as Update Agents and then adding them to the list.

Configuring Customized Update Sources for OfficeScan Clients

Procedure

1. Navigate to **Updates** > **Networked Computers** > **Update Source**.
2. Select **Customized Update Source** and click **Add**.
3. In the screen that displays, specify the clients' IP addresses. You can type an IPv4 range and/or an IPv6 prefix and length.
4. Specify the update source. You can select an Update Agent if one has been assigned or type the URL of a specific source.

Note

Ensure that the OfficeScan clients can connect to the update source using their IP addresses. For example, if you specified an IPv4 address range, the update source must have an IPv4 address. If you specified an IPv6 prefix and length, the update source must have an IPv6 address. For details about IPv6 support for client updates, see *OfficeScan Client Update Sources on page 6-28*.

5. Click **Save**.

6. Perform miscellaneous tasks in the screen.

   a. Select any of the following settings. For details on how these settings work, see *OfficeScan Client Update Process on page 6-29*.

      - **Update Agents update components, domain settings, and client programs and hot fixes, only from the OfficeScan server**
      - **Update components from the OfficeScan server if all customized sources are unavailable or not found**
      - **Update domain settings from the OfficeScan server if all customized sources are unavailable or not found**
      - **Update client programs and hot fixes from the OfficeScan server if all customized sources are unavailable or not found**

   b. If you specified at least one Update Agent as source, click **Update Agent Analytical Report** to generate a report that highlights the update status of clients. For details about the report, see *Update Agent Analytical Report on page 6-57*.

   c. Edit an update source by clicking the IP address range link. Modify the settings in the screen that displays and click **Save**.

   d. Remove an update source from the list by selecting the check box and clicking **Delete**.

   e. To move an update source, click the up or down arrow. You can only move one source at a time.

7. Click **Notify All Clients**.

OfficeScan Client Update Process

Note

This topic discusses the update process for OfficeScan clients. The update process for Update Agents is discussed in *Customized Update Sources for Update Agents on page 6-53*.

After you have set up and saved the customized update source list, the update process proceeds as follows:

1. An OfficeScan client updates from the first source on the list.
2. If unable to update from the first source, the OfficeScan client updates from the second source, and so on.
3. If unable to update from all sources, the OfficeScan client checks the following settings on the Update Source screen:

TABLE 6-7. Additional Settings for Custom Update Sources

SETTING	DESCRIPTION
Update Agents update components, domain settings, and client programs and hot fixes, only from the OfficeScan server	If this setting is enabled, Update Agents update directly from the OfficeScan server and disregard the Customized Update Source List. If disabled, Update Agents apply the customized update source settings configured for normal clients.

SETTING	DESCRIPTION
Clients update the following items from the OfficeScan server if all customized sources are unavailable or not found: Components	If this setting is enabled, the client updates components from the OfficeScan server. If disabled, the client then tries connecting directly to the Trend Micro ActiveUpdate server if any of the following is true: • In **Networked Computers** > **Client Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings (tab)** > **Update Settings**, the option **Clients download updates from the Trend Micro ActiveUpdate Server** is enabled. • The ActiveUpdate server is not included in the Customized Update Source List. **Note** Only components can be updated from the ActiveUpdate server. Domain settings, programs and hot fixes can only be downloaded from the OfficeScan server or Update Agents. You can speed up the update process by configuring clients to only download pattern files from the ActiveUpdate server. For more information, see *ActiveUpdate Server as the OfficeScan Client Update Source on page 6-34*.
Clients update the following items from the OfficeScan server if all customized sources are unavailable or not found: Domain settings	If this setting is enabled, the client updates domain-level settings from the OfficeScan server.
Clients update the following items from the OfficeScan server if all customized sources are unavailable or not found: Client programs and hot fixes	If this setting enabled, the client updates programs and hot fixes from the OfficeScan server.

4. If unable to update from all possible sources, the client quits the update process.

ActiveUpdate Server as the OfficeScan Client Update Source

When OfficeScan clients download updates directly from the Trend Micro ActiveUpdate server, you can limit the download to only the pattern files to reduce the bandwidth consumed during updates and speed up the update process.

Scan engines and other components are not updated as frequently as pattern files, which is another reason to limit the download to only the pattern files.

A pure IPv6 client cannot update directly from the Trend Micro ActiveUpdate Server. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the OfficeScan clients to connect to the ActiveUpdate server.

Limiting Downloads from the ActiveUpdate Server

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Go to the **Updates** section.
3. Select **Download only the pattern files from the ActiveUpdate server when performing updates**.

OfficeScan Client Update Methods

OfficeScan clients that update components from the OfficeScan server or a customized update source can use the following update methods:

- **Automatic client updates**: Client update runs automatically when certain events occur or based on a schedule. For details, see *OfficeScan Client Automatic Updates on page 6-35*.

- **Manual client updates**: When an update is critical, use manual update to immediately notify clients to perform component update. For details, see *OfficeScan Client Manual Updates on page 6-41*.

- **Privilege-based updates**: Users with update privileges have greater control over how the OfficeScan client on their computers gets updated. For details, see *Update Privileges and Other Settings for OfficeScan Clients on page 6-43*.

OfficeScan Client Automatic Updates

Automatic update relieves you of the burden of notifying all clients to update and eliminates the risk of client computers not having up-to-date components.

In addition to components, OfficeScan clients also receive updated configuration files during automatic update. Clients need the configuration files to apply new settings. Each time you modify OfficeScan settings through the web console, the configuration files change. To specify how often configuration files are applied to clients, see step 3 *Updating OfficeScan Client Components Automatically on page 6-37*.

Note

You can configure clients to use proxy settings during automatic update. See *Proxy for OfficeScan Client Component Updates on page 6-45* for details.

There are two types of automatic updates:

- *Event-triggered Updates on page 6-35*
- *Schedule-based Updates on page 6-37*

Event-triggered Updates

The server can notify online clients to update components after it downloads the latest components, and offline clients when they restart and then connect to the server. Optionally initiate Scan Now (manual scan) on OfficeScan client computers after the update.

TABLE 6-8. Event-triggered Update Options

OPTION	DESCRIPTION
Initiate component update on clients immediately after the OfficeScan server downloads a new component	The server notifies clients to update as soon as it completes an update. Frequently updated clients only need to download incremental patterns, thus reducing the time it takes to complete the update (see *OfficeScan Server Component Duplication on page 6-19* for details about incremental patterns). However, updating frequently may adversely affect the server's performance, especially if you have a large number of clients updating at the same time. If you have clients on roaming mode and you want these clients to update as well, select Include roaming and offline client(s). See *OfficeScan Client Roaming Privilege on page 14-19* for details about roaming mode.
Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)	A client that missed an update immediately downloads components when it establishes connection with the server. A client may miss an update if it is offline or if the computer where it is installed is not up and running.
Perform Scan Now after updating (excluding roaming clients)	The server notifies clients to scan after an event-triggered update. Consider enabling this option if a particular update is a response to a security risk that has already spread within the network.

Note

If the OfficeScan server is unable to successfully send an update notification to clients after it downloads components, it automatically resends the notification after 15 minutes. The server continues to send update notifications up to a maximum of five times until the client responds. If the fifth attempt is unsuccessful, the server stops sending notifications. If you select the option to update components when clients restart and then connect to the server, component update will still proceed.

Schedule-based Updates

Running scheduled updates is a privilege. You need to first select OfficeScan clients that will have the privilege and these OfficeScan clients will then run updates based on the schedule.

Note

To use schedule-based update with Network Address Translation, see *Configuring Scheduled OfficeScan Client Updates with NAT on page 6-39*.

Updating OfficeScan Client Components Automatically

Procedure

1. Navigate to **Updates** > **Networked Computers** > **Automatic Update**.
2. Select the events that will trigger component update.
   - **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)**
   - **Perform Scan Now after updating (excluding roaming clients)**
3. Select how often clients with scheduled update privilege will perform scheduled update.
   - If you have granted clients scheduled update privilege, proceed to the next step.
   - If you have not granted clients scheduled update privilege, perform the following steps first:

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

   b. In the client tree, select the clients that you want to have the privilege.

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

- Option 1: On the **Privileges** tab, go to the **Component Update Privileges** section. You will see the **Enable scheduled update** option.
- Option 2: On the **Other Settings** tab, go to the **Update Settings** section. You will see another **Enable scheduled update** option.

Note

If you want to give client users the ability to enable or disable scheduled update on the OfficeScan client console, enable options 1 and 2. After you save the settings, updates will run on the client computer as scheduled. Scheduled updates will only stop running when a client user right-clicks the OfficeScan client icon on the system tray and selects **Disable scheduled update**.

If you want scheduled update to always run and prevent client users from disabling scheduled update, disable option 1 and enable option 2.

d. Save the settings.

4. Configure the schedule.

a. If you select **Minute(s)** or **Hour(s)**, you have the option to **Update client configurations only once per day**. If you do not select this option, the OfficeScan client retrieves both the updated components and any updated configuration files available on the server at the interval specified. If you select this option, OfficeScan updates only the components at the interval specified, and the configuration files once per day.

Tip

Trend Micro often updates components; however, OfficeScan configuration settings probably change less frequently. Updating the configuration files with the components requires more bandwidth and increases the time OfficeScan needs to complete the update. For this reason, Trend Micro recommends updating OfficeScan client configurations only once per day.

b. If you select **Daily** or **Weekly**, specify the time of the update and the time period the OfficeScan server will notify clients to update components. For example, if the start time is 12pm and the time period is 2 hours, OfficeScan randomly notifies all online clients to update components from 12pm until 2pm. This setting prevents all online clients from simultaneously connecting

to the server at the specified start time, significantly reducing the amount of traffic directed to the server.

5. Click **Save**.

Offline clients will not be notified. Offline clients that become online after the time period expires can still update components if you selected **Let clients initiate component when they restart**. under **Event-triggered Update**. Otherwise, they update components on the next schedule or if you initiate manual update.

Configuring Scheduled OfficeScan Client Updates with NAT

The following issues may arise if the local network uses NAT:

- OfficeScan clients appear offline on the web console.
- The OfficeScan server is not able to successfully notify clients of updates and configuration changes.

Work around these issues by deploying updated components and configuration files from the server to the OfficeScan client with a scheduled update as described below.

Procedure

- Before installing the OfficeScan client on client computers:
  a. Configure the client update schedule in the **Schedule-based Update** section of **Updates** > **Networked Computers** > **Automatic Update**.
  b. Grant clients the privilege to enable scheduled update in **Networked Computers** > **Client Management**, click **Settings** > **Privileges and Other Settings** > **Privileges (tab)** > **Component Update Privileges**.
- If OfficeScan clients already exist on client computers:
  a. Grant clients the privilege to perform "Update Now" in **Networked Computers** > **Client Management**, click **Settings** > **Privileges and Other Settings** > **Privileges (tab)** > **Component Update Privileges**.

b. Instruct users to manually update components on the client computer (by right-clicking the OfficeScan client icon in the system tray and clicking "Update Now") to obtain the updated configuration settings.

When OfficeScan clients update, they will receive both the updated components and the configuration files.

Using the Domains Schedule Update Tool

The update schedule configured in automatic client updates only applies to clients with scheduled update privileges. For other clients, you can set a separate update schedule. To do this, you will need to configure a schedule by client tree domains. All clients belonging to the domain will apply the schedule.

Note

It is not possible to set an update schedule for a specific client or a specific subdomain. All subdomains apply the schedule configured for their parent domain.

Procedure

1. Record the client tree domain names and update schedules.
2. Navigate to <*Server installation folder*>`\PCCSRV\Admin\Utility\DomainScheduledUpdate`.
3. Copy the following files to `<Server installation folder>\PCCSRV`:
   - `DomainSetting.ini`
   - `dsu_convert.exe`
4. Open `DomainSetting.ini` using a text editor such as Notepad.
5. Specify a client tree domain and then configure the update schedule for the domain. Repeat this step to add more domains.

   Note

   Detailed configuration instructions are provided in the `.ini` file.

6. Save `DomainSetting.ini`.
7. Open a command prompt and change to the directory of the `PCCSRV` folder.
8. Type the following command and press `Enter`.

   ```
   dsuconvert.exe DomainSetting.ini
   ```

9. On the web console, navigate to **Networked Computers** > **Global Client Settings**.
10. Click **Save**.

OfficeScan Client Manual Updates

Update OfficeScan client components manually when OfficeScan client components are severely out-of-date and whenever there is an outbreak. OfficeScan client components become severely out-of-date when the OfficeScan client is unable to update components from the update source for an extended period of time.

In addition to components, OfficeScan clients also receive updated configuration files automatically during manual update. OfficeScan clients need the configuration files to apply new settings. Each time you modify OfficeScan settings through the web console, the configuration files change.

Note

In addition to initiating manual updates, you can grant users the privilege to run manual updates (also called "Update Now" on OfficeScan client computers). For details, see *Update Privileges and Other Settings for OfficeScan Clients on page 6-43*.

Updating OfficeScan Clients Manually

Procedure

1. Navigate to **Updates** > **Networked Computers** > **Manual Update**.
2. The components currently available on the OfficeScan server and the date these components were last updated display on top of the screen. Ensure the components are up-to-date before notifying clients to update.

Note

Manually update any outdated components on the server. See *OfficeScan Client Manual Updates on page 6-41* for details.

3. To update only clients with outdated components:

   a. Click **Select clients with outdated components**.

   b. (Optional) Select **Include roaming and offline client(s)**:

      - To update roaming clients with functional connection to the server.
      - To update offline clients when they become online.

   c. Click **Initiate Update**.

Note

The server searches for clients whose component versions are earlier than the versions on the server and then notifies these clients to update. To check the notification status, go to the **Updates** > **Summary** screen.

4. To update the clients of your choice:

   a. Select **Manually select clients**.

   b. Click **Select**.

   c. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.

   d. Click **Initiate Component Update**.

Note

The server starts notifying each client to download updated components. To check the notification status, go to the **Updates** > **Summary** screen.

Update Privileges and Other Settings for OfficeScan Clients

Grant client users certain privileges, such as performing "Update Now" and enabling scheduled update.

Perform "Update Now"

Users with this privilege can update components on demand by right-clicking the OfficeScan client icon on the system tray and selecting **Update Now**. You can allow client users to use proxy settings during "Update Now". See *Proxy Configuration Privileges for Clients on page 14-48* for details.

WARNING!

Incorrect user-configured proxy settings can cause update problems. Exercise caution when allowing users to configure their own proxy settings.

Enable Scheduled Update

This privilege allows clients to enable/disable scheduled update. Users with the privilege can enable/disable scheduled update but they cannot configure the actual schedule. You need to specify the schedule in the **Schedule-based Update** section of **Updates** > **Networked Computers** > **Automatic Update**.

Clients Download Updates From the Trend Micro ActiveUpdate Server

When initiating updates, OfficeScan clients first get updates from the update source specified on the **Updates** > **Networked Computers** > **Update Source** screen. If the update is unsuccessful, the clients attempt to update from the OfficeScan server. Selecting this option enables clients to attempt to update from the Trend Micro ActiveUpdate server if the update from the OfficeScan server is unsuccessful.

A pure IPv6 client cannot update directly from the Trend Micro ActiveUpdate Server. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the clients to connect to the ActiveUpdate server.

Clients Can Update Components but not Upgrade the Client Program or Deploy Hot Fixes

This option allows component updates to proceed but prevents hot fix deployment and OfficeScan client upgrade.

If you do not select this option, all clients simultaneously connect to the server to upgrade or install a hot fix. This may significantly affect server performance if you have a large number of clients. If you select this option, plan how to minimize the impact of OfficeScan client upgrade or hot fix deployment on the server and then execute your plan.

Granting Update Privileges to OfficeScan Clients

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Component Update Privileges** section.
5. Select the following options:
   - **Perform "Update Now"**
   - **Enable scheduled update**
6. Click the **Other Settings** tab and go to the **Update Settings** section.
7. Select the following options:
   - **Clients download updates from the Trend Micro ActiveUpdate Server**
   - **Enable scheduled update**
   - **Clients can update components but not upgrade the client program or deploy hot fixes**

8. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Configuring Reserved Disk Space for OfficeScan Clients Updates

OfficeScan can allocate a certain amount of client disk space for hot fixes, pattern files, scan engines, and program updates. OfficeScan reserves 60MB of disk space by default.

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Go to the **Reserved Disk Space** section.
3. Select **Reserve __ MB of disk space for updates**.
4. Select the amount of disk space.
5. Click **Save**.

Proxy for OfficeScan Client Component Updates

OfficeScan clients can use proxy settings during automatic update or if they have the privilege to perform "Update Now".

TABLE 6-9. Proxy Settings Used During OfficeScan client Component Updates

UPDATE METHOD	PROXY SETTINGS USED	USAGE
Automatic client update	• Automatic proxy settings. For details, see *Automatic Proxy Settings for the OfficeScan Client on page 14-49*. • Internal proxy settings. For details, see *Internal Proxy for OfficeScan Clients on page 14-46*.	1. OfficeScan clients will first use automatic proxy settings to update components. 2. If automatic proxy settings are not enabled, internal proxy settings will be used. 3. If both are disabled, clients will not use any proxy settings.
Update Now	• Automatic proxy settings. For details, see *Automatic Proxy Settings for the OfficeScan Client on page 14-49*. • User-configured proxy settings. You can grant client users the privilege to configure proxy settings. For details, see *Proxy Configuration Privileges for Clients on page 14-48*.	1. OfficeScan clients will first use automatic proxy settings to update components. 2. If automatic proxy settings are not enabled, user-configured proxy settings will be used. 3. If both are disabled, or if automatic proxy settings are disabled and client users do not have the required privilege, clients will not use any proxy when updating components.

Configuring OfficeScan Client Update Notifications

OfficeScan notifies client users when update-related events occur.

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Go to the **Alert Settings** section.

3. Select the following options:

   - **Show the alert icon on the windows taskbar if the virus pattern file is not updated after __ day(s)**: An alert icon displays on the Windows task bar to remind users to update a Virus Pattern that has not been updated within the specified number of days. To update the pattern, use any of the update methods discussed in *OfficeScan Client Update Methods on page 6-34*.

     All clients managed by the server will apply this setting.

   - **Display a notification message if the client computer needs to restart to load a kernel mode driver**: After installing a hot fix or an upgrade package that contains a new version of a kernel mode driver, the driver's previous version may still exist on the computer. The only way to unload the previous version and load the new one is to restart the computer. After restarting the computer, the new version automatically installs and no further restart is necessary.

     The notification message displays immediately after a client computer installs the hot fix or upgrade package.

4. Click **Save**.

Viewing OfficeScan Client Update Logs

Check the client update logs to determine if there are problems updating the Virus Pattern on clients.

Note

In this product version, only logs for Virus Pattern updates can be queried from the web console.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Procedure

1. Navigate to **Logs** > **Networked Computer Logs** > **Component Update**.
2. To view the number of client updates, click **View** under the **Progress** column. In the **Component Update Progress** screen that displays, view the number of clients updated for every 15-minute interval and the total number of clients updated.
3. To view clients that have updated the Virus Pattern, click **View** under the **Details** column.
4. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Enforcement of OfficeScan Client Updates

Use Security Compliance to ensure that clients have the latest components. Security Compliance determines component inconsistencies between the OfficeScan server and clients. Inconsistencies typically occur when clients cannot connect to the server to update components. If the client obtains an update from another source (such as the ActiveUpdate server), it is possible for a component in the client to be newer than the one in the server.

For more information, see *Security Compliance for Managed Clients on page 14-53*.

Rolling Back Components for OfficeScan Clients

Rollback refers to reverting to the previous version of the Virus Pattern, Smart Scan Agent Pattern, and Virus Scan Engine. If these components do not function properly, roll them back to their previous versions. OfficeScan retains the current and the previous versions of the Virus Scan Engine, and the last five versions of the Virus Pattern and Smart Scan Agent Pattern.

Note

Only the above-mentioned components can be rolled back.

OfficeScan uses different scan engines for clients running 32-bit and 64-bit platforms. You need to roll back these scan engines separately. The rollback procedure for all types of scan engines is the same.

Procedure

1. Navigate to **Updates** > **Rollback**
2. Click **Synchronize with Server** under the appropriate section.
   a. In the client tree that displays, click the root domain icon ( ) to include all clients or select specific domains or clients.
   b. Click **Rollback**.
   c. Click **View Update Logs** to check the result or **Back** to return to the Rollback screen.
3. If an older version pattern file exists on the server, click **Rollback Server and Client Versions** to roll back the pattern file for both the OfficeScan client and the server.

Running the Touch Tool for OfficeScan Client Hot Fixes

The Touch Tool synchronizes the time stamp of one file with the time stamp of another file or with the system time of the computer. If you unsuccessfully attempt to deploy a hot fix on the OfficeScan server, use the Touch Tool to change the time stamp of the hot fix. This causes OfficeScan to interpret the hot fix file as new, which makes the server attempt to automatically deploy the hot fix again.

Procedure

1. On the OfficeScan server, go to <*Server installation folder*>`\PCCSRV\Admin\Utility\Touch`.
2. Copy `TMTouch.exe` to the folder that contains the file you want to change. If synchronizing the file time stamp with the time stamp of another file, put both files in the same location with the Touch tool.
3. Open a command prompt and go to the location of the Touch Tool.

4. Type the following:

```
TmTouch.exe <destination file name> <source file name>
```

Where:

- `<destination file name>` is the name of the hot fix file whose time stamp you want to change
- `<source file name>` is the name of the file whose time stamp you want to replicate

Note

If you do not specify a source file name, the tool sets the destination file time stamp to the system time of the computer. Use the wild card character (*) for the destination file, but not for the source file name.

5. To check if the time stamp changed, type `dir` in the command prompt, or check the file's properties from Windows Explorer.

Update Agents

To distribute the task of deploying components, domain settings, or client programs and hot fixes to OfficeScan clients, assign some OfficeScan clients to act as Update Agents, or update sources for other clients. This helps ensure that clients receive updates in a timely manner without directing a significant amount of network traffic to the OfficeScan server.

If the network is segmented by location and the network link between segments experiences a heavy traffic load, assign at least one Update Agent on each location.

Update Agent System Requirements

Visit the following website for a complete list of system requirements:

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

Update Agent Configuration

Update Agent configuration is a 2-step process:

1. Assign an OfficeScan client as an Update Agent for specific components.
2. Specify the clients that will update from this Update Agent.

Note

The number of concurrent client connections that a single Update Agent can handle depends on the hardware specifications of the computer.

Assigning an OfficeScan Client as an Update Agent

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, select the clients that will be designated as Update Agents.

Note

It is not possible to select the root domain icon as this will designate all clients as Update Agents. A pure IPv6 Update Agent cannot distribute updates directly to pure IPv4 clients. Similarly, a pure IPv4 Update Agent cannot distribute updates directly to pure IPv6 clients. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Update Agent to distribute updates to the clients.

3. Click **Settings** > **Update Agent Settings**.
4. Select the items that Update Agents can share.
   - Component updates
   - Domain settings
   - Client programs and hot fixes
5. Click **Save**.

Specifying the OfficeScan Clients that Update from an Update Agent

Procedure

1. Navigate to **Updates** > **Networked Computers** > **Update Source**.
2. Under **Customized Update Source List**, click **Add**.
3. In the screen that displays, specify the clients' IP addresses. You can type an IPv4 range and/or an IPv6 prefix and length.
4. In the **Update agent** field, select the Update Agent you wish to assign to the clients.

   Note

   Ensure that the clients can connect to the Update Agent using their IP addresses. For example, if you specified an IPv4 address range, the Update Agent must have an IPv4 address. If you specified an IPv6 prefix and length, the Update Agent must have an IPv6 address.

5. Click **Save**.

Update Sources for Update Agents

Update Agents can obtain updates from various sources, such as the OfficeScan server or a customized update source. Configure the update source from the web console's Update Source screen.

IPv6 Support for Update Agents

A pure IPv6 Update Agent cannot update directly from pure IPv4 update sources, such as:

- A pure IPv4 OfficeScan server
- Any pure IPv4 custom update source
- Trend Micro ActiveUpdate server

Similarly, a pure IPv4 Update Agent cannot update directly from pure IPv6 update sources, such as a pure IPv6 OfficeScan server.

A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Update Agent to connect to the update sources.

Standard Update Source for Update Agents

The OfficeScan server is the standard update source for Update Agents. If you configure agents to update directly from the OfficeScan server, the update process proceeds as follows:

1. The Update Agent obtains updates from the OfficeScan server.
2. If unable to update from the OfficeScan server, the agent tries connecting directly to the Trend Micro ActiveUpdate server if any of the following are true:
   - In **Networked Computers** > **Client Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings** > **Update Settings**, the option **Clients download updates from the Trend Micro ActiveUpdate Server** is enabled.
   - The ActiveUpdate server is the first entry in the Customized Update Source List.

   Tip

   Place the ActiveUpdate server at the top of the list only if you experience problems updating from the OfficeScan server. When Update Agents update directly from the ActiveUpdate server, significant bandwidth is consumed between the network and the Internet.

3. If unable to update from all possible sources, the Update Agent quits the update process.

Customized Update Sources for Update Agents

Aside from the OfficeScan server, Update Agents can update from custom update sources. Custom update sources help reduce client update traffic directed to the OfficeScan server. Specify the custom update sources on the Customized Update Source

List, which can accommodate up to 1024 update sources. See *Customized Update Sources for OfficeScan Clients on page 6-30* for steps to configure the list.

Note

Ensure that the **Update Agents update components, domain settings, and client programs and hot fixes, only from the OfficeScan server** option is disabled on the

Update Source (Networked Computers) screen (**Updates** > **Networked Computers** > **Update Source**) in order for Update Agents to connect to the customized update sources.

After you have set up and saved the list, the update process proceeds as follows:

1. The Update Agent updates from the first entry on the list.
2. If unable to update from the first entry, the agent updates from the second entry, and so on.
3. If unable to update from all entries, the agent checks the following options:
   - **Update components from the OfficeScan server if all customized sources are not available or not found**: If enabled, the agent updates from the OfficeScan server.

     If the option is disabled, the agent then tries connecting directly to the Trend Micro ActiveUpdate server if any of the following are true:

     Note

     You can only update components from the Active Update server. Domain settings, programs and hot fixes can only be downloaded from the server or Update Agents.

     - In **Networked Computers** > **Client Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings** > **Update Settings**, the option **Clients download updates from the Trend Micro ActiveUpdate Server** is enabled.
     - The ActiveUpdate server is not included in the Customized Update Source List.

- **Update domain settings from the OfficeScan server if all customized sources are not available or not found**: If enabled, the agent updates from the OfficeScan server.
- **Update client programs and hot fixes from the OfficeScan server if all customized sources are not available or not found**: If enabled, the agent updates from the OfficeScan server.

4. If unable to update from all possible sources, the Update Agent quits the update process.

The update process is different if the option **Update agent: always update from standard update source (OfficeScan server)** is enabled and the OfficeScan server notifies the agent to update components. The process is as follows:

1. The agent updates directly from the OfficeScan server and disregards the update source list.
2. If unable to update from the server, the agent tries connecting directly to the Trend Micro ActiveUpdate server if any of the following are true:
   - In **Networked Computers** > **Client Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings** > **Update Settings**, the option **Clients download updates from the Trend Micro ActiveUpdate Server** is enabled.
   - The ActiveUpdate server is the first entry in the Customized Update Source List.

Tip

Place the ActiveUpdate server at the top of the list only if you experience problems updating from the OfficeScan server. When OfficeScan clients update directly from the ActiveUpdate server, significant bandwidth is consumed between the network and the Internet.

3. If unable to update from all possible sources, the Update Agent quits the update process.

Configuring the Update Source for the Update Agent

Procedure

1. Navigate to **Updates** > **Networked Computers** > **Update Source**.
2. Select whether to update from the standard update source for Update Agents (OfficeScan server) or customized update source for update agents.
3. Click **Notify All Clients**.

Update Agent Component Duplication

Like the OfficeScan server, Update Agents also use component duplication when downloading components. See *OfficeScan Server Component Duplication on page 6-19* for details on how the server performs component duplication.

The component duplication process for Update Agents is as follows:

1. The Update Agent compares its current full pattern version with the latest version on the update source. If the difference between the two versions is 14 or less, the Update Agent downloads the incremental pattern that accounts for the difference between the two versions.

   Note

   If the difference is more than 14, the Update Agent automatically downloads the full version of the pattern file.

2. The Update Agent merges the incremental pattern it downloaded with its current full pattern to generate the latest full pattern.
3. The Update Agent downloads all the remaining incremental patterns on the update source.
4. The latest full pattern and all the incremental patterns are made available to clients.

Update Methods for Update Agents

Update Agents use the same update methods available to regular clients. For details, see *OfficeScan Client Update Methods on page 6-34*.

You can also use the Scheduled Update Configuration tool to enable and configure scheduled updates on an Update Agent that was installed using Client Packager.

Note

This tool is not available if the Update Agent was installed using other installation methods. See *Deployment Considerations on page 5-10* for more information.

Using the Scheduled Update Configuration Tool

Procedure

1. On the Update Agent computer, navigate to <*Client installation folder*>.
2. Double-click `SUCTool.exe` to run the tool. The Schedule Update Configuration Tool console opens.
3. Select **Enable Scheduled Update**.
4. Specify the update frequency and time.
5. Click **Apply**.

Update Agent Analytical Report

Generate the Update Agent Analytical Report to analyze the update infrastructure and determine which clients download partial updates from Update Agents and other update sources.

Note

This report includes all OfficeScan clients configured to receive partial updates from Update Agents. If you have delegated the task of managing one or several domains to other administrators, they will also see all OfficeScan clients configured to receive partial updates from Update Agents belonging to the domains that they are not managing.

OfficeScan exports the Update Agent Analytical Report to a comma-separated value (`.csv`) file.

This report contains the following information:

- OfficeScan client computer
- IP address
- Client tree path
- Update source
- If clients download the following from Update Agents:
  - Components
  - Domain settings
  - OfficeScan client programs and hot fixes

Important

The Update Agent Analytical Report only lists OfficeScan clients configured to receive partial updates from an Update Agent. OfficeScan clients configured to perform complete updates from an Update Agent (including components, domain settings, and OfficeScan client programs and hot fixes) do not appear in the report.

For details on generating the report, see *Customized Update Sources for OfficeScan Clients on page 6-30*.

Component Update Summary

The web console provides an **Update Summary** screen (navigate to **Updates** > **Summary**) that informs you of the overall component update status and lets you update outdated components. If you enable server scheduled update, the screen will also show the next update schedule.

Refresh the screen periodically to view the latest component update status.

Note

To view component updates on the integrated Smart Protection Server, go to **Smart Protection** > **Integrated Server**.

Update Status for OfficeScan Clients

If you initiated component update to clients, view the following information in this section:

- Number of clients notified to update components.
- Number of clients not yet notified but already in the notification queue. To cancel the notification to these clients, click **Cancel Notification**.

Components

In the **Update Status** table, view the update status for each component that the OfficeScan server downloads and distributes.

For each component, view its current version and the last update date. Click the number link to view clients with out-of-date components. Manually update clients with out-of-date components.

Chapter 7

Scanning for Security Risks

This chapter describes how to protect computers from security risks using file-based scanning.

Topics in this chapter:

- *About Security Risks on page 7-2*
- *Scan Methods on page 7-7*
- *Scan Types on page 7-13*
- *Settings Common to All Scan Types on page 7-26*
- *Scan Privileges and Other Settings on page 7-49*
- *Global Scan Settings on page 7-64*
- *Security Risk Logs on page 7-83*
- *Security Risk Notifications on page 7-74*

About Security Risks

Security risk is the collective term for viruses/malware and spyware/grayware. OfficeScan protects computers from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak. OfficeScan can help contain outbreaks by enforcing outbreak prevention policies and isolating infected computers until they are completely risk-free. Notifications and logs help you keep track of security risks and alert you if you need to take immediate action.

Viruses and Malware

Tens of thousands of virus/malware exist, with more being created each day. Although once most common in DOS or Windows, computer viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and websites.

- **Joke program**: A virus-like program that often manipulates the appearance of things on a computer monitor.
- **Probable virus/malware**: Suspicious files that have some of the characteristics of virus/malware. For details, see the Trend Micro Virus Encyclopedia:

  http://www.trendmicro.com/vinfo/virusencyclo/
- **Rootkit**: A program (or collection of programs) that installs and executes code on a system without end user consent or knowledge. It uses stealth to maintain a persistent and undetectable presence on the machine. Rootkits do not infect machines, but rather, seek to provide an undetectable environment for malicious code to execute. Rootkits are installed on systems via social engineering, upon execution of malware, or simply by browsing a malicious website. Once installed, an attacker can perform virtually any function on the system to include remote access, eavesdropping, as well as hide processes, files, registry keys and communication channels.
- **Trojan horse**: This type of threat often uses ports to gain access to computers or executable programs. Trojan horse programs do not replicate but instead reside on systems to perform malicious acts, such as opening ports for hackers to enter. A

Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those already running on the system.

- **Virus**: A program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes, including:
  - **ActiveX malicious code**: Code that resides on web pages that execute ActiveX™ controls.
  - **Boot sector virus**: A virus that infects the boot sector of a partition or a disk.
  - **COM and EXE file infector**: An executable program with `.com` or `.exe` extension.
  - **Java malicious code**: Operating system-independent virus code written or embedded in Java™.
  - **Macro virus**: A virus encoded as an application macro and often included in a document.
  - **Network Virus**: A virus spreading over a network is not, strictly speaking, a network virus. Only some virus/malware types, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of client computers, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.

    The OfficeScan firewall works with the Common Firewall Pattern to identify and block network viruses. See *About the OfficeScan Firewall on page 12-2* for details.
  - **Packer**: A compressed and/or encrypted Windows or Linux™ executable program, often a Trojan horse program. Compressing executables makes packer more difficult for antivirus products to detect.
  - **Test virus**: An inert file that acts like a real virus and is detectable by virus-scanning software. Use test viruses, such as the EICAR test script, to verify that your antivirus installation scans properly.

- **VBScript**, **JavaScript** or **HTML virus**: A virus that resides on web pages and downloaded through a browser.
- **Worm**: A self-contained program or set of programs able to spread functional copies of itself or its segments to other computer systems, often through email.
- **Others**: Virus/Malware not categorized under any of the other virus/malware types.

Spyware and Grayware

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

If you find an application or file that OfficeScan cannot detect as grayware but you think is a type of grayware, send it to Trend Micro for analysis:

http://subwiz.trendmicro.com/SubWiz

Types of Spyware/Grayware

- **Spyware**: Gathers data, such as account user names and passwords, and transmits them to third parties.
- **Adware**: Displays advertisements and gathers data, such as user web surfing preferences, used for targeting advertisements at the user through a web browser.
- **Dialer**: Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem. These are often pay-per-call or international numbers that can result in a significant expense for your organization.
- **Joke program**: Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes.

- **Hacking tool**: Helps hackers enter computers.
- **Remote access tool**: Helps hackers remotely access and control computers.
- **Password cracking application**: Helps hackers decipher account user names and passwords.
- **Others**: Other types of potentially malicious programs.

How Spyware/Grayware Gets into the Network

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

Potential Risks and Threats

The existence of spyware and other types of grayware on the network has the potential to introduce the following:

- **Reduced Computer Performance**: To perform their tasks, spyware/grayware applications often require significant CPU and system memory resources.
- **Increased Web Browser-related Crashes**: Certain types of grayware, such as adware, often display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a computer restart.
- **Reduced User Efficiency**: By needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users become unnecessarily distracted from their main tasks.
- **Degradation of Network Bandwidth**: Spyware/Grayware applications often regularly transmit the data they collect to other applications running on or outside the network.
- **Loss of Personal and Corporate Information**: Not all data spyware/grayware applications collect is as innocuous as a list of websites users visit. Spyware/

Grayware can also collect user credentials, such as those used to access online banking accounts and corporate networks.

- **Higher Risk of Legal Liability**: If computer resources on the network are hijacked, hackers may be able to utilize client computers to launch attacks or install spyware/grayware on computers outside the network. The participation of network resources in these types of activities could leave an organization legally liable to damages incurred by other parties.

Guarding Against Spyware/Grayware and Other Threats

There are many steps you can take to prevent the installation of spyware/grayware onto your computer. Trend Micro suggests the following:

- Configure all types of scans (Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now) to scan for and remove spyware/grayware files and applications. See *Scan Types on page 7-13* for more information.
- Educate your client users to do the following:
  - Read the End User License Agreement (EULA) and included documentation of applications they download and install on their computers.
  - Click **No** to any message asking for authorization to download and install software unless client users are certain both the creator of the software and the website they view are trustworthy.
  - Disregard unsolicited commercial email (spam), especially if the spam asks users to click a button or hyperlink.
- Configure web browser settings that ensure a strict level of security. Trend Micro recommends requiring web browsers to prompt users before installing ActiveX controls.
- If using Microsoft Outlook, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages.
- Do not allow the use of peer-to-peer file-sharing services. Spyware and other grayware applications may be masked as other types of files your users may want to download, such as MP3 music files.

- Periodically examine the installed software on your agent computers and look for applications that may be spyware or other grayware.
- Keep your Windows operating systems updated with the latest patches from Microsoft. See the Microsoft website for details.

Scan Methods

OfficeScan clients can use one of two scan methods when scanning for security risks. The scan methods are smart scan and conventional scan.

- **Smart Scan**

  Clients that use smart scan are referred to as **smart scan clients** in this document. Smart scan clients benefit from local scans and in-the-cloud queries provided by File Reputation Services.

- **Conventional Scan**

  Clients that do not use smart scan are called **conventional scan clients**. A conventional scan client stores all OfficeScan components on the client computer and scans all files locally.

Default Scan Method

In this OfficeScan version, the default scan method for fresh installations is smart scan. This means that if you perform an OfficeScan server fresh installation and do not change the scan method on the web console, all clients that the server manages use smart scan.

If you upgrade the OfficeScan server from an earlier version and automatic client upgrade is enabled, all clients managed by the server still use the scan method configured before the upgrade. For example, upgrading from OfficeScan 8.x, which only supports conventional scan, means that all clients still use conventional scan upon upgrade. If you upgrade from OfficeScan 10, which supports smart scan and conventional scan, all upgraded clients that use smart scan continue to use smart scan and all clients using conventional scan continue to use conventional scan.

Scan Methods Compared

The following table provides a comparison between the two scan methods:

TABLE 7-1. Conventional Scan and Smart Scan Compared

BASIS OF COMPARISON	CONVENTIONAL SCAN	SMART SCAN
Availability	Available in this OfficeScan version and all earlier OfficeScan versions	Available starting in OfficeScan 10
Scanning behavior	The conventional scan client performs scanning on the local computer.	• The smart scan client performs scanning on the local computer. • If the client cannot determine the risk of the file during the scan, the client verifies the risk by sending a scan query to a smart protection source. • The client "caches" the scan query result to improve the scan performance.
Components in use and updated	All components available on the update source, except the Smart Scan Agent Pattern	All components available on the update source, except the Virus Pattern and Spyware Active-monitoring Pattern
Typical update source	OfficeScan server	OfficeScan server

Changing the Scan Method

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.

3. Click **Settings** > **Scan Settings** > **Scan Methods**.
4. Select **Conventional scan** or **Smart scan**.
5. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Switching from Smart Scan to Conventional Scan

When you switch clients to conventional scan, consider the following:

1. **Number of clients to switch**

   Switching a relatively small number of clients at a time allows efficient use of OfficeScan server and Smart Protection Server resources. These servers can perform other critical tasks while clients change their scan methods.

2. **Timing**

   When switching back to conventional scan, clients will likely download the full version of the Virus Pattern and Spyware-active Monitoring Pattern from the OfficeScan server. These pattern files are only used by conventional scan clients.

   Consider switching during off-peak hours to ensure the download process finishes within a short amount of time. Also consider switching when no client is scheduled to update from the server. Also temporarily disable "Update Now" on clients and re-enable it after the clients have switched to smart scan.

3. **Client tree settings**

   Scan method is a granular setting that can be set on the root, domain, or individual client level. When switching to conventional scan, you can:

- Create a new client tree domain and assign conventional scan as its scan method. Any client you move to this domain will use conventional scan. When you move the client, enable the setting **Apply settings of new domain to selected clients**.
- Select a domain and configure it to use conventional scan. Smart scan clients belonging to the domain will switch to conventional scan.
- Select one or several smart scan clients from a domain and then switch them to conventional scan.

Note

Any changes to the domain's scan method overrides the scan method you have configured for individual clients.

Switching from Conventional Scan to Smart Scan

If you are switching clients from conventional scan to smart scan, ensure that you have set up Smart Protection Services. For details, see *Setting Up Smart Protection Services on page 4-12*.

The following table provides other considerations when switching to smart scan:

TABLE 7-2. Considerations When Switching to Smart Scan

CONSIDERATION	DETAILS
Unavailable features and functions	Smart scan clients cannot report Smart Scan Pattern and Smart Scan Agent Pattern information to the Policy Server.
Product license	To use smart scan, ensure that you have activated the licenses for the following services and that the licenses are not expired: • Antivirus • Web Reputation and Anti-spyware

CONSIDERATION	DETAILS
OfficeScan server	Ensure that clients can connect to the OfficeScan server. Only online clients will be notified to switch to smart scan. Offline clients get notified when they become online. Roaming clients are notified when they become online or, if the client has scheduled update privileges, when scheduled update runs. Also verify that the OfficeScan server has the latest components because smart scan clients need to download the Smart Scan Agent Pattern from the server. To update components, see *OfficeScan Server Updates on page 6-14*.
Number of clients to switch	Switching a relatively small number of clients at a time allows efficient use of OfficeScan server resources. The OfficeScan server can perform other critical tasks while clients change their scan methods.
Timing	When switching to smart scan for the first time, clients need to download the full version of the Smart Scan Agent Pattern from the OfficeScan server. The Smart Scan Pattern is only used by smart scan clients. Consider switching during off-peak hours to ensure the download process finishes within a short amount of time. Also consider switching when no client is scheduled to update from the server. Also temporarily disable "Update Now" on clients and re-enable it after the clients have switched to smart scan.

CONSIDERATION	DETAILS
Client tree settings	Scan method is a granular setting that can be set on the root, domain, or individual client level. When switching to smart scan, you can: • Create a new client tree domain and assign smart scan as its scan method. Any client you move to this domain will use smart scan. When you move the client, enable the setting **Apply settings of new domain to selected clients**. • Select a domain and configure it to use smart scan. Conventional scan clients belonging to the domain will switch to smart scan. • Select one or several conventional scan clients from a domain and then switch them to smart scan. **Note** Any changes to the domain's scan method overrides the scan method you have configured for individual clients.

Consideration	Details
IPv6 support	Smart scan clients send scan queries to smart protection sources. A pure IPv6 smart scan client cannot send queries directly to pure IPv4 sources, such as: • Smart Protection Server 2.0 (integrated or standalone) **Note** IPv6 support for Smart Protection Server starts in version 2.5. • Trend Micro Smart Protection Network Similarly, a pure IPv4 smart scan client cannot send queries to pure IPv6 Smart Protection Servers. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow smart scan clients to connect to the sources.

Scan Types

OfficeScan provides the following scan types to protect OfficeScan client computers from security risks:

Table 7-3. Scan Types

Scan Type	Description
Real-time Scan	Automatically scans a file on the computer as it is received, opened, downloaded, copied, or modified See *Real-time Scan on page 7-14* for details.
Manual Scan	A user-initiated scan that scans a file or a set of files requested by the user See *Manual Scan on page 7-17* for details.

Scan Type	Description
Scheduled Scan	Automatically scans files on the computer based on the schedule configured by the administrator or end user See *Scheduled Scan on page 7-19* for details.
Scan Now	An administrator-initiated scan that scans files on one or several target computers See *Scan Now on page 7-21* for details.
Intensive scanning	An automatically initiated scan that provides heightened scanning for probable malware on computers determined to be high risks See *Intensive Scanning on page 7-24* for details.

Real-time Scan

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If OfficeScan detects no security risk, the file remains in its location and users can proceed to access the file. If OfficeScan detects a security risk or a probable virus/malware, it displays a notification message, showing the name of the infected file and the specific security risk.

Note

To modify the notification message, open the web console and go to **Notifications** > **Client User Notifications**.

Configure and apply Real-time Scan settings to one or several clients and domains, or to all clients that the server manages.

Configuring Real-time Scan Settings

Procedure

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

2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Scan Settings** > **Real-time Scan Settings**.
4. On the **Target** tab, select the following options:
   - Enable virus/malware scan
   - Enable spyware/grayware scan

   Note

   If you disable virus/malware scanning, spyware/grayware scanning also becomes disabled. During a virus outbreak, Real-time Scan cannot be disabled (or will automatically be enabled if initially disabled) to prevent the virus from modifying or deleting files and folders on client computers.

5. Configure the following scan criteria:
   - *User Activity on Files on page 7-26*
   - *Files to Scan on page 7-26*
   - *Scan Settings on page 7-27*
   - *Scan Exclusions on page 7-29*
6. Click the **Action** tab and then configure the following:

TABLE 7-4. Real-time Scan Actions

ACTION	REFERENCE
Virus/Malware action	Primary action (select one): • *Use ActiveAction on page 7-36* • *Use the Same Action for all Virus/Malware Types on page 7-37* • *Use a Specific Action for Each Virus/Malware Type on page 7-37* **Note** For details about the different actions, see *Virus/Malware Scan Actions on page 7-34*. Additional virus/malware actions: • *Quarantine Directory on page 7-38* • *Back Up Files Before Cleaning on page 7-39* • *Damage Cleanup Services on page 7-40* • *Display a Notification Message When Virus/Malware is Detected on page 7-41* • *Display a Notification Message When Probable Virus/Malware is Detected on page 7-41*
Spyware/Grayware action	Primary action: • *Spyware/Grayware Scan Actions on page 7-45* Additional spyware/grayware action: • *Display a Notification Message When Spyware/Grayware is Detected on page 7-45*

7. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Manual Scan

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the OfficeScan client console. The time it takes to complete scanning depends on the number of files to scan and the OfficeScan client computer's hardware resources.

Configure and apply Manual Scan settings to one or several clients and domains, or to all clients that the server manages.

Configuring a Manual Scan

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Scan Settings** > **Manual Scan Settings**.
4. On the **Target** tab, configure the following:
   - *Files to Scan on page 7-26*
   - *Scan Settings on page 7-27*
   - *CPU Usage on page 7-28*
   - *Scan Exclusions on page 7-29*
5. Click the **Action** tab and then configure the following:

TABLE 7-5. Manual Scan Actions

ACTION	REFERENCE
Virus/Malware action	Primary action (select one): • *Use ActiveAction on page 7-36* • *Use the Same Action for all Virus/Malware Types on page 7-37* • *Use a Specific Action for Each Virus/Malware Type on page 7-37* **Note** For details about the different actions, see *Virus/Malware Scan Actions on page 7-34*. Additional virus/malware actions: • *Quarantine Directory on page 7-38* • *Back Up Files Before Cleaning on page 7-39* • *Damage Cleanup Services on page 7-40*
Spyware/Grayware action	Primary action: • *Spyware/Grayware Scan Actions on page 7-45*

6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Scheduled Scan

Scheduled Scan runs automatically on the appointed date and time. Use Scheduled Scan to automate routine scans on the client and improve scan management efficiency.

Configure and apply Scheduled Scan settings to one or several clients and domains, or to all clients that the server manages.

Configuring a Scheduled Scan

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Scan Settings** > **Scheduled Scan Settings**.
4. On the **Target** tab, select the following options:
   - **Enable virus/malware scan**
   - **Enable spyware/grayware scan**

   Note

   If you disable virus/malware scanning, spyware/grayware scanning also becomes disabled.

5. Configure the following scan criteria:
   - *Schedule on page 7-29*
   - *Files to Scan on page 7-26*
   - *Scan Settings on page 7-27*
   - *CPU Usage on page 7-28*
   - *Scan Exclusions on page 7-29*

6. Click the **Action** tab and then configure the following:

TABLE 7-6. Scheduled Scan Actions

ACTION	REFERENCE
Virus/Malware action	Primary action (select one): • *Use ActiveAction on page 7-36* • *Use the Same Action for all Virus/Malware Types on page 7-37* • *Use a Specific Action for Each Virus/Malware Type on page 7-37* **Note** For details about the different actions, see *Virus/Malware Scan Actions on page 7-34*. Additional virus/malware actions: • *Quarantine Directory on page 7-38* • *Back Up Files Before Cleaning on page 7-39* • *Damage Cleanup Services on page 7-40* • *Display a Notification Message When Virus/Malware is Detected on page 7-41* • *Display a Notification Message When Probable Virus/Malware is Detected on page 7-41*
Spyware/Grayware action	Primary action: • *Spyware/Grayware Scan Actions on page 7-45* Additional spyware/grayware action: • *Display a Notification Message When Spyware/Grayware is Detected on page 7-45*

7. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Scan Now

Scan Now is initiated remotely by an OfficeScan administrator through the web console and can be targeted to one or several client computers.

Configure and apply Scan Now settings to one or several clients and domains, or to all clients that the server manages.

Configuring Scan Now Settings

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Scan Settings** > **Scan Now Settings**.
4. On the **Target** tab, select the following options:
   - **Enable virus/malware scan**
   - **Enable spyware/grayware scan**

   Note

   If you disable virus/malware scanning, spyware/grayware scanning also becomes disabled.

5. Configure the following scan criteria:

- *Files to Scan on page 7-26*
- *Scan Settings on page 7-27*
- *CPU Usage on page 7-28*
- *Scan Exclusions on page 7-29*

6. Click the **Action** tab and then configure the following:

TABLE 7-7. Scan Now Actions

ACTION	REFERENCE
Virus/Malware action	Primary action (select one): • *Use ActiveAction on page 7-36* • *Use the Same Action for all Virus/Malware Types on page 7-37* • *Use a Specific Action for Each Virus/Malware Type on page 7-37* **Note** For details about the different actions, see *Virus/Malware Scan Actions on page 7-34*. Additional virus/malware actions: • *Quarantine Directory on page 7-38* • *Back Up Files Before Cleaning on page 7-39* • *Damage Cleanup Services on page 7-40*
Spyware/Grayware action	Primary action: • *Spyware/Grayware Scan Actions on page 7-45*

7. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Initiating Scan Now

Initiate Scan Now on computers that you suspect to be infected.

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Tasks** > **Scan Now**.
4. To change the pre-configured **Scan Now** settings before initiating the scan, click **Settings**.

   The **Scan Now Settings screen** opens. See *Scan Now on page 7-21* for details.
5. In the client tree, select the clients that will perform scanning and then click **Initiate Scan Now**.

   Note

   If you do not select any client, OfficeScan automatically notifies all clients in the client tree.

   The server sends a notification to the clients.
6. Check the notification status and see if there are clients that did not receive the notification.
7. Click **Select Un-notified Computers** and then **Initiate Scan Now** to immediately resend the notification to un-notified clients.

   Example: Total number of clients: 50

TABLE 7-8. Un-notified Client Scenarios

CLIENT TREE SELECTION	NOTIFIED CLIENTS (AFTER CLICKING "INITIATE SCAN NOW")	UN-NOTIFIED CLIENTS
None (all 50 clients automatically selected)	35 out of 50 clients	15 clients
Manual selection (45 out of 50 clients selected)	40 out of 45 clients	5 clients + another 5 clients not included in the manual selection

8. Click **Stop Notification** to prompt OfficeScan to stop notifying clients currently being notified. Clients already notified and in the process of scanning will ignore this command.

9. For clients already in the process of scanning, click **Stop Scan Now** to notify them to stop scanning.

Intensive Scanning

OfficeScan automatically initiates intensive scanning during a manual scan when OfficeScan detects a specified number of malware threats on the client computer. The OfficeScan client restarts scanning the endpoint using a heightened level of threat detection. The intensive scan detects more probable malware than the on-demand scans.

Note

Intensive scanning requires more system resources than normal on-demand scans.

The default actions for intensive scanning are:

- First action: Quarantine
- Second action: Delete

Note

Administrators cannot modify the intensive scanning actions.

Configuring Intensive Scanning Using ofcscan.ini

OfficeScan triggers intensive scanning once the OfficeScan client computer detects an infection threshold. Administrators can configure the number of malware detections necessary to trigger the intensive scan by modifying the `ofcscan.ini` file.

Procedure

1. Access <*Server installation folder*>`\PCCSRV`.
2. Open the `ofcscan.ini` file using a text editor such as Notepad.
3. Search for the string "`IntensiveScanThreshold`" and then type the new value next to it.

   The default value is 0 detections (disabled).

   Note

   Intensive scanning requires more system resources than normal on-demand scans. Ensure that the threshold configured is high enough to avoid unnecessary scanning.

4. Save the file.
5. Go to **Networked Computers** > **Global Client Settings**.
6. Click **Save**.

   OfficeScan deploys the updated setting to all OfficeScan clients.

Settings Common to All Scan Types

For each scan type, configure three sets of settings: scan criteria, scan exclusions, and scan actions. Deploy these settings to one or several clients and domains, or to all clients that the server manages.

Scan Criteria

Specify which files a particular scan type should scan using file attributes such as file type and extension. Also specify conditions that will trigger scanning. For example, configure Real-time Scan to scan each file after it is downloaded to the computer.

User Activity on Files

Choose activities on files that will trigger Real-time Scan. Select from the following options:

- **Scan files being created/modified**: Scans new files introduced into the computer (for example, after downloading a file) or files being modified
- **Scan files being retrieved**: Scans files as they are opened
- **Scan files being created/modified and retrieved**

For example, if the third option is selected, a new file downloaded to the computer will be scanned and stays in its current location if no security risk is detected. The same file will be scanned when a user opens the file and, if the user modified the file, before the modifications are saved.

Files to Scan

Select from the following options:

- **All scannable files**: Scan all files
- **File types scanned by IntelliScan**: Only scan files known to potentially harbor malicious code, including files disguised by a harmless extension name. See *IntelliScan on page E-6* for details.

- **Files with certain extensions**: Only scan files whose extensions are included in the file extension list. Add new extensions or remove any of the existing extensions.

Scan Settings

Select one or more of the following options:

- **Scan floppy disk during system shutdown**: Scans any floppy disk for boot viruses before shutting down the computer. This prevents any virus/malware from executing when a user reboots the computer from the disk.
- **Scan hidden folders**: Allows OfficeScan to detect and then scan hidden folders on the computer during Manual Scan
- **Scan network drive**: Scans network drives or folders mapped to the OfficeScan client computer during Manual Scan or Real-time Scan.
- **Scan the boot sector of the USB storage device after plugging in**: Automatically scans only the boot sector of a USB storage device every time the user plugs it in (Real-time Scan).
- **Scan compressed files**: Allows OfficeScan to scan up to a specified number of compression layers and skip scanning any excess layers. OfficeScan also cleans or deletes infected files within compressed files. For example, if the maximum is two layers and a compressed file to be scanned has six layers, OfficeScan scans two layers and skips the remaining four. If a compressed file contains security threats, OfficeScan cleans or deletes the file.

  Note

  OfficeScan treats Microsoft Office 2007 files in Office Open XML format as compressed files. Office Open XML, the file format for Office 2007 applications, uses ZIP compression technologies. If you want files created using these applications to be scanned for viruses/malware, you need to enable scanning of compressed files.

- **Scan OLE objects**: When a file contains multiple Object Linking and Embedding (OLE) layers, OfficeScan scans the specified number of layers and ignores the remaining layers.

All OfficeScan clients managed by the server check this setting during Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now. Each layer is scanned for virus/malware and spyware/grayware.

For example:

The number of layers you specify is 2. Embedded within a file is a Microsoft Word document (first layer), within the Word document is a Microsoft Excel spreadsheet (second layer), and within the spreadsheet is an `.exe` file (third layer). OfficeScan will scan the Word document and Excel spreadsheet, and skip the `.exe` file.

- **Detect exploit code in OLE files**: OLE Exploit Detection heuristically identifies malware by checking Microsoft Office files for exploit code.

> **Note**
>
> The specified number of layers is applicable to both **Scan OLE objects** and **Detect exploit code** options.

- **Enable IntelliTrap**: Detects and removes virus/malware on compressed executable files. This option is available only for Real-time Scan. See *IntelliTrap on page E-6* for details.
- **Scan boot area**: Scans the boot sector of the client computer's hard disk for virus/malware during Manual Scan, Scheduled Scan and Scan Now

CPU Usage

OfficeScan can pause after scanning one file and before scanning the next file. This setting is used during Manual Scan, Scheduled Scan, and Scan Now.

Select from the following options:

- **High**: No pausing between scans
- **Medium**: Pause between file scans if CPU consumption is higher than 50%, and do not pause if 50% or lower
- **Low**: Pause between file scans if CPU consumption is higher than 20%, and do not pause if 20% or lower

If you choose Medium or Low, when scanning is launched and CPU consumption is within the threshold (50% or 20%), OfficeScan will not pause between scans, resulting in faster scanning time. OfficeScan uses more CPU resource in the process but because CPU consumption is optimal, computer performance is not drastically affected. When CPU consumption begins to exceed the threshold, OfficeScan pauses to reduce CPU usage, and stops pausing when consumption is within the threshold again.

If you choose High, OfficeScan does not check the actual CPU consumption and scans files without pausing.

Schedule

Configure how often (daily, weekly, or monthly) and what time Scheduled Scan will run.

For monthly Scheduled Scans, you can choose either a particular day of a month or a day of a week and the order of its occurrence.

- **A particular day of a month**: Select between the 1st and 31st day. If you selected the 29th, 30th, or 31st day and a month does not have this day, OfficeScan runs Scheduled Scan on the last day of the month. Therefore:
  - If you selected 29, Scheduled Scan runs on February 28 (except on a leap year) and on the 29th day of all the other months.
  - If you selected 30, Scheduled Scan runs on February 28 or 29, and on the 30th day of all the other months.
  - If you selected 31, Scheduled Scan runs on February 28 or 29, April 30, June 30, September 30, November 30, and on the 31st day of all the other months.
- **A day of a week and the order of its occurrence**: A day of a week occurs four or five times a month. For example, there are typically four Mondays in a month. Specify a day of a week and the order in which it occurs during a month. For example, choose to run Scheduled Scan on the second Monday of each month. If you choose the fifth occurrence of a day and it does not exist during a particular month, the scan runs on the fourth occurrence.

Scan Exclusions

Configure scan exclusions to increase the scanning performance and skip scanning files causing false alarms. When a particular scan type runs, OfficeScan checks the scan

exclusion list to determine which files on the computer will be excluded from both virus/malware and spyware/grayware scanning.

When you enable scan exclusion, OfficeScan will not scan a file under the following conditions:

- The file is found under a specific directory (or any of its sub-directories).
- The file name matches any of the names in the exclusion list.
- The file extension matches any of the extensions in the exclusion list.

Tip

For a list of products that Trend Micro recommends excluding from Real-Time scans, go to:

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

Wildcard Exceptions

Scan exclusion lists for files and directories support the use of wildcard characters. Use the "?" character to replace one character and "*" to replace several characters.

Use wildcard characters cautiously. Using the wrong character might exclude incorrect files or directories. For example, `C:\*` would exclude the entire `C:\` drive.

TABLE 7-9. Scan Exclusions Using Wildcard Characters

VALUE	EXCLUDED	NOT EXCLUDED

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`

VALUE	EXCLUDED	NOT EXCLUDED
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	All `.txt` files in the `C:\` directory	All other file types in the `C:\` directory
`[]`	Not supported	Not supported
`*.*`	Not supported	Not supported

Scan Exclusion List (Directories)

OfficeScan will not scan all files found under a specific directory on the computer. You can specify a maximum of 256 directories.

Note

By excluding a directory from scans, OfficeScan automatically excludes all of the directory's sub-directories from scans.

You can also choose **Exclude directories where Trend Micro products are installed**. If you select this option, OfficeScan automatically excludes the directories of the following Trend Micro products from scanning:

- <*Server installation folder*>
- ScanMail™ for Microsoft Exchange (all versions except version 7). If you use version 7, add the following folders to the exclusion list:
  - `\Smex\Temp`
  - `\Smex\Storage`
  - `\Smex\ShareResPool`
- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT

- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan E-mail VirusWall
- InterScan NSAPI Plug-in
- InterScan eManager 3.5x
- IM Security

If you have a Trend Micro product NOT included in the list, add the product directories to the scan exclusion list.

Also configure OfficeScan to exclude Microsoft Exchange 2000/2003 directories by going to the **Scan Settings** section of **Networked Computers** > **Global Client Settings**. If you use Microsoft Exchange 2007 or later, manually add the directory to the scan exclusion list. Refer to the following site for scan exclusion details:

http://technet.microsoft.com/en-us/library/bb332342.aspx

When you configure the file list, choose from the following options:

- **Retains client computer's exclusion list**: This is the default selection. If you make changes to the exclusion list and this option is enabled, you will not be able to save the changes. This option is provided to prevent overwriting a client's existing exclusion list accidentally. If you want to deploy the changes you made, select any of the other options.
- **Overwrites the client computer's exclusion list**: This option removes the entire exclusion list on the client and replaces it with the list you just configured. If you choose this option, OfficeScan displays a warning. To proceed, you must click **OK** in the message window.
- **Adds path to the client computer's exclusion list**: This option adds the items in the list you just configured to the client's existing exclusion list. If an item already exists in the client's exclusion list, the client ignores the item.

- **Removes path from the client computer's exclusion list**: The client removes an item in its exclusion list if it matches an item in the list you just configured.

Scan Exclusion List (Files)

OfficeScan will not scan a file if its file name matches any of the names included in this exclusion list. If you want to exclude a file found under a specific location on the computer, include the file path, such as `C:\Temp\sample.jpg`.

You can specify a maximum of 256 files.

When you configure the file list, choose from the following options:

- **Retains client computer's exclusion list**: This is the default selection. If you make changes to the exclusion list and this option is enabled, you will not be able to save the changes. This option is provided to prevent overwriting a client's existing exclusion list accidentally. If you want to deploy the changes you made, select any of the other options.
- **Overwrites the client computer's exclusion list**: This option removes the entire exclusion list on the client and replaces it with the list you just configured. If you choose this option, OfficeScan displays a warning. To proceed, you must click **OK** in the message window.
- **Adds path to the client computer's exclusion list**: This option adds the items in the list you just configured to the client's existing exclusion list. If an item already exists in the client's exclusion list, the client ignores the item.
- **Removes path from the client computer's exclusion list**: The client removes an item in its exclusion list if it matches an item in the list you just configured.

Scan Exclusion List (File Extensions)

OfficeScan will not scan a file if its file extension matches any of the extensions included in this exclusion list. You can specify a maximum of 256 file extensions. A period (.) is not required before the extension.

For Real-time Scan, use an asterisk (*) as a wildcard character when specifying extensions. For example, if you do not want to scan all files with extensions starting with D, such as `DOC`, `DOT`, or `DAT`, type `D*`.

For Manual Scan, Scheduled Scan, and Scan Now, use a question mark (?) or asterisk (*) as a wildcard character.

Apply Scan Exclusion Settings to All Scan Types

OfficeScan allows you to configure scan exclusion settings for a particular scan type and then apply the same settings to all the other scan types. For example:

On January 1, OfficeScan administrator Chris found out that there are a large number of `JPG` files on client computers and realized that these files do not pose any security threat. Chris added `JPG` in the file exclusion list for Manual Scan and then applied this setting to all scan types. Real-time Scan, Scan Now, and Scheduled Scan are now set to skip scanning `.jpg` files.

A week later, Chris removed `JPG` from the exclusion list for Real-time Scan but did not apply scan exclusion settings to all scan types. `JPG` files will now be scanned but only during Real-time Scan.

Scan Actions

Specify the action OfficeScan performs when a particular scan type detects a security risk. OfficeScan has a different set of scan actions for virus/malware and spyware/grayware.

Virus/Malware Scan Actions

The scan action OfficeScan performs depends on the virus/malware type and the scan type that detected the virus/malware. For example, when OfficeScan detects a Trojan horse program (virus/malware type) during Manual Scan (scan type), it cleans (action) the infected file.

For information on the different virus/malware types, see *Viruses and Malware on page 7-2*.

The following are the actions OfficeScan can perform against viruses/malware:

TABLE 7-10. Virus/Malware Scan Actions

ACTION	DESCRIPTION
Delete	OfficeScan deletes the infected file.
Quarantine	OfficeScan renames and then moves the infected file to a temporary quarantine directory on the client computer located in <*Client installation folder*>`\Suspect`. The OfficeScan client then sends quarantined files to the designated quarantine directory. See *Quarantine Directory on page 7-38* for details. The default quarantine directory is on the OfficeScan server, under <*Server installation folder*>`\PCCSRV\Virus`. OfficeScan encrypts quarantined files sent to this directory. If you need to restore any of the quarantined files, use the VSEncrypt tool. For information on using this tool, see *Server Tuner on page 13-44*.
Clean	OfficeScan cleans the infected file before allowing full access to the file. If the file is uncleanable, OfficeScan performs a second action, which can be one of the following actions: Quarantine, Delete, Rename, and Pass. To configure the second action, go to **Networked Computers** > **Client Management**. Click **Settings** > **Scan Settings** > **{Scan Type}** > **Action** tab. This action can be performed on all types of malware except probable virus/malware.
Rename	OfficeScan changes the infected file's extension to "`vir`". Users cannot open the renamed file initially, but can do so if they associate the file with a certain application. The virus/malware may execute when opening the renamed infected file.
Pass	OfficeScan can only use this scan action when it detects any type of virus during Manual Scan, Scheduled Scan, and Scan Now. OfficeScan cannot use this scan action during Real-time Scan because performing no action when an attempt to open or execute an infected file is detected will allow virus/malware to execute. All the other scan actions can be used during Real-time Scan.

Action	Description
Deny Access	This scan action can only be performed during Real-time Scan. When OfficeScan detects an attempt to open or execute an infected file, it immediately blocks the operation. Users can manually delete the infected file.

Use ActiveAction

Different types of virus/malware require different scan actions. Customizing scan actions requires knowledge about virus/malware and can be a tedious task. OfficeScan uses ActiveAction to counter these issues.

ActiveAction is a set of pre-configured scan actions for viruses/malware. If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus/malware, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:

- ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- Virus writers constantly change the way virus/malware attack computers. ActiveAction settings are updated to protect against the latest threats and the latest methods of virus/malware attacks.

Note

ActiveAction is not available for spyware/grayware scan.

The following table illustrates how ActiveAction handles each type of virus/malware:

TABLE 7-11. Trend Micro Recommended Scan Actions Against Viruses and Malware

VIRUS/MALWARE TYPE	REAL-TIME SCAN		MANUAL SCAN/SCHEDULED SCAN/ SCAN NOW	
	FIRST ACTION	SECOND ACTION	FIRST ACTION	SECOND ACTION
Joke program	Quarantine	Delete	Quarantine	Delete
Trojan horse program	Quarantine	Delete	Quarantine	Delete
Virus	Clean	Quarantine	Clean	Quarantine
Test virus	Deny Access	N/A	N/A	N/A
Packer	Quarantine	N/A	Quarantine	N/A
Others	Clean	Quarantine	Clean	Quarantine
Probable virus/ malware	Deny Access or user-configured action	N/A	Pass or user-configured action	N/A

For probable virus/malware, the default action is "Deny Access" during Real-time Scan and "Pass" during Manual Scan, Scheduled Scan, and Scan Now. If these are not your preferred actions, you can change them to Quarantine, Delete, or Rename.

Use the Same Action for all Virus/Malware Types

Select this option if you want the same action performed on all types of virus/malware, except probable virus/malware. If you choose "Clean" as the first action, select a second action that OfficeScan performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable.

If you choose "Clean" as the first action, OfficeScan performs the second action when it detects probable virus/malware.

Use a Specific Action for Each Virus/Malware Type

Manually select a scan action for each virus/malware type.

For all virus/malware types except probable virus/malware, all scan actions are available. If you choose "Clean" as the first action, select a second action that OfficeScan performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable.

For probable virus/malware, all scan actions, except "Clean", are available.

Quarantine Directory

If the action for an infected file is "Quarantine", the OfficeScan client encrypts the file and moves it to a temporary quarantine folder located in <*Client installation folder*> `\SUSPECT` and then sends the file to the designated quarantine directory.

Note

You can restore encrypted quarantined files in case you need to access them in the future. For details, see *Restoring Encrypted Files on page 7-41*.

Accept the default quarantine directory, which is located on the OfficeScan server computer. The directory is in URL format and contains the server's host name or IP address.

- If the server is managing both IPv4 and IPv6 clients, use the host name so that all clients can send quarantined files to the server.
- If the server only has or is identified by its IPv4 address, only pure IPv4 and dual-stack clients can send quarantined files to the server.
- If the server only has or is identified by its IPv6 address, only pure IPv6 and dual-stack clients can send quarantined files to the server.

You can also specify an alternative quarantine directory by typing the location in URL, UNC path, or absolute file path format. Clients should be able to connect to this alternative directory. For example, the alternative directory should have an IPv6 address if it will receive quarantined files from dual-stack and pure IPv6 clients. Trend Micro recommends designating a dual-stack alternative directory, identifying the directory by its host name, and using UNC path when typing the directory.

Refer to the following table for guidance on when to use URL, UNC path, or absolute file path:

TABLE 7-12. Quarantine Directory

QUARANTINE DIRECTORY	ACCEPTED FORMAT	EXAMPLE	NOTES
A directory on the OfficeScan server computer	URL	`http://<osceserver>`	This is the default directory. Configure settings for this directory, such as the size of the quarantine folder. For details, see *Quarantine Manager on page 13-43*.
	UNC path	`\\<osceserver>\ofcscan\Virus`	
A directory on another OfficeScan server computer (if you have other OfficeScan servers on the network)	URL	`http://<osceserver2>`	Ensure that clients can connect to this directory. If you specify an incorrect directory, the OfficeScan client keeps the quarantined files on the SUSPECT folder until a correct quarantine directory is specified. In the server's virus/malware logs, the scan result is "Unable to send the quarantined file to the designated quarantine folder". If you use UNC path, ensure that the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this group.
	UNC path	`\\<osceserver2>\ofcscan\Virus`	
Another computer on the network	UNC path	`\\<computer_name>\temp`	
A different directory on the OfficeScan client	Absolute path	`C:\temp`	

Back Up Files Before Cleaning

If OfficeScan is set to clean an infected file, it can first back up the file. This allows you to restore the file in case you need it in the future. OfficeScan encrypts the backup file to prevent it from being opened, and then stores the file on the <*Client installation folder*>`\Backup` folder.

To restore encrypted backup files, see *Restoring Encrypted Files on page 7-41*.

Damage Cleanup Services

Damage Cleanup Services cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, and viral files).

The client triggers Damage Cleanup Services before or after virus/malware scanning, depending on the scan type.

- When Manual Scan, Scheduled Scan, or Scan Now runs, the OfficeScan client triggers Damage Cleanup Services first and then proceeds with virus/malware scanning. During virus/malware scanning, the client may trigger Damage Cleanup Services again if cleanup is required.
- During Real-time Scan, the OfficeScan client first performs virus/malware scanning and then triggers Damage Cleanup Services if cleanup is required.

You can select the type of cleanup that Damage Cleanup Services runs:

- **Standard cleanup**: The OfficeScan client performs any of the following actions during standard cleanup:
  - Detects and removes live Trojans
  - Kills processes that Trojans create
  - Repairs system files that Trojans modify
  - Deletes files and applications that Trojans drop
- **Advanced cleanup**: In addition to the standard cleanup actions, the OfficeScan client stops activities by rogue security software, also known as FakeAV. The OfficeScan client also uses advanced cleanup rules to proactively detect and stop applications that exhibit FakeAV behavior.

Note

While providing proactive protection, advanced cleanup also results in a high number of false-positives.

Damage Cleanup Services does not run cleanup on probable virus/malware unless you select the option **Run cleanup when probable virus/malware is detected**. You can only select this option if the action on probable virus/malware is not **Pass** or **Deny Access**.

For example, if the OfficeScan client detects probable virus/malware during Real-time Scan and the action is quarantine, the OfficeScan client first quarantines the infected file and then runs cleanup if necessary. The cleanup type (standard or advanced) depends on your selection.

Display a Notification Message When Virus/Malware is Detected

When OfficeScan detects virus/malware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection.

To modify the notification message, go to the **Virus/Malware** tab in **Notifications** > **Client User Notifications**.

Display a Notification Message When Probable Virus/ Malware is Detected

When OfficeScan detects probable virus/malware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection.

To modify the notification message, go to the **Virus/Malware** tab in **Notifications** > **Client User Notifications**.

Restoring Encrypted Files

To prevent infected from being opened, OfficeScan encrypts the file during the following instances:

- Before quarantining a file
- When backing up a file before cleaning it

OfficeScan provides a tool that decrypts and then restores the file in case you need to retrieve information from it. OfficeScan can decrypt and restore the following files:

TABLE 7-13. Files that OfficeScan can Decrypt and Restore

FILE	DESCRIPTION
Quarantined files on the client computer	These files are found in the <*Client installation folder*> `\SUSPECT\Backup` folder and are automatically purged after 7 days. These files are also uploaded to the designated quarantine directory on the OfficeScan server.
Quarantined files on the designated quarantine directory	By default, this directory is located on the OfficeScan server computer. For details, see *Quarantine Directory on page 7-38*.
Backed up encrypted files	These are the backup of infected files that OfficeScan was able to clean. These files are found in the `<Client installation folder>\Backup` folder. To restore these files, users need to move them to the `<Client installation folder>\SUSPECT\Backup` folder. OfficeScan only backs up and encrypts files before cleaning if you select **Backup files before cleaning** in **Networked Computers** > **Client Management > Settings** > **Scan Settings** > **{Scan Type}** > **Action** tab.

WARNING!

Restoring an infected file may spread the virus/malware to other files and computers. Before restoring the file, isolate the infected computer and move important files on this computer to a backup location.

Decrypting and Restoring Files

Procedure

- If the file is on the OfficeScan client computer:

  a. Open a command prompt and navigate to <*Client installation folder*>.

  b. Run `VSEncode.exe` by typing the following:

```
VSEncode.exe /u
```

This parameter opens a screen with a list of files found under `<Client installation folder>\SUSPECT\Backup`.

c. Select a file to restore and click **Restore**. The tool can only restore one file at a time.

d. In the screen that opens, specify the folder where to restore the file.

e. Click **Ok**. The file is restored to the specified folder.

> **Note**
>
> It might be possible for OfficeScan to scan the file again and treat it as infected as soon as the file is restored. To prevent the file from being scanned, add it to the scan exclusion list. See *Scan Exclusions on page 7-29* for details.

f. Click **Close** when you have finished restoring files.

- If the file is on the OfficeScan server or a custom quarantine directory:

  a. If the file is on the OfficeScan server computer, open a command prompt and navigate to <*Server installation folder*>`\PCCSRV\Admin\Utility\VSEncrypt`.

  If the file is on a custom quarantine directory, navigate to `<Server installation folder>\PCCSRV\Admin\Utility` and copy the `VSEncrypt` folder to the computer where the custom quarantine directory is located.

  b. Create a text file and then type the full path of the files you want to encrypt or decrypt.

  For example, to restore files in `C:\My Documents\Reports`, type `C:\My Documents\Reports\*.*` in the text file.

  Quarantined files on the OfficeScan server computer are found under `<Server installation folder>\PCCSRV\Virus`.

  c. Save the text file with an `INI` or `TXT` extension. For example, save it as `ForEncryption.ini` on the `C:` drive.

  d. Open a command prompt and navigate to the directory where the `VSEncrypt` folder is located.

e. Run `VSEncode.exe` by typing the following:

```
VSEncode.exe /d /i <location of the INI or TXT file>
```

Where:

`<location of the INI or TXT file>` is the path of the `INI` or `TXT` file you created (for example, `C:\ForEncryption.ini`).

f. Use the other parameters to issue various commands.

TABLE 7-14. Restore Parameters

PARAMETER	DESCRIPTION
None (no parameter)	Encrypt files
/d	Decrypt files
/debug	Create a debug log and save it to the computer. On the OfficeScan client computer, the debug log `VSEncrypt.log` is created in the `<Client installation folder>`.
/o	Overwrite an encrypted or decrypted file if it already exists
/f <filename>	Encrypt or decrypt a single file
/nr	Do not restore the original file name
/v	Display information about the tool
/u	Launch the tool's user interface
/r <Destination folder>	The folder where a file will be restored
/s <Original file name>	The file name of the original encrypted file

For example, type `VSEncode [/d] [/debug]` to decrypt files in the `Suspect` folder and create a debug log. When you decrypt or encrypt a file, OfficeScan creates the decrypted or encrypted file in the same folder. Before decrypting or encrypting a file, ensure that it is not locked.

Spyware/Grayware Scan Actions

The scan action OfficeScan performs depends on the scan type that detected the spyware/grayware. While specific actions can be configured for each virus/malware type, only one action can be configured for all types of spyware/grayware (for information on the different type of spyware/grayware, see *Spyware and Grayware on page 7-4*). For example, when OfficeScan detects any type of spyware/grayware during Manual Scan (scan type), it cleans (action) the affected system resources.

The following are the actions OfficeScan can perform against spyware/grayware:

TABLE 7-15. Spyware/Grayware Scan Actions

ACTION	DESCRIPTION
Clean	OfficeScan terminates processes or delete registries, files, cookies, and shortcuts. After cleaning spyware/grayware, OfficeScan clients back up spyware/grayware data, which you can restore if you consider the spyware/grayware safe to access. See *Restoring Spyware/Grayware on page 7-48* for details.
Pass	OfficeScan performs no action on detected spyware/grayware components but records the spyware/grayware detection in the logs. This action can only be performed during Manual Scan, Scheduled Scan, and Scan Now. During Real-time Scan, the action is "Deny Access". OfficeScan will not perform any action if the detected spyware/grayware is included in the approved list. See *Spyware/Grayware Approved List on page 7-46* for details.
Deny Access	OfficeScan denies access (copy, open) to the detected spyware/grayware components. This action can only be performed during Real-time Scan. During Manual Scan, Scheduled Scan, and Scan Now, the action is "Pass".

Display a Notification Message When Spyware/Grayware is Detected

When OfficeScan detects spyware/grayware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection.

To modify the notification message, go to **Notifications** > **Client User Notifications**, click the **Spyware/Grayware** tab.

Spyware/Grayware Approved List

OfficeScan provides a list of "approved" spyware/grayware, which contains files or applications that you do not want treated as spyware or grayware. When a particular spyware/grayware is detected during scanning, OfficeScan checks the approved list and performs no action if it finds a match in the approved list.

Apply the approved list to one or several clients and domains, or to all clients that the server manages. The approved list applies to all scan types, which means that the same approved list will be used during Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now.

Adding Already Detected Spyware/Grayware to the Approved List

Procedure

1. Navigate to one of the following:
   - **Networked Computers** > **Client Management**
   - **Logs** > **Networked Computer Logs** > **Security Risks**
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Logs** > **Spyware/Grayware Logs** or **View Logs** > **Spyware/Grayware Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. Select logs and click **Add to Approved List**.
6. Apply the approved spyware/grayware only to the selected client computers or to certain domain(s).

7. Click **Save**. The selected clients apply the setting and the OfficeScan server adds the spyware/grayware to the approved list found in **Networked Computers** > **Client Management** > **Settings** > **Spyware/Grayware Approved List**.

Note

OfficeScan can accommodate a maximum of 1024 spyware/grayware in the approved list.

Managing the Spyware/Grayware Approved List

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Spyware/Grayware Approved List**.
4. On the **Spyware/Grayware names** table, select a spyware/grayware name. To select multiple names, hold the **Ctrl** key while selecting.
   - You can also type a keyword in the **Search** field and click **Search**. OfficeScan refreshes the table with the names that match the keyword.
5. Click **Add**.

   The names move to the **Approved List** table.
6. To remove names from the approved list, select the names and click **Remove**. To select multiple names, hold the **Ctrl** key while selecting.
7. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Restoring Spyware/Grayware

After cleaning spyware/grayware, OfficeScan clients back up spyware/grayware data. Notify an online client to restore backed up data if you consider the data harmless. Choose the spyware/grayware data to restore based on the backup time.

Note

OfficeScan client users cannot initiate spyware/grayware restore and are not notified about which backup data the client was able to restore.

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, open a domain and then select a client.

   Note

   Only one client at a time can perform spyware/grayware restore.

3. Click **Tasks** > **Spyware/Grayware Restore**.
4. To view the items to restore for each data segment, click **View**.

   A new screen displays. Click **Back** to return to the previous screen.

5. Select the data segments that you want to restore.
6. Click **Restore**.

   OfficeScan notifies you of the restoration status. Check the spyware/grayware restore logs for a full report. See *Viewing Spyware/Grayware Restore Logs on page 7-92* for details.

Scan Privileges and Other Settings

Users with scan privileges have greater control over how files on their computers get scanned. Scan privileges allow users or the OfficeScan client to perform the following tasks:

- Users can configure Manual Scan, Scheduled Scan, and Real-time Scan settings. For details, see *Scan Type Privileges on page 7-49*.
- Users can postpone, stop, or skip Scheduled Scan. For details, see *Scheduled Scan Privileges and Other Settings on page 7-52*.
- Users enable scanning of Microsoft Outlook and POP3 email messages for virus/malware. For details, see *Mail Scan Privileges and Other Settings on page 7-58*.
- The OfficeScan client can use cache settings to improve its scan performance. For details, see *Cache Settings for Scans on page 7-60*.

Scan Type Privileges

Allow users to configure their own Manual Scan, Real-time Scan and Scheduled Scan settings.

Granting Scan Type Privileges

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Scan Privileges** section.
5. Select the scan types that users are allowed to configure.

6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Configuring Scan Settings for the OfficeScan Client Computers

Procedure

1. Right-click the OfficeScan client icon on the system tray and select **OfficeScan Console**.
2. Click **Settings** > **{Scan Type}**.

FIGURE 7-1. Scan settings on the OfficeScan client console

3. Configure the following settings:

   - Manual Scan settings: Files to Scan, Scan Settings, CPU Usage, Scan Exclusions, Scan Actions

- Real-time Scan settings: User Activity on Files, Files to Scan, Scan Settings, Scan Exclusions, Scan Actions
- Scheduled Scan settings: Schedule, Files to Scan, Scan Settings, CPU Usage, Scan Exclusions, Scan Actions

4. Click **OK**.

Scheduled Scan Privileges and Other Settings

If Scheduled Scan is set to run on the client, users can postpone and skip/stop Scheduled Scan.

Postpone Scheduled Scan

Userswith the "Postpone Scheduled Scan" privilege can perform the following actions:

- Postpone Scheduled Scan before it runs and then specify the postpone duration. Scheduled Scan can only be postponed once.
- If Scheduled Scan is in progress, users can stop scanning and restart it later. Users then specify the amount of time that should elapse before scanning restarts. When scanning restarts, all previously scanned files are scanned again. Scheduled Scan can be stopped and then restarted only once.

Note

The minimum postpone duration/elapsed time users can specify is 15 minutes. The maximum is 12 hours and 45 minutes, which you can reduce by going to **Networked Computers** > **Global Client Settings**. In the **Scheduled Scan Settings** section, modify the **Postpone Scheduled Scan for up to __ hours and __ minutes** setting.

Skip and Stop Scheduled Scan

This privilege allows users to perform the following actions:

- Skip Scheduled Scan before it runs

- Stop Scheduled Scan when it is in progress

Scheduled Scan Privilege Notification

To allow users to take advantage of Scheduled Scan privileges, remind them about the privileges you have granted them by configuring OfficeScan to display a notification message before Scheduled Scan runs.

Granting Scheduled Scan Privileges and Displaying the Privilege Notification

---

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Scheduled Scan Privileges** section.
5. Select the following options:
   - Postpone Scheduled Scan
   - Skip and stop Scheduled Scan
6. Click the **Other Settings** tab and go to the **Scheduled Scan Settings** section.
7. Select **Display a notification before a scheduled scan occurs**.

   When you enable this option, a notification message displays on the client computer minutes before Scheduled Scan runs. Users are notified of the scan schedule (date and time) and their Scheduled Scan privileges, such as postponing, skipping, or stopping Scheduled Scan.

Note

The number of minutes is configurable. To configure the number of minutes, go to **Networked Computers** > **Global Client Settings**. In the **Scheduled Scan Settings** section, modify the **Remind users of the Scheduled Scan __ minutes before it runs** setting.

8. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Postponing/Skipping and Stopping Scheduled Scan on the Client Computer

Procedure

- If Scheduled Scan has not started:

  a. Right-click the OfficeScan client icon on the system tray and select **Scheduled Scan Advanced Settings**.

FIGURE 7-2. Scheduled Scan Advanced Settings option

Note

Users do not need to perform this step if the notification message is enabled and is set to display minutes before Scheduled Scan runs. For details about the notification message, see *Scheduled Scan Privilege Notification on page 7-53*.

---

b. On the notification window that displays, select from the following options:

- **Postpone scanning for __ hours and __ minutes.**
- **Skip this Scheduled Scan. The next Scheduled Scan runs on <date> at <time>.**

FIGURE 7-3. Scheduled Scan privileges on the OfficeScan client computer

- If Scheduled Scan is in progress:

  a. Right-click the OfficeScan client icon on the system tray and select **Scheduled Scan Advanced Settings**.

  b. On the notification window that displays, select from the following options:

     - **Stop scanning. Restart the scan after __ hours and __ minutes.**
     - **Stop scanning. The next Scheduled Scan runs on <date> at <time>.**

FIGURE 7-4. Scheduled Scan privileges on the OfficeScan client computer

Mail Scan Privileges and Other Settings

When clients have the mail scan privileges, the **Mail Scan** tab displays on the OfficeScan client console. The Mail Scan tab shows two mail scan programs - Outlook mail scan and POP3 mail scan.

FIGURE 7-5. Mail Scan tab on the OfficeScan client console

The following table describes the Outlook mail scan and POP3 mail scan programs.

TABLE 7-16. Mail Scan Programs

DETAILS	OUTLOOK MAIL SCAN	POP3 MAIL SCAN
Purpose	Scans Microsoft Outlook email messages for viruses/malware	Scans POP3 email messages for viruses/malware
Prerequisites	Must be installed by users from the OfficeScan client console before they can use it	• Must be enabled by administrators from the web console before users can use it **Note** To enable POP3 Mail Scan, see *Granting Mail Scan Privileges and Enabling POP3 Mail Scan on page 7-60*. • Action against viruses/malware configurable from the OfficeScan client console but not from the web console
Scan types supported	Manual Scan Scanning only occurs when users click **Scan Now** from the **Mail Scan** tab on the OfficeScan client console.	Real-time Scan Scanning is done as email messages are retrieved from the POP3 mail server.
Scan results	• Information about detected security risks available after scanning is complete • Scan results not logged on the OfficeScan client console's Logs screen • Scan results not sent to the server	• Information about detected security risks available after scanning is complete • Scan results not logged on the OfficeScan client console's Logs screen • Scan results not sent to the server
Other details	None	Shares the OfficeScan NT Proxy Service (`TMProxy.exe`) with the web reputation feature

Granting Mail Scan Privileges and Enabling POP3 Mail Scan

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Mail Scan Privileges** section.
5. Select **Display the Mail Scan tab on the client console**.
6. Click the **Other Settings** tab and go to the **POP3 Email Scan Settings** section.
7. Select **Scan POP3 email**.
8. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Cache Settings for Scans

The OfficeScan client can build the digital signature and on-demand scan cache files to improve its scan performance. When an on-demand scan runs, the OfficeScan client first checks the digital signature cache file and then the on-demand scan cache file for files to exclude from the scan. Scanning time is reduced if a large number of files are excluded from the scan.

Digital Signature Cache

The digital signature cache file is used during Manual Scan, Scheduled Scan, and Scan Now. Clients do not scan files whose caches have been added to the digital signature cache file.

The OfficeScan client uses the same Digital Signature Pattern used for Behavior Monitoring to build the digital signature cache file. The Digital Signature Pattern contains a list of files that Trend Micro considers trustworthy and therefore can be excluded from scans.

Note

Behavior Monitoring is automatically disabled on Windows server platforms (64-bit support for Windows XP, 2003, and Vista without SP1 is not available). If the digital signature cache is enabled, OfficeScan clients on these platforms download the Digital Signature Pattern for use in the cache and do not download the other Behavior Monitoring components.

Clients build the digital signature cache file according to a schedule, which is configurable from the web console. Clients do this to:

- Add the cache for new files that were introduced to the system since the last cache file was built
- Remove the cache for files that have been modified or deleted from the system

During the cache building process, clients check the following folders for trustworthy files and then adds the caches for these files to the digital signature cache file:

- `%PROGRAMFILES%`
- `%WINDIR%`

The cache building process does not affect a computer's performance because clients use minimal system resources during the process. Clients are also able to resume a cache building task that was interrupted for some reason (for example, when the host machine is powered off or when a wireless computer's AC adapter is unplugged).

On-demand Scan Cache

The on-demand scan cache file is used during Manual Scan, Scheduled Scan, and Scan Now. OfficeScan clients do not scan files whose caches have been added to the on-demand scan cache file.

Each time scanning runs, the OfficeScan client checks the properties of threat-free files. If a threat-free file has not been modified for a certain period of time (the time period is configurable), the OfficeScan client adds the cache of the file to the on-demand scan cache file. When the next scan occurs, the file will not be scanned if its cache has not expired.

The cache for a threat-free file expires within a certain number of days (the time period is also configurable). When scanning occurs on or after the cache expiration, the OfficeScan client removes the expired cache and scans the file for threats. If the file is threat-free and remains unmodified, the cache of the file is added back to the on-demand scan cache file. If the file is threat-free but was recently modified, the cache is not added and the file will be scanned again on the next scan.

The cache for a threat-free file expires to prevent the exclusion of infected files from scans, as illustrated in the following examples:

- It is possible that a severely outdated pattern file may have treated an infected, unmodified file as threat-free. If the cache does not expire, the infected file remains in the system until it is modified and detected by Real-time Scan.
- If a cached file was modified and Real-time Scan is not functional during the file modification, the cache needs to expire so that the modified file can be scanned for threats.

The number of caches added to the on-demand scan cache file depends on the scan type and its scan target. For example, the number of caches may be less if the OfficeScan client only scanned 200 of the 1,000 files in a computer during Manual Scan.

If on-demand scans are run frequently, the on-demand scan cache file reduces the scanning time significantly. In a scan task where all caches are not expired, scanning that usually takes 12 minutes can be reduced to 1 minute. Reducing the number of days a file must remain unmodified and extending the cache expiration usually improve the performance. Since files must remain unmodified for a relatively short period of time, more caches can be added to the cache file. The caches also expire longer, which means that more files are skipped from scans.

If on-demand scans are seldom run, you can disable the on-demand scan cache since caches would have expired when the next scan runs.

Configuring Cache Settings for Scans

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Cache Settings for Scans** section.
5. Configure settings for the digital signature cache.
   a. Select **Enable the digital signature cache**.
   b. In **Build the cache every __ days**, specify how often the client builds the cache.
6. Configure settings for the on-demand scan cache.
   a. Select **Enable the on-demand scan cache**.
   b. In **Add the cache for safe files that are unchanged for __ days**, specify the number of days a file must remain unchanged before it is cached.
   c. In **The cache for each safe file expires within __ days**, specify the maximum number of days a cache remains in the cache file.

> **Note**
> To prevent all caches added during a scan from expiring on the same day, caches expire randomly within the maximum number of days you specified. For example, if 500 caches were added to the cache today and the maximum number of days you specified is 10, a fraction of the caches will expire the next day and the majority will expire on the succeeding days. On the 10th day, all caches that remain will expire.

7. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Global Scan Settings

There are a number of ways global scan settings get applied to clients.

- A particular scan setting can apply to all clients that the server manages or only to clients with certain scan privileges. For example, if you configure the postpone Scheduled Scan duration, only clients with the privilege to postpone Scheduled Scan will use the setting.
- A particular scan setting can apply to all or only to a particular scan type. For example, on computers with both the OfficeScan server and OfficeScan client installed, you can exclude the OfficeScan server database from scanning. However, this setting applies only during Real-time Scan.
- A particular scan setting can apply when scanning for either virus/malware or spyware/grayware, or both. For example, assessment mode only applies during spyware/grayware scanning.

Configuring Global Scan Settings

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Configure the Global Scan Settings in each of the available sections.

- *Scan Settings Section on page 7-65*
- *Scheduled Scan Settings Section on page 7-71*
- *Virus/Malware Log Bandwidth Settings Section on page 7-73*

3. Click **Save**.

Scan Settings Section

The Scan Settings section of the Global Scan Settings allows administrators to configure the following:

- *Configure Scan Settings for Large Compressed Files on page 7-65*
- *Add Manual Scan to the Windows Shortcut Menu on OfficeScan client Computers on page 7-66*
- *Exclude the OfficeScan Server Database Folder from Real-time Scan on page 7-66*
- *Exclude Microsoft Exchange Server Folders and Files from Scans on page 7-67*
- *Enable Deferred Scanning on File Operations on page 7-67*
- *Clean/Delete Infected Files Within Compressed Files on page 7-68*
- *Enable Assessment Mode on page 7-70*
- *Scan for Cookies on page 7-71*

Configure Scan Settings for Large Compressed Files

All OfficeScan clients managed by the server check the following settings when scanning compressed files for virus/malware and spyware/grayware during Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now:

- **Do not scan files in the compressed file if the size exceeds __ MB**: OfficeScan does not scan any file that exceeds the limit.

- **In a compressed file, scan only the first __ files**: After decompressing a compressed file, OfficeScan scans the specified number of files and ignores any remaining files, if any.

Add Manual Scan to the Windows Shortcut Menu on OfficeScan client Computers

When this setting is enabled, all OfficeScan clients managed by the server add a **Scan with OfficeScan Client** option to the right-click menu in Windows Explorer. When users right-click a file or folder on the Windows desktop or in Windows Explorer and select the option, Manual Scan scans the file or folder for virus/malware and spyware/grayware.

FIGURE 7-6. Scan with OfficeScan client option

Exclude the OfficeScan Server Database Folder from Real-time Scan

If the OfficeScan client and OfficeScan server exist on the same computer, the OfficeScan client will not scan the server database for virus/malware and spyware/grayware during Real-time Scan.

Tip

Enable this setting to prevent database corruption that may occur during scanning.

Exclude Microsoft Exchange Server Folders and Files from Scans

If the OfficeScan client and a Microsoft Exchange 2000/2003 server exist on the same computer, OfficeScan will not scan the following Microsoft Exchange folders and files for virus/malware and spyware/grayware during Manual Scan, Real-time Scan, Scheduled Scan and Scan Now.:

- The following folders in `\Exchsrvr\Mailroot\vsi 1`: `Queue`, `PickUp`, and `BadMail`
- `.\Exchsrvr\mdbdata`, including these files: `priv1.stm`, `priv1.edb`, `pub1.stm`, and `pub1.edb`
- `.\Exchsrvr\Storage Group`

For Microsoft Exchange 2007 or later folders, you need to manually add the folders to the scan exclusion list. For scan exclusion details, see the following website:

http://technet.microsoft.com/en-us/library/bb332342.aspx

See *Scan Exclusions on page 7-29* for steps in configuring the scan exclusion list.

Enable Deferred Scanning on File Operations

Administrators can configure OfficeScan to defer the scanning of files. OfficeScan allows the user to copy files and then scans the files after the copy process completes. This deferred scanning improves the performance of the copy and scan processes.

Note

Deferred scanning requires that the Virus Scan Engine (VSAPI) be version 9.713 or later. For details on upgrading the server, see *Manually Updating the OfficeScan Server on page 6-24*.

Clean/Delete Infected Files Within Compressed Files

When all clients managed by the server detect virus/malware within compressed files during Manual Scan, Real-time Scan, Scheduled Scan and Scan Now, and the following conditions are met, clients clean or delete the infected files.

- "Clean" or "Delete" is the action OfficeScan is set to perform. Check the action OfficeScan performs on infected files by going to **Networked Computers** > **Client Management** > **Settings** > **Scan Settings** > **{Scan Type}** > **Action** tab.
- You enable this setting. Enabling this setting may increase computer resource usage during scanning and scanning may take longer to complete. This is because OfficeScan needs to decompress the compressed file, clean/delete infected files within the compressed file, and then re-compress the file.
- The compressed file format is supported. OfficeScan only supports certain compressed file formats, including ZIP and Office Open XML, which uses ZIP compression technologies. Office Open XML is the default format for Microsoft Office 2007 applications such as Excel, PowerPoint, and Word.

Note

Contact your support provider for a complete list of supported compressed file formats.

For example, Real-time Scan is set to delete files infected with a virus. After Real-time Scan decompresses a compressed file named `abc.zip` and detects an infected file `123.doc` within the compressed file, OfficeScan deletes `123.doc` and then re-compresses `abc.zip`, which is now safe to access.

The following table describes what happens if any of the conditions is not met.

Table 7-17. Compressed File Scenarios and Results

Status of "Clean/Delete infected files within compressed files"	Action OfficeScan is set to perform	Compressed file format	Result
Enabled	Clean or Delete	Not supported Example: `def.rar` contains an infected file `123.doc`.	OfficeScan encrypts `def.rar` but does not clean, delete, or perform any other action on `123.doc`.
Disabled	Clean or Delete	Supported/Not supported Example: `abc.zip` contains an infected file `123.doc`.	OfficeScan does not clean, delete, or perform any other action on both `abc.zip` and `123.doc`.

Status of "Clean/ Delete infected files within compressed files"	Action OfficeScan is set to perform	Compressed file format	Result
Enabled/ Disabled	Not Clean or Delete (in other words, any of the following: Rename, Quarantine, Deny Access or Pass)	Supported/Not supported Example: `abc.zip` contains an infected file `123.doc`.	OfficeScan performs the configured action (Rename, Quarantine, Deny Access or Pass) on `abc.zip`, not `123.doc`. If the action is: **Rename**: OfficeScan renames `abc.zip` to `abc.vir`, but does not rename `123.doc`. **Quarantine**: OfficeScan quarantines `abc.zip` (`123.doc` and all non-infected files are quarantined). **Pass**: OfficeScan performs no action on both `abc.zip` and `123.doc` but logs the virus detection. **Deny Access**: OfficeScan denies access to `abc.zip` when it is opened (`123.doc` and all non-infected files cannot be opened).

Enable Assessment Mode

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

Trend Micro provides assessment mode to allow you to evaluate items that Trend Micro detects as spyware/grayware and then take appropriate action based on your evaluation.

For example, detected spyware/grayware that you do not consider a security risk can be added to the spyware/grayware approved list..

When in assessment mode, OfficeScan performs the following scan actions:

- **Pass**: During Manual Scan, Scheduled Scan and Scan Now
- **Deny Access**: During Real-time Scan

Note

Assessment mode overrides any user-configured scan action. For example, even if you choose "Clean" as the scan action during Manual Scan, "Pass" remains as the scan action when the client is on assessment mode.

Scan for Cookies

Select this option if you consider cookies as potential security risks. When selected, all clients managed by the server will scan cookies for spyware/grayware during Manual Scan, Scheduled Scan, Real-time Scan, and Scan Now.

Scheduled Scan Settings Section

Only clients set to run Scheduled Scan will use the following settings. Scheduled Scan can scan for virus/malware and spyware/grayware.

The Scheduled Scan Settings section of the Global Scan Settings allows administrators to configure the following:

- *Remind Users of the Scheduled Scan __ Minutes Before it Runs on page 7-72*
- *Postpone Scheduled Scan for up to __ Hours and __ Minutes on page 7-72*
- *Automatically Stop Scheduled Scan When Scanning Lasts More Than __ Hours and __ Minutes on page 7-72*
- *Skip Scheduled Scan When a Wireless Computer's Battery Life is Less Than __ % and its AC Adapter is Unplugged on page 7-72*
- *Resume a Missed Scheduled Scan on page 7-73*

Remind Users of the Scheduled Scan __ Minutes Before it Runs

OfficeScan displays a notification message minutes before scanning runs to remind users of the scan schedule (date and time) and any Scheduled Scan privilege you grant them.

The notification message can be enabled/disabled from **Networked Computers** > **Client Management** > **Settings** > **Privileges and Other Settings** > **Other Settings (tab)** > **Scheduled Scan Settings**. If disabled, no reminder displays.

Postpone Scheduled Scan for up to __ Hours and __ Minutes

Only users with the "Postpone Scheduled Scan" privilege can perform the following actions:

- Postpone Scheduled Scan before it runs and then specify the postpone duration.
- If Scheduled Scan is in progress, users can stop scanning and restart it later. Users then specify the amount of time that should elapse before scanning restarts. When scanning restarts, all previously scanned files are scanned again.

  The maximum postpone duration/elapsed time users can specify is 12 hours and 45 minutes, which you can reduce by specifying the number of hour(s) and/or minute(s) in the fields provided.

Automatically Stop Scheduled Scan When Scanning Lasts More Than __ Hours and __ Minutes

OfficeScan stops scanning when the specified amount of time is exceeded and scanning is not yet complete. OfficeScan immediately notifies users of any security risk detected during scanning.

Skip Scheduled Scan When a Wireless Computer's Battery Life is Less Than __ % and its AC Adapter is Unplugged

OfficeScan immediately skips scanning when Scheduled Scan launches if it detects that a wireless computer's battery life is running low and its AC adapter is not connected to

any power source. If battery life is low but the AC adapter is connected to a power source, scanning proceeds.

Resume a Missed Scheduled Scan

When Scheduled Scan did not launch because OfficeScan is not running on the day and time of Scheduled Scan, you can specify when OfficeScan will resume scanning:

- **Same time next day**: If OfficeScan is running at the exact same time next day, scanning is resumed.
- **__ minutes after the computer starts**: OfficeScan resumes scanning a number of minutes after the user turns on the computer. The number of minutes is between 10 and 120.

Note

Users can postpone or skip a resumed Scheduled Scan if the administrator enabled this privilege. For details, see *Scheduled Scan Privileges and Other Settings on page 7-52*.

Virus/Malware Log Bandwidth Settings Section

The Virus/Malware Log Bandwidth Settings section of the Global Scan Settings allows administrators to configure:

Enable OfficeScan Clients to Create a Single Virus/Malware Log Entry for Recurring Detections of the Same Virus/Malware Within an Hour on page 7-73

Enable OfficeScan Clients to Create a Single Virus/Malware Log Entry for Recurring Detections of the Same Virus/Malware Within an Hour

OfficeScan consolidates virus log entries when detecting multiple infections from the same virus/malware over a short period of time. OfficeScan may detect a single virus/malware multiple times, quickly filling the virus/malware log and consuming network bandwidth when the OfficeScan client sends log information to the server. Enabling this feature helps reduce both the number of virus/malware log entries made and the

amount of network bandwidth OfficeScan clients consume when they report virus log information to the server.

Security Risk Notifications

OfficeScan comes with a set of default notification messages that inform you, other OfficeScan administrators, and OfficeScan client users of detected security risks.

For details on notifications sent to administrators, see *Security Risk Notifications for Administrators on page 7-74*.

For details on notifications sent to OfficeScan client users, see *Security Risk Notifications for OfficeScan Client Users on page 7-80*.

Security Risk Notifications for Administrators

Configure OfficeScan to send you and other OfficeScan administrators a notification when it detects a security risk, or only when the action on the security risk is unsuccessful and therefore requires your intervention.

OfficeScan comes with a set of default notification messages that inform you and other OfficeScan administrators of security risk detections. You can modify the notifications and configure additional notification settings to suit your requirements.

Note

OfficeScan can send notifications through email, pager, SNMP trap, and Windows NT Event logs. Configure settings when OfficeScan sends notifications through these channels. For details, see *Administrator Notification Settings on page 13-29*.

Configuring Security Risk Notifications for Administrators

Procedure

1. Navigate to **Notifications** > **Administrator Notifications** > **Standard Notifications**.
2. In the **Criteria** tab:

a. Go to the **Virus/Malware** and **Spyware/Grayware** sections.

b. Specify whether to send notifications when OfficeScan detects virus/malware and spyware/grayware, or only when the action on these security risks is unsuccessful.

3. In the **Email** tab:

a. Go to the **Virus/Malware Detections** and **Spyware/Grayware Detections** sections.

b. Select **Enable notification via email**.

c. Select **Send notifications to users with client tree domain permissions**.

You can use Role-based Administration to grant client tree domain permissions to users. If a detection occurs on an OfficeScan client belonging to a specific domain, the email will be sent to the email addresses of the users with domain permissions. See the following table for examples:

TABLE 7-18. Client Tree Domains and Permissions

CLIENT TREE DOMAIN	ROLES WITH DOMAIN PERMISSIONS	USER ACCOUNT WITH THE ROLE	EMAIL ADDRESS FOR THE USER ACCOUNT
Domain A	Administrator (built-in)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domain B	Administrator (built-in)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

If an OfficeScan client belonging to Domain A detects a virus, the email will be sent to mary@xyz.com, john@xyz.com, and chris@xyz.com.

If an OfficeScan client belonging to Domain B detects spyware, the email will be sent to mary@xyz.com and jane@xyz.com.

Note

If you enable this option, all users with domain permissions must have a corresponding email address. The email notification will not be sent to users without an email address. Users and email addresses are configured from **Administration** > **User Accounts**.

d. Select **Send notifications to the following email address(es)** and then type the email addresses.

e. Accept or modify the default subject and message. You can use token variables to represent data in the **Subject** and **Message** fields.

TABLE 7-19. Token Variables for Security Risk Notifications

VARIABLE	DESCRIPTION
Virus/Malware detections	
%v	Virus/Malware name
%s	Computer with virus/malware
%i	IP address of the computer
%c	MAC address of the computer
%m	Domain of the computer
%p	Location of virus/malware
%y	Date and time of virus/malware detection
%e	Virus Scan Engine version
%r	Virus Pattern version
%a	Action performed on the security risk
%n	Name of the user logged on to the infected computer
Spyware/Grayware detections	
%s	Computer with spyware/grayware
%i	IP address of the computer

VARIABLE	DESCRIPTION
%m	Domain of the computer
%y	Date and time of spyware/grayware detection
%n	Name of the user logged on to the computer at the time of detection
%T	Spyware/Grayware and scan result

4. In the **Pager** tab:

   a. Go to the **Virus/Malware Detections** and **Spyware/Grayware Detections** sections.

   b. Select **Enable notification via pager**.

   c. Type the message.

5. In the **SNMP Trap** tab:

   a. Go to the **Virus/Malware Detections** and **Spyware/Grayware Detections** sections.

   b. Select **Enable notification via SNMP trap**.

   c. Accept or modify the default message. You can use token variables in the following table to represent data in the **Message** field.

TABLE 7-20. Token Variables for Security Risk Notifications

VARIABLE	DESCRIPTION
Virus/Malware detections	
%v	Virus/Malware name
%s	Computer with virus/malware
%i	IP address of the computer
%c	MAC address of the computer
%m	Domain of the computer

VARIABLE	DESCRIPTION
%p	Location of virus/malware
%y	Date and time of virus/malware detection
%e	Virus Scan Engine version
%r	Virus Pattern version
%a	Action performed on the security risk
%n	Name of the user logged on to the infected computer
Spyware/Grayware detections	
%s	Computer with spyware/grayware
%i	IP address of the computer
%m	Domain of the computer
%y	Date and time of spyware/grayware detection
%n	Name of the user logged on to the computer at the time of detection
%T	Spyware/Grayware and scan result
%v	Spyware/Grayware name
%a	Action performed on the security risk

6. In the **NT Event Log** tab:

   a. Go to the **Virus/Malware Detections** and **Spyware/Grayware Detections** sections.

   b. Select **Enable notification via NT Event Log**.

   c. Accept or modify the default message. You can use token variables in the following table to represent data in the **Message** field.

TABLE 7-21. Token Variables for Security Risk Notifications

VARIABLE	DESCRIPTION
Virus/Malware detections	
%v	Virus/Malware name
%s	Computer with virus/malware
%i	IP address of the computer
%c	MAC address of the computer
%m	Domain of the computer
%p	Location of virus/malware
%y	Date and time of virus/malware detection
%e	Virus Scan Engine version
%r	Virus Pattern version
%a	Action performed on the security risk
%n	Name of the user logged on to the infected computer
Spyware/Grayware detections	
%s	Computer with spyware/grayware
%i	IP address of the computer
%m	Domain of the computer
%y	Date and time of spyware/grayware detection
%n	Name of the user logged on to the computer at the time of detection
%T	Spyware/Grayware and scan result
%v	Spyware/Grayware name
%a	Action performed on the security risk

7. Click **Save**.

Security Risk Notifications for OfficeScan Client Users

OfficeScan can display notification messages on OfficeScan client computers:

- Immediately after Real-time Scan and Scheduled Scan detect virus/malware and spyware/grayware. Enable the notification message and optionally modify its content.
- If a client computer restart is necessary to finish cleaning infected files. For Real-time Scan, the message displays after a particular security risk has been scanned. For Manual Scan, Scheduled Scan, and Scan Now, the message displays once and only after OfficeScan finishes scanning all the scan targets.

Notifying Users of Virus/Malware and Spyware/Grayware Detections

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Scan Settings** > **Real-time Scan Settings** or **Settings** > **Scan Settings** > **Scheduled Scan Settings**.
4. Click the Action tab.
5. Select the following options:
   - **Display a notification message on the client computer when virus/malware is detected**
   - **Display a notification message on the client computer when probable virus/malware is detected**

6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Configuring Virus/Malware Notifications

Procedure

1. Navigate to **Notifications** > **Client User Notifications**.
2. Click the **Virus/Malware** tab.
3. Configure detection settings.
   a. Choose to display one notification for all virus/malware related events, or separate notifications depending on the following severity levels:
      - **High**: The OfficeScan client was unable to handle critical malware
      - **Medium**: The OfficeScan client was unable to handle malware
      - **Low**: The OfficeScan client was able to resolve all threats
   b. Accept or modify the default messages.
4. To display a notification message if virus/malware originated from the client user's computer:
   a. Select the check box under **Virus/Malware Infection Source**.
   b. Specify an interval for sending notifications.
   c. Optionally modify the default notification message.

Note

This notification message displays only if you enable Windows Messenger Service. Check the status of this service in the Services screen (**Control Panel** > **Administrative Tools** > **Services** > **Messenger**).

5. Click **Save**.

Configuring Spyware/Grayware Notifications

Procedure

1. Navigate to **Notifications** > **Client User Notifications**.
2. Click the **Spyware/Grayware** tab.
3. Accept or modify the default message.
4. Click **Save**.

Notifying Clients of a Restart to Finish Cleaning Infected Files

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Restart Notification** section.
5. Select **Display a notification message if the client computer needs to restart to finish cleaning infected files**.

6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Security Risk Logs

OfficeScan generates logs when it detects virus/malware or spyware/grayware, and when it restores spyware/grayware.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing Virus/Malware Logs

The OfficeScan client generates logs when it detects viruses and malware and sends the logs to the server.

Procedure

1. Navigate to one of the following:
   - **Logs** > **Networked Computer Logs** > **Security Risks**
   - **Networked Computers** > **Client Management**
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Logs** > **Virus/Malware Logs** or **View Logs** > **Virus/Malware Logs**.

4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date and time of virus/malware detection
   - Infected computer
   - Virus/Malware name
   - Infection source
   - Infected file
   - Scan type that detected the virus/malware
   - Scan results

     Note

     For more information on scan results, see *Virus/Malware Scan Results on page 7-84*.

   - IP address
   - MAC address
   - Log details (Click **View** to see the details.)
6. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

   The CSV file contains the following information:

   - All information in the logs
   - User name logged on to the computer at the time of detection

Virus/Malware Scan Results

The following scan results display in the virus/malware logs:

- **Deleted**

  - First action is Delete and the infected file was deleted.
  - First action is Clean but cleaning was unsuccessful. Second action is Delete and the infected file was deleted.
- **Quarantined**
  - First action is Quarantine and the infected file was quarantined.
  - First action is Clean but cleaning was unsuccessful. Second action is Quarantine and the infected file was quarantined.
- **Cleaned**

  An infected file was cleaned.
- **Renamed**
  - First action is Rename and the infected file was renamed.
  - First action is Clean but cleaning was unsuccessful. Second action is Rename and the infected file was renamed.
- **Access denied**
  - First action is Deny Access and access to the infected file was denied when the user attempted to open the file.
  - First action is Clean but cleaning was unsuccessful. Second action is Deny Access and access to the infected file was denied when the user attempted to open the file.
  - Probable Virus/Malware was detected during Real-time Scan.
  - Real-time Scan may deny access to files infected with a boot virus even if the scan action is Clean (first action) and Quarantine (second action). This is because attempting to clean a boot virus may damage the Master Boot Record (MBR) of the infected computer. Run Manual Scan so OfficeScan can clean or quarantine the file.
- **Passed**
  - First action is Pass. OfficeScan did not perform any action on the infected file.

  - First action is Clean but cleaning was unsuccessful. Second action is Pass so OfficeScan did not perform any action on the infected file.

- **Passed a potential security risk**

  This scan result only displays when OfficeScan detects "probable virus/malware" during Manual Scan, Scheduled Scan, and Scan Now. Refer to the following page on the Trend Micro online Virus Encyclopedia for information about probable virus/malware and how to submit suspicious files to Trend Micro for analysis.

  http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn

- **Unable to clean or quarantine the file**

  Clean is the first action. Quarantine is the second action, and both actions were unsuccessful.

  Solution: See *Unable to quarantine the file/Unable to rename the file on page 7-86*.

- **Unable to clean or delete the file**

  Clean is the first action. Delete is the second action, and both actions were unsuccessful.

  Solution: See *Unable to delete the file on page 7-87*.

- **Unable to clean or rename the file**

  Clean is the first action. Rename is the second action, and both actions were unsuccessful.

  Solution: See *Unable to quarantine the file/Unable to rename the file on page 7-86*.

- **Unable to quarantine the file/Unable to rename the file**

  Explanation 1

  The infected file may be locked by another application, is executing, or is on a CD. OfficeScan will quarantine/rename the file after the application releases the file or after it has been executed.

Solution

For infected files on a CD, consider not using the CD as the virus may infect other computers on the network.

Explanation 2

The infected file is in the Temporary Internet Files folder of the client computer. Since the computer downloads files while you are browsing, the web browser may have locked the infected file. When the web browser releases the file, OfficeScan will quarantine/rename the file.

Solution: None

- **Unable to delete the file**

Explanation 1

The infected file may be contained in a compressed file and the **Clean/Delete infected files within compressed files** setting in **Networked Computers** > **Global Client Settings** is disabled.

Solution

Enable the **Clean/Delete infected files within compressed files** option. When enabled, OfficeScan decompresses a compressed file, cleans/deletes infected files within the compressed file, and then re-compresses the file.

Note

Enabling this setting may increase computer resource usage during scanning and scanning may take longer to complete.

Explanation 2

The infected file may be locked by another application, is executing, or is on a CD. OfficeScan will delete the file after the application releases the file or after it has been executed.

Solution

For infected files on a CD, consider not using the CD as the virus may infect other computers on the network.

Explanation 3

The infected file is in the Temporary Internet Files folder of the OfficeScan client computer. Since the computer downloads files while you are browsing, the web browser may have locked the infected file. When the web browser releases the file, OfficeScan will delete the file.

Solution: None

- **Unable to send the quarantined file to the designated quarantine folder**

Although OfficeScan successfully quarantined a file in the `\Suspect` folder of the OfficeScan client computer, it cannot send the file to the designated quarantine directory.

Solution

Determine which scan type (Manual Scan, Real-time Scan, Scheduled Scan, or Scan Now) detected the virus/malware and then check the quarantine directory specified in **Networked Computers** > **Client Management** > **Settings** > **{Scan Type}** > **Action** tab.

If the quarantine directory is on the OfficeScan server computer or is on another OfficeScan server computer:

1. Check if the client can connect to the server.
2. If you use URL as the quarantine directory format:
   a. Ensure that the computer name you specify after "http://" is correct.
   b. Check the size of the infected file. If it exceeds the maximum file size specified in **Administration** > **Quarantine Manager**, adjust the setting to accommodate the file. You may also perform other actions such as deleting the file.
   c. Check the size of the quarantine directory folder and determine whether it has exceeded the folder capacity specified in **Administration** > **Quarantine Manager**. Adjust the folder capacity or manually delete files in the quarantine directory.
3. If you use UNC path, ensure that the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this

group. Also check if the quarantine directory folder exists and if the UNC path is correct.

If the quarantine directory is on another computer on the network (You can only use UNC path for this scenario):

1. Check if the OfficeScan client can connect to the computer.
2. Ensure that the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this group.
3. Check if the quarantine directory folder exists.
4. Check if the UNC path is correct.

If the quarantine directory is on a different directory on the OfficeScan client computer (you can only use absolute path for this scenario), check if the quarantine directory folder exists.

- **Unable to clean the file**

Explanation 1

The infected file may be contained in a compressed file and the Clean/Delete infected files within compressed files setting in **Networked Computers** > **Global Client Settings** is disabled.

Solution

Enable the **Clean/Delete infected files within compressed files** option. When enabled, OfficeScan decompresses a compressed file, cleans/deletes infected files within the compressed file, and then re-compresses the file.

Note

Enabling this setting may increase computer resource usage during scanning and scanning may take longer to complete.

Explanation 2

The infected file is in the Temporary Internet Files folder of the OfficeScan client computer. Since the computer downloads files while you are browsing, the web

browser may have locked the infected file. When the web browser releases the file, OfficeScan will clean the file.

Solution: None

Explanation 3

The file may be uncleanable. For details and solutions, see *Uncleanable File on page E-16*.

Viewing Spyware/Grayware Logs

The OfficeScan client generates logs when it detects spyware and grayware and sends the logs to the server.

Procedure

1. Navigate to one of the following:
   - **Logs** > **Networked Computer Logs** > **Security Risks**
   - **Networked Computers** > **Client Management**
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Logs** > **Spyware/Grayware Logs** or **View Logs** > **Spyware/Grayware Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date and time of spyware/grayware detection
   - Affected computer
   - Spyware/Grayware name
   - Scan type that detected the spyware/grayware
   - Details about the spyware/grayware scan results (if scan action was performed successfully or not). See *Spyware/Grayware Scan Results on page 7-91* for details.

- IP address
- MAC address
- Log details (Click **View** to see the details.)

6. Add spyware/grayware you consider harmless to the spyware/grayware approved list.
7. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

   The CSV file contains the following information:

   - All information in the logs
   - User name logged on to the computer at the time of detection

Spyware/Grayware Scan Results

The following scan results display in the spyware/grayware logs:

- **Successful, No Action Required**

  This is the first level result if the scan action was successful. The second level result can be any of the following:

  - **Cleaned**: OfficeScan terminated processes or deleted registries, files, cookies and shortcuts.
  - **Access denied**: OfficeScan denied access (copy, open) to the detected spyware/grayware components.

- **Further Action Required**

  This is the first level result if the scan action was unsuccessful. The second level results will have at least one of the following messages:

  - **Passed**: OfficeScan did not perform any action but logged the spyware/grayware detection for assessment.

    Solution: Add spyware/grayware that you consider safe to the spyware/grayware approved list.

- **Spyware/Grayware unsafe to clean**: This message displays if the Spyware Scan Engine attempts to clean any single folder and the following criteria are met:
  - Items to clean exceed 250MB.
  - The operating system uses the files in the folder. The folder may also be necessary for normal system operation.
  - The folder is a root directory (such as `C:` or `F:`)

  Solution: Contact your support provider for assistance.

- **Spyware/Grayware scan stopped manually. Please perform a complete scan**: A user stopped scanning before it was completed.

  Solution: Run a Manual Scan and wait for the scan to finish.

- **Spyware/Grayware cleaned, restart required. Please restart the computer**: OfficeScan cleaned spyware/grayware components but a computer restart is required to complete the task.

  Solution: Restart the computer immediately.

- **Spyware/Grayware cannot be cleaned**: Spyware/Grayware was detected on a CD-ROM or network drive. OfficeScan cannot clean spyware/grayware detected on these locations.

  Solution: Manually remove the infected file.

- **Spyware/Grayware scan result unidentified. Please contact Trend Micro technical support**: A new version of the Spyware Scan Engine provides a new scan result that OfficeScan has not been configured to handle.

  Solution: Contact your support provider for help in determining the new scan result.

Viewing Spyware/Grayware Restore Logs

After cleaning spyware/grayware, OfficeScan clients back up spyware/grayware data. Notify an online client to restore backed up data if you consider the data harmless. Information about which spyware/grayware backup data was restored, the affected computer, and the restore result available in the logs.

Procedure

1. Navigate to **Logs** > **Networked Computer Logs** > **Spyware/Grayware Restore**.
2. Check the **Result** column to see if OfficeScan successfully restored the spyware/grayware data.
3. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Scan Logs

When Manual Scan, Scheduled Scan, or Scan Now runs, the OfficeScan client creates a scan log that contains information about the scan. You can view the scan log by accessing the OfficeScan client console. Clients do not send the scan log to the server.

Scan logs show the following information:

- Date and time OfficeScan started scanning
- Date and time OfficeScan stopped scanning
- Scan status
  - **Completed**: The scan was completed without problems.
  - **Stopped**: The user stopped the scan before it can be completed.
  - **Stopped Unexpectedly**: The scan was interrupted by the user, system, or an unexpected event. For example, the OfficeScan Real-time Scan service might have terminated unexpectedly or the user performed a forced restart of the client.
- Scan type
- Number of scanned objects
- Number of infected files
- Number of unsuccessful actions
- Number of successful actions

- Virus Pattern version
- Smart Scan Agent Pattern version
- Spyware Pattern version

Security Risk Outbreaks

A security risk outbreak occurs when detections of virus/malware, spyware/grayware, and shared folder sessions over a certain period of time exceed a certain threshold. There are several ways to respond to and contain outbreaks in the network, including:

- Enabling OfficeScan to monitor the network for suspicious activity
- Blocking critical client computer ports and folders
- Sending outbreak alert messages to clients
- Cleaning up infected computers

Security Risk Outbreak Criteria and Notifications

Configure OfficeScan to send you and other OfficeScan administrators a notification when the following events occur:

- Virus/Malware outbreak
- Spyware/Grayware outbreak
- Firewall Violations outbreak
- Shared folder session outbreak

Define an outbreak by the number of detections and the detection period. An outbreak is triggered when the number of detections within the detection period is exceeded.

OfficeScan comes with a set of default notification messages that inform you and other OfficeScan administrators of an outbreak. You can modify the notifications and configure additional notification settings to suit your requirements.

Note

OfficeScan can send security risk outbreak notifications through email, pager, SNMP trap, and Windows NT Event logs. For shared folder session outbreaks, OfficeScan sends notifications through email. Configure settings when OfficeScan sends notifications through these channels. For details, see *Administrator Notification Settings on page 13-29*.

Configuring the Security Risk Outbreak Criteria and Notifications

Procedure

1. Navigate to **Notifications** > **Administrator Notifications** > **Outbreak Notifications**.
2. In the **Criteria** tab:
   a. Go to the **Virus/Malware** and **Spyware/Grayware** sections:
   b. Specify the number of unique sources of detections.
   c. Specify the number of detections and the detection period for each security risk.

   Tip

   Trend Micro recommends accepting the default values in this screen.

   OfficeScan sends a notification message when the number of detections is exceeded. For example, under the **Virus/Malware** section, if you specify 10 unique sources, 100 detections, and a time period of 5 hours, OfficeScan sends the notification when 10 different clients have reported a total of 101 security risks within a 5-hour period. If all instances are detected on only one client within a 5-hour period, OfficeScan does not send the notification.
3. In the **Criteria** tab:
   a. Go to the **Shared Folder Sessions** section.
   b. Select **Monitor shared folder sessions on your network**.

c. In **Shared folder sessions recorded**, click the number link to view the computers with shared folders and the computers accessing the shared folders.

d. Specify the number of shared folder sessions and the detection period.

OfficeScan sends a notification message when the number of shared folder sessions is exceeded.

4. In the **Email** tab:

a. Go to the **Virus/Malware Outbreaks**, **Spyware/Grayware Outbreaks**, and **Shared Folder Session Outbreaks** sections.

b. Select **Enable notification via email**.

c. Specify the email recipients.

d. Accept or modify the default email subject and message. You can use token variables to represent data in the **Subject** and **Message** fields.

TABLE 7-22. Token Variables for Security Risk Outbreak Notifications

VARIABLE	DESCRIPTION
Virus/Malware outbreaks	
%CV	Total number of viruses/malware detected
%CC	Total number of computers with virus/malware
Spyware/Grayware outbreaks	
%CV	Total number of spyware/grayware detected
%CC	Total number of computers with spyware/grayware
Shared folder session outbreaks	
%S	Number of shared folder sessions
%T	Time period when shared folder sessions accumulated
%M	Time period, in minutes

e. Select additional virus/malware and spyware/grayware information to include in the email. You can include the client/domain name, security risk name, date and time of detection, path and infected file, and scan result.

f. Accept or modify the default notification messages.

5. In the **Pager** tab:

   a. Go to the **Virus/Malware Outbreaks** and **Spyware/Grayware Outbreaks** sections.

   b. Select **Enable notification via pager.**

   c. Type the message.

6. In the **SNMP Trap** tab:

   a. Go to the **Virus/Malware Outbreaks** and **Spyware/Grayware Outbreaks** sections.

   b. Select **Enable notification via SNMP trap**.

   c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 7-22: Token Variables for Security Risk Outbreak Notifications on page 7-96* for details.

7. In the **NT Event Log** tab:

   a. Go to the **Virus/Malware Outbreaks** and **Spyware/Grayware Outbreaks** sections.

   b. Select **Enable notification via NT Event Log**.

   c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 7-22: Token Variables for Security Risk Outbreak Notifications on page 7-96* for details.

8. Click **Save**.

Configuring Security Risk Outbreak Prevention

When an outbreak occurs, enforce outbreak prevention measures to respond to and contain the outbreak. Configure prevention settings carefully because incorrect configuration may cause unforeseen network issues.

Procedure

1. Navigate to **Networked Computers** > **Outbreak Prevention**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Start Outbreak Prevention**.
4. Click any of the following outbreak prevention policies and then configure the settings for the policy:
   - *Limiting/Denying Access to Shared Folders on page 7-99*
   - *Blocking Vulnerable Ports on page 7-100*
   - *Denying Write Access to Files and Folders on page 7-102*
5. Select the policies you want to enforce.
6. Select the number of hours outbreak prevention will stay in effect. The default is 48 hours. You can manually restore network settings before the outbreak prevention period expires.

   WARNING!
   Do not allow outbreak prevention to remain in effect indefinitely. To block or deny access to certain files, folders, or ports indefinitely, modify computer and network settings directly instead of using OfficeScan.

7. Accept or modify the default client notification message.

   Note
   To configure OfficeScan to notify you during an outbreak, go to **Notifications** > **Administrator Notifications** > **Outbreak Notifications**.

8. Click **Start Outbreak Notification**.

   The outbreak prevention measures you selected display in a new window.

9. Back in the Outbreak Prevention client tree, check the **Outbreak Prevention** column.

   A check mark appears on computers applying outbreak prevention measures.

OfficeScan records the following events in the system event logs:

- Server events (initiating outbreak prevention and notifying clients to enable outbreak prevention)
- OfficeScan client event (enabling outbreak prevention)

Outbreak Prevention Policies

When outbreaks occur, enforce any of the following policies:

- *Limiting/Denying Access to Shared Folders on page 7-99*
- *Blocking Vulnerable Ports on page 7-100*
- *Denying Write Access to Files and Folders on page 7-102*

Limiting/Denying Access to Shared Folders

During outbreaks, limit or deny access to shared folders on the network to prevent security risks from spreading through the shared folders.

When this policy takes effect, users can still share folders but the policy will not apply to the newly shared folders. Therefore, inform users not to share folders during an outbreak or deploy the policy again to apply the policy to the newly shared folders.

Procedure

1. Navigate to **Networked Computers** > **Outbreak Prevention**.

2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Start Outbreak Prevention**.
4. Click **Limit/Deny access to shared folders**.
5. Select from the following options:
   - **Allow read access only**: Limits access to shared folders
   - **Deny Full Access**

   Note

   The read access only setting does not apply to shared folders already configured to deny full access.

6. Click **Save**.

   The Outbreak Prevention Settings screen displays again.

7. Click **Start Outbreak Notification**.

   The outbreak prevention measures you selected display in a new window.

Blocking Vulnerable Ports

During outbreaks, block vulnerable ports that viruses/malware might use to gain access to OfficeScan client computers.

WARNING!

Configure Outbreak Prevention settings carefully. Blocking ports that are in use makes network services that depend on them unavailable. For example, if you block the trusted port, OfficeScan cannot communicate with the client for the duration of the outbreak.

Procedure

1. Navigate to **Networked Computers** > **Outbreak Prevention**.

2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Start Outbreak Prevention**.
4. Click **Block Ports**.
5. Select whether to Block trusted port.
6. Select the ports to block under the **Blocked Ports** column.
   a. If there are no ports in the table, click **Add**. In the screen that opens, select the ports to block and click **Save**.
      - **All ports (including ICMP)**: Blocks all ports except the trusted port. If you also want to block the trusted port, select the Block trusted port check box in the previous screen.
      - **Commonly used ports**: Select at least one port number for OfficeScan to save the port blocking settings.
      - **Trojan ports**: Blocks ports commonly used by Trojan horse programs. See *Trojan Port on page E-13* for details.
      - **A port number or port range**: Optionally specify the direction of the traffic to block and some comments, such as the reason for blocking the ports you specified.
      - **Ping protocol (Reject ICMP)**: Click if you only want to block ICMP packets, such as ping requests.
   b. To edit settings for the blocked port(s), click the port number.
   c. In the screen that opens, modify the settings and click **Save**.
   d. To remove a port from the list, select the check box next to the port number and click **Delete**.
7. Click **Save**.

   The Outbreak Prevention Settings screen displays again.
8. Click **Start Outbreak Notification**.

The outbreak prevention measures you selected display in a new window.

Denying Write Access to Files and Folders

Viruses/Malware can modify or delete files and folders on the host computers. During an outbreak, configure OfficeScan to prevent viruses/malware from modifying or deleting files and folders on OfficeScan client computers.

Procedure

1. Navigate to **Networked Computers** > **Outbreak Prevention**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Start Outbreak Prevention**.
4. Click **Deny write access to files and folders**.
5. Type the directory path. When you finish typing the directory path you want to protect, click **Add**.

   Note

   Type the absolute path, not the virtual path, for the directory.

6. Specify the files to protect in the protected directories. Select all files or files based on specific file extensions. For file extensions, specify an extension that is not in the list, type it in the text box, and then click **Add**.
7. To protect specific files, under **Files to Protect**, type the full file name and click **Add**.
8. Click **Save**.

   The Outbreak Prevention Settings screen displays again.

9. Click **Start Outbreak Notification**.

The outbreak prevention measures you selected display in a new window.

Disabling Outbreak Prevention

When you are confident that an outbreak has been contained and that OfficeScan already cleaned or quarantined all infected files, restore network settings to normal by disabling Outbreak Prevention.

Procedure

1. Navigate to **Networked Computers** > **Outbreak Prevention**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Restore Settings**.
4. To inform users that the outbreak is over, select **Notify client users after restoring the original settings**.
5. Accept or modify the default client notification message.
6. Click **Restore Settings**.

Note

If you do not restore network settings manually, OfficeScan automatically restores these settings after the number of hours specified in **Automatically restore network settings to normal after __ hours** on the **Outbreak Prevention Settings** screen. The default setting is 48 hours.

OfficeScan records the following events in the system event logs:

- Server events (initiating outbreak prevention and notifying OfficeScan clients to enable outbreak prevention)
- OfficeScan client event (enabling outbreak prevention)

7. After disabling outbreak prevention, scan networked computers for security risks to ensure that the outbreak has been contained.

Chapter 8

Using Behavior Monitoring

This chapter describes how to protect computers from security risks using the Behavior Monitoring feature.

Topics in this chapter:

- *Behavior Monitoring on page 8-2*
- *Behavior Monitoring Privileges on page 8-10*
- *Behavior Monitoring Notifications for OfficeScan Client Users on page 8-11*
- *Behavior Monitoring Logs on page 8-12*

Behavior Monitoring

Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through **Malware Behavior Blocking** and **Event Monitoring**. Complementing these two features are a user-configured **exception list** and the **Certified Safe Software Service**.

Important

Behavior Monitoring does not support Windows XP or Windows 2003 64-bit platforms.

Behavior Monitoring does support Windows Vista 64-bit platforms with SP1 or later.

By default, Behavior Monitoring is disabled on all versions of Windows Server 2003, Windows Server 2008, and Windows Server 2012. Before enabling Behavior Monitoring on these server platforms, read the guidelines and best practices outlined in *OfficeScan Client Services on page 14-6*.

Malware Behavior Blocking

Malware Behavior Blocking provides a necessary layer of additional threat protection from programs that exhibit malicious behavior. It observes system events over a period of time. As programs execute different combinations or sequences of actions, Malware Behavior Blocking detects known malicious behavior and blocks the associated programs. Use this feature to ensure a higher level of protection against new, unknown, and emerging threats.

When a program is blocked and notifications are enabled, OfficeScan displays a notification on the OfficeScan client computer. For details about notifications, see *Behavior Monitoring Notifications for OfficeScan Client Users on page 8-11*.

Event Monitoring

Event Monitoring provides a more generic approach to protecting against unauthorized software and malware attacks. It monitors system areas for certain events, allowing administrators to regulate programs that trigger such events. Use Event Monitoring if

you have specific system protection requirements that are above and beyond what is provided by Malware Behavior Blocking.

The following table provides a list of monitored system events.

TABLE 8-1. Monitored System Events

EVENTS	DESCRIPTION
Duplicated System File	Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.
Hosts File Modification	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the web browser is redirected to infected, non-existent, or fake websites.
Suspicious Behavior	Suspicious behavior can be a specific action or a series of actions that is rarely carried out by legitimate programs. Programs exhibiting suspicious behavior should be used with caution.
New Internet Explorer Plugin	Spyware/grayware programs often install unwanted Internet Explorer plugins, including toolbars and Browser Helper Objects.
Internet Explorer Setting Modification	Many virus/malware change Internet Explorer settings, including the home page, trusted websites, proxy server settings, and menu extensions.
Security Policy Modification	Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.
Program Library Injection	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.
Shell Modification	Many malicious programs modify Windows shell settings to associate themselves to certain file types. This routine allows malicious programs to launch automatically if users open the associated files in Windows Explorer. Changes to Windows shell settings can also allow malicious programs to track the programs used and start alongside legitimate applications.

Events	Description
New Service	Windows services are processes that have special functions and typically run continuously in the background with full administrative access. Malicious programs sometimes install themselves as services to stay hidden.
System File Modification	Certain Windows system files determine system behavior, including startup programs and screen saver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.
Firewall Policy Modification	The Windows Firewall policy determines the applications that have access to the network, the ports that are open for communication, and the IP addresses that can communicate with the computer. Many malicious programs modify the policy to allow themselves to access to the network and the Internet.
System Process Modification	Many malicious programs perform various actions on built-in Windows processes. These actions can include terminating or modifying running processes.
New Startup Program	Malicious applications usually add or modify autostart entries in the Windows registry to automatically launch every time the computer starts.

When Event Monitoring detects a monitored system event, it performs the action configured for the event.

The following table lists possible actions that administrators can take on monitored system events.

TABLE 8-2. Actions on Monitored System Events

ACTION	DESCRIPTION
Assess	OfficeScan always allows programs associated with an event but records this action in the logs for assessment. This is the default action for all monitored system events. **Note** This option is not supported for Program Library Injections on 64-bit systems.
Allow	OfficeScan always allows programs associated with an event.
Ask when necessary	OfficeScan prompts users to allow or deny programs associated with an event and add the programs to the exception list If the user does not respond within a certain time period, OfficeScan automatically allows the program to run. The default time period is 30 seconds. To modify the time period, see *Configuring Global Behavior Monitoring Settings on page 8-7*. **Note** This option is not supported for Program Library Injections on 64-bit systems.
Deny	OfficeScan always blocks programs associated with an event and records this action in the logs. When a program is blocked and notifications are enabled, OfficeScan displays a notification on the OfficeScan client computer. For details about notifications, see *Behavior Monitoring Notifications for OfficeScan Client Users on page 8-11*.

Behavior Monitoring Exception List

The Behavior Monitoring exception list contains programs that are not monitored by Behavior Monitoring.

- **Approved Programs**: Programs in this list can be run. An approved program will still be checked by other OfficeScan features (such as file-based scanning) before it is finally allowed to run.
- **Blocked Programs**: Programs in this list can never be started. To configure this list, Event Monitoring should be enabled.

Configure the exception list from the web console. You can also grant users the privilege to configure their own exception list from the OfficeScan client console. For details, see *Behavior Monitoring Privileges on page 8-10*.

Configuring Malware Behavior Blocking, Event Monitoring, and the Exception List

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Behavior Monitoring Settings**.
4. Select **Enable Malware Behavior Blocking**.
5. Configure Event Monitoring settings.
   a. Select **Enable Event Monitoring**.
   b. Choose the system events to monitor and select an action for each of the selected events. For information about monitored system events and actions, see *Event Monitoring on page 8-2*.
6. Configure the exception list.
   a. Under **Enter Program Full Path**, type the full path of the program to approve or block. Separate multiple entries with semicolons (;). The exception list supports wildcards and UNC paths.
   b. Click **Approve Programs or Block Programs**.

c. To remove a blocked or approved program from the list, click the trash bin icon ( ) next to the program.

Note

OfficeScan accepts a maximum of 100 approved programs and 100 blocked programs.

7. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Configuring Global Behavior Monitoring Settings

OfficeScan applies global client settings to all clients or only to clients with certain privileges.

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Go to the **Behavior Monitoring Settings** section.
3. Configure the following settings as required:

Option	Description
Automatically allow program if client does not respond within __ seconds	This setting only works if Event Monitoring is enabled and the action for a monitored system event is "Ask when necessary". This action prompts a user to allow or deny programs associated with the event. If the user does not respond within a certain time period, OfficeScan automatically allows the program to run. For details, see *Event Monitoring on page 8-2*.
Enable Certified Safe Software Service	The Certified Safe Software Service queries Trend Micro datacenters to verify the safety of a program detected by either Malware Behavior Blocking or Event Monitoring. Enable Certified Safe Software Service to reduce the likelihood of false positive detections. **Note** Ensure that OfficeScan clients have the correct proxy settings (for details, see *OfficeScan Client Proxy Settings on page 14-46*) before enabling Certified Safe Software Service. Incorrect proxy settings, along with an intermittent Internet connection, can result in delays or failure to receive a response from Trend Micro datacenters, causing monitored programs to appear unresponsive. In addition, pure IPv6 OfficeScan clients cannot query directly from Trend Micro datacenters. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the OfficeScan clients to connect to the Trend Micro datacenters.

OPTION	DESCRIPTION
Prompt users before executing newly encountered programs downloaded through HTTP or email applications (Server platforms excluded)	Behavior Monitoring works in conjunction with Web Reputation Services to verify the prevalence of files downloaded through HTTP channels or email applications. After detecting a "newly encountered" file, administrators can choose to prompt users before executing the file. Trend Micro classifies a program as newly encountered based on the number of file detections or historical age of the file as determined by the Smart Protection Network. **Note** • Administrators must enable Web Reputation Services on the client to allow OfficeScan to scan HTTP traffic before this prompt can display. • For Windows 7/Vista/XP systems, this prompt only supports ports 80, 81, and 8080. • OfficeScan matches the file names downloaded through email applications during the execution process. If the file name has been changed, the user does not receive a prompt.

4. Click **Save**.

Behavior Monitoring Privileges

If clients have the Behavior Monitoring privileges, the Behavior Monitoring tab displays on the OfficeScan client console. Users can then manage their own exception list.

FIGURE 8-1. Behavior Monitoring tab on the OfficeScan client console

Granting Behavior Monitoring Privileges

Procedure

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

2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Behavior Monitoring Privileges** section.
5. Select **Display the Behavior Monitoring tab on the client console**.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Behavior Monitoring Notifications for OfficeScan Client Users

OfficeScan can display a notification message on an OfficeScan client computer immediately after Behavior Monitoring blocks a program. Enable the sending of notification messages and optionally modify the content of the message.

Enabling the Sending of Notification Messages

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.

4. Click the **Other Settings** tab and go to the **Behavior Monitoring Settings** section.
5. Select **Display a notification when a program is blocked**.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Modifying the Content of the Notification Message

Procedure

1. Navigate to **Notifications** > **Client User Notifications**.
2. Click the **Behavior Monitoring Policy Violations** tab.
3. Modify the default message in the text box provided.
4. Click **Save**.

Behavior Monitoring Logs

OfficeScan clients log unauthorized program access instances and send the logs to the server. An OfficeScan client that runs continuously aggregates the logs and sends them at specified intervals, which is every 60 minutes by default.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing Behavior Monitoring Logs

Procedure

1. Navigate to **Logs** > **Networked Computer Logs** > **Security Risks** or **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Logs** > **Behavior Monitoring Logs** or **View Logs** > **Behavior Monitoring Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date/Time unauthorized process was detected
   - Computer where unauthorized process was detected
   - Computer's domain
   - Violation, which is the event monitoring rule violated by the process
   - Action performed when violation was detected
   - Event, which is the type of object accessed by the program
   - Risk level of the unauthorized program
   - Program, which is the unauthorized program
   - Operation, which is the action performed by the unauthorized program
   - Target, which is the process that was accessed
6. To save logs to a comma-separated value (`CSV`) file, click **Export to CSV**. Open the file or save it to a specific location.

Configuring the Behavior Monitoring Log Sending Schedule

Procedure

1. Access <*Server installation folder*>`\PCCSRV`.
2. Open the `ofcscan.ini` file using a text editor such as Notepad.
3. Search for the string "`SendBMLogPeriod`" and then check the value next to it.

   The default value is 3600 seconds and the string appears as `SendBMLogPeriod=3600`.
4. Specify the value in seconds.

   For example, to change the log period to 2 hours, change the value to 7200.
5. Save the file.
6. Go to **Networked Computers** > **Global Client Settings**.
7. Click **Save** without changing any settings.
8. Restart the client.

Chapter 9

Using Device Control

This chapter describes how to protect computers from security risks using the Device Control feature.

Topics in this chapter:

- *Device Control on page 9-2*
- *Permissions for Storage Devices on page 9-3*
- *Permissions for Non-storage Devices on page 9-10*
- *Modifying Device Control Notifications on page 9-16*
- *Device Control Logs on page 9-17*

Device Control

Device Control regulates access to external storage devices and network resources connected to computers. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

You can configure Device Control policies for internal and external clients. OfficeScan administrators typically configure a stricter policy for external clients.

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

After you deploy the policies, clients use the location criteria you have set in the Computer Location screen (see *Computer Location on page 14-2*) to determine their location and the policy to apply. Clients switch policies each time the location changes.

Important:

- By default, Device Control is disabled on all versions of Windows Server 2003, Windows Server 2008, and Windows Server 2012. Before enabling Device Control on these server platforms, read the guidelines and best practices outlined in *OfficeScan Client Services on page 14-6*.
- The types of devices that OfficeScan can monitor depends on whether the Data Protection license is activated. Data Protection is a separately licensed module and must be activated before you can use it. For details about the Data Protection license, see *Data Protection License on page 3-4*.

TABLE 9-1. Device Types

	DATA PROTECTION ACTIVATED	DATA PROTECTION NOT ACTIVATED
Storage Devices		
CD/DVD	Monitored	Monitored
Floppy disks	Monitored	Monitored
Network drives	Monitored	Monitored

	Data Protection Activated	Data Protection Not Activated
USB storage devices	Monitored	Monitored
Non-storage Devices		
Bluetooth adapters	Monitored	Not monitored
COM and LPT ports	Monitored	Not monitored
IEEE 1394 interface	Monitored	Not monitored
Imaging devices	Monitored	Not monitored
Infrared devices	Monitored	Not monitored
Modems	Monitored	Not monitored
PCMCIA card	Monitored	Not monitored
Print screen key	Monitored	Not monitored
Wireless NICs	Monitored	Not monitored

- For a list of supported device models, see the *Data Protection Lists* document at:

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

Permissions for Storage Devices

Device Control permissions for storage devices are used when you:

- Allow access to USB storage devices, CD/DVD, floppy disks, and network drives. You can grant full access to these devices or limit the level of access.
- Configure the list of approved USB storage devices. Device Control allows you to block access to all USB storage devices, except those that have been added to the list of approved devices. You can grant full access to the approved devices or limit the level of access.

The following table lists the permissions for storage devices.

TABLE 9-2. Device Control Permissions for Storage Devices

PERMISSIONS	FILES ON THE DEVICE	INCOMING FILES
Full access	Permitted operations: Copy, Move, Open, Save, Delete, Execute	Permitted operations: Save, Move, Copy This means that a file can be saved, moved, and copied to the device.
Modify	Permitted operations: Copy, Move, Open, Save, Delete Prohibited operations: Execute	Permitted operations: Save, Move, Copy
Read and execute	Permitted operations: Copy, Open, Execute Prohibited operations: Save, Move, Delete	Prohibited operations: Save, Move, Copy
Read	Permitted operations: Copy, Open Prohibited operations: Save, Move, Delete, Execute	Prohibited operations: Save, Move, Copy
List device content only	Prohibited operations: All operations The device and the files it contains are visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy
Block (available after installing Data Protection)	Prohibited operations: All operations The device and the files it contains are not visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy

The file-based scanning function in OfficeScan complements and may override the device permissions. For example, if the permission allows a file to be opened but OfficeScan detects that the file is infected with malware, a specific scan action will be

performed on the file to eliminate the malware. If the scan action is Clean, the file opens after it is cleaned. However, if the scan action is Delete, the file is deleted.

Tip

Device Control for Data Protection supports all 64-bit platforms. For Unauthorized Change Prevention monitoring on systems that OfficeScan does not support (for details, see *Device Control 64-bit Support for Unauthorized Change Prevention on page 1-9*), set the device permission to **Block** to limit access to these devices.

Advanced Permissions for Storage Devices

Advanced permissions apply when you grant limited permissions to storage devices. The permission can be any of the following:

- Modify
- Read and execute
- Read
- List device content only

You can keep the permissions limited but grant advanced permissions to certain programs on the storage devices and on the local computer.

To define programs, configure the following program lists.

TABLE 9-3. Program Lists

PROGRAM LIST	DESCRIPTION	VALID INPUTS
Programs with read and write access to devices	This list contains local programs and programs on storage devices that have read and write access to the devices. An example of a local program is Microsoft Word (`winword.exe`), which is usually found in `C:\Program Files\Microsoft Office\Office`. If the permission for USB storage devices is "List device content only" but "`C:\Program Files\Microsoft Office\Office\winword.exe`" is included in this list: • A user will have read and write access to any file on the USB storage device that is accessed from Microsoft Word. • A user can save, move, or copy a Microsoft Word file to the USB storage device.	Program path and name For details, see *Specifying a Program Path and Name on page 9-8*.
Programs on devices that are allowed to execute	This list contains programs on storage devices that users or the system can execute. For example, if you want to allow users to install software from a CD, add the installation program path and name, such as "`E:\Installer\Setup.exe`", to this list.	Program path and name or Digital Signature Provider For details, see *Specifying a Program Path and Name on page 9-8* or *Specifying a Digital Signature Provider on page 9-7*.

There are instances when you need to add a program to both lists. Consider the data lock feature in a USB storage device, which, if enabled, prompts users for a valid user name and password before the device can be unlocked. The data lock feature uses a program on the device called "`Password.exe`", which must be allowed to execute so that users can unlock the device successfully. "`Password.exe`" must also have read and write access to the device so that users can change the user name or password.

Each program list on the user interface can contain up to 100 programs. If you want to add more programs to a program list, you will need to add them to the `ofcscan.ini` file, which can accommodate up to 1,000 programs. For instructions on adding programs to the `ofcscan.ini` file, see *Adding Programs to the Device Control Lists Using ofcscan.ini on page 9-15*.

WARNING!

Programs added to the `ofcscan.ini` file will be deployed to the root domain and will overwrite programs on individual domains and clients.

Specifying a Digital Signature Provider

Specify a Digital Signature Provider if you trust programs issued by the provider. For example, type Microsoft Corporation or Trend Micro, Inc. You can obtain the Digital

Signature Provider by checking the properties of a program (for example, by right-clicking the program and selecting **Properties**).

FIGURE 9-1. Digital Signature Provider for the OfficeScan client program (`PccNTMon.exe`)

Specifying a Program Path and Name

A program path and name should have a maximum of 259 characters and must only contain alphanumeric characters (A-Z, a-z, 0-9). It is not possible to specify only the program name.

You can use wildcards in place of drive letters and program names. Use a question mark (?) to represent single-character data, such as a drive letter. Use an asterisk (*) to represent multi-character data, such as a program name.

Note

Wildcards cannot be used to represent folder names. The exact name of a folder must be specified.

Wildcards are used correctly in the following examples:

TABLE 9-4. Correct Usage of Wildcards

EXAMPLE	MATCHED DATA
?:\Password.exe	The "Password.exe" file located directly under any drive
C:\Program Files\Microsoft *.exe	Any file in C:\Program Files that has a file extension
C:\Program Files*.*	Any file in C:\Program Files that has a file extension
C:\Program Files\a**?**c.exe	Any .exe file in C:\Program Files that has 3 characters starting with the letter "a" and ending with the letter "c"
C:*	Any file located directly under the C:\ drive, with or without file extensions

Wildcards are used incorrectly in the following examples:

TABLE 9-5. Incorrect Usage of Wildcards

EXAMPLE	REASON
??:\Buffalo\Password.exe	?? represents two characters and drive letters only have a single alphabetic character.
*****:\Buffalo\Password.exe	* represents multi-character data and drive letters only have a single alphabetic character.
C:*****\Password.exe	Wildcards cannot be used to represent folder names. The exact name of a folder must be specified.
C:**?**\Password.exe	

Permissions for Non-storage Devices

You can allow or block access to non-storage devices. There are no granular or advanced permissions for these devices.

Managing Access to External Devices (Data Protection Activated)

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Device Control Settings**.
4. Click the **External Clients** tab to configure settings for external clients or the **Internal Clients** tab to configure settings for internal clients.
5. Select **Enable Device Control**.
6. Apply settings as follows:
   - If you are on the **External Clients** tab, you can apply settings to internal clients by selecting **Apply all settings to internal clients**.
   - If you are on the **Internal Clients** tab, you can apply settings to external clients by selecting **Apply all settings to external clients**.
7. Choose to allow or block the AutoRun function (`autorun.inf`) on USB storage devices.
8. Configure settings for storage devices.
   a. Select a permission for each storage device. For details about permissions, see *Permissions for Storage Devices on page 9-3*.
   b. If the permission for USB storage devices is **Block**, configure a list of approved devices. Users can access these devices and you can control the

level of access using permissions. See *Configuring an Approved List of USB Devices on page 9-12*.

9. For each non-storage device, select **Allow** or **Block**.

10. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

    - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

    - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Configuring Advanced Permissions

Although you can configure advanced permissions and notifications for a specific storage device on the user interface, the permissions and notifications are actually applied to all storage devices. This means that when you click **Advanced permissions and notifications** for CD/DVD, you are actually defining permissions and notifications for all storage devices.

Note

For details about advanced permissions and how to correctly define programs with advanced permissions, see *Advanced Permissions for Storage Devices on page 9-5*.

Procedure

1. Click **Advanced permissions and notifications**.

   A new screen opens.

2. Below **Programs with read and write access to storage devices**, type a program path and file name and then click **Add**.

   Digital Signature Provider is not accepted.

3. Below **Programs on storage devices that are allowed to execute**, type the program path and name or the Digital Signature Provider and then click **Add**.

4. Select **Display a notification message on the client computer when OfficeScan detects unauthorized device access**.

   - Unauthorized device access refers to prohibited device operations. For example, if the device permission is "Read", users will not be able to save, move, delete, or execute a file on the device. For a list of prohibited device operations based on permissions, see *Permissions for Storage Devices on page 9-3*.

   - You can modify the notification message. For details, see *Modifying Device Control Notifications on page 9-16*.

5. Click **Back**.

Configuring an Approved List of USB Devices

The approved list for USB devices supports the use of the asterisk (*) wildcard. Replace any field with the asterisk (*) to include all devices that satisfy the other fields. For example, [vendor]-[model]-* places all USB devices from the specified vendor and the specified model type, regardless of serial ID, to the approved list.

Procedure

1. Click **Approved devices**.

2. Type the device vendor.

3. Type the device model and serial ID.

   Tip

   Use the Device List Tool to query devices connected to endpoints. The tool provides the device vendor, model, and serial ID for each device. For details, see *Device List Tool on page 9-13*.

4. Select the permission for the device.

For details about permissions, see *Permissions for Storage Devices on page 9-3*.

5. To add more devices, click the plus (+) icon.
6. Click **< Back**.

Device List Tool

Run the Device List Tool locally on each endpoint to query external devices connected to the endpoint. The tool scans an endpoint for external devices and then displays device information in a browser window. You can then use the information when configuring device settings for Data Loss Prevention and Device Control.

Running the Device List Tool

Procedure

1. On the OfficeScan server computer, navigate to `\PCCSRV\Admin\Utility\ListDeviceInfo`.
2. Copy `listDeviceInfo.exe` to the target endpoint.
3. On the endpoint, run the `listDeviceInfo.exe`.
4. View device information in the browser window that displays. Data Loss Prevention and Device Control use the following information:
   - Vendor (required)
   - Model (optional)
   - Serial ID (optional)

Managing Access to External Devices (Data Protection Not Activated)

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Device Control Settings**.
4. Click the **External Clients** tab to configure settings for external clients or the **Internal Clients** tab to configure settings for internal clients.
5. Select **Enable Device Control**.
6. Apply settings as follows:
   - If you are on the **External Clients** tab, you can apply settings to internal clients by selecting **Apply all settings to internal clients**.
   - If you are on the **Internal Clients** tab, you can apply settings to external clients by selecting **Apply all settings to external clients**.
7. Choose to allow or block the AutoRun function (`autorun.inf`) on USB storage devices.
8. Select a permission for each storage device. For details about permissions, see *Permissions for Storage Devices on page 9-3*.
9. Configure advanced permissions and notifications if the permission for a storage device is any of the following: **Modify**, **Read and execute**, **Read**, or **List device content only**. See *Configuring Advanced Permissions on page 9-11*.
10. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
    - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Adding Programs to the Device Control Lists Using ofcscan.ini

Note

For details about program lists and how to correctly define programs that can be added to the lists, see *Advanced Permissions for Storage Devices on page 9-5*.

Procedure

1. On the OfficeScan server computer, navigate to <*Server installation folder*> `\PCCSRV`.
2. Open `ofcscan.ini` using a text editor.
3. To add programs with read and write access to storage devices:
   a. Locate the following lines:

      ```
      [DAC_APPROVED_LIST]
      Count=x
      ```

   b. Replace "x" with the number of programs in the program list.
   c. Below "Count=x", add programs by typing the following:

      ```
      Item<number>=<program path and name or Digital Signature Provider>
      ```

      For example:

      ```
      [DAC_APPROVED_LIST]
      Count=3
      Item0=C:\Program Files\program.exe
      ```

```
Item1=?:\password.exe

Item2=Microsoft Corporation
```

4. To add programs on storage devices that are allowed to execute:

   a. Locate the following lines:

   ```
   [DAC_EXECUTABLE_LIST]

   Count=x
   ```

   b. Replace "x" with the number of programs in the program list.

   c. Below "Count=x", add programs by typing the following:

   ```
   Item<number>=<program path and name or Digital Signature
   Provider>
   ```

   For example:

   ```
   [DAC_EXECUTABLE_LIST]

   Count=3

   Item0=?:\Installer\Setup.exe

   Item1=E:\*.exe

   Item2=Trend Micro, Inc.
   ```

5. Save and close the `ofcscan.ini` file.

6. Open the OfficeScan web console and go to **Networked Computers** > **Global Client Settings**.

7. Click **Save** to deploy the program lists to all clients.

Modifying Device Control Notifications

Notification messages display on endpoints when Device Control violations occur. Administrators can modify the default notification message, if needed.

Procedure

1. Navigate to **Notifications** > **Client User Notifications**.
2. Click the **Device Control Violation** tab.
3. Modify the default messages in the text box provided.
4. Click **Save**.

Device Control Logs

OfficeScan clients log unauthorized device access instances and send the logs to the server. A client that runs continuously aggregates the logs and sends them after a 24-hour time period. A client that got restarted checks the last time the logs were sent to the server. If the elapsed time exceeds 24 hours, the client sends the logs immediately.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing Device Control Logs

Procedure

1. Navigate to **Logs** > **Networked Computer Logs** > **Security Risks** or **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Logs** > **Device Control Logs** or **View Logs** > **Device Control Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date/Time unauthorized access was detected

- Computer where external device is connected or where network resource is mapped
- Computer domain where external device is connected or where network resource is mapped
- Device type or network resource accessed
- Target, which is the item on the device or network resource that was accessed
- Accessed by, which specifies where access was initiated
- Permissions set for the target

6. To save logs to a comma-separated value (`CSV`) file, click **Export to CSV**. Open the file or save it to a specific location.

Chapter 10

Using Data Loss Prevention

This chapter discusses how to use the Data Loss Prevention feature.

Topics in this chapter:

- *About Data Loss Prevention on page 10-2*
- *Data Loss Prevention Policies on page 10-3*
- *Data Identifier Types on page 10-4*
- *Data Loss Prevention Templates on page 10-18*
- *DLP Channels on page 10-23*
- *Data Loss Prevention Actions on page 10-34*
- *Data Loss Prevention Exceptions on page 10-35*
- *Data Loss Prevention Policy Configuration on page 10-40*
- *Data Loss Prevention Notifications on page 10-45*
- *Data Loss Prevention Logs on page 10-49*

About Data Loss Prevention

Traditional security solutions are focused on preventing external security threats from reaching the network. In today's security environment, this is only half the story. Data breaches are now commonplace, exposing an organization's confidential and sensitive data – referred to as digital assets – to outside unauthorized parties. A data breach may occur as a result of internal employee mistakes or carelessness, data outsourcing, stolen or misplaced computing devices, or malicious attacks.

Data breaches can:

- Damage brand reputation
- Erode customer trust in the organization
- Result in unnecessary costs to cover for remediation and to pay fines for violating compliance regulations
- Lead to lost business opportunities and revenue when intellectual property is stolen

With the prevalence and damaging effects of data breaches, organizations now see digital asset protection as a critical component of their security infrastructure.

Data Loss Prevention safeguards an organization's sensitive data against accidental or deliberate leakage. Data Loss Prevention allows you to:

- Identify the sensitive information that requires protection using data identifiers
- Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email and external devices
- Enforce compliance to established privacy standards

Before you can monitor sensitive information for potential loss, you must be able to answer the following questions:

- What data needs protection from unauthorized users?
- Where does the sensitive data reside?
- How is the sensitive data transmitted?
- What users are authorized to access or transmit the sensitive data?

- What action should be taken if a security violation occurs?

This important audit typically involves multiple departments and personnel familiar with the sensitive information in your organization.

If you already defined your sensitive information and security policies, you can begin to define data identifiers and company policies.

Data Loss Prevention Policies

OfficeScan evaluates a file or data against a set of rules defined in DLP policies. Policies determine files or data that must be protected from unauthorized transmission and the action that OfficeScan performs when it detects transmission.

Note

Data transmissions between the OfficeScan server and its clients are not monitored.

You can configure policies for internal and external clients. OfficeScan administrators typically configure a stricter policy for external clients.

You can enforce specific policies to client groups or individual clients. You can also enforce a single policy to all clients.

After you deploy the policies, clients use the location criteria you have set in the **Computer Location** screen (see *Computer Location on page 14-2*) to determine their location and the policy to apply. Clients switch policies each time the location changes.

Policy Configuration

Define DLP policies by configuring the following settings and deploying the settings to selected clients:

TABLE 10-1. Settings that Define a DLP Policy

SETTINGS	DESCRIPTION
Data Identifiers	OfficeScan uses data identifiers to identify sensitive information. Data identifiers include expressions, file attributes, and keywords which act as the building blocks for DLP templates.
Rules	A DLP rule can consist of multiple templates, channels, and actions. Each rule is a subset of the encompassing DLP policy.
Templates	A DLP template combines data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a DLP rule. OfficeScan comes with a set of predefined templates and allows you to create customized templates. A DLP rule can contain one or several templates. OfficeScan uses the first-match rule when checking templates. This means that if a file or data matches the data identifiers in a template, OfficeScan will no longer check the other templates.
Channels	Channels are entities that transmit sensitive information. OfficeScan supports popular transmission channels, such as email, removable storage devices, and instant messaging applications.
Actions	OfficeScan performs one or several actions when it detects an attempt to transmit sensitive information through any of the channels.
Exceptions	Exceptions act as overrides to the configured DLP rules. Configure exceptions to manage non-monitored targets, monitored targets, and compressed file scanning.

Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. You can define digital assets using the following data identifiers:

- **Expressions**: Data that has a certain structure. For details, see *Expressions on page 10-5*.

- **File attributes**: File properties such as file type and file size. For details, see *File Attributes on page 10-10*.
- **Keywords**: A list of special words or phrases. For details, see *Keywords on page 10-12*.

Note

It is not possible to delete a data identifier that is being used in a DLP template. Delete the template before deleting the data identifier.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

You can use predefined and customized expressions. For details, see *Predefined Expressions on page 10-5* and *Customized Expressions on page 10-6*.

Predefined Expressions

OfficeScan comes with a set of predefined expressions. These expressions cannot be modified or deleted.

OfficeScan verifies these expressions using pattern matching and mathematical equations. After OfficeScan matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Viewing Settings for Predefined Expressions

Note

Predefined expressions cannot be modified or deleted.

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Expression** tab.
3. Click the expression name.
4. View settings in the screen that opens.

Customized Expressions

Create customized expressions if none of the predefined expressions meet your requirements.

Expressions are a powerful string-matching tool. Ensure that you are comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, if you are creating an expression that includes a date, you can refer to the expressions prefixed with "Date".
- Note that OfficeScan follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:

  http://www.pcre.org/
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

There are several criteria that you can choose from when creating expressions. An expression must satisfy your chosen criteria before OfficeScan subjects it to a DLP policy. For details about the different criteria options, see *Criteria for Customized Expression on page 10-7*.

Criteria for Customized Expression

TABLE 10-2. Criteria Options for Customized Expressions

CRITERIA	RULE	EXAMPLE
None	None	All - Names from US Census Bureau Expression: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Specific characters	An expression must include the characters you have specified. In addition, the number of characters in the expression must be within the minimum and maximum limits.	US - ABA Routing Number Expression: [^\d]([0123678]\d{8})[^\d] Characters: 0123456789 Minimum characters: 9 Maximum characters: 9
Suffix	Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters. In addition, the number of characters in the expression must be within the minimum and maximum limits.	All - Home Address Expression: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] Suffix characters: 0123456789- Number of characters: 5 Minimum characters in the expression: 25 Maximum characters in the expression: 80

CRITERIA	RULE	EXAMPLE
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] Separator: @ Minimum characters to the left: 3 Maximum characters to the left: 15 Maximum characters to the right: 30

Creating a Customized Expression

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Add**.

   A new screen displays.
4. Type a name for the expression. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /
5. Type a description that does not exceed 256 bytes in length.
6. Type the expression and specify whether it is case-sensitive.
7. Type the displayed data.

   For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.

8. Choose one of the following criteria and configure additional settings for the chosen criteria (see *Criteria for Customized Expression on page 10-7*):
   - None
   - Specific characters
   - Suffix
   - Single-character separator
9. Test the expression against an actual data.

   For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.
10. Click **Save** if you are satisfied with the result.

> **Note**
> Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

11. A message appears, reminding you to deploy the settings to clients. Click **Close**.
12. Back in the **DLP Data Identifiers** screen, click **Apply to All Clients**.

Importing Customized Expressions

Use this option if you have a properly-formatted `.dat` file containing the expressions. You can generate the file by exporting the expressions from either the OfficeScan server you are currently accessing or from another OfficeScan server.

> **Note**
> The `.dat` expression files generated by this OfficeScan version are not compatible with previous versions.

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Data Identifiers**.

2. Click the **Expression** tab.
3. Click **Import** and then locate the `.dat` file containing the expressions.
4. Click **Open**.

   A message appears, informing you if the import was successful. If an expression to be imported already exists, it will be skipped.
5. Click **Apply to All Clients**.

File Attributes

File attributes are specific properties of a file. You can use two file attributes when defining data identifiers, namely, file type and file size. For example, a software development company may want to limit the sharing of the company's software installer to the R&D department, whose members are responsible for the development and testing of the software. In this case, the OfficeScan administrator can create a policy that blocks the transmission of executable files that are 10 to 40MB in size to all departments except R&D.

By themselves, file attributes are poor identifiers of sensitive files. Continuing the example in this topic, third-party software installers shared by other departments will most likely be blocked. Trend Micro therefore recommends combining file attributes with other DLP data identifiers for a more targeted detection of sensitive files.

For a complete list of supported file types see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Creating a File Attribute List

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **File Attribute** tab.
3. Click **Add**.

A new screen displays.

4. Type a name for the file attribute list. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /

5. Type a description that does not exceed 256 bytes in length.

6. Select your preferred true file types.

7. If a file type you want to include is not listed, select **File extensions** and then type the file type's extension. OfficeScan checks files with the specified extension but does not check their true file types. Guidelines when specifying file extensions:

   - Each extension must start with an asterisk (*), followed by a period (.), and then the extension. The asterisk is a wildcard, which represents a file's actual name. For example, `*.pol` matches `12345.pol` and `test.pol`.

   - You can include wildcards in extensions. Use a question mark (?) to represent a single character and an asterisk (*) to represent two or more characters. See the following examples:

     - `*.*m` matches the following files: `ABC.dem`, `ABC.prm`, `ABC.sdcm`

     - `*.m*r` matches the following files: `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

     - `*.fm?` matches the following files: `ABC.fme`, `ABC.fml`, `ABC.fmp`

   - Be careful when adding an asterisk at the end of an extension as this might match parts of a file name and an unrelated extension. For example: `*.do*` matches `abc.doctor_john.jpg` and `abc.donor12.pdf`.

   - Use semicolons (;) to separate file extensions. There is no need to add a space after a semicolon.

8. Type the minimum and maximum file sizes in bytes. Both file sizes must be whole numbers larger than zero.

9. Click **Save**.

10. A message appears, reminding you to deploy the settings to clients. Click **Close**.

11. Back in the **DLP Data Identifiers** screen, click **Apply to All Clients**.

Importing a File Attribute List

Use this option if you have a properly-formatted `.dat` file containing the file attribute lists. You can generate the file by exporting the file attribute lists from either the OfficeScan server you are currently accessing or from another OfficeScan server.

Note

The `.dat` file attribute files generated by this OfficeScan version are not compatible with previous versions.

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **File Attribute** tab.
3. Click **Import** and then locate the `.dat` file containing the file attribute lists.
4. Click **Open**.

   A message appears, informing you if the import was successful. If a file attribute list to be imported already exists, it will be skipped.
5. Click **Apply to All Clients**.

Keywords

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure OfficeScan to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see *Predefined Keyword Lists on page 10-13* and *Customized Keyword Lists on page 10-14*.

Predefined Keyword Lists

OfficeScan comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation

For details about the predefined keyword lists in OfficeScan, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

How Keyword Lists Work

Number of Keywords Condition

Each keyword list contains a condition that requires a certain number of keywords be present in a document before the list will trigger a violation.

The number of keywords condition contains the following values:

- **All**: All of the keywords in the list must be present in the document.
- **Any**: Any one of the keywords in the list must be present in the document.
- **Specific number**: There must be at least the specified number of keywords in the document. If there are more keywords in the document than the number specified, a violation will trigger.

Distance Condition

Some of the lists contain a “distance” condition to determine if a violation is present. “Distance” refers to the amount of characters between the first character of one keyword and the first character of another keyword. Consider the following entry:

First Name:_John_ Last Name:_Smith_

The **Forms - First Name, Last Name** list has a "distance" condition of fifty (50) and the commonly used form fields of "First Name" and "Last Name". In the example above, a violation will trigger as the number of characters between the "F" in First Name and the "L" in Last Name is equal to eighteen (18).

For an example of an entry that would not trigger a violation, consider the following:

The **first name of our new employee from Switzerland is John. His l**ast name is Smith.

In this example, the number of characters between the "f" in "first name" and the "l" in "last name" is sixty-one (61). This exceeds the distance threshold and does not trigger a violation.

Customized Keyword Lists

Create customized keyword lists if none of the predefined keyword lists meet your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before OfficeScan subjects it to a DLP policy. Choose one of the following criteria for each keyword list:

- **Any keyword**
- **All keywords**
- **All keywords within <x> characters**
- **Combined score for keywords exceeds threshold**

For details regarding the criteria rules, see *Customized Keyword List Criteria on page 10-15*.

Customized Keyword List Criteria

TABLE 10-3. Criteria for a Keyword List

CRITERIA	RULE
Any keyword	A file must contain at least one keyword in the keyword list.
All keywords	A file must contain all the keywords in the keyword list.
All keywords within <x> characters	A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within <x> characters of each other. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If OfficeScan detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "W" (in WEB) and from the "W" to the "U" (in USB) must be 20 characters or less. The following data matches the criteria: DISK####WEB############USB The following data does not match the criteria: DISK**********WEB****USB(23 characters between "D" and "W") When deciding on the number of characters, remember that a small number, such as 10, will usually result in faster scanning time but will only cover a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.

CRITERIA	RULE
Combined score for keywords exceeds threshold	A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.

Creating a Keyword List

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Add**.

   A new screen displays.
4. Type a name for the keyword list. The name must not exceed 100 bytes in length and cannot contain the following characters:
   - > < * ^ | & ? \ /
5. Type a description that does not exceed 256 bytes in length.
6. Choose one of the following criteria and configure additional settings for the chosen criteria:
   - **Any keyword**
   - **All keywords**

- **All keywords within <x> characters**
- **Combined score for keywords exceeds threshold**

7. To manually add keywords to the list:
   a. Type a keyword that is 3 to 40 bytes in length and specify whether it is case-sensitive.
   b. Click **Add**.
8. To add keywords by using the "import" option:

> **Note**
> Use this option if you have a properly-formatted .csv file containing the keywords. You can generate the file by exporting the keywords from either the OfficeScan server you are currently accessing or from another OfficeScan server.

   a. Click **Import** and then locate the `.csv` file containing the keywords.
   b. Click **Open**.

      A message appears, informing you if the import was successful. If a keyword to be imported already exists in the list, it will be skipped.
9. To delete keywords, select the keywords and click **Delete**.
10. To export keywords:

> **Note**
> Use the "export" feature to back up the keywords or to import them to another OfficeScan server. All keywords in the keyword list will be exported. It is not possible to export individual keywords.

   a. Click **Export**.
   b. Save the resulting `.csv` file to your preferred location.
11. Click **Save**.
12. A message appears, reminding you to deploy the settings to clients. Click **Close**.

13. Back in the **DLP Data Identifiers** screen, click **Apply to All Clients**.

Importing a Keyword List

Use this option if you have a properly-formatted `.dat` file containing the keyword lists. You can generate the file by exporting the keyword lists from either the OfficeScan server you are currently accessing or from another OfficeScan server.

Note

The `.dat` keyword list files generated by this OfficeScan version are not compatible with previous versions.

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Import** and then locate the `.dat` file containing the keyword lists.
4. Click **Open**.

   A message appears, informing you if the import was successful. If a keyword list to be imported already exists, it will be skipped.
5. Click **Apply to All Clients**.

Data Loss Prevention Templates

A DLP template combines DLP data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a DLP policy.

For example, a file must be a Microsoft Word file (file attribute) AND must contain certain legal terms (keywords) AND must contain ID numbers (expressions) for it to be subject to the "Employment Contracts" policy. This policy allows Human Resources

personnel to transmit the file through printing so that the printed copy can be signed by an employee. Transmission through all other possible channels, such as email, is blocked.

You can create your own templates if you have configured DLP data identifiers. You can also use predefined templates. For details, see *Customized DLP Templates on page 10-19* and *Predefined DLP Templates on page 10-19*.

Note

It is not possible to delete a template that is being used in a DLP policy. Remove the template from the policy before deleting it.

Predefined DLP Templates

OfficeScan comes with the following set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

- **GLBA**: Gramm-Leach-Billey Act
- **HIPAA**: Health Insurance Portability and Accountability Act
- **PCI-DSS**: Payment Card Industry Data Security Standard
- **SB-1386**: US Senate Bill 1386
- **US PII**: United States Personally Identifiable Information

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized DLP Templates

Create your own templates if you have configured data identifiers. A template combines data identifiers and logical operators (And, Or, Except) to form condition statements.

For more information and examples on how condition statements and logical operators work, see *Condition Statements and Logical Operators on page 10-20*.

Condition Statements and Logical Operators

OfficeScan evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

See the examples in the following table.

TABLE 10-4. Sample Condition Statements

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
[Data Identifier1] **And** [Data Identifier 2] **Except** [Data Identifier 3]	A file must satisfy [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 3]. For example: A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].
[Data Identifier 1] **Or** [Data Identifier 2]	A file must satisfy [Data Identifier 1] or [Data Identifier 2]. For example: A file must be [an Adobe PDF document] or [a Microsoft Word document].
Except [Data Identifier 1]	A file must not satisfy [Data Identifier 1]. For example: A file must not be [a multimedia file].

As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not satisfy all of the data identifiers in the statement. In most cases, however, the first data identifier does not have an operator.

Creating a Template

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Templates**.
2. Click **Add**.

   A new screen displays.
3. Type a name for the template. The name must not exceed 100 bytes in length and cannot contain the following characters:
   - > < * ^ | & ? \ /
4. Type a description that does not exceed 256 bytes in length.
5. Select data identifiers and then click the "add" icon.

   When selecting definitions:
   - Select multiple entries by pressing and holding the **CTRL** key and then selecting the data identifiers.
   - Use the search feature if you have a specific definition in mind. You can type the full or partial name of the data identifier.
   - Each template can contain a maximum of 30 data identifiers.
6. To create a new expression, click **Expressions** and then click **Add new expression**. In the screen that appears, configure settings for the expression.
7. To create a new file attribute list, click **File attributes** and then click **Add new file attribute**. In the screen that appears, configure settings for the file attribute list.
8. To create a new keyword list, click **Keywords** and then click **Add new keyword**. In the screen that appears, configure settings for the keyword list.
9. If you selected an expression, type the number of occurrences, which is the number of times an expression must occur before OfficeScan subjects it to a DLP policy.
10. Choose a logical operator for each definition.

Note

Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see *Condition Statements and Logical Operators on page 10-20*.

11. To remove a data identifier from the list of selected identifiers, click the trash bin icon.
12. Below **Preview**, check the condition statement and make changes if this is not your intended statement.
13. Click **Save**.
14. A message appears, reminding you to deploy the settings to clients. Click **Close**.
15. Back in the **DLP Templates** screen, click **Apply to All Clients**.

Importing Templates

Use this option if you have a properly-formatted `.dat` file containing the templates. You can generate the file by exporting the templates from either the OfficeScan server you are currently accessing or from another OfficeScan server.

Note

To import DLP templates from OfficeScan 10.6, import the associated data identifiers (previously named Definitions) first. OfficeScan cannot import templates that are missing their associated data identifiers.

Procedure

1. Navigate to **Networked Computers** > **Data Loss Prevention** > **Templates**.
2. Click **Import** and then locate the `.dat` file containing the templates.
3. Click **Open**.

   A message appears, informing you if the import was successful. If a template to be imported already exists, it will be skipped.

4. Click **Apply to All Clients**.

DLP Channels

Users can transmit sensitive information through various channels. OfficeScan can monitor the following channels:

- **Network channels**: Sensitive information is transmitted using network protocols, such as HTTP and FTP.
- **System and application channels**: Sensitive information is transmitted using a local computer's applications and peripherals.

Network Channels

OfficeScan can monitor data transmission through the following network channels:

- Email clients
- FTP
- HTTP and HTTPS
- IM Applications
- SMB protocol
- Webmail

To determine data transmissions to monitor, OfficeScan checks the transmission scope, which you need to configure. Depending on the scope that you selected, OfficeScan will monitor all data transmissions or only transmissions outside the Local Area Network (LAN). For details about transmission scope, see *Transmission Scope and Targets for Network Channels on page 10-27*.

Email Clients

OfficeScan monitors email transmitted through various email clients. OfficeScan checks the email's subject, body, and attachments for data identifiers. For a list of supported email clients, see the *Data Protection Lists* document at:

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

Monitoring occurs when a user attempts to send the email. If the email contains data identifiers, OfficeScan will either allow or block the email.

You can define monitored and non-monitored internal email domains.

- **Monitored email domains**: When OfficeScan detects email transmitted to a monitored domain, it checks the action for the policy. Depending on the action, the transmission is allowed or blocked.

  Note

  If you select email clients as a monitored channel, an email must match a policy for it to be monitored. In contrast, an email sent to monitored email domains is automatically monitored, even if it does not match a policy.

- **Non-monitored email domains**: OfficeScan immediately allows the transmission of emails sent to non-monitored domains.

  Note

  Data transmissions to non-monitored email domains and to monitored email domains where "Monitor" is the action are similar in that the transmission is allowed. The only difference is that for non-monitored email domains, OfficeScan does not log the transmission, whereas for monitored email domains, the transmission is always logged.

Specify domains using any of the following formats, separating multiple domains with commas:

- X400 format, such as /O=Trend/OU=USA, /O=Trend/OU=China
- Email domains, such as example.com

For email messages sent through the SMTP protocol, OfficeScan checks if the target SMTP server is on the following lists:

1. Monitored targets
2. Non-monitored targets

> **Note**
>
> For details about monitored and non-monitored targets, see *Defining Non-monitored and Monitored Targets on page 10-35*.

3. Monitored email domains
4. Non-monitored email domains

This means that if an email is sent to an SMTP server on the monitored targets list, the email is monitored. If the SMTP server is not on the monitored targets list, OfficeScan checks the other lists.

For emails sent through other protocols, OfficeScan only checks the following lists:

1. Monitored email domains
2. Non-monitored email domains

FTP

When OfficeScan detects that an FTP client is attempting to upload files to an FTP server, it checks for the presence of data identifiers in the files. No file has been uploaded at this point. Depending on the DLP policy, OfficeScan will allow or block the upload.

When you configure a policy that blocks file uploads, remember the following:

- When OfficeScan blocks an upload, some FTP clients will try to re-upload the files. In this case, OfficeScan terminates the FTP client to prevent the re-upload. Users do not receive a notification after the FTP client terminates. Inform them of this situation when you roll out your DLP policies.
- If a file to be uploaded will overwrite a file on the FTP server, the file on the FTP server may be deleted.

For a list of supported FTP clients, see the *Data Protection Lists* document at:

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

HTTP and HTTPS

OfficeScan monitors data to be transmitted through HTTP and HTTPS. For HTTPS, OfficeScan checks the data before it is encrypted and transmitted.

For a list of supported web browsers and applications, see the *Data Protection Lists* document at:

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

IM Applications

OfficeScan monitors messages and files that users send through instant messaging (IM) applications. Messages and files that users receive are not monitored.

For a list of supported IM applications, see the *Data Protection Lists* document at:

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

When OfficeScan blocks a message or file sent through AOL Instant Messenger, MSN, Windows Messenger, or Windows Live Messenger, it also terminates the application. If OfficeScan does not do this, the application will become unresponsive and users will be forced to terminate the application anyway. Users do not receive a notification after the application terminates. Inform them of this situation when you roll out your DLP policies.

SMB Protocol

OfficeScan monitors data transmissions through the Server Message Block (SMB) protocol, which facilitates shared file access. When another user attempts to copy or read a user's shared file, OfficeScan checks if the file is or contains a data identifier and then allows or blocks the operation.

Note

The Device Control action has a higher priority than the DLP action. For example, if Device Control does not allow files on mapped network drives to be moved, transmission of sensitive data does not proceed even if DLP allows it. For details on Device Control actions, see *Permissions for Storage Devices on page 9-3*.

For a list of applications that OfficeScan monitors for shared file access, see the *Data Protection Lists* document at:

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

Webmail

Web-based email services transmit data through HTTP. If OfficeScan detects outgoing data from supported services, it checks the data for the presence of data identifiers.

For a list of supported web-based email services, see the *Data Protection Lists* document at:

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

Transmission Scope and Targets for Network Channels

Transmission scope and targets define data transmissions on network channels that OfficeScan must monitor. For transmissions that should be monitored, OfficeScan checks for the presence of data identifiers before allowing or blocking the transmission. For transmissions that should not be monitored, OfficeScan does not check for the presence of data identifiers and immediately allows the transmission.

Transmission Scope: All Transmissions

OfficeScan monitors data transmitted outside the host computer.

Note

Trend Micro recommends choosing this scope for external clients.

If you do not want to monitor data transmissions to certain targets outside the host computer, define the following:

- **Non-monitored targets**: OfficeScan does not monitor data transmitted to these targets.

> **Note**
>
> Data transmissions to non-monitored targets and to monitored targets where "Monitor" is the action are similar in that the transmission is allowed. The only difference is that for non-monitored targets, OfficeScan does not log the transmission, whereas for monitored targets, the transmission is always logged.

- **Monitored targets**: These are specific targets within the non-monitored targets that should be monitored. Monitored targets are:
  - Optional if you defined non-monitored targets.
  - Not configurable if you did not define non-monitored targets.

For example:

The following IP addresses are assigned to your company's Legal Department:

- 10.201.168.1 to 10.201.168.25

You are creating a policy that monitors the transmission of Employment Certificates to all employees except the Legal Department's full time staff. To do this, you would select **All transmissions** as the transmission scope and then:

Option 1:

1. Add 10.201.168.1-10.201.168.25 to the non-monitored targets.
2. Add the IP addresses of the Legal Department's part-time staff to the monitored targets. Assume that there are 3 IP addresses, 10.201.168.21-10.201.168.23.

Option 2:

Add the IP addresses of the Legal Department's full time staff to the non-monitored targets:

- 10.201.168.1-10.201.168.20

- 10.201.168.24-10.201.168.25

For guidelines on defining monitored and non-monitored targets, see *Defining Non-monitored and Monitored Targets on page 10-35*.

Transmission Scope: Only Transmissions Outside the Local Area Network

OfficeScan monitors data transmitted to any target outside the Local Area Network (LAN).

Note

Trend Micro recommends choosing this scope for internal clients.

"Network" refers to the company or local network. This includes the current network (IP address of the endpoint and netmask) and the following standard private IP addresses:

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 172.16.0.0 to 172.31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

If you select this transmission scope, you can define the following:

- **Non-monitored targets**: Define targets outside the LAN that you consider safe and therefore should not be monitored.

  Note

  Data transmissions to non-monitored targets and to monitored targets where "Monitor" is the action are similar in that the transmission is allowed. The only difference is that for non-monitored targets, OfficeScan does not log the transmission, whereas for monitored targets, the transmission is always logged.

- **Monitored targets**: Define targets within the LAN that you want to monitor.

For guidelines on defining monitored and non-monitored targets, see *Defining Non-monitored and Monitored Targets on page 10-35*.

Resolving Conflicts

If settings for transmission scope, monitored targets, and non-monitored targets conflict, OfficeScan recognizes the following priorities, in order of highest priority to lowest:

- Monitored targets
- Non-monitored targets
- Transmission scope

System and Application Channels

OfficeScan can monitor the following system and application channels:

- Data recorders (CD/DVD)
- Peer-to-peer applications
- PGP Encryption
- Printer
- Removable storage
- Synchronization software (ActiveSync)
- Windows clipboard

Data Recorders (CD/DVD)

OfficeScan monitors data recorded to a CD or DVD. For a list of supported data recording devices and software, see the *Data Protection Lists* document at:

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

When OfficeScan detects a "burn" command initiated on any of the supported devices or software and the action is Pass, data recording proceeds. If the action is Block,

OfficeScan checks if any of the files to be recorded is or contains a data identifier. If OfficeScan detects at least one data identifier, all files—including those that are not, or do not contain, data identifiers—will not be recorded. OfficeScan may also prevent the CD or DVD from ejecting. If this issue occurs, instruct users to restart the software process or reset the device.

OfficeScan implements additional CD/DVD recording rules:

- To reduce false positives, OfficeScan does not monitor the following files:

```
.bud      .dll      .gif      .gpd      .htm      .ico      .ini

.jpg      .lnk      .sys      .ttf      .url      .xml
```

- Two file types used by Roxio data recorders (`*.png` and `*.skn`) are not monitored to increase performance.

- OfficeScan does not monitor files in the following directories:

```
*:\autoexec.bat                    *:\Windows

..\Application Data                ..\Cookies

..\Local Settings                  ..\ProgramData

..\Program Files                   ..\Users\*\AppData

..\WINNT
```

- ISO images created by the devices and software are not monitored.

Peer-to-Peer Applications

OfficeScan monitors files that users share through peer-to-peer applications.

For a list of supported peer-to-peer applications, see the *Data Protection Lists* document at:

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

PGP Encryption

OfficeScan monitors data to be encrypted by PGP encryption software. OfficeScan checks the data before encryption proceeds.

For a list of supported PGP encryption software, see the *Data Protection Lists* document at:

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

Printer

OfficeScan monitors printer operations initiated from various applications.

OfficeScan does not block printer operations on new files that have not been saved because printing information has only been stored in the memory at this point.

For a list of supported applications that can initiate printer operations, see the *Data Protection Lists* document at:

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

Removable Storage

OfficeScan monitors data transmissions to or within removable storage devices. Activities related to data transmission include:

- Creation of a file within the device
- Copying of a file from the host machine to the device
- Closing of a modified file within the device
- Modifying of file information (such as the file's extension) within the device

When a file to be transmitted contains a data identifier, OfficeScan either blocks or allows the transmission.

Note

The Device Control action has a higher priority than the DLP action. For example, If Device Control does not allow copying of files to a removable storage device, transmission of sensitive information does not proceed even if DLP allows it. For details on Device Control actions, see *Permissions for Storage Devices on page 9-3*.

For a list of supported removable storage devices and applications that facilitate data transmission activities, see the *Data Protection Lists* document at:

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

The handling of file transmission to a removable storage device is a straightforward process. For example, a user who creates a file from Microsoft Word may want to save the file to an SD card (it does not matter which file type the user saves the file as). If the file contains a data identifier that should not be transmitted, OfficeScan prevents the file from being saved.

For file transmission within the device, OfficeScan first backs up the file (if its size is 75MB or less) to `%WINDIR%\system32\dgagent\temp` before processing it. OfficeScan removes the backup file if it allowed the file transmission. If OfficeScan blocked the transmission, it is possible that the file may have been deleted in the process. In this case, OfficeScan will copy the backup file to the folder containing the original file.

OfficeScan allows you to define non-monitored devices. OfficeScan always allows data transmissions to or within these devices. Identify devices by their vendors and optionally provide the device models and serial IDs.

Tip

Use the Device List Tool to query devices connected to endpoints. The tool provides the device vendor, model, and serial ID for each device. For details, see *Device List Tool on page 9-13*.

Synchronization Software (ActiveSync)

OfficeScan monitors data transmitted to a mobile device through synchronization software.

For a list of supported synchronization software, see the *Data Protection Lists* document at:

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

If the data has a source IP address of 127.0.0.1 and is sent through either port 990 or 5678 (the ports used for synchronization), OfficeScan checks if the data is a data identifier before allowing or blocking its transmission.

When OfficeScan blocks a file transmitted on port 990, a file of the same name containing malformed characters may still be created at the destination folder on the mobile device. This is because parts of the file have been copied to the device before OfficeScan blocked the transmission.

Windows Clipboard

OfficeScan monitors data to be transmitted to Windows clipboard before allowing or blocking the transmission.

OfficeScan can also monitor clipboard activities between the host machine and VMWare or Remote Desktop. Monitoring occurs on the entity with the OfficeScan client. For example, an OfficeScan client on a VMware virtual machine can prevent clipboard data on the virtual machine from being transmitted to the host machine. Similarly, a host machine with an OfficeScan client may not copy clipboard data to an endpoint accessed through Remote Desktop.

Data Loss Prevention Actions

When OfficeScan detects the transmission of data identifiers, it checks the DLP policy for the detected data identifiers and performs the action configured for the policy.

The following table lists the Data Loss Prevention actions.

TABLE 10-5. Data Loss Prevention Actions

ACTION	DESCRIPTION
Actions	

ACTION	DESCRIPTION
Pass	OfficeScan allows and logs the transmission
Block	OfficeScan blocks and logs the transmission
Additional Actions	
Notify the client user	OfficeScan displays a notification message to inform the user of the data transmission and whether it was passed or blocked.
Record data	Regardless of the primary action, OfficeScan records the sensitive information to `<Client installation folder>\DLPLite\Forensic`. Select this action to evaluate sensitive information that is being flagged by Data Loss Prevention. Recorded sensitive information may consume too much hard disk space. Therefore, Trend Micro highly recommends that you choose this option only for highly sensitive information.

Data Loss Prevention Exceptions

DLP exceptions apply to the entire policy, including all rules defined within the policy. OfficeScan applies the exception settings to all transmissions before scanning for digital assets. If a transmission matches one of the exception rules, OfficeScan immediately allows or scans the transmission depending on the exception type.

Defining Non-monitored and Monitored Targets

Define the non-monitored and monitored targets based on the transmission scope configured on the **Channel** tab. For details on how to define non-monitored and monitored targets for **All transmissions**, see *Transmission Scope: All Transmissions on page 10-27*. For details on how to define non-monitored and monitored targets for **Only transmissions outside the Local Area Network**, see *Transmission Scope: Only Transmissions Outside the Local Area Network on page 10-29*.

Follow these guidelines when defining monitored and non-monitored targets:

1. Define each target by:
   - IP address
   - Host name
   - FQDN
   - Network address and subnet mask, such as 10.1.1.1/32

   Note

   For the subnet mask, OfficeScan only supports a classless inter-domain routing (CIDR) type port. That means that you can only type a number like 32 instead of 255.255.255.0.

2. To target specific channels, include the default or company-defined port numbers for those channels. For example, port 21 is typically for FTP traffic, port 80 for HTTP, and port 443 for HTTPS. Use a colon to separate the target from the port numbers.
3. You can also include port ranges. To include all ports, ignore the port range.

   Below are some examples of targets with port numbers and port ranges:
   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. Separate targets with commas.

Decompression Rules

Files contained in compressed files can be scanned for digital assets. To determine the files to scan, OfficeScan subjects a compressed file to the following rules:

- Size of a decompressed file exceeds: __ MB (1-512MB)
- Compression layers exceed: __ (1-20)

- Number of files to scan exceeds: __ (1-2000)

Rule 1: Maximum Size of a Decompressed File

A compressed file – upon decompression – must meet the specified limit.

Example: You set the limit to 20MB.

Scenario 1: If the size of `archive.zip` upon decompression is 30MB, none of the files contained in `archive.zip` will be scanned. The other two rules are no longer checked.

Scenario 2: If the size of `my_archive.zip` upon decompression is 10MB:

- If `my_archive.zip` does not contain compressed files, OfficeScan skips Rule 2 and proceeds to Rule 3.
- If `my_archive.zip` contains compressed files, the size of all decompressed files must be within the limit. For example, if `my_archive.zip` contains `AAA.rar`, `BBB.zip` and `EEE.zip`, and `EEE.zip` contains `222.zip`:

`my_archive.zip`	= 10MB upon decompression
`\AAA.rar`	= 25MB upon decompression
`\BBB.zip`	= 3MB upon decompression
`\EEE.zip`	= 1MB upon decompression
`\222.zip`	= 2MB upon decompression

`my_archive.zip`, `BBB.zip`, `EEE.zip`, and `222.zip` will be checked against Rule 2 because the combined size of these files is within the 20MB limit. `AAA.rar` is skipped.

Rule 2: Maximum Compression Layers

Files within the specified number of layers will be flagged for scanning.

For example:

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

If you set the limit to two layers:

- OfficeScan will ignore `333.txt` because it is located on the third layer.
- OfficeScan will flag the following files for scanning and then check Rule 3:
  - `DDD.txt` (located on the first layer)
  - `CCC.xls` (located on the second layer)
  - `111.pdf` (located on the second layer)

Rule 3: Maximum Number of Files to Scan

OfficeScan scans files up to the specified limit. OfficeScan scans files and folders in numeric and then alphabetic order.

Continuing from the example in Rule 2, OfficeScan has flagged the highlighted files for scanning:

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

In addition, `my_archive.zip` contains a folder named `7Folder`, which was not checked against Rule 2. This folder contains `FFF.doc` and `GGG.ppt`. This brings the total number of files to be scanned to 5, as highlighted below:

```
my_archive.zip
                    \7Folder          \FFF.doc
                    \7Folder          \GGG.ppt
                    \BBB.zip          \CCC.xls
                    \DDD.txt
                    \EEE.zip          \111.pdf
                                      \222.zip          \333.txt
```

If you set the limit to 4 files, the following files are scanned:

- `FFF.doc`
- `GGG.ppt`
- `CCC.xls`
- `DDD.txt`

Note

For files that contain embedded files, OfficeScan extracts the content of the embedded files.

If the extracted content is text, the host file (such as `123.doc`) and embedded files (such as `abc.txt` and `xyz.xls`) are counted as one.

If the extracted content is not text, the host file (such as `123.doc`) and embedded files (such as `abc.exe`) are counted separately.

Events that Trigger Decompression Rules

The following events trigger decompression rules:

- **Event 1:**

  A compressed file to be transmitted matches a policy and the action on the compressed file is Pass (transmit the file).

For example, to monitor .ZIP files that users are transmitting, you defined a file attribute (.ZIP), added it to a template, used the template in a policy, and then set the action to **Pass**.

Note

If the action is Block, the entire compressed file is not transmitted and therefore, there is no need to scan the files it contains.

- **Event 2:**

  A compressed file to be transmitted does not match a policy.

  In this case, OfficeScan will still subject the compressed file to the decompression rules to determine which of the files it contains should be scanned for digital assets and whether to transmit the entire compressed file.

- **Result:**

  Events 1 and 2 have the same result. When OfficeScan encounters a compressed file:

  - If Rule 1 is not satisfied, OfficeScan allows the transmission of the entire compressed file.
  - If Rule 1 is satisfied, the other two rules are checked. OfficeScan allows the transmission of the entire compressed file if:
    - All scanned files do not match a policy.
    - All scanned files match a policy and the action is **Pass**.

      The transmission of the entire compressed file is blocked if at least one scanned file matches a policy and the action is **Block**.

Data Loss Prevention Policy Configuration

You can start to create Data Loss Prevention policies after you have configured data identifiers and organized them in templates.

In addition to data identifiers and templates, you need to configure channels and actions when creating a policy. For details about policies, see *Data Loss Prevention Policies on page 10-3*.

Creating a Data Loss Prevention Policy

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **DLP Settings**.
4. Click the **External Clients** tab to configure a policy for external clients or the **Internal Clients** tab to configure a policy for internal clients.

   Note

   Configure client location settings if you have not done so. Clients will use these settings to determine their location and apply the correct Data Loss Prevention policy. For details, see *Computer Location on page 14-2*.

5. Select **Enable Data Loss Prevention**.
6. Choose one of the following:
   - If you are on the **External Clients** tab, you can apply all Data Loss Prevention settings to internal clients by selecting **Apply all settings to internal clients**.
   - If you are on the **Internal Clients** tab, you can apply all Data Loss Prevention settings to external clients by selecting **Apply all settings to external clients**.
7. On the **Rules** tab, click **Add**.

   A policy can contain a maximum of 40 rules.

8. Configure the rule settings.

For details creating DLP rules, see *Creating Data Loss Prevention Rules on page 10-42*.

9. Click the **Exceptions** tab and configure any necessary exception settings.

   For details on the available exception settings, see *Data Loss Prevention Exceptions on page 10-35*.

10. If you selected domain(s) or client(s) in the client tree, click **Save and Apply the Settings to Clients**. If you clicked the root domain icon, choose from the following options:

    - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
    - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Creating Data Loss Prevention Rules

Procedure

1. Select **Enable this rule**.
2. Specify a name for the rule.

   Configure the template settings:

3. Click the **Template** tab.
4. Select templates from the **Available templates** list and then click **Add**.

   When selecting templates:

   - Select multiple entries by clicking the template names which highlights the name.
   - Use the search feature if you have a specific template in mind. You can type the full or partial name of the template.

Note

Each rule can contain a maximum of 200 templates.

5. If your preferred template is not found in the **Available templates** list:

   a. Click **Add new template**.

      The **Data Loss Prevention Templates** screen displays.

      For instructions on adding templates in the **Data Prevention Templates screen**, see *Data Loss Prevention Templates on page 10-18*.

   b. After creating the template, select it and then click **Add**.

Note

OfficeScan uses the first-match rule when checking templates. This means that if a file or data matches the definition on a template, OfficeScan will no longer check the other templates. Priority is based on the order of the templates in the list.

Configure the channel settings:

6. Click the **Channel** tab.

7. Select the channels for the rule.

   For details about channels, see *Network Channels on page 10-23* and *System and Application Channels on page 10-30*.

8. If you selected any of the network channels, select the transmission scope:

   - **All transmissions**
   - **Only transmissions outside the Local Area Network**

   See *Transmission Scope and Targets for Network Channels on page 10-27* for details on transmission scope, how targets work depending on the transmission scope, and how to define targets correctly.

9. If you selected **Email clients**:

   a. Click **Exceptions**.

b. Specify monitored and non-monitored internal email domains. For details on monitored and non-monitored email domains, see *Email Clients on page 10-24*.

10. If you selected **Removable storage**:

    a. Click **Exceptions**.

    b. Add non-monitored removable storage devices, identifying them by their vendors. The device model and serial ID are optional.

    The approved list for USB devices supports the use of the asterisk (*) wildcard. Replace any field with the asterisk (*) to include all devices that satisfy the other fields.

    For example, [vendor]-[model]-* places all USB devices from the specified vendor and the specified model type, regardless of serial ID, to the approved list.

    c. To add more devices, click the plus (+) icon.

Tip

Use the Device List Tool to query devices connected to endpoints. The tool provides the device vendor, model, and serial ID for each device. For details, see *Device List Tool on page 9-13*.

Configure the action settings:

11. Click the **Action** tab.

12. Select a primary action and any additional actions. For details about actions, see *Data Loss Prevention Actions on page 10-34*.

13. After configuring the **Template**, **Channel**, and **Action** settings, click **Save**.

Importing, Exporting, and Copying DLP Rules

Administrators can import previously defined rules (contained in a properly formatted `.dat` file) or export the list of configured DLP rules. Copying a DLP rule allows an administrator to modify the contents of a previously defined rule to save time.

The following table describes how each function works.

TABLE 10-6. Import, Export, and Copy Functions for DLP Rules

FUNCTION	DESCRIPTION
Import	Importing a rule list appends non-existing rules to the existing DLP rule list. OfficeScan skips rules that already exist in the target list. OfficeScan maintains all pre-configured settings for each rule, including the enabled or disabled status.
Export	Exporting a rule list exports the entire list to a `.dat` file that administrators can then import and deploy to other domains or clients. OfficeScan saves all rule settings based on the current configuration. **Note** • Administrators must save or apply any new or modified rules before exporting the list. • OfficeScan does not export any exceptions configured for the policy, only the settings configured for each rule.
Copy	Copying a rule creates an exact replica of the current configuration settings for the rule. Administrators must type a new name for the rule and can make any configuration modifications necessary for the new rule.

Data Loss Prevention Notifications

OfficeScan comes with a set of default notification messages that inform OfficeScan administrators and client users of digital asset transmissions.

For details on notifications sent to administrators, see *Data Loss Prevention Notifications for Administrators on page 10-46*.

For details on notifications sent to client users, see *Data Loss Prevention Notifications for Client Users on page 10-49*.

Data Loss Prevention Notifications for Administrators

Configure OfficeScan to send administrators a notification when it detects the transmission of digital assets, or only when the transmission is blocked.

OfficeScan comes with a set of default notification messages that inform administrators of digital asset transmissions. Modify the notifications and configure additional notification settings to suit company requirements.

Note

OfficeScan can send notifications through email, pager, SNMP trap, and Windows NT Event logs. Configure settings when OfficeScan sends notifications through these channels. For details, see *Administrator Notification Settings on page 13-29*.

Configuring Data Loss Prevention Notifications for Administrators

Procedure

1. Navigate to **Notifications** > **Administrator Notifications** > **Standard Notifications**.
2. On the **Criteria** tab:
   a. Go to the **Digital Asset Transmissions** section.
   b. Specify whether to send notifications when transmission of digital assets is detected (the action can be blocked or passed) or only when the transmission is blocked.
3. On the **Email** tab:
   a. Go to the **Digital Asset Transmissions** section.
   b. Select **Enable notification via email**.
   c. Select **Send notifications to users with client tree domain permissions**.

      Use Role-based Administration to grant client tree domain permissions to users. If transmission occurs on a client belonging to a specific domain, the

email are sent to the email addresses of the users with domain permissions. See the following table for examples:

TABLE 10-7. Client Tree Domains and Permissions

CLIENT TREE DOMAIN	ROLES WITH DOMAIN PERMISSIONS	USER ACCOUNT WITH THE ROLE	EMAIL ADDRESS FOR THE USER ACCOUNT
Domain A	Administrator (built-in)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domain B	Administrator (built-in)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

If an OfficeScan client belonging to Domain A detects a digital asset transmission, the email will be sent to mary@xyz.com, john@xyz.com, and chris@xyz.com.

If a client belonging to Domain B detects the transmission, the email is sent to mary@xyz.com and jane@xyz.com.

Note

When enabling this option, all users with domain permissions must have a corresponding email address. The email notification will not be sent to users without an email address. Users and email addresses are configured from **Administration** > **User Accounts**.

d. Select **Send notifications to the following email address(es)** and then type the email addresses.

e. Accept or modify the default subject and message. Use token variables to represent data in the **Subject** and **Message** fields.

TABLE 10-8. Token Variables for Data Loss Prevention Notifications

VARIABLE	DESCRIPTION
%USER%	The user logged on to the computer when transmission was detected
%COMPUTER%	Computer where transmission was detected
%DOMAIN%	Domain of the computer
%DATETIME%	Date and time transmission was detected
%CHANNEL%	The channel through which transmission was detected
%TEMPLATE%	The digital asset template that triggered the detection

4. On the **Pager** tab:
   a. Go to the **Digital Asset Transmissions** section.
   b. Select **Enable notification via pager**.
   c. Type the message.
5. On the **SNMP Trap** tab:
   a. Go to the **Digital Asset Transmissions** section.
   b. Select **Enable notification via SNMP trap**.
   c. Accept or modify the default message. Use token variables to represent data in the **Message** field. See *Table 10-8: Token Variables for Data Loss Prevention Notifications on page 10-48* for details.
6. On the **NT Event Log** tab:
   a. Go to the **Digital Asset Transmissions** section.
   b. Select **Enable notification via NT Event Log**.
   c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 10-8: Token Variables for Data Loss Prevention Notifications on page 10-48* for details.

7. Click **Save**.

Data Loss Prevention Notifications for Client Users

OfficeScan can display notification messages on client computers immediately after it allows or blocks the transmission of digital assets.

To notify users that digital asset transmission was blocked or allowed, select the option **Notify the client user** when creating a Data Loss Prevention policy. For instructions on creating a policy, see *Data Loss Prevention Policy Configuration on page 10-40*.

Configuring Data Loss Prevention Notification for Clients

Procedure

1. Navigate to **Notifications** > **Client User Notifications**.
2. Click the **Digital Asset Transmissions** tab.
3. Accept or modify the default message.
4. Click **Save**.

Data Loss Prevention Logs

Clients log digital asset transmissions (blocked and allowed transmissions) and send the logs to the server immediately. If the client is unable to send logs, it retries after 5 minutes.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing Data Loss Prevention Logs

Procedure

1. Navigate to **Networked Computers** > **Client Management** or **Logs** > **Networked Computer Logs** > **Security Risks**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Logs** > **Data Loss Prevention Logs** or **View Logs** > **DLP Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs.

   Logs contain the following information:

TABLE 10-9. Data Loss Prevention Log Information

COLUMN	DESCRIPTION
Date/Time	The date and time that OfficeScan logged the incident
User Name	The user name logged on to the computer
Computer	The name of computer where OfficeScan detected the transmission
Domain	The domain of the computer
IP	The IP address of the computer
Rule Name	The rule name(s) that triggered the incident **Note** Policies created in a previous version of OfficeScan display the default name of LEGACY_DLP_Policy.
Channel	The channel through which the transmission occurred

Column	Description
Process	The process that facilitated the transmission of a digital asset (the process depends on the channel) For details, see *Processes by Channel on page 10-51*.
Source	The source of the file containing the digital asset, or channel (if no source is available)
Destination	The intended destination of the file containing the digital asset, or channel (if no source is available)
Action	The action taken on the transmission
Details	A link which includes additional details about the transmission For details, see *Data Loss Prevention Log Details on page 10-54*.

6. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Processes by Channel

The following table lists the processes that display under the Process column in the Data Loss Prevention logs.

Table 10-10. Processes by Channel

Channel	Process
Synchronization software (ActiveSync)	Full path and process name of the synchronization software Example: `C:\Windows\system32\WUDFHost.exe`
Data recorder (CD/DVD)	Full path and process name of the data recorder Example: `C:\Windows\Explorer.exe`

Channel	Process
Windows clipboard	Not applicable
Email client - Lotus Notes	Full path and process name of Lotus Notes Example: `C:\Program Files\IBM\Lotus\Notes\nlnotes.exe`
Email client - Microsoft Outlook	Full path and process name of Microsoft Outlook Example: `C:\Program Files\Microsoft Office\Office12\ OUTLOOK.EXE`
Email client - All clients that use the SMTP protocol	Full path and process name of the email client Example: `C:\Program Files\Mozilla Thunderbird\thunderbird.exe`
Removable storage	Process name of the application that transmitted data to or within the storage device Example: `explorer.exe`
FTP	Full path and process name of the FTP client Example: `D:\Program Files\FileZilla FTP Client\filezilla.exe`
HTTP	"HTTP application"
HTTPS	Full path and process name of the browser or application Example: `C:\Program Files\Internet Explorer\iexplore.exe`
IM application	Full path and process name of the IM application Example: `C:\Program Files\Skype\Phone\Skype.exe`

Channel	Process
IM application - MSN	• Full path and process name of MSN Example: `C:\Program Files\Windows Live\Messenger\msnmsgr.exe` • "HTTP application" if data is transmitted from a chat window
Peer-to-peer application	Full path and process name of the peer-to-peer application Example: `D:\Program Files\BitTorrent\bittorrent.exe`
PGP encryption	Full path and process name of the PGP encryption software Example: `C:\Program Files\PGP Corporation\PGP Desktop\PGPmnApp.exe`
Printer	Full path and process name of the application that initiated a printer operation Example: `C:\Program Files\Microsoft Office\Office12\ WINWORD.EXE`
SMB protocol	Full path and process name of the application from which shared file access (copying or creating a new file) was performed Example: `C:\Windows\Explorer.exe`
Webmail (HTTP mode)	"HTTP application"
Webmail (HTTPS mode)	Full path and process name of the browser or application Example: `C:\Program Files\Mozilla Firefox\firefox.exe`

Data Loss Prevention Log Details

The **Data Loss Prevention Log Details** screen shows additional details about the digital asset transmission. The details of a transmission vary based on the channel and process through which OfficeScan detected the incident.

The following table lists the details that display.

TABLE 10-11. Data Loss Prevention Log Details

DETAIL	DESCRIPTION
Date/Time	The date and time that OfficeScan logged the incident
Violation ID	The unique ID of the incident
User Name	The user name logged on to the computer
Computer	The name of computer where OfficeScan detected the transmission
Domain	The domain of the computer
IP	The IP address of the computer
Channel	The channel through which the transmission occurred
Process	The process that facilitated the transmission of a digital asset (the process depends on the channel) For details, see *Processes by Channel on page 10-51*.
Source	The source of the file containing the digital asset, or channel (if no source is available)
Email Sender	The email address where the transmission originated
Email Subject	The subject line of the email message containing the digital asset
Email Recipients	The destination email address(es) of the email message
URL	The URL of a website or web page
FTP User	The user name used to log on to the FTP server
File Class	The type of file in which OfficeScan detected the digital asset

Detail	Description
Rule/Template	A list of the exact rule name(s) and template(s) that triggered the detection **Note** Each rule can contain multiple templates that triggered the incident. Multiple template names are separated by commas.
Action	The action taken on the transmission

Data Protection Debug Logs

Enabling Debug Logging for the Data Protection Module

Procedure

1. Obtain the `logger.cfg` file from your support provider.
2. Add the following data in `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`:
   - **Type**: `String`
   - **Name**: `debugcfg`
   - **Value**: `C:\Log\logger.cfg`
3. Create a folder named "Log" in the `C:\ directory`.
4. Copy `logger.cfg` to the "Log" folder.
5. Deploy Data Loss Prevention and Device Control settings from the web console to start collecting logs.

Note

Disable debug logging for the Data Protection module by deleting `debugcfg` in the registry key and restarting the computer.

Chapter 11

Protecting Computers from Web-based Threats

This chapter describes web-based threats and using OfficeScan to protect your network and computers from web-based threats.

Topics in this chapter:

- *About Web Threats on page 11-2*
- *Command & Control Contact Alert Services on page 11-2*
- *Web Reputation on page 11-4*
- *Web Reputation Policies on page 11-5*
- *Web Threat Notifications for Client Users on page 11-11*
- *Configuring C&C Callback Notifications for Administrators on page 11-13*
- *C&C Callback Outbreaks on page 11-16*
- *Web Reputation Logs on page 11-18*

About Web Threats

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, web threat creators constantly change the version or variant used. Because the web threat is in a fixed location of a website rather than on an infected computer, the web threat creator constantly modifies its code to avoid detection.

In recent years, individuals once characterized as hackers, virus writers, spammers, and spyware makers have become known as cyber criminals. Web threats help these individuals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is leakage of confidential information in the form of identity loss. The infected computer may also become a vector to deliver phish attacks or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in web commerce, corrupting the trust needed for Internet transactions. The second goal is to hijack a user's CPU power to use it as an instrument to conduct profitable activities. Activities include sending spam or conducting extortion in the form of distributed denial-of-service attacks or pay-per-click activities.

Command & Control Contact Alert Services

Trend Micro Command & Control (C&C) Contact Alert Services provides enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks. C&C Contact Alert Services integrate with Web Reputation Services which determines the action taken on detected callback addresses based on the web reputation security level.

The C&C IP list further enhances C&C callback detections using the Network Content Inspection Engine to identify C&C contacts through any network channel.

For details on configuring the Web Reputation Services security level, see *Configuring a Web Reputation Policy on page 11-5*.

TABLE 11-1. C&C Contact Alert Services Features

FEATURE	DESCRIPTION
Global Intelligence list	Trend Micro Smart Protection Network compiles the Global Intelligence list from sources all over the world and tests and evaluates the risk level of each C&C callback address. Web Reputation Services uses the Global Intelligence list in conjunction with the reputation scores for malicious websites to provide enhanced security against advanced threats. The web reputation security level determines the action taken on malicious websites or C&C servers based on assigned risk levels.
Deep Discovery Advisor integration and the Virtual Analyzer list	Smart Protection Servers can integrate with Deep Discovery Advisor to obtain the Virtual Analyzer C&C server list. The Deep Discovery Advisor Virtual Analyzer evaluates potential risks in a secure environment and, through use of advanced heuristics and behavioral testing methods, assigns a risk level to the analyzed threats. The Virtual Analyzer populates the Virtual Analyzer list with any threat that attempts to connect to a possible C&C server. The Virtual Analyzer list is highly company-specific and provides a more customized defense against targeted attacks. Smart Protection Servers retrieve the list from Deep Discovery Advisor and can evaluate all possible C&C threats against both the Global Intelligence and the local Virtual Analyzer list. For details on connecting the integrated Smart Protection Server to Deep Discovery Advisor, see *Configuring Integrated Smart Protection Server Settings on page 4-20*.
C&C IP list	The C&C IP list works in conjunction with the Network Content Inspection Engine (NCIE) to detect network connections with known C&C servers. NCIE detects C&C server contact through any network channel. OfficeScan logs all connection information to servers in the C&C IP list for evaluation. For details on configuring the C&C IP list logs, see *Configuring Global C&C Callback Settings on page 11-11*.

FEATURE	DESCRIPTION
Administrator notifications	Administrators can choose to receive detailed and customizable notifications after detecting a C&C callback. For details, see *Configuring C&C Callback Notifications for Administrators on page 11-13*.
Endpoint notifications	Administrators can choose to send detailed and customizable notifications to end users after detecting a C&C callback on an endpoint. For details, see *Enabling Web Reputation and C&C Callback Notifications on page 11-11*.
Outbreak notifications	Administrators can customize outbreak notifications specific to C&C callback events and specify whether the outbreak occurs on a single endpoint or across the entire network. For details, see *C&C Callback Outbreaks on page 11-16*.
C&C callback logs	Logs provide detailed information regarding all C&C callback events. For details, see *Viewing C&C Callback Logs on page 11-19*.

Web Reputation

Web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. It will then continue to scan sites and block users from accessing infected ones.

OfficeScan clients send queries to smart protection sources to determine the reputation of websites that users are attempting to access. A website's reputation is correlated with the specific web reputation policy enforced on the computer. Depending on the policy in use, the OfficeScan client will either block or allow access to the website.

Note

For details about smart protection sources, see *Smart Protection Source List on page 4-23*.

Add websites that you consider safe or dangerous to the approved or blocked list. When an OfficeScan client detects access to any of these websites, it automatically allows or blocks the access and no longer sends a query to smart protection sources.

Web Reputation Policies

Web reputation policies dictate whether OfficeScan will block or allow access to a website.

You can configure policies for internal and external clients. OfficeScan administrators typically configure a stricter policy for external clients.

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

After you deploy the policies, clients use the location criteria you have set in the Computer Location screen (see *Computer Location on page 14-2*) to determine their location and the policy to apply. Clients switch policies each time the location changes.

Configuring a Web Reputation Policy

Before you begin

Specify proxy server authentication credentials if you have set up a proxy server to handle HTTP communication in your organization and authentication is required before web access is allowed.

For instructions on configuring the proxy settings, see *External Proxy for OfficeScan Clients on page 14-47*.

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. Select the targets in the client tree.

- To configure a policy for clients running Windows XP, Vista, 7, or 8, select the root domain icon ( ), specific domains, or clients.

Note

When you select the root domain or specific domains, the setting will only apply to clients running Windows XP, Vista, 7, or 8. The setting will not apply to clients running Windows Server 2003, Windows Server 2008, or Windows Server 2012 even if they part of the domains.

- To configure a policy for clients running Windows Server 2003, Windows Server 2008, or Windows Server 2012, select a specific client.

3. Click **Settings** > **Web Reputation Settings**.

4. Click the **External Clients** tab to configure a policy for external clients or the **Internal Clients** tab to configure a policy for internal clients.

Tip

Configure client location settings if you have not done so. Clients will use these settings to determine their location and apply the correct web reputation policy. For details, see *Computer Location on page 14-2*.

5. Select **Enable Web reputation policy on the following operating systems**. The operating systems listed in the screen depends on the targets you selected in step 1.

Tip

Trend Micro recommends disabling web reputation for internal clients if you already use a Trend Micro product with the web reputation capability, such as InterScan Web Security Virtual Appliance.

When a web reputation policy is enabled:

- External clients send web reputation queries to the Smart Protection Network.
- Internal clients send web reputation queries to:

- Smart Protection Servers if the **Send queries to Smart Protection Servers** option is enabled. For details about this option, see step 7.
- Smart Protection Network if the **Send queries to Smart Protection Servers** option is disabled.

6. Select **Enable assessment**.

Note

When in assessment mode, clients will allow access to all websites but will log access to websites that are supposed to be blocked if assessment was disabled. Trend Micro provides assessment mode to allow you to evaluate websites and then take appropriate action based on your evaluation. For example, websites that you consider safe can be added to the approved list.

7. Select **Check HTTPS URLs**.

HTTPS communication uses certificates to identify web servers. It encrypts data to prevent theft and eavesdropping. Although more secure, accessing websites using HTTPS still has risks. Compromised sites, even those with valid certificates, can host malware and steal personal information. In addition, certificates are relatively easy to obtain, making it easy to set up malicious web servers that use HTTPS.

Enable checking of HTTPS URLs to reduce exposure to compromised and malicious sites that use HTTPS. OfficeScan can monitor HTTPS traffic on the following browsers:

TABLE 11-2. Supported Browsers for HTTPS Traffic

BROWSER	VERSION
Microsoft Internet Explorer	• 6 with SP2 or higher • 7.x • 8.x • 9.x • 10.x
Mozilla Firefox	3.5 or later

Important

- HTTPS scanning only supports Windows 8 or Windows 2012 platforms operating in desktop mode.
- After enabling HTTPS scanning for the first time on OfficeScan clients running Internet Explorer 9 or 10, users must enable the `TmIEPlugInBHO Class` add-on in the browser pop-up window before HTTPS scanning is operational.

  For more information on configuring Internet Explorer settings for web reputation, see the following Knowledge Base articles:

  - http://esupport.trendmicro.com/solution/en-us/1060643.aspx
  - http://esupport.trendmicro.com/solution/en-us/1060644.aspx

8. Select **Scan common HTTP ports only** to restrict web reputation scanning to traffic through ports 80, 81, and 8080. By default, OfficeScan scans all traffic through all ports.

9. Select **Send queries to Smart Protection Servers** if you want internal clients to send web reputation queries to Smart Protection Servers.

   - If you enable this option:
     - Clients refer to the smart protection source list to determine the Smart Protection Servers to which they send queries. For details about the smart protection source list, see *Smart Protection Source List on page 4-23*.
     - Be sure that Smart Protection Servers are available. If all Smart Protection Servers are unavailable, clients do not send queries to Smart Protection Network. The only remaining sources of web reputation data for clients are the approved and blocked URL lists (configured in step 10).
     - If you want clients to connect to Smart Protection Servers through a proxy server, specify proxy settings in **Administration** > **Proxy Settings** > **Internal Proxy** tab.
     - Be sure to update Smart Protection Servers regularly so that protection remains current.

- Clients will not block untested websites. Smart Protection Servers do not store web reputation data for these websites.

- If you disable this option:
  - Clients send web reputation queries to Smart Protection Network. Client computers must have Internet connection to send queries successfully.
  - If connection to Smart Protection Network requires proxy server authentication, specify authentication credentials in **Administration** > **Proxy Settings** > **External Proxy (tab)** > **Client Connection with Trend Micro Servers**.
  - Clients will block untested websites if you select **Block pages that have not been tested by Trend Micro** in step 9.

10. Select from the available web reputation security levels: **High**, **Medium**, or **Low**

> **Note**
>
> The security levels determine whether OfficeScan will allow or block access to a URL. For example, if you set the security level to Low, OfficeScan only blocks URLs that are known to be web threats. As you set the security level higher, the web threat detection rate improves but the possibility of false positives also increases.

11. If you disabled the **Send queries to Smart Protection Servers** option in step 7, you can select **Block pages that have not been tested by Trend Micro**.

> **Note**
>
> While Trend Micro actively tests web pages for safety, users may encounter untested pages when visiting new or less popular websites. Blocking access to untested pages can improve safety but can also prevent access to safe pages.

12. Configure the approved and blocked lists.

> **Note**
>
> The approved list takes precedence over the blocked list. When a URL matches an entry in the approved list, clients always allows access to the URL, even if it is in the blocked list.

a. Select **Enable approved/blocked list**.

b. Type a URL.

You can add a wildcard character (*) anywhere on the URL.

For example:

- Typing `www.trendmicro.com/*` means that all pages in the Trend Micro website will be approved.
- Typing `*.trendmicro.com/*` means that all pages on any sub-domain of trendmicro.com will be approved.

You can type URLs containing IP addresses. If a URL contains an IPv6 address, enclose the address in parentheses.

c. Click **Add to Approved List** or **Add to Blocked List**.

d. To export the list to a `.dat` file, click **Export** and then click **Save**.

e. If you have exported a list from another server and want to import it to this screen, click **Import** and locate the `.dat` file. The list loads on the screen.

13. To submit web reputation feedback, click the URL provided under **Reassess URL**. The Trend Micro Web Reputation Query system opens in a browser window.

14. Select whether to allow the OfficeScan client to send web reputation logs to the server. Allow clients to send logs if you want to analyze URLs being blocked by OfficeScan and take the appropriate action on URLs you think are safe to access.

15. If you selected domain(s) or client(s) in the clients tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Configuring Global C&C Callback Settings

Administrators can configure OfficeScan to log all connections between clients and confirmed C&C IP addresses.

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Go to the **C&C Contact Alert Settings** section.
3. Enable the **Log network connections between agents and Trend Micro confirmed C&C IP addresses** option.
4. Select to log connections from all endpoints, or only endpoints running specific operating systems.
5. Click **Save**.

Web Threat Notifications for Client Users

OfficeScan can display a notification message on an OfficeScan client computer immediately after it blocks a URL that violates a web reputation policy. You need to enable the notification message and optionally modify the content of the notification message.

Enabling Web Reputation and C&C Callback Notifications

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.

4. Click the **Other Settings** tab.
5. In the **Web Reputation Settings** section, select **Display a notification when a web site is blocked**.
6. In the **C&C Callback Settings** section, select **Display a notification when a C&C callback is detected**.
7. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Modifying the Web Threat Notifications

Procedure

1. Navigate to **Notifications** > **Client User Notifications**.
2. From the **Type** drop-down, select the type of web threat notification to modify:
   - **Web Reputation Violations**
   - **C&C Callbacks**
3. Modify the default message in the text box provided.
4. Click **Save**.

Configuring C&C Callback Notifications for Administrators

OfficeScan comes with a set of default notification messages that inform you and other OfficeScan administrators of C&C callback detections. You can modify the notifications and configure additional notification settings to suit your requirements.

Procedure

1. Navigate to **Notifications** > **Administrator Notifications** > **Standard Notifications**.
2. On the **Criteria** tab:
   a. Go to the **C&C Callbacks** section.
   b. Specify whether to send notifications when OfficeScan detects a C&C callback (the action can be blocked or logged) or only when the risk level of the callback address is High.
3. On the **Email** tab:
   a. Go to the **C&C Callbacks** section.
   b. Select **Enable notification via email**.
   c. Select **Send notifications to users with client tree domain permissions**.

      Use Role-based Administration to grant client tree domain permissions to users. If transmission occurs on a client belonging to a specific domain, the email are sent to the email addresses of the users with domain permissions. See the following table for examples:

TABLE 11-3. Client Tree Domains and Permissions

CLIENT TREE DOMAIN	ROLES WITH DOMAIN PERMISSIONS	USER ACCOUNT WITH THE ROLE	EMAIL ADDRESS FOR THE USER ACCOUNT
Domain A	Administrator (built-in)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domain B	Administrator (built-in)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

If an OfficeScan client belonging to Domain A detects a C&C callback, the email will be sent to mary@xyz.com, john@xyz.com, and chris@xyz.com.

If a client belonging to Domain B detects the C&C callback, the email is sent to mary@xyz.com and jane@xyz.com.

Note

When enabling this option, all users with domain permissions must have a corresponding email address. The email notification will not be sent to users without an email address. Users and email addresses are configured from **Administration** > **User Accounts**.

d. Select **Send notifications to the following email address(es)** and then type the email addresses.

e. Accept or modify the default subject and message. Use token variables to represent data in the **Subject** and **Message** fields.

TABLE 11-4. Token Variables for C&C Callback Notifications

VARIABLE	DESCRIPTION
%CLIENTCOMPUTER%	Target computer that sent the callback

VARIABLE	DESCRIPTION
%IP%	IP address of the targeted computer
%DOMAIN%	Domain of the computer
%DATETIME%	Date and time the transmission was detected
%CALLBACKADDRESS%	Callback address of the C&C server
%CNCRISKLEVEL%	Risk level of the C&C server
%CNCLISTSOURCE%	Indicates the C&C source list
%ACTION%	Action taken

4. On the **SNMP Trap** tab:
   a. Go to the **C&C Callbacks** section.
   b. Select **Enable notification via SNMP trap**.
   c. Accept or modify the default message. Use token variables to represent data in the **Message** field. See *Table 11-4: Token Variables for C&C Callback Notifications on page 11-14* for details.
5. On the **NT Event Log** tab:
   a. Go to the **C&C Callbacks** section.
   b. Select **Enable notification via NT Event Log**.
   c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 11-4: Token Variables for C&C Callback Notifications on page 11-14* for details.
6. Click **Save**.

C&C Contact Alert Notifications for Client Users

OfficeScan can display a notification message on OfficeScan client computers immediately after blocking a C&C server URL. You need to enable the notification message and optionally modify the content of the notification message

C&C Callback Outbreaks

Define a C&C callback outbreak by the number, source, and risk level of the callbacks.

OfficeScan comes with a default notification message that inform you and other OfficeScan administrators of an outbreak. You can modify the notification message to suit your requirements.

Note

OfficeScan can send C&C callback outbreak notifications through email. Configure email settings to allow OfficeScan to send emails successfully. For details, see *Administrator Notification Settings on page 13-29*.

Configuring the C&C Callback Outbreak Criteria and Notifications

Procedure

1. Navigate to **Notifications** > **Administrator Notifications** > **Outbreak Notifications**.
2. On the **Criteria** tab, configure the following options:

Option	Description
Same compromised host	Select to define an outbreak based on the callback detections per endpoint

Option	Description
C&C list source	Specify whether to include all C&C source lists, only the Global Intelligence list, or only the Virtual Analyzer list
C&C risk level	Specify whether to trigger an outbreak on all C&C callbacks or only high risk sources
Action	Select from **Any action**, **Logged**, or **Blocked**
Detections	Indicate the required number of detections that defines an outbreak
Time Period	Indicate the number of hours that the number of detections must occur within

Tip

Trend Micro recommends accepting the default values in this screen.

3. In the **Email** tab:

   a. Go to the **C&C Callbacks** section.

   b. Select **Enable notification via email**.

   c. Specify the email recipients.

   d. Accept or modify the default email subject and message. You can use token variables to represent data in the **Subject** and **Message** fields.

   Table 11-5. Token Variables for C&C Callbacks Outbreak Notifications

Variable	Description
%C	Number of C&C callback logs
%T	Time period when the C&C callback logs accumulated

   e. Select from the available additional C&C callback information to include in the email.

4. In the **SNMP Trap** tab:

   a. Go to the **C&C Callbacks** section.

b. Select **Enable notification via SNMP trap**.

c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 11-5: Token Variables for C&C Callbacks Outbreak Notifications on page 11-17* for details.

5. In the **NT Event Log** tab:

a. Go to the **C&C Callbacks** section.

b. Select **Enable notification via NT Event Log**.

c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 11-5: Token Variables for C&C Callbacks Outbreak Notifications on page 11-17* for details.

6. Click **Save**.

Web Reputation Logs

Configure both internal and external clients to send web reputation logs to the server. Do this if you want to analyze URLs that OfficeScan blocks and take appropriate action on URLs you think are safe to access.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing Web Reputation Logs

Procedure

1. Navigate to **Logs** > **Networked Computer Logs** > **Security Risks** or **Networked Computers** > **Client Management**.

2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.

3. Click **View Logs** > **Web Reputation Logs** or **Logs** > **Web Reputation Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date/Time OfficeScan blocked the URL
   - Computer where the user accessed the URL
   - Computer domain where the user accessed the URL
   - Blocked URL
   - URL's risk level
6. If there are URLs that should not be blocked, click the **Add to Approved List** button to add the website to the Approved URL list.
7. To save logs to a comma-separated value (`CSV`) file, click **Export to CSV**. Open the file or save it to a specific location.

Viewing C&C Callback Logs

Procedure

1. Navigate to **Logs** > **Networked Computer Logs** > **Security Risks** or **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **View Logs** > **C&C Callback Logs** or **Logs** > **C&C Callback Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date/Time OfficeScan logged the callback
   - Compromised host from which the callback originated

- IP address of the compromised host
- Domain from which the callback originated
- Callback address to which the endpoint sent the callback
- C&C list source that identified the C&C server
- C&C server's risk level
- Action taken on the callback

6. If there are URLs that should not be blocked, click the **Add to Web Reputation Approved List** button to add the website to the Web Reputation Approved URL list.

Note

OfficeScan always passes C&C servers detected by the C&C IP list and administrators cannot add these IP addresses to the Approved lists directly from the log table.

7. To save logs to a comma-separated value (`CSV`) file, click **Export to CSV**. Open the file or save it to a specific location.

Chapter 12

Using the OfficeScan Firewall

This chapter describes the OfficeScan Firewall features and configurations.

Topics in this chapter:

- *About the OfficeScan Firewall on page 12-2*
- *Enabling or Disabling the OfficeScan Firewall on page 12-6*
- *Firewall Policies and Profiles on page 12-7*
- *Firewall Privileges on page 12-22*
- *Global Firewall Settings on page 12-24*
- *Firewall Violation Notifications for OfficeScan Client Users on page 12-26*
- *Firewall Logs on page 12-27*
- *Firewall Violation Outbreaks on page 12-29*
- *Testing the OfficeScan Firewall on page 12-30*

About the OfficeScan Firewall

The OfficeScan firewall protects clients and servers on the network using stateful inspection and high performance network virus scanning. Through the central management console, you can create rules to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.

Note

You can enable, configure, and use the OfficeScan firewall on Windows XP computers that also have Windows Firewall enabled. However, manage policies carefully to avoid creating conflicting firewall policies and producing unexpected results. See the Microsoft documentation for details on Windows Firewall.

The OfficeScan firewall includes the following key features and benefits:

- *Traffic Filtering on page 12-2*
- *Application Filtering on page 12-3*
- *Certified Safe Software List on page 12-3*
- *Scanning for Network Viruses on page 12-3*
- *Customizable Profiles and Policies on page 12-4*
- *Stateful Inspection on page 12-4*
- *Intrusion Detection System on page 12-4*
- *Firewall Violation Outbreak Monitor on page 12-5*
- *OfficeScan Client Firewall Privileges on page 12-5*

Traffic Filtering

The OfficeScan firewall filters all incoming and outgoing traffic, providing the ability to block certain types of traffic based on the following criteria:

- Direction (inbound/outbound)

- Protocol (TCP/UDP/ICMP/ICMPv6)
- Destination ports
- Source and destination computers

Application Filtering

The OfficeScan firewall filters incoming and outgoing traffic for specific applications, allowing these applications to access the network. However, network connections will depend on the policies set by the administrator.

Note

OfficeScan does not support specific application exceptions on Windows 8 and Windows Server 2012 platforms. OfficeScan allows or denies all application traffic on computers with these platforms.

Certified Safe Software List

The Certified Safe Software List provides a list of applications that can bypass firewall policy security levels. If the security level is set to Medium or High, OfficeScan will still allow applications to run and access the network.

Enable querying of the global Certified Safe Software List that provides a more complete list. This is a list dynamically updated by Trend Micro.

Note

This feature works with Behavior Monitoring. Ensure that you enable the Unauthorized Change Prevention Service and Certified Safe Software Service, before enabling the global Certified Safe Software List.

Scanning for Network Viruses

The OfficeScan firewall also examines each packet for network viruses. For details, see *Viruses and Malware on page 7-2*.

Customizable Profiles and Policies

The OfficeScan firewall gives you the ability to configure policies to block or allow specified types of network traffic. Assign a policy to one or more profiles, which you can then deploy to specified OfficeScan clients. This provides a highly customized method of organizing and configuring firewall settings for clients.

Stateful Inspection

The OfficeScan firewall is a stateful inspection firewall; it monitors all connections to the OfficeScan client and remembers all connection states. It can identify specific conditions in any connection, predict what actions should follow, and detect disruptions in a normal connection. Therefore, effective use of the firewall not only involves creating profiles and policies, but also analyzing connections and filtering packets that pass through the firewall.

Intrusion Detection System

The OfficeScan firewall also includes an Intrusion Detection System (IDS). When enabled, IDS can help identify patterns in network packets that may indicate an attack on the OfficeScan client. The OfficeScan firewall can help prevent the following well-known intrusions:

- **Too Big Fragment**: A Denial of Service attack where a hacker directs an oversized TCP/UDP packet at a target computer. This can cause the computer's buffer to overflow, which can freeze or reboot the computer.
- **Ping of Death**: A Denial of Service attack where a hacker directs an oversized ICMP/ICMPv6 packet at a target computer. This can cause the computer's buffer to overflow, which can freeze or reboot the computer.
- **Conflicted ARP**: A type of attack where a hacker sends an Address Resolution Protocol (ARP) request with the same source and destination IP address to a computer. The target computer continually sends an ARP response (its MAC address) to itself, causing it to freeze or crash.
- **SYN Flood**: A Denial of Service attack where a program sends multiple TCP synchronization (SYN) packets to a computer, causing the computer to continually

send synchronization acknowledgment (SYN/ACK) responses. This can exhaust computer memory and eventually crash the computer.

- **Overlapping Fragment**: Similar to a Teardrop attack, this Denial of Service attack sends overlapping TCP fragments to a computer. This overwrites the header information in the first TCP fragment and may pass through a firewall. The firewall may then allow subsequent fragments with malicious code to pass through to the target computer.
- **Teardrop**: Similar to an overlapping fragment attack, this Denial of Service attack deals with IP fragments. A confusing offset value in the second or later IP fragment can cause the receiving computer's operating system to crash when attempting to reassemble the fragments.
- **Tiny Fragment Attack**: A type of attack where a small TCP fragment size forces the first TCP packet header information into the next fragment. This can cause routers that filter traffic to ignore the subsequent fragments, which may contain malicious data.
- **Fragmented IGMP**: A Denial of Service attack that sends fragmented IGMP packets to a target computer, which cannot properly process the IGMP packets. This can freeze or slow down the computer.
- **LAND Attack**: A type of attack that sends IP synchronization (SYN) packets with the same source and destination address to a computer, causing the computer to send the synchronization acknowledgment (SYN/ACK) response to itself. This can freeze or slow down the computer.

Firewall Violation Outbreak Monitor

The OfficeScan firewall sends a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack.

OfficeScan Client Firewall Privileges

Grant OfficeScan client users the privilege to view their firewall settings on the OfficeScan client console. Also grant users the privilege to enable or disable the firewall, the Intrusion Detection System, and the firewall violation notification message.

Enabling or Disabling the OfficeScan Firewall

During the OfficeScan server installation, you are prompted to enable or disable the OfficeScan firewall.

If you enabled the firewall during installation and noticed an impact on performance, especially on server platforms (Windows Server 2003, Windows Server 2008, and Windows Server 2012), consider disabling the firewall.

If you disabled the firewall during installation but now want to enable it to protect a client from intrusions, first read the guidelines and instructions in *OfficeScan Client Services on page 14-6*.

You can enable or disable the firewall on all or select OfficeScan client computers.

Enabling or Disabling the OfficeScan Firewall on Selected Computers

Method A: Create a new policy and apply it to OfficeScan clients.

Procedure

1. Create a new policy that enables/disables the firewall. For steps in creating a new policy, see *Adding or Modifying a Firewall Policy on page 12-10*.
2. Apply the policy to the OfficeScan clients.

Method B: Enable/Disable the firewall driver and service.

Procedure

1. Enable/Disable the firewall driver.
   a. Open **Windows Network Connection Properties**.

b. Select or clear the **Trend Micro Common Firewall Driver** check box from the network card.

2. Enable/Disable the firewall service.

   a. Open a command prompt and type `services.msc`.

   b. Start or stop **OfficeScan NT Firewall** from Microsoft Management Console (MMC).

Method C: Enable/Disable the firewall service from the web console

For the detailed steps, see *OfficeScan Client Services on page 14-6*.

Enabling or Disabling the OfficeScan Firewall on All Computers

Procedure

1. Navigate to **Administration** > **Product License**.
2. Go to the **Additional Services** section.
3. In the **Additional Services** section, beside the Firewall for networked computers row, click **Enable** or **Disable**.

Firewall Policies and Profiles

The OfficeScan firewall uses policies and profiles to organize and customize methods for protecting networked computers.

With Active Directory integration and role-based administration, each user role, depending on the permission, can create, configure, or delete policies and profiles for specific domains.

Tip

Multiple firewall installations on the same computer may produce unexpected results. Consider uninstalling other software-based firewall applications on OfficeScan clients before deploying and enabling the OfficeScan firewall.

The following steps are necessary to successfully use the OfficeScan firewall:

1. Create a policy. The policy allows you to select a security level that blocks or allows traffic on networked computers and enables firewall features.
2. Add exceptions to the policy. Exceptions allow OfficeScan clients to deviate from a policy. With exceptions, you can specify clients, and allow or block certain types of traffic, despite the security level setting in the policy. For example, block all traffic for a set of clients in a policy, but create an exception that allows HTTP traffic so clients can access a web server.
3. Create and assign profiles to OfficeScan clients. A firewall profile includes a set of client attributes and is associated with a policy. When a client matches the attributes specified in the profile, the associated policy is triggered.

Firewall Policies

Firewall policies allow you to block or allow certain types of network traffic not specified in a policy exception. A policy also defines which firewall features get enabled or disabled. Assign a policy to one or multiple firewall profiles.

OfficeScan comes with a set of default policies, which you can modify or delete.

With Active Directory integration and role-based administration, each user role, depending on the permission, can create, configure, or delete policies for specific domains.

The following table lists the default firewall policies.

TABLE 12-1. Default Firewall Policies

POLICY NAME	SECURITY LEVEL	CLIENT SETTINGS	EXCEPTIONS	RECOMMENDED USE
All access	Low	Enable firewall	None	Use to allow clients unrestricted access to the network
Cisco Trust Agent for Cisco NAC	Low	Enable firewall	Allow incoming and outgoing UDP traffic through port 21862	Use when clients have a Cisco Trust Agent (CTA) installation
Communication Ports for Trend Micro Control Manager	Low	Enable firewall	Allow all incoming and outgoing TCP/UDP traffic through ports 80 and 10319	Use when clients have an MCP agent installation
ScanMail for Microsoft Exchange console	Low	Enable firewall	Allow all incoming and outgoing TCP traffic through port 16372	Use when clients need to access the ScanMail console
InterScan Messaging Security Suite (IMSS) console	Low	Enable firewall	Allow all incoming and outgoing TCP traffic through port 80	Use when clients need to access the IMSS console

Also create new policies if you have requirements not covered by any of the default policies.

All default and user-created firewall policies display on the firewall policy list on the web console.

Configuring the Firewall Policy List

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Policies**.
2. To add a new policy, click **Add**.

If the new policy you want to create has similar settings with an existing policy, select the existing policy and click **Copy**. To edit an existing policy, click the policy name.

A policy configuration screen appears. See *Adding or Modifying a Firewall Policy on page 12-10* for more information.

3. To delete an existing policy, select the check box next to the policy and click **Delete**.

4. To edit the firewall exception template, click **Edit Exception Template**.

   See *Editing the Firewall Exception Template on page 12-13* for more information.

   The Exception Template Editor appears.

Adding or Modifying a Firewall Policy

Configure the following for each policy:

- **Security level**: A general setting that blocks or allows all inbound and/or all outbound traffic on the OfficeScan client computer
- **Firewall features**: Specify whether to enable or disable the OfficeScan firewall, the Intrusion Detection System (IDS), and the firewall violation notification message. See *Intrusion Detection System on page 12-4* for more information on IDS.
- **Certified Safe Software List**: Specify whether to allow certified safe applications to connect to the network. See *Certified Safe Software List on page 12-3* for more information on Certified Safe Software List.
- **Policy exception list**: A list of configurable exceptions that block or allow various types of network traffic

Adding a Firewall Policy

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Policies**.

2. To add a new policy, click **Add**.

   If a new policy you want to create has similar settings with an existing policy, select the existing policy and click **Copy**.

3. Type a name for the policy.

4. Select a security level.

   The selected security level will not apply to traffic that meet the firewall policy exception criteria.

5. Select the firewall features to use for the policy.

   - The firewall violation notification message displays when the firewall blocks an outgoing packet. To modify the message, see *Modifying the Content of the Firewall Notification Message on page 12-27*.

   - Enabling all the firewall features grants the OfficeScan client users the privileges to enable/disable the features and modify firewall settings in the OfficeScan client console.

     WARNING!

     You cannot use the OfficeScan server web console to override OfficeScan client console settings that the user configures.

   - If you do not enable the features, the firewall settings you configure from the OfficeScan server web console display under Network card list on the OfficeScan client console.

   - The information under **Settings** on the OfficeScan client console's **Firewall** tab always reflects the settings configured from the OfficeScan client console, not from the server web console.

6. Enable the local or global Certified Safe Software List.

   Note

   Ensure that the Unauthorized Change Prevention Service and Certified Safe Software Services have been enabled before enabling this service.

7. Under Exception, select the firewall policy exceptions. The policy exceptions included here are based on the firewall exception template. See *Editing the Firewall Exception Template on page 12-13* for details.

   - Modify an existing policy exception by clicking the policy exception name and changing the settings in the page that opens.

     Note

     The modified policy exception will only apply to the policy to be created. If you want the policy exception modification to be permanent, you will need to make the same modification to the policy exception in the firewall exception template.

   - Click **Add** to create a new policy exception. Specify the settings in the page that opens.

     Note

     The policy exception will also apply only to the policy to be created. To apply this policy exception to other policies, you need to add it first to the list of policy exceptions in the firewall exception template.

8. Click **Save**.

Modifying an Existing Firewall Policy

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Policies**.
2. Click a policy.
3. Modify the following:
   - Policy name
   - Security level
   - Firewall features to use for the policy

- Certified Safe Software Service List status
- Firewall policy exceptions to include in the policy
  - Edit an existing policy exception (click the policy exception name and change settings in the page that opens)
  - Click **Add** to create a new policy exception. Specify the settings in the page that opens.

4. Click **Save** to apply the modifications to the existing policy.

Editing the Firewall Exception Template

The firewall exception template contains policy exceptions that you can configure to allow or block different kinds of network traffic based on the OfficeScan client computer's port number(s) and IP address(es). After creating a policy exception, edit the policies to which the policy exception applies.

Decide which type of policy exception you want to use. There are two types:

- **Restrictive**

  Blocks only specified types of network traffic and applies to policies that allow all network traffic. An example use of a restrictive policy exception is to block OfficeScan client ports vulnerable to attack, such as ports that Trojans often use.

- **Permissive**

  Allows only specified types of network traffic and applies to policies that block all network traffic. For example, you may want to permit OfficeScan clients to access only the OfficeScan server and a web server. To do this, allow traffic from the trusted port (the port used to communicate with the OfficeScan server) and the port the OfficeScan client uses for HTTP communication.

  OfficeScan client listening port: **Networked Computers** > **Client Management** > **Status**. The port number is under **Basic Information**.

  Server listening port: **Administration** > **Connection Settings**. The port number is under **Connection Settings for Networked Computers**.

OfficeScan comes with a set of default firewall policy exceptions, which you can modify or delete.

TABLE 12-2. Default Firewall Policy Exceptions

EXCEPTION NAME	ACTION	PROTOCOL	PORT	DIRECTION
DNS	Allow	TCP/UDP	53	Incoming and outgoing
NetBIOS	Allow	TCP/UDP	137, 138, 139, 445	Incoming and outgoing
HTTPS	Allow	TCP	443	Incoming and outgoing
HTTP	Allow	TCP	80	Incoming and outgoing
Telnet	Allow	TCP	23	Incoming and outgoing
SMTP	Allow	TCP	25	Incoming and outgoing
FTP	Allow	TCP	21	Incoming and outgoing
POP3	Allow	TCP	110	Incoming and outgoing
LDAP	Allow	TCP/UDP	389	Incoming and outgoing

Note

Default exceptions apply to all clients. If you want a default exception to apply only to certain clients, edit the exception and specify the IP addresses of the clients.

The LDAP exception is not available if you upgrade from a previous OfficeScan version. Manually add this exception if you do not see it on the exception list.

Adding a Firewall Policy Exception

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Policies**.
2. Click **Edit Exception Template**.
3. Click **Add**.

4. Type a name for the policy exception.
5. Select the type of application. You can select all applications, or specify application path or registry keys.

> **Note**
> Verify the name and full paths entered. Application exception does not support wildcards.

6. Select the action OfficeScan will perform on network traffic (block or allow traffic that meets the exception criteria) and the traffic direction (inbound or outbound network traffic on the OfficeScan client computer).
7. Select the type of network protocol: TCP, UDP, ICMP, or ICMPv6.
8. Specify ports on the OfficeScan client computer on which to perform the action.
9. Select OfficeScan client computer IP addresses to include in the exception. For example, if you chose to deny all network traffic (inbound and outbound) and type the IP address for a single computer on the network, then any OfficeScan client that has this exception in its policy will not be able to send or receive data to or from that IP address.
   - **All IP addresses**: Includes all IP addresses
   - **Single IP address**: Type an IPv4 or IPv6 address, or a host name.
   - **Range (for IPv4 or IPv6)**: Type an IPv4 or IPv6 address range.
   - **Range (for IPv6)**: Type an IPv6 address prefix and length.
   - **Subnet mask**: Type an IPv4 address and its subnet mask.
10. Click **Save**.

Modifying a Firewall Policy Exception

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Policies**.

2. Click **Edit Exception Template**.
3. Click a policy exception.
4. Modify the following:
   - Policy exception name
   - Application type, name, or path
   - Action OfficeScan will perform on network traffic and the traffic direction
   - Type of network protocol
   - Port numbers for the policy exception
   - OfficeScan client computer IP addresses
5. Click **Save**.

Saving the Policy Exception List Settings

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Policies**.
2. Click **Edit Exception Template**.
3. Click one of the following save options:
   - **Save Template Changes**: Saves the exception template with the current policy exceptions and settings. This option only applies the template to policies created in the future, not existing policies.
   - **Save and Apply to Existing Policies**: Saves the exception template with the current policy exceptions and settings. This option applies the template to existing and future policies.

Firewall Profiles

Firewall profiles provide flexibility by allowing you to choose the attributes that a client or group of clients must have before applying a policy. Create user roles that can create, configure, or delete profiles for specific domains.

Users using the built-in administrator account or users with full management permissions can also enable the **Overwrite client security level exception list** option to replace the OfficeScan client profile settings with the server settings.

Profiles include the following:

- **Associated policy**: Each profile uses a single policy
- **Client attributes**: OfficeScan clients with one or more of the following attributes apply the associated policy:
  - **IP address**: An OfficeScan client that has a specific IP address, an IP address that falls within a range of IP addresses, or an IP address belonging to a specified subnet
  - **Domain**: An OfficeScan client that belongs to a certain OfficeScan domain
  - **Computer**: An OfficeScan client with a specific computer name
  - **Platform**: An OfficeScan client running a specific platform
  - **Logon name**: OfficeScan client computers to which specified users have logged on
  - **NIC description**: An OfficeScan client computer with a matching NIC description
  - **Client connection status**: If an OfficeScan client is online or offline

    Note

    An OfficeScan client is online if it can connect to the OfficeScan server or any of the reference servers, and offline if it cannot connect to any server.

- User privileges: Allow or prevent OfficeScan client users from doing the following:
  - Changing the security level specified in a policy

- Editing the exception list associated with a policy

Note

These privileges apply only to clients that match the attributes specified in the profile. You can assign other firewall privileges to selected client users. See *Firewall Privileges on page 12-22* for details.

OfficeScan comes with a default profile named "All clients profile", which uses the "All access" policy. You can modify or delete this default profile. You can also create new profiles. All default and user-created firewall profiles, including the policy associated to each profile and the current profile status, display on the firewall profile list on the web console. Manage the profile list and deploy all profiles to OfficeScan clients. OfficeScan clients store all the firewall profiles on the client computer.

Configuring the Firewall Profile List

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Profiles**.
2. For users using the built-in administrator account or users with full management permissions, optionally enable the **Overwrite client security level exception list** option to replace the OfficeScan client profile settings with the server settings.
3. To add a new profile, click **Add**. To edit an existing profile, select the profile name.

   A profile configuration screen appears. See *Adding and Editing a Firewall Profile on page 12-20* more information.
4. To delete an existing policy, select the check box next to the policy and click **Delete**.
5. To change the order of profiles in the list, select the check box next to the profile to move, and then click **Move Up** or **Move Down**.

   OfficeScan applies firewall profiles to OfficeScan clients in the order in which the profiles appear in the profile list. For example, if a client matches the first profile, OfficeScan applies the actions configured for that profile to the client. OfficeScan ignores the other profiles configured for that client.

Tip

The more exclusive a policy, the better it is at the top of the list. For example, move a policy you create for a single client to the top, followed by those for a range of clients, a network domain, and all clients.

6. To manage reference servers, click **Edit Reference Server List**. Reference servers are computers that act as substitutes for the OfficeScan server when it applies firewall profiles. A reference server can be any computer on the network (see *Reference Servers on page 13-27* for more information). OfficeScan makes the following assumptions when you enable reference servers:

   - OfficeScan clients connected to reference servers are online, even if the clients cannot communicate with the OfficeScan server.
   - Firewall profiles applied to online OfficeScan clients also apply to OfficeScan clients connected to reference servers.

Note

Only users using the built-in administrator account or those with full management permissions can see and configure the reference server list.

7. To save the current settings and assign the profiles to OfficeScan clients:

   a. Select whether to **Overwrite client security level/exception list**. This option overwrites all user-configured firewall settings.

   b. Click **Assign Profile to Clients**. OfficeScan assigns all profiles on the profile list to all the OfficeScan clients.

8. To verify that you successfully assigned profiles to OfficeScan clients:

   a. Go to **Networked Computers** > **Client Management**. In the client tree view drop-down box, select **Firewall view**.

   b. Ensure that a green check mark exists under the **Firewall** column in the client tree. If the policy associated with the profile enables the Intrusion Detection System, a green check mark also exists under the **IDS** column.

c. Verify that the client applied the correct firewall policy. The policy appears under the **Firewall Policy** column in the client tree.

Adding and Editing a Firewall Profile

OfficeScan client computers may require different levels of protection. Firewall profiles allow you to specify the client computers to which an associated policy applies, and grant client users privileges to modify firewall settings. Generally, one profile is necessary for each policy in use.

Adding a Firewall Profile

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Profiles**.
2. Click **Add**.
3. Click **Enable this profile** to allow OfficeScan to deploy the profile to OfficeScan clients.
4. Type a name to identify the profile and an optional description.
5. Select a policy for this profile.
6. Specify the client computers to which OfficeScan applies the policy. Select computers based on the following criteria:
   - IP address
   - Domain: Click the button to open and select domains from the client tree.

     Note

     Only users with full domain permissions can select domains.
   - Computer name: Click the button to open, and select OfficeScan client computers from, the client tree.
   - Platform

- Logon name
- NIC description: Type a full or partial description, without wildcards.

> **Tip**
>
> Trend Micro recommends typing the NIC card manufacturer because NIC descriptions typically start with the manufacturer's name. For example, if you typed "Intel", all Intel-manufactured NICs will satisfy the criteria. If you typed a particular NIC model, such as "Intel(R) Pro/100", only NIC descriptions that start with "Intel(R) Pro/100" will satisfy the criteria.

- Client connection status

7. Select whether to grant users the privilege to change the firewall security level or edit a configurable list of exceptions to allow specified types of traffic.

   See *Adding or Modifying a Firewall Policy on page 12-10* for more information about these options.

8. Click **Save**.

Modifying a Firewall Profile

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Profiles**.
2. Click a profile.
3. Click **Enable this profile** to allow OfficeScan to deploy this profile to OfficeScan clients. Modify the following:
   - Profile name and description
   - Policy assigned to the profile
   - OfficeScan client computers, based on the following criteria:
     - IP address

- Domain: Click the button to open the client tree and select domains from there.
- Computer name: Click the button to open the client tree and select client computers from there.
- Platform
- Logon name
- NIC description: Type a full or partial description, without wildcards.

Tip

Trend Micro recommends typing the NIC card manufacturer because NIC descriptions typically start with the manufacturer's name. For example, if you typed "Intel", all Intel-manufactured NICs will satisfy the criteria. If you typed a particular NIC model, such as "Intel(R) Pro/100", only NIC descriptions that start with "Intel(R) Pro/100" will satisfy the criteria.

- Client connection status

- Privileges: Select whether to grant users the privilege to change the firewall security level or edit a configurable list of exceptions to allow specified types of traffic. See *Adding or Modifying a Firewall Policy on page 12-10* for more information about these options.

4. Click **Save**.

Firewall Privileges

Allow users to configure their own firewall settings. All user-configured settings cannot be overridden by settings deployed from the OfficeScan server. For example, if the user disables Intrusion Detection System (IDS) and you enable IDS on the OfficeScan server, IDS remains disabled on the OfficeScan client computer.

Enable the following settings to allow users to configure the firewall:

- **Display the Firewall tab on the client console**

The **Firewall** tab displays all firewall settings on the OfficeScan client and allows users with firewall privileges to configure their own settings.

- **Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message**

  The OfficeScan firewall protects clients and servers on the network using stateful inspection, high performance network virus scanning, and elimination. If you grant users the privilege to enable or disable the firewall and its features, warn them not to disable the firewall for an extended period of time to avoid exposing the computer to intrusions and hacker attacks.

  If you do not grant users the privileges, the firewall settings you configure from the OfficeScan server web console display under Network card list on the OfficeScan client console.

- **Allow clients to send firewall logs to the OfficeScan server**

  Select this option to analyze traffic the OfficeScan firewall blocks and allows. For details about firewall logs, see *Firewall Logs on page 12-27*.

  If you select this option, configure the log sending schedule in **Networked Computers** > **Global Client Settings**. Go to the **Firewall Settings** section. The schedule only applies to clients with the firewall log sending privilege. For instructions, see *Global Firewall Settings on page 12-24*.

Granting Firewall Privileges

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Firewall Privileges** section.
5. Select the following options:

- *Display the Firewall tab on the client console on page 12-22*
- *Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message on page 12-23*
- *Allow clients to send firewall logs to the OfficeScan server on page 12-23*

6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Global Firewall Settings

There are a number of ways global firewall settings get applied to OfficeScan clients.

- A particular firewall setting can apply to all clients that the server manages.
- A setting can apply only to OfficeScan clients with certain firewall privileges. For example, the firewall log sending schedule only applies to OfficeScan clients with the privilege to send logs to the server.

Enable the following global settings as required:

- **Send firewall logs to the server**

  You can grant certain OfficeScan clients the privilege to send firewall logs to the OfficeScan server. Configure the log sending schedule in this section. Only clients with the privilege to send firewall logs will use the schedule.

  See *Firewall Privileges on page 12-22* for information on firewall privileges available to selected clients.

- **Update the OfficeScan firewall driver only after a system reboot**

Enable the OfficeScan client to update the Common Firewall Driver only after the OfficeScan client computer restarts. Enable this option to avoid potential client computer disruptions (such as temporary disconnection from the network) when the Common Firewall Driver updates during client upgrade.

Note

This feature only supports clients upgraded from OfficeScan 8.0 SP1 and above.

- **Send firewall log information to the OfficeScan server hourly to determine the possibility of a firewall outbreak**

  When you enable this option, OfficeScan clients will send firewall log counts once every hour to the OfficeScan server. For details about firewall logs, see *Firewall Logs on page 12-27*.

  OfficeScan uses log counts and the firewall violation outbreak criteria to determine the possibility of a firewall violation outbreak. OfficeScan sends email notifications to OfficeScan administrators in the event of an outbreak.

Configuring Global Firewall Settings

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Go to the following sections and configure the settings:

TABLE 12-3. Global Firewall Settings

SECTION	SETTINGS
Firewall Settings	• *Send firewall logs to the server on page 12-24* • *Update the OfficeScan firewall driver only after a system reboot on page 12-24*
Firewall Log Count	*Send firewall log information to the OfficeScan server hourly to determine the possibility of a firewall outbreak on page 12-25*

3. Click **Save**.

Firewall Violation Notifications for OfficeScan Client Users

OfficeScan can display a notification message on a client computer immediately after the OfficeScan firewall blocks outbound traffic that violated firewall policies. Grant users the privilege to enable/disable the notification message.

Note

You can also enable the notification when you configure a particular firewall policy. To configure a firewall policy, see *Adding or Modifying a Firewall Policy on page 12-10*.

Granting Users the Privilege to Enable/Disable the Notification Message

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Firewall Privileges** section.
5. Select **Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message**.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Modifying the Content of the Firewall Notification Message

Procedure

1. Navigate to **Notifications** > **Client User Notifications**.
2. Click the **Firewall Violations** tab.
3. Modify the default messages in the text box provided.
4. Click **Save**.

Firewall Logs

Firewall logs available on the server are sent by OfficeScan clients with the privilege to send firewall logs. Grant specific clients this privilege to monitor and analyze traffic on the client computers that the OfficeScan firewall is blocking.

For information about firewall privileges, see *Firewall Privileges on page 12-22*.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing Firewall Logs

Procedure

1. Navigate to **Logs** > **Networked Computer Logs** > **Security Risks** or **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Logs** > **Firewall Logs** or **View Logs** > **Firewall Logs**.
4. To ensure that the most up-to-date logs are available to you, click **Notify Clients**. Allow some time for clients to send firewall logs before proceeding to the next step.
5. Specify the log criteria and then click **Display Logs**.
6. View logs. Logs contain the following information:
   - Date and time of the firewall violation detection
   - Computer where the firewall violation occurred
   - Computer domain where the firewall violation occurred
   - Remote host IP address
   - Local host IP address
   - Protocol
   - Port number
   - Direction: If inbound (Receive) or outbound (Send) traffic violated a firewall policy
   - Process: The executable program or service running on the computer that caused the firewall violation
   - Description: Specifies the actual security risk (such as a network virus or IDS attack) or the firewall policy violation

7. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Firewall Violation Outbreaks

Define a firewall violation outbreak by the number of firewall violations and the detection period.

OfficeScan comes with a default notification message that inform you and other OfficeScan administrators of an outbreak. You can modify the notification message to suit your requirements.

Note

OfficeScan can send firewall outbreak notifications through email. Configure email settings to allow OfficeScan to send emails successfully. For details, see *Administrator Notification Settings on page 13-29*.

Configuring the Firewall Violation Outbreak Criteria and Notifications

Procedure

1. Navigate to **Notifications** > **Administrator Notifications** > **Outbreak Notifications**.
2. In the **Criteria** tab:
   a. Go to the **Firewall Violations** section.
   b. Select **Monitor firewall violations on networked computers**.
   c. Specify the number of IDS logs, firewall logs, and network virus logs.
   d. Specify the detection period.

Tip

Trend Micro recommends accepting the default values in this screen.

OfficeScan sends a notification message when the number of logs is exceeded. For example, if you specify 100 IDS logs, 100 firewall logs, 100 network virus logs, and a time period of 3 hours, OfficeScan sends the notification when the server receives 301 logs within a 3-hour period.

3. In the **Email** tab:

   a. Go to the **Firewall Violation Outbreaks** section.

   b. Select **Enable notification via email**.

   c. Specify the email recipients.

   d. Accept or modify the default email subject and message. You can use token variables to represent data in the **Subject** and **Message** fields.

   TABLE 12-4. Token Variables for Firewall Violation Outbreak Notifications

VARIABLE	DESCRIPTION
%A	Log type exceeded
%C	Number of firewall violation logs
%T	Time period when firewall violation logs accumulated

4. Click **Save**.

Testing the OfficeScan Firewall

To ensure that the OfficeScan firewall works properly, perform a test on a OfficeScan client or group of OfficeScan clients.

WARNING!

Test OfficeScan client program settings in a controlled environment only. Do not perform tests on client computers connected to the network or to the Internet. Doing so may expose OfficeScan client computers to viruses, hacker attacks, and other risks.

Procedure

1. Create and save a test policy. Configure the settings to block the types of traffic you want to test. For example, to prevent the OfficeScan client from accessing the Internet, do the following:
   a. Set the security level to **Low** (allow all inbound/outbound traffic).
   b. Select **Enable firewall and Notify users when a firewall violation occurs**.
   c. Create an exception that blocks HTTP (or HTTPS) traffic.
2. Create and save a test profile, selecting the clients to which you will test firewall features. Associate the test policy with the test profile.
3. Click **Assign Profile to Clients**.
4. Verify the deployment.
   a. Click **Networked Computers** > **Client Management**.
   b. Select the domain to which a client belongs.
   c. Select **Firewall view** from the client tree view.
   d. Check if there is a green check mark under the **Firewall** column of the client tree. If you enabled the Intrusion Detection System for that client, check that a green check mark also exists under the **IDS** column.
   e. Verify that the client applied the correct firewall policy. The policy appears under the **Firewall Policy** column in the client tree.
5. Test the firewall on the client computer by attempting to send or receive the type of traffic you configured in the policy.
6. To test a policy configured to prevent the client from accessing the Internet, open a web browser on the client computer. If you configured OfficeScan to display a

notification message for firewall violations, the message displays on the client computer when an outbound traffic violation occurs.

Part III

Managing the OfficeScan Server and Clients

Chapter 13

Managing the OfficeScan Server

This chapter describes OfficeScan server management and configurations.

Topics in this chapter:

- *Role-based Administration on page 13-2*
- *Reference Servers on page 13-27*
- *Administrator Notification Settings on page 13-29*
- *System Event Logs on page 13-32*
- *Log Management on page 13-33*
- *OfficeScan Database Backup on page 13-39*
- *OfficeScan Web Server Information on page 13-41*
- *Web Console Password on page 13-42*
- *Server Tuner on page 13-44*
- *Smart Feedback on page 13-47*

Role-based Administration

Use Role-based Administration to grant and control access to the OfficeScan web console. If there are several OfficeScan administrators in your organization, you can use this feature to assign specific web console privileges to the administrators and present them with only the tools and permissions necessary to perform specific tasks. You can also control access to the client tree by assigning them one or several domains to manage. In addition, you can grant non-administrators "view only" access to the web console.

Each user (administrator or non-administrator) is assigned a specific role. A role defines the level of access to the web console. Users log on to the web console using custom user accounts or Active Directory accounts.

Role-based administration involves the following tasks:

1. Define user roles. For details, see *User Roles on page 13-2*.
2. Configure user accounts and assign a particular role to each user account. For details, see *User Accounts on page 13-17*.

View web console activities for all users from the system event logs. The following activities are logged:

- Logging on to the console
- Password modification
- Logging off from the console
- Session timeout (user is automatically logged off)

User Roles

A user role determines the web console menu items accessible to a user. A role is assigned a permission for each menu item.

Assign permissions for the following:

- *Menu Item Permissions on page 13-3*

- *Menu Item Types on page 13-3*
- *Menu Items for Servers and Clients on page 13-4*
- *Menu Items for Managed Domains on page 13-7*
- *Client Management Menu Items on page 13-8*

Menu Item Permissions

Permissions determine the level of access to each menu item. The permission for a menu item can either be:

- **Configure**: Allows full access to a menu item. Users can configure all settings, perform all tasks, and view data in a menu item.
- **View**: Only allows users to view settings, tasks, and data in a menu item.
- **No Access**: Hides a menu item from view.

Menu Item Types

There are 3 types of menu items in OfficeScan.

TABLE 13-1. Menu Item Types

TYPE	SCOPE
Menu Items for Servers/Clients	• Server settings, tasks, and data • Global client settings, tasks, and data For a complete list of available menu items, see *Menu Items for Servers and Clients on page 13-4*.
Menu items for managed domains	Granular client settings, tasks, and data that are available outside the client tree For a complete list of available menu items, see *Menu Items for Managed Domains on page 13-7*.

Type	Scope
Client management menu items	Granular client settings, tasks, and data that are available in the client tree For a complete list of available menu items, see *Client Management Menu Items on page 13-8*.

Menu Items for Servers and Clients

The following table lists the menu items for servers/clients:

Table 13-2. Menu Items for Servers/Clients

Main Menu Item	Submenus
Scan Now for All Domains **Note** Only those using built-in administrator roles can access this feature.	None

Networked Computers	• Client Management
	• Client Grouping
	• Global Client Settings
	• Computer Location
	• Data Loss Prevention
	  • Data Identifiers
	  • Templates
	• Connection Verification
	• Outbreak Prevention

Main Menu Item	Submenus
Smart Protection	• Smart Protection Sources • Integrated Server • Smart Feedback

Updates	• Server
	  • Scheduled Update
	  • Manual Update
	  • Update Source
	• Networked Computers
	  • Automatic Update
	  • Update Source
	• Rollback

Logs	• Networked Computer Logs
	  • Security Risks
	  • Component Update
	• Server Update Logs
	• System Event Logs
	• Log Maintenance

Cisco NAC	• Policy Servers • Agent Management • Agent Deployment • Client Certificate

Notifications	• Administrator Notifications
	  • General Settings
	  • Outbreak Notifications
	• Client User Notifications

Main Menu Item	Submenus

Administration	• User Accounts
	• User Roles
	
	Note
	Only users using the built-in administrator account can access User Accounts and Roles.
	
	• Active Directory
	  • Active Directory Integration
	  • Scheduled Synchronization
	• Proxy Settings
	• Connection Settings
	• Inactive Clients
	• Quarantine Manager
	• Product License
	• Control Manager Settings
	• Web Console Settings
	• Database Backup

Tools	• Administrative Tools • Client Tools
Plug-in Manager **Note** Only users using the built-in administrator account can access this feature.	None

Menu Items for Managed Domains

The following table lists the menu items for managed domains:

TABLE 13-3. Menu Items for Managed Domains

MAIN MENU ITEM	SUBMENUS
Summary **Note** Any user can access this page, regardless of permission.	None

Security Compliance	• Compliance Assessment
	  • Compliance Report
	  • Scheduled Compliance Report
	• Outside Server Management

Networked Computers	• Firewall
	  • Policies
	  • Profiles
	• Client Installation
	  • Browser Based
	  • Remote

Updates	• Summary • Networked Computers • Manual Update

Logs	• Networked Computer Logs
	  • Connection Verification
	  • Spyware/Grayware Restore

Main Menu Item	Submenus
Notifications	• Administrator Notifications • Standard Notifications

Client Management Menu Items

The following table lists the client management menu items:

Table 13-4. Client Management Menu Items

Main Menu Item	Submenus
Status	None
Tasks	• Scan Now • Client Uninstallation • Spyware/Grayware Restore

Main Menu Item	Submenus

Settings	• Scan Settings
	  • Scan Methods
	  • Manual Scan Settings
	  • Real-time Scan Settings
	  • Scheduled Scan Settings
	  • Scan Now Settings
	• Web Reputation Settings
	• Behavior Monitoring Settings
	• Device Control Settings
	• DLP Settings
	• Update Agent Settings
	• Privileges and Other Settings
	• Additional Service Settings
	• Spyware/Grayware Approved List
	• Export Settings
	• Import Settings

Logs	• Virus/Malware Logs • Spyware/Grayware Logs • Firewall Logs • Web Reputation Logs • C&C Callback Logs • Behavior Monitoring Logs • Device Control Logs • DLP Logs • Delete Logs

Main Menu Item	Submenus
Manage Client Tree	• Add Domain • Rename Domain • Move Client • Sort Client • Remove Domain/Client
Export	None

Built-in User Roles

OfficeScan comes with a set of built-in user roles that you cannot modify or delete. The built-in roles are as follows:

Table 13-5. Built-in User Roles

Role Name	Description
Administrator	Delegate this role to other OfficeScan administrators or users with sufficient knowledge of OfficeScan. Users with this role have "Configure" permission to all menu items.

Guest User	Delegate this role to users who want to view the web console for reference purposes.
	• Users with this role have no access to the following menu items:
	  • Scan Now for All Domains
	  • Plug-in Manager
	  • **Administration** > **User Roles**
	  • **Administration** > **User Accounts**
	• Users have "View" permission to all other menu items.

Role Name	Description
Trend Power User	This role is only available if you upgrade from OfficeScan 10. This role inherits the permissions of the "Power User" role in OfficeScan 10. Users with this role have "Configure" permission to all client tree domains but will have no access to the new features in this release.

Custom Roles

You can create custom roles if none of the built-in roles meet your requirement.

Only users with the built-in administrator role and those using the root account created during OfficeScan installation can create custom user roles and assign these roles to user accounts.

Adding a Custom Role

Procedure

1. Navigate to **Administration** > **User Roles**.
2. Click **Add**. If the role you want to create has similar settings with an existing role, select the existing role and click **Copy**. A new screen appears.
3. Type a name for the role and optionally provide a description.
4. Define the client tree scope.
   a. Click **Define Client Tree Scope**. A new screen opens.
   b. Select the root domain icon, or one or several domains in the client tree.
   c. Click **Save**.

Note

You will not be able to save a custom role if you do not define the client tree scope.

Only the domains have been defined at this point. The level of access to the selected domains will be defined in step 6 and step 7.

5. Click the **Global Menu Items** tab.

6. Click **Menu Items for Servers/Clients** and specify the permission for each available menu item. For a list of available menu items, see *Menu Items for Servers and Clients on page 13-4*.

   The client tree scope you configured in step 3 determines the level of permission to the menu items and defines the targets for the permission. The client tree scope can either be the root domain (all clients) or specific client tree domains.

TABLE 13-6. Menu Items for Server/Clients and Client Tree Scope

CRITERIA	CLIENT TREE SCOPE	
	ROOT DOMAIN	SPECIFIC DOMAINS
Menu item permission	Configure, View, or No Access	View or No Access
Target	OfficeScan server and all clients For example, if you grant a role "Configure" permission to all menu items for servers/clients, the user can: • Manage server settings, tasks, and data • Deploy global client settings • Initiate global client tasks • Manage global client data	OfficeScan server and all clients For example, if you grant a role "Configure" permission to all menu items for servers/clients, the user can: • View server settings, tasks, and data • View global client settings, tasks, and data

- Some menu items are not available to custom roles. For example, Plug-in Manager, User Roles, and User Accounts are only available to users with the built-in administrator role.
- If you select the check box under **Configure**, the check box under **View** is automatically selected.

- If you do not select any check box, the permission is "No Access".

7. Click **Menu items for managed domains** and specify the permission for each available menu item. For a list of available menu items, see .

   The client tree scope you configured in step 3 determines the level of permission to the menu items and defines the targets for the permission. The client tree scope can either be the root domain (all clients) or specific client tree domains.

TABLE 13-7. Menu Items for Managed Domains and Client Tree Scope

CRITERIA	CLIENT TREE SCOPE	
	ROOT DOMAIN	SPECIFIC DOMAINS
Menu item permission	Configure, View, or No Access	Configure, View, or No Access
Target	All or specific clients Examples: • If a user deployed firewall policies, the policies will be deployed to all clients. • The user can initiate manual client update on all or specific clients. • A compliance report can include all or specific clients.	Clients in the selected domains Examples: • If a user deployed firewall policies, the policies will only be deployed to clients in the selected domains. • The user can initiate manual client update only on clients in the selected domains. • A compliance report only includes clients in the selected domains.

   - If you select the check box under **Configure**, the check box under **View** is automatically selected.
   - If you do not select any check box, the permission is "No Access".

8. Click the **Client Management Menu Items** tab and then specify the permission for each available menu item. For a list of available menu items, see .

The client tree scope you configured in step 3 determines the level of permission to the menu items and defines the targets for the permission. The client tree scope can either be the root domain (all clients) or specific client tree domains.

TABLE 13-8. Client Management Menu Items and Client Tree Scope

CRITERIA	CLIENT TREE SCOPE	
	ROOT DOMAIN	SPECIFIC DOMAINS
Menu item permission	Configure, View, or No Access	Configure, View, or No Access
Target	Root domain (all clients) or specific domains For example, you can grant a role "Configure" permission to the "Tasks" menu item in the client tree. If the target is the root domain, the user can initiate the tasks on all clients. If the targets are Domains A and B, the tasks can only be initiated on clients in Domains A and B.	Only the selected domains For example, you can grant a role "Configure" permission to the "Settings" menu item in the client tree. This means that the user can deploy the settings but only to the clients in the selected domains.
	The client tree will only display if the permission to the "Client Management" menu item in "Menu Items for Servers/Clients" is "View".	

- If you select the check box under **Configure**, the check box under **View** is automatically selected.
- If you do not select any check box, the permission is "No Access".
- If you are configuring permissions for a specific domain, you can copy the permissions to other domains by clicking **Copy settings of the selected domain to other domains**.

9. Click **Save**. The new role displays on the User Roles list.

Modifying a Custom Role

Procedure

1. Navigate to **Administration** > **User Roles**.
2. Click the role name. A new screen appears.
3. Modify any of the following:
   - Description
   - Client tree scope
   - Role permissions
     - Menu items for servers/clients
     - Menu items for managed domains
     - Client management menu items
4. Click **Save**.

Deleting a Custom Role

Procedure

1. Navigate to **Administration** > **User Roles**.
2. Select the check box next to the role.
3. Click **Delete**.

Note

A role cannot be deleted if it is assigned to at least one user account.

Importing or Exporting Custom Roles

Procedure

1. Navigate to **Administration** > **User Roles**.
2. To export custom roles to a `.zip` file:
   a. Select the roles and click **Export**.
   b. Save the `.zip` file. If you are managing another OfficeScan server, use the `.zip` file to import custom roles to that server.

   Note
   Exporting roles can only be done between servers that have the same version.

3. To export custom roles to a `.csv` file:
   a. Select the roles and click **Export Role Settings**.
   b. Save the `.csv` file. Use this file to check the information and permissions for the selected roles.
4. If you have saved custom roles from a different OfficeScan server and want to import those roles into the current OfficeScan server, click **Import** and locate the `.zip` file containing the custom roles.
   - A role on the User Roles screen will be overwritten if you import a role with the same name.
   - Importing roles can only be done between servers that have the same version.
   - A role imported from another OfficeScan server:
     - Retains the permissions for menu items for servers/clients and menu items for managed domains.
     - Applies the default permissions for client management menu items. On the other server, record the role's permissions for client management menu items and then re-apply them to the role that was imported.

User Accounts

Set up user accounts and assign a particular role to each user. The user role determines the web console menu items a user can view or configure.

During OfficeScan server installation, Setup automatically creates a built-in account called "root". Users who log on using the root account can access all menu items. You cannot delete the root account but you can modify account details, such as the password and full name or the account description. If you forget the root account password, contact your support provider for help in resetting the password.

Add custom accounts or Active Directory accounts. All user accounts display on the User Accounts list on the web console.

OfficeScan user accounts can be used to perform "single sign-on". Single sign-on allows users to access the OfficeScan web console from the Trend Micro Control Manager console. For details, see the procedure below.

Adding a Custom Account

Procedure

1. Navigate to **Administration** > **User Accounts**.
2. Click **Add**.
3. Select **Custom Account**.
4. Type the user name, full name, and password and then confirm the password.
5. Type an email address for the account.

   Note

   OfficeScan sends notifications to this email address. Notifications inform the recipient about security risk detections and digital asset transmissions. For details about notifications, see *Security Risk Notifications for Administrators on page 7-74* and *Data Loss Prevention Notifications for Administrators on page 10-46*.

6. Select a role for the account.

7. Click **Save**.
8. Send the account details to the user.

Modifying a Custom Account

Procedure

1. Navigate to **Administration** > **User Accounts**.
2. Click the user account.
3. Enable or disable the account using the check box provided.
4. Modify the following:
   - Full name
   - Password
   - Email address
   - Role
5. Click **Save**.
6. Send the new account details to the user.

Adding an Active Directory Account or Group

Procedure

1. Navigate to **Administration** > **User Accounts**.
2. Click **Add**.
3. Select **Active Directory User or group**.
4. Specify the account name (user name or group) and the domain to which the account belongs.

Include the complete account and domain names. OfficeScan will not return a result for incomplete account and domain names or if the default group "Domain Users" is used.

All members belonging to a group get the same role. If a particular account belongs to at least two groups and the role for both groups are different:

- The permissions for both roles are merged. If a user configures a particular setting and there is a conflict between permissions for the setting, the higher permission applies.
- All user roles display in the System Event logs. For example, "User John Doe logged on with the following roles: Administrator, Guest User".

5. Select a role for the account.
6. Click **Save**.
7. Inform the user to log on to the web console using his or her domain account and password.

Adding Several Active Directory Accounts or Groups

Procedure

1. Navigate to **Administration** > **User Accounts**.
2. Click **Add from Active Directory**.
3. Search for an account (user name or group) by specifying the user name and domain to which the account belongs.

Note

Use the character (*) to search for multiple accounts. If you do not specify the wildcard character, include the complete account name. OfficeScan will not return a result for incomplete account names or if the default group "Domain Users" is used.

4. When OfficeScan finds a valid account, it displays the account name under **User and Groups**. Click the forward icon (>) to move the account under **Selected Users and Groups**.

   If you specify an Active Directory group, all members belonging to a group get the same role. If a particular account belongs to at least two groups and the role for both groups are different:

   - The permissions for both roles are merged. If a user configures a particular setting and there is a conflict between permissions for the setting, the higher permission applies.
   - All user roles display in the System Event logs. For example, "User John Doe logged on with the following roles: Administrator, Power User".

5. Add more accounts or groups.
6. Select a role for the accounts or groups.
7. Click **Save**.
8. Inform users to log on to the web console using their domain names and passwords.

Changing a Custom or Active Directory Account's Role

Procedure

1. Navigate to **Administration** > **User Accounts**.
2. Select one or several custom or Active Directory accounts.
3. Click **Change Role**.
4. On the screen that displays, select the new role and click **Save**.

Enabling or Disabling a Custom or Active Directory Account

Procedure

1. Navigate to **Administration** > **User Accounts**.
2. Click the icon under **Enable**.

Note

The root account cannot be disabled.

Using OfficeScan User Accounts in Control Manager

Refer to the Control Manager documentation for the detailed steps.

Procedure

1. Create a new user account in Control Manager. When specifying the user name, type the account name that appears on the OfficeScan web console.
2. Assign the new account "access" and "configure" rights to the OfficeScan server.

Note

If a Control Manager user has "access" and "configure" rights to OfficeScan but does not have an OfficeScan account, the user cannot access OfficeScan. The user sees a message with a link that opens the OfficeScan web console's logon screen.

Trend Micro Control Manager

Trend Micro Control Manager™ is a central management console that 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 managed products and services throughout the network.

Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Control Manager allows both manual and pre-scheduled updates, and the configuration and administration of products as groups or as individuals for added flexibility.

Control Manager Integration in this OfficeScan Release

This OfficeScan release includes the following features and capabilities when managing OfficeScan servers from Control Manager:

- Create, manage, and deploy policies for OfficeScan Antivirus, Data Loss Prevention, and Device Control, and assign privileges directly to OfficeScan clients from the Control Manager console.

  The following table lists the policy configurations available in Control Manager 6.0.

TABLE 13-9. OfficeScan Policy Management Types in Control Manager

POLICY TYPE	FEATURES
OfficeScan Antivirus and Client Settings	• Additional Service Settings • Behavior Monitoring Settings • Device Control Settings • Manual Scan Settings • Privileges and Other Settings • Real-time Scan Settings • Spyware/Grayware Approved List • Scan Methods • Scan Now Settings • Scheduled Scan Settings • Update Agent Settings • Web Reputation Settings

Policy Type	Features
Data Protection	Data Loss Prevention Policy Settings **Note** Manage the Device Control permissions for Data Protection in the OfficeScan Client policies.

- Replicate the following settings from one OfficeScan server to another from the Control Manager console:
  - *Data Identifier Types on page 10-4*
  - *Data Loss Prevention Templates on page 10-18*

Note

If these settings are replicated to an OfficeScan server where the Data Protection license has not been activated, the settings will only take effect when the license is activated.

Supported Control Manager Versions

This OfficeScan version supports Control Manager 6.0, 5.5 SP1, 5.5, and 5.0.

Table 13-10. Supported Control Manager Versions

OfficeScan Server	Control Manager Version			
	6.0	5.5 SP1	5.5	5.0
Dual-stack	Yes	Yes	Yes	Yes
Pure IPv4	Yes	Yes	Yes	Yes
Pure IPv6	Yes	No	No	No

Note

IPv6 support for Control Manager starts in version 5.5 Service Pack 1.

For details on the IP addresses that the OfficeScan server and OfficeScan clients report to Control Manager, see *Screens That Display IP Addresses on page A-7*.

Apply the latest patches and critical hot fixes for these Control Manager versions to enable Control Manager to manage OfficeScan. To obtain the latest patches and hot fixes, contact your support provider or visit the Trend Micro Update Center at:

http://www.trendmicro.com/download

After installing OfficeScan, register it to Control Manager and then configure settings for OfficeScan on the Control Manager management console. See the *Control Manager documentation* for information on managing OfficeScan servers.

Registering OfficeScan to Control Manager

Procedure

1. Navigate to **Administration** > **Control Manager Settings**.
2. Specify the entity display name, which is the name of the OfficeScan server that will display in Control Manager.

   By default, entity display name includes the server computer's host name and this product's name (for example, Server01_OSCE).

   Note

   In Control Manager, OfficeScan servers and other products managed by Control Manager are referred to as "entities".

3. Specify the Control Manager server FQDN or IP address and the port number to use to connect to this server. Optionally connect with increased security using HTTPS.

   - For a dual-stack OfficeScan server, type the Control Manager FQDN or IP address (IPv4 or IPv6, if available).

- For a pure IPv4 OfficeScan server, type the Control Manager FQDN or IPv4 address.
- For a pure IPv6 OfficeScan server, type the Control Manager FQDN or IPv6 address.

Note

Only Control Manager 5.5 SP1 and later versions support IPv6.

4. If the IIS web server of Control Manager requires authentication, type the user name and password.
5. If you will use a proxy server to connect to the Control Manager server, specify the following proxy settings:
   - Proxy protocol
   - Server FQDN or IPv4/IPv6 address and port
   - Proxy server authentication user ID and password
6. Decide whether to use one-way communication or two-way communication port forwarding, and then specify the IPv4/IPv6 address and port.
7. To check whether OfficeScan can connect to the Control Manager server based on the settings you specified, click **Test Connection**.

   Click **Register** if connection was successfully established.
8. If you change any of the settings on this screen after registration, click **Update Settings** after changing the settings to notify the Control Manager server of the changes.
9. If you no longer want the Control Manager server to manage OfficeScan, click **Unregister**.

Checking the OfficeScan Status on the Control Manager Management Console

Procedure

1. Open the Control Manager management console.

   To open the Control Manager console, on any computer on the network, open a web browser and type the following:

   `https://<Control Manager server name>/Webapp/login.aspx`

   Where `<Control Manager server name>` is the IP address or host name of the Control Manager server

2. In Main Menu, click **Products**.

3. Check if the OfficeScan server icon displays.

The Policy Export Tool

The Trend Micro OfficeScan Server Policy Export Tool helps administrators export OfficeScan policy settings supported by Control Manager 6.0 or later. Administrators also require the Control Manager Import Tool in order to import policies. The Policy Export Tool supports OfficeScan 10.6 Service Pack 1 and later.

- Real-time Scan settings
- Scheduled Scan settings
- Manual Scan settings
- Scan Now settings
- Update Agent settings
- Web reputation settings
- Scan method
- Behavior Monitoring settings
- Device Control settings
- Data Loss Prevention settings
- Privileges and Other Settings
- Additional Service settings
- Spyware/Grayware approved list

Using the Policy Export Tool

Procedure

1. On the OfficeScan server computer, navigate to <*Server installation folder*> `\PCCSRV\Admin\Utility\PolicyExportTool`.
2. Double-click `PolicyExportTool.exe` to start the Policy Export Tool.

   A command line interface screen opens and the Policy Export Tool starts exporting settings. The tool creates two folders (`PolicyClient` and `PolicyDLP`) in the `PolicyExportTool` folder containing the exported settings.
3. Copy the two folders to the Control Manager installation folder.
4. Execute the Policy Import Tool on the Control Manager server.

   For details on the Policy Import Tool, see the *Policy Import Tool Readme*.

Note

The Policy Export Tool does not export customized data identifiers or customized DLP templates. For administrators needing to export customized data identifiers and DLP templates, perform a manual export from the OfficeScan console and then manually import the file using the Control Manager console.

Reference Servers

One of the ways the OfficeScan client determines which policy or profile to use is by checking its connection status with the OfficeScan server. If an internal OfficeScan client (or a client within the corporate network) cannot connect to the server, the client status becomes offline. The client then applies a policy or profile intended for external clients. Reference servers address this issue.

An OfficeScan client that loses connection with the OfficeScan server will try connecting to reference servers. If the client successfully establishes connection with a reference server, it applies the policy or profile for internal clients.

Policies and profiles managed by reference servers include:

- Firewall profiles
- Web reputation policies
- Data Protection policies
- Device Control policies

Take note of the following:

- Assign computers with server capabilities, such as a web server, SQL server, or FTP server, as reference servers. You can specify a maximum of 32 reference servers.
- OfficeScan clients connect to the first reference server on the reference server list. If connection cannot be established, the client tries connecting to the next server on the list.
- OfficeScan clients use reference servers when determining the antivirus (Behavior Monitoring, Device Control, firewall profiles, the web reputation policy) or Data Protection settings to use. Reference servers do not manage clients or deploy updates and client settings. The OfficeScan server performs these tasks.
- An OfficeScan client cannot send logs to reference servers or use them as update sources

Managing the Reference Server List

Procedure

1. Navigate to **Networked Computers** > **Firewall** > **Profiles** or **Networked Computers** > **Computer Location**.
2. Depending on the displayed screen, do the following:
   - If you are on the Firewall Profiles for Networked Computers screen, click **Edit Reference Server List**.
   - If you are on the Computer Location screen, click **reference server list**.

3. Select **Enable the Reference Server list**.
4. To add a computer to the list, click **Add**.
   a. Specify the computer's IPv4/IPv6 address, name, or fully qualified domain name (FQDN), such as:
      - `computer.networkname`
      - `12.10.10.10`
      - `mycomputer.domain.com`
   b. Type the port through which clients communicate with this computer. Specify any open contact port (such as ports 20, 23 or 80) on the reference server.

      Note

      To specify another port number for the same reference server, repeat steps 2a and 2b. The OfficeScan client uses the first port number on the list and, if connection is unsuccessful, uses the next port number.

   c. Click **Save**.
5. To edit the settings of a computer on the list, click the computer name. Modify the computer name or port, and then click **Save**.
6. To remove a computer from the list, select the computer name and then click **Delete**.
7. To enable the computers to act as reference servers, click **Assign to Clients**.

Administrator Notification Settings

Configure administrator notification settings to allow OfficeScan to successfully send notifications through email, pager, and SNMP Trap. OfficeScan can also send notifications through Windows NT event log but no settings are configured for this notification channel.

OfficeScan can send notifications to you and other OfficeScan administrators when the following are detected:

TABLE 13-11. Detections that Trigger Administrator Notifications

DETECTIONS	NOTIFICATION CHANNELS			
	EMAIL	PAGER	SNMP TRAP	WINDOWS NT EVENT LOGS
Viruses and malware	Yes	Yes	Yes	Yes
Spyware and grayware	Yes	Yes	Yes	Yes
Digital asset transmissions	Yes	Yes	Yes	Yes
C&C callbacks	Yes	No	Yes	Yes
Virus and malware outbreaks	Yes	Yes	Yes	Yes
Spyware and grayware outbreaks	Yes	Yes	Yes	Yes
Firewall violation outbreaks	Yes	No	No	No
Shared folder session outbreaks	Yes	No	No	No
C&C callbacks	Yes	No	Yes	Yes

Configuring Administrator Notification Settings

Procedure

1. Navigate to **Notifications** > **Administrator Notifications** > **General Settings**.
2. Configure email notification settings.
   a. Specify either an IPv4/IPv6 address or computer name in the **SMTP server** field.

b. Specify a port number between 1 and 65535.

c. Specify an email address.

If you want to enable ESMTP in the next step, specify a valid email address.

d. Optionally enable **ESMTP**.

e. Specify the user name and password for the email address you specified in the **From** field.

f. Choose a method for authenticating the client to the server:

- **Login**: Login is an older version of the mail user agent. The server and client both use BASE64 to authenticate the username and password.
- **Plain Text**: Plain Text is the easiest to use but can also be unsafe because the username and password are sent as one string and BASE64 encoded before being sent over the Internet.
- **CRAM-MD5**: CRAM-MD5 uses a combination of a challenge-response authentication mechanism and a cryptographic Message Digest 5 algorithm to exchange and authenticate information.

3. Configure pager notification settings.

a. For the **Pager number** field, the following characters are allowed:

- 0 to 9
- #
- *
- ,

b. Specify a COM port between 1 and 16.

4. Configure SNMP Trap notification settings.

a. Specify either an IPv4/IPv6 address or computer name in the **Server IP address** field.

b. Specify a community name that is difficult to guess.

5. Click **Save**.

System Event Logs

OfficeScan records events related to the server program, such as shutdown and startup. Use these logs to verify that the OfficeScan server and services work properly.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing System Event Logs

Procedure

1. Navigate to **Logs** > **System Event Logs**.
2. Under **Event Description**, check for logs that need further action. OfficeScan logs the following events:

TABLE 13-12. System Event Logs

LOG TYPE	EVENTS
OfficeScan Master Service and Database Server	• Master Service started • Master Service stopped successfully • Master Service stopped unsuccessfully
Outbreak Prevention	• Outbreak Prevention enabled • Outbreak Prevention disabled • Number of shared folder sessions in the last <number of minutes>
Database backup	• Database backup successful • Database backup unsuccessful

Log Type	Events
Role-based web console access	• Logging on to the console • Password modification • Logging off from the console • Session timeout (user automatically gets logged off)

3. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Log Management

OfficeScan keeps comprehensive logs about security risk detections, events, and updates. Use these logs to assess your organization's protection policies and to identify OfficeScan clients at a higher risk of infection or attack. Also use these logs to check client-server connection and verify that component updates were successful.

OfficeScan also uses a central time verification mechanism to ensure time consistency between OfficeScan server and clients. This prevents log inconsistencies caused by time zones, Daylight Saving Time, and time differences, which can cause confusion during log analysis.

Note

OfficeScan performs time verification for all logs except for Server Update and System Event logs.

The OfficeScan server receives the following logs from OfficeScan clients:

- *Viewing Virus/Malware Logs on page 7-83*
- *Viewing Spyware/Grayware Logs on page 7-90*
- *Viewing Spyware/Grayware Restore Logs on page 7-92*
- *Viewing Firewall Logs on page 12-28*

- *Viewing Web Reputation Logs on page 11-18*
- *Viewing C&C Callback Logs on page 11-19*
- *Viewing Behavior Monitoring Logs on page 8-13*
- *Viewing Device Control Logs on page 9-17*
- *Viewing Data Loss Prevention Logs on page 10-50*
- *Viewing OfficeScan Client Update Logs on page 6-47*
- *Viewing Connection Verification Logs on page 14-41*

The OfficeScan server generates the following logs:

- *OfficeScan Server Update Logs on page 6-25*
- *System Event Logs on page 13-32*

The following logs are also available on the OfficeScan server and OfficeScan clients:

- *Windows Event Logs on page 18-22*
- *OfficeScan Server Logs on page 18-3*
- *OfficeScan Client Logs on page 18-15*

Log Maintenance

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule from the web console.

Deleting Logs Based on a Schedule

Procedure

1. Navigate to **Logs** > **Log Maintenance**.
2. Select **Enable scheduled deletion of logs**.

3. Select the log types to delete. All OfficeScan-generated logs, except debug logs, can be deleted based on a schedule. For debug logs, disable debug logging to stop collecting logs.

> **Note**
>
> For virus/malware logs, you can delete logs generated from certain scan types and Damage Cleanup Services. For spyware/grayware logs, you can delete logs from certain scan types. For details about scan types, see *Scan Types on page 7-13*.

4. Select whether to delete logs for all the selected log types or only logs older than a certain number of days.
5. Specify the log deletion frequency and time.
6. Click **Save**.

Manually Deleting Logs

Procedure

1. Navigate to **Logs** > **Networked Computer Logs** > **Security Risks**, or **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Perform one of the following steps:
   - If you are accessing the **Security Risk Logs for Networked Computers** screen, click **Delete Logs** or **View Logs** > **Delete Logs**.
   - If you are accessing the **Client Management** screen, click **Logs** > **Delete Logs**.
4. Select the log types to delete. Only the following logs can be deleted manually:
   - Virus/Malware logs
   - Spyware/Grayware logs
   - Firewall logs

- Web reputation logs
- C&C Callback logs
- Behavior Monitoring logs
- Device Control logs
- Data Loss Prevention logs

Note

For virus/malware logs, you can delete logs generated from certain scan types and Damage Cleanup Services. For spyware/grayware logs, you can delete logs from certain scan types. For details about scan types, see *Scan Types on page 7-13*.

5. Select whether to delete logs for all the selected log types or only logs older than a certain number of days.
6. Click **Delete**.

Licenses

View, activate, and renew OfficeScan license services on the web console, and enable/disable the OfficeScan firewall. The OfficeScan firewall is part of the Antivirus service, which also includes support for Cisco NAC and outbreak prevention.

Note

Some native OfficeScan features, such as Data Protection and Virtual Desktop Support, have their own licenses. The licenses for these features are activated and managed from Plug-in Manager. For details about licensing for these features, see *Data Protection License on page 3-4* and *Virtual Desktop Support License on page 14-72*.

A pure IPv6 OfficeScan server cannot connect to the Trend Micro Online Registration Server to activate/renew the license. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the OfficeScan server to connect to the registration server.

Log off and then log on again to the web console during the following instances:

- After activating a license for the following license services:
  - Antivirus
  - Web Reputation and Anti-spyware

Note

Re-logon is required to enable the full functionality of the service.

- After enabling or disabling the OfficeScan firewall. If you disable firewall, OfficeScan hides all firewall features on the server and client.

Viewing Product License Information

Procedure

1. Navigate to **Administration** > **Product License**.
2. View license status summary, which appears on top of the screen. Reminders about licenses display during the following instances:

TABLE 13-13. License Reminders

LICENSE TYPE	REMINDER
Full Version	During the product's grace period. The duration of the grace period varies by region. Please verify the grace period with your Trend Micro representative. When the license expires and grace period elapses. During this time, you will not be able to obtain technical support or perform component updates. The scan engines will still scan computers but will use out-of-date components. These out-of-date components may not be able to protect you completely from the latest security risks.

License Type	Reminder
Evaluation Version	When the license expires. During this time, OfficeScan disables component updates, scanning, and all client features.

3. View license information. The License Information section provides you the following information:
   - **Services**: Includes all the OfficeScan license services
   - **Status**: Displays either "Activated", "Not Activated" or "Expired". If a service has multiple licenses and at least one license is still active, the status that displays is "Activated".
   - **Version**: Displays either "Full" or "Evaluation" version. If you have both full and evaluation versions, the version that displays is "Full".
   - **Expiration Date**: If a service has multiple licenses, the latest expiration date displays. For example, if the license expiration dates are 12/31/2007 and 06/30/2008, 06/30/2008 displays.

   Note

   The version and expiration date of license services that have not been activated are "N/A".

4. OfficeScan allows you to activate multiple licenses for a license service. Click the service name to view all the licenses (both active and expired) for that service.

Activating or Renewing a License

Procedure

1. Navigate to **Administration** > **Product License**.
2. Click the name of the license service.
3. In the **Product License Details** screen that opens, click **New Activation Code**.
4. In the screen that opens, type the Activation Code and click **Save**.

Note

Register a service before activating it. Contact your Trend Micro representative for more information about the Registration Key and Activation Code.

5. Back in the **Product License Details** screen, click **Update Information** to refresh the screen with the new license details and the status of the service. This screen also provides a link to the Trend Micro website where you can view detailed information about your license.

OfficeScan Database Backup

The OfficeScan server database contains all OfficeScan settings, including scan settings and privileges. If the server database becomes corrupted, you can restore it if you have a backup. Back up the database manually at any time or configure a backup schedule.

When backing up the database, OfficeScan automatically helps defragment the database and repairs any possible corruption to the index file.

Check the system event logs to determine the backup status. For more information, see *System Event Logs on page 13-32*.

Tip

Trend Micro recommends configuring a schedule for automatic backup. Back up the database during non-peak hours when server traffic is low.

WARNING!

Do not perform the backup with any other tool or software. Configure database backup from the OfficeScan web console only.

Backing up the OfficeScan Database

Procedure

1. Navigate to **Administration** > **Database Backup**.
2. Type the location where you want to save the database. If the folder does not exist yet, select **Create the folder if not already present**. Include the drive and full directory path, such as `C:\OfficeScan\DatabaseBackup`.

   By default, OfficeScan saves the backup in the following directory: <*Server installation folder*>`\DBBackup`

   Note

   OfficeScan creates a subfolder under the backup path. The folder name indicates the time of the backup and is in the following format: YYYYMMDD_HHMMSS. OfficeScan preserves the 7 most recent backup folders, automatically deleting older folder(s).

3. If the backup path is on a remote computer (using a UNC path), type an appropriate account name and the corresponding password. Ensure that the account has write privileges on the computer.
4. To configure a backup schedule:
   a. Select **Enable scheduled database backup**.
   b. Specify the backup frequency and time.
   c. To back up the database and save the changes you made, click **Backup Now**. To save only without backing up the database, click **Save**.

Restoring the Database Backup Files

Procedure

1. Stop the OfficeScan Master Service.

2. Overwrite the database files in <*Server installation folder*>\PCCSRV\HTTPDB with the backup files.
3. Restart the OfficeScan Master Service.

OfficeScan Web Server Information

During OfficeScan server installation, Setup automatically sets up a web server (IIS or Apache web server) that enables networked computers to connect to the OfficeScan server. Configure the web server to which networked computer clients will connect.

If you modify the web server settings externally (for example, from the IIS management console), replicate the changes in OfficeScan. For example, if you change the IP address of the server for networked computers manually or if you assign a dynamic IP address to it, you need to reconfigure the server settings of OfficeScan.

WARNING!

Changing the connection settings may result in the permanent loss of connection between the server and clients and require the re-deployment of OfficeScan clients.

Configuring Connection Settings

Procedure

1. Navigate to **Administration** > **Connection Settings**.
2. Type the domain name or IPv4/IPv6 address and port number of the web server.

   Note

   The port number is the trusted port that the OfficeScan server uses to communicate with OfficeScan clients.

3. Click **Save**.

Web Console Password

The screen for managing the web console password (or the password for the root account created during OfficeScan server installation) will only be accessible if the server computer does not have the resources required to use role-based administration. For example, if the server computer runs Windows Server 2003 and Authorization Manager Runtime is not installed, the screen is accessible. If resources are adequate, this screen does not display and the password can be managed by modifying the root account in the **User Accounts** screen.

If OfficeScan is not registered to Control Manager, contact your support provider for instructions on how to gain access to the web console.

Web Console Settings

Use the **Web Console Settings** screen for the following:

- Configure the OfficeScan server to refresh the Summary dashboard periodically. By default, the server will refresh the dashboard every 30 seconds. The number of seconds can be from 10 to 300.
- Specify the web console timeout settings. By default, a user is automatically logged off from the web console after 30 minutes of inactivity. The number of minutes can be from 10 to 60.

Configuring Web Console Settings

Procedure

1. Navigate to **Administration** > **Web Console Settings**.
2. Select **Enable auto refresh** and then select the refresh interval.
3. Select **Enable automatic log out from the web console** and then select the timeout interval.

4. Click **Save**.

Quarantine Manager

Whenever the OfficeScan client detects a security risk and the scan action is quarantine, it encrypts the infected file and then moves it to the local quarantine folder located in <*Client installation folder*>`\SUSPECT`.

After moving the file to the local quarantine directory, the OfficeScan client sends it to the designated quarantine directory. Specify the directory in **Networked Computers** > **Client Management** > **Settings** > **{Scan Type} Settings** > **Action** tab. Files in the designated quarantine directory are encrypted to prevent them from infecting other files. See *Quarantine Directory on page 7-38* for more information.

If the designated quarantine directory is on the OfficeScan server computer, modify the server's quarantine directory settings from the web console. The server stores quarantined files in <*Server installation folder*>`\PCCSRV\Virus`.

Note

If the OfficeScan client is unable to send the encrypted file to the OfficeScan server for any reason, such as a network connection problem, the encrypted file remains in the OfficeScan client quarantine folder. The OfficeScan client will attempt to resend the file when it connects to the OfficeScan server.

Configuring Quarantine Directory Settings

Procedure

1. Navigate to **Administration** > **Quarantine Manager**.
2. Accept or modify the default capacity of the quarantine folder and the maximum size of an infected file that OfficeScan can store on the quarantine folder.

   The default values display on the screen.
3. Click **Save Quarantine Settings**.

4. To remove all existing files in the quarantine folder, click **Delete All Quarantined Files**.

Server Tuner

Use Server Tuner to optimize the performance of the OfficeScan server using parameters for the following server-related performance issues:

- **Download**

  When the number of OfficeScan clients (including update agents) requesting updates from the OfficeScan server exceeds the server's available resources, the server moves the client update request into a queue and processes the requests when resources become available. After a client successfully updates components from the OfficeScan server, it notifies the server that the update is complete. Set the maximum number of minutes the OfficeScan server waits to receive an update notification from the client. Also set the maximum number of times the server tries to notify the client to perform an update and to apply new configuration settings. The server keeps trying only if it does not receive client notification.

- **Buffer**

  When the OfficeScan server receives multiple requests from OfficeScan clients, such as a request to perform an update, the server handles as many requests as it can and puts the remaining requests in a buffer. The server then handles the requests saved in the buffer one at a time when resources become available. Specify the size of the buffer for events, such as client requests for updates, and for client log reporting.

- **Network Traffic**

  The amount of network traffic varies throughout the day. To control the flow of network traffic to the OfficeScan server and to other update sources, specify the number of OfficeScan clients that can simultaneously update at any given time of the day.

Server Tuner requires the following file: `SvrTune.exe`

Running Server Tuner

Procedure

1. On the OfficeScan server computer, navigate to <*Server installation folder*> `\PCCSRV\Admin\Utility\SvrTune`.

2. Double-click `SvrTune.exe` to start Server Tuner.

   The Server Tuner console opens.

3. Under **Download**, modify the following settings:

   - **Timeout for client**: Type the number of minutes for the OfficeScan server to wait to receive an update response from clients. If the client does not respond within this time, the OfficeScan server does not consider the client to have current components. When a notified client times out, a slot for another client awaiting notification becomes available.

   - **Timeout for update agent**: Type the number of minutes for the OfficeScan server to wait to receive an update response from an Update Agent. When a notified client times out, a slot for another client awaiting notification becomes available.

   - **Retry count**: Type the maximum number of times the OfficeScan server tries to notify a client to perform an update or to apply new configuration settings.

   - **Retry interval**: Type the number of minutes the OfficeScan server waits between notification attempts.

4. Under **Buffer**, modify the following settings:

   - **Event Buffer**: Type the maximum number of client event reports to the server (such as updating components) that OfficeScan holds in the buffer. The connection to the client breaks while the client request waits in the buffer. OfficeScan establishes a connection toa client when it processes the client report and removes it from the buffer.

   - **Log Buffer**: Type the maximum number of client log information reports to the server that OfficeScan holds in the buffer. The connection to the client breaks while the client request waits in the buffer. OfficeScan establishes a

connection to a client when it processes the client report and removes it from the buffer.

Note

If a large number of clients report to the server, increase the buffer size. A higher buffer size, however, means higher memory utilization on the server.

5. Under **Network Traffic**, modify the following settings:

   - **Normal hours**: Click the radio buttons that represent the hours of the day you consider network traffic to be normal.
   - **Off-peak hours**: Click the radio buttons that represent the hours of the day you consider network traffic to be at its lowest.
   - **Peak hours**: Click the radio buttons that represent the hours of the day you consider network traffic to be at its peak.
   - **Maximum client connections**: Type the maximum number of clients that can simultaneously update components from both "other update source" and from the OfficeScan server. Type a maximum number of clients for each of the time periods. When the maximum number of connections is reached, a client can update components only after a current client connection closes (due to either the completion of the update or the client response reaching the timeout value you specified in the **Timeout for client** or **Timeout for Update Agent** field).

6. Click **OK**. A prompt appears asking you to restart the OfficeScan Master Service.

Note

Only the service restarts, not the computer.

7. Select from the following restart options:

   - Click **Yes** to save the Server Tuner settings and restart the service. The settings take effect immediately after restart.

- Click **No** to save the Server Tuner settings but not restart the service. Restart the OfficeScan Master Service or restart the OfficeScan server computer for settings to take effect.

Smart Feedback

Trend Micro Smart Feedback shares anonymous threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. You can disable Smart Feedback anytime through this console.

Participating in the Smart Feedback Program

Procedure

1. Navigate to **Smart Protection** > **Smart Feedback**.
2. Click **Enable Trend Micro Smart Feedback**.
3. To help Trend Micro understand your organization, select the **Industry** type.
4. To send information about potential security threats in the files on your client computers, select the **Enable feedback of suspicious program files** check box.

   Note

   Files sent to Smart Feedback contain no user data and are submitted only for threat analysis.

5. To configure the criteria for sending feedback, select the number of detections for the specific amount of time that triggers the feedback.
6. Specify the maximum bandwidth OfficeScan can use when sending feedback to minimize network interruptions.
7. Click **Save**.

Chapter 14

Managing the OfficeScan Client

This chapter describes OfficeScan client management and configurations.

Topics in this chapter:

- *Computer Location on page 14-2*
- *OfficeScan Client Program Management on page 14-6*
- *Client-Server Connection on page 14-24*
- *OfficeScan Client Proxy Settings on page 14-46*
- *Viewing OfficeScan Client Information on page 14-50*
- *Importing and Exporting Client Settings on page 14-51*
- *Security Compliance on page 14-52*
- *Trend Micro Virtual Desktop Support on page 14-70*
- *Global Client Settings on page 14-83*
- *Configuring Client Privileges and Other Settings on page 14-84*

Computer Location

OfficeScan provides a location awareness feature that determines whether a OfficeScan client's location is internal or external. Location awareness is leveraged in the following OfficeScan features and services:

TABLE 14-1. Features and Services that Leverage Location Awareness

FEATURE/SERVICE	DESCRIPTION
Web Reputation Services	The OfficeScan client's location determines the web reputation policy that the OfficeScan client will apply. Administrators typically enforce a stricter policy for external clients. For details about web reputation policies, see *Web Reputation Policies on page 11-5*.
File Reputation Services	For clients that use smart scan, the OfficeScan client's location determine the smart protection source to which clients send scan queries. External clients send scan queries to Smart Protection Network while internal clients send the queries to the sources defined in the smart protection source list. For details about smart protection sources, see *Smart Protection Sources on page 4-5*.
Data Loss Prevention	A OfficeScan client's location determines the Data Loss Prevention policy that the client will apply. Administrators typically enforce a stricter policy for external clients. For details about Data Loss Prevention policies, see *Data Loss Prevention Policies on page 10-3*.
Device Control	A OfficeScan client's location determines the Device Control policy that the client will apply. Administrators typically enforce a stricter policy for external clients. For details about Device Control policies, see *Device Control on page 9-2*.

Location Criteria

Specify whether location is based on the OfficeScan client computer's gateway IP address or the OfficeScan client's connection status with the OfficeScan server or any reference server.

- **Gateway IP and MAC address**: If the OfficeScan client computer's gateway IP address matches any of the gateway IP addresses you specified on the Computer Location screen, the computer's location is internal. Otherwise, the computer's location is external.
- **Client connection status**: If the OfficeScan client can connect to the OfficeScan server or any of the assigned reference servers on the intranet, the computer's location is internal. Additionally, if a computer outside the corporate network can establish connection with the OfficeScan server/reference server, its location is also internal. If none of these conditions apply, the computer's location is external.

Configuring Location Settings

Procedure

1. Navigate to **Networked Computers** > **Computer Location**.
2. Choose whether location is based on **Client connection status** or **Gateway IP and MAC address**.
3. If you choose **Client connection status**, decide if you want to use a reference server.

   See *Reference Servers on page 13-27* for details.

   a. If you did not specify a reference server, the OfficeScan client checks the connection status with the OfficeScan server when the following events occur:

      - OfficeScan client switches from roaming to normal (online/offline) mode.
      - OfficeScan client switches from one scan method to another. See *Scan Methods on page 7-7* for details.

- OfficeScan client detects IP address change in the computer.
- OfficeScan client restarts.
- Server initiates connection verification. See *OfficeScan Client Icons on page 14-24* for details.
- Web reputation location criteria changes while applying global settings.
- Outbreak prevention policy is no longer enforced and pre-outbreak settings are restored.

b. If you specified a reference server, the OfficeScan client checks its connection status with the OfficeScan server first, and then with the reference server if connection to the OfficeScan server is unsuccessful. The OfficeScan client checks the connection status every hour and when any of the above events occur.

4. If you choose **Gateway IP and MAC address**:

   a. Type the gateway IPv4/IPv6 address in the text box provided.

   b. Type the MAC address.

   c. Click **Add**.

      If you do not type a MAC address, OfficeScan will include all the MAC addresses belonging to the specified IP address.

   d. Repeat step a to step c until you have all the gateway IP addresses you want to add.

   e. Use the Gateway Settings Importer tool to import a list of gateway settings.

      See *Gateway Settings Importer on page 14-4* for details.

5. Click **Save**.

Gateway Settings Importer

OfficeScan checks a computer's location to determine the web reputation policy to use and the smart protection source to which to connect. One of the ways OfficeScan

identifies the location is by checking the computer's gateway IP address and MAC address.

Configure the gateway settings on the **Computer Location** screen or use the Gateway Settings Importer tool to import a list of gateway settings to the **Computer Location** screen.

Using Gateway Settings Importer

Procedure

1. Prepare a text file (`.txt`) containing the list of gateway settings. On each line, type an IPv4 or IPv6 address and optionally type a MAC address.

   Separate IP addresses and MAC addresses by a comma. The maximum number of entries is 4096.

   For example:

   ```
   10.1.111.222,00:17:31:06:e6:e7
   ```

   ```
   2001:0db7:85a3:0000:0000:8a2e:0370:7334
   ```

   ```
   10.1.111.224,00:17:31:06:e6:e7
   ```

2. On the server computer, go to <*Server installation folder*>`\PCCSRV\Admin\Utility\GatewaySettingsImporter` and double-click `GSImporter.exe`.

   Note

   You cannot run the Gateway Settings Importer tool from Terminal Services.

3. On the **Gateway Settings Importer** screen, browse to the file created in step 1 and click **Import**.

4. Click **OK**.

   The gateway settings display on the **Computer Location** screen and the OfficeScan server deploys the settings to OfficeScan clients.

5. To delete all entries, click **Clear All**.

If you only need to delete a particular entry, remove it from the **Computer Location** screen.

6. To export the settings to a file, click **Export All** and then specify the file name and type.

OfficeScan Client Program Management

The following topics discuss ways to manage and protect the OfficeScan client program:

- *OfficeScan Client Services on page 14-6*
- *OfficeScan Client Service Restart on page 14-11*
- *Client Self-protection on page 14-12*
- *OfficeScan Client Security on page 14-16*
- *OfficeScan Client Console Access Restriction on page 14-17*
- *OfficeScan Client Unloading on page 14-18*
- *OfficeScan Client Roaming Privilege on page 14-19*
- *Client Mover on page 14-21*
- *Inactive OfficeScan Clients on page 14-23*

OfficeScan Client Services

The OfficeScan client runs the services listed in the following table. You can view the status of these services from Microsoft Management Console.

TABLE 14-2. OfficeScan client Services

SERVICE	FEATURES CONTROLLED
Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)	• Behavior Monitoring • Device Control • Certified Safe Software Service • OfficeScan client Self-protection **Note** OfficeScan client Self-protection prevents OfficeScan client services from being terminated when they are enabled and running.
OfficeScan NT Firewall (`TmPfw.exe`)	OfficeScan firewall
OfficeScan Data Protection Service (`dsagent.exe`)	• Data Loss Prevention • Device Control
OfficeScan NT Listener (`tmlisten.exe`)	Communication between the OfficeScan client and OfficeScan server
OfficeScan NT Proxy Service (`TmProxy.exe`)	• Web reputation • POP3 mail scan
OfficeScan NT RealTime Scan (`ntrtscan.exe`)	• Real-time Scan • Scheduled Scan • Manual Scan/Scan Now

The following services provide robust protection but their monitoring mechanisms can strain system resources, especially on servers running system-intensive applications:

- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
- OfficeScan NT Firewall (`TmPfw.exe`)
- OfficeScan Data Protection Service (`dsagent.exe`)

For this reason, these services are disabled by default on server platforms (Windows Server 2003, Windows Server 2008, and Windows Server 2012). If you want to enable these services:

- Monitor the system's performance constantly and take the necessary action when you notice a drop in performance.
- For `TMBMSRV.exe`, you can enable the service if you exempt system-intensive applications from Behavior Monitoring policies. You can use a performance tuning tool to identify system intensive applications. For details, see *Using the Trend Micro Performance Tuning Tool on page 14-9*.

For desktop platforms, disable the services only if you notice a significant drop in performance.

Enabling or Disabling the Client Services from the Web Console

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. For OfficeScan clients running Windows XP, Vista, 7, or 8:
   a. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.

   Note

   When you select the root domain or specific domains, the setting will only apply to clients running Windows XP, Vista, 7, or 8. The setting will not apply to clients running any Windows Server platforms even if they are part of the domains.

   b. Click **Settings** > **Additional Service Settings**.
   c. Select or clear the check box under the following sections:
      - **Unauthorized Change Prevention Service**
      - **Firewall Service**

- **Data Protection Service**

d. Click **Save** to apply settings to the domain(s). If you selected the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing Windows XP/Vista/7/8 clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configure the settings.
- **Apply to Future Domains Only**: Applies settings only to Windows XP/Vista/7/8 clients added to future domains. This option will not apply settings to new clients added to an existing domain.

3. For OfficeScan clients running Windows Server 2003, Windows Server 2008, or Windows Server 2012:

a. Select a client in the client tree.

b. Click **Settings** > **Additional Service Settings**.

c. Select or clear the check box under the following sections:

- **Unauthorized Change Prevention Service**
- **Firewall Service**
- **Data Protection Service**

d. Click **Save**.

Using the Trend Micro Performance Tuning Tool

Procedure

1. Download Trend Micro Performance Tuning Tool from:

   http://esupport.trendmicro.com/solution/en-us/1056425.aspx

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**.

FIGURE 14-1. System-intensive process highlighted

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

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 *Behavior Monitoring Exception List on page 8-5*.

OfficeScan Client Service Restart

OfficeScan restarts OfficeScan client services that stopped responding unexpectedly and were not stopped by a normal system process. For details about client services, see *OfficeScan Client Services on page 14-6*.

Configure the necessary settings to enable OfficeScan client services to restart.

Configuring Service Restart Settings

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Go to the **OfficeScan Service Restart** section.
3. Select **Automatically restart an OfficeScan client service if the service terminates unexpectedly**.
4. Configure the following:
   - **Restart the service after __ minutes**: Specify the amount of time (in number of minutes) that must elapse before OfficeScan restarts a service.
   - **If the first attempt to restart the service fails, retry __ times**: Specify the maximum retry attempts for restarting a service. Manually restart a service if it remains stopped after the maximum retry attempts.

- **Reset the restart failure count after __ hours**: If a service remains stopped after exhausting the maximum retry attempts, OfficeScan waits a certain number of hours to reset the failure count. If a service remains stopped after the number of hours elapses, OfficeScan restarts the service.

Client Self-protection

OfficeScan client self-protection provides ways for the OfficeScan client to protect the processes and other resources required to function properly. OfficeScan client self-protection helps thwart attempts by programs or actual users to disable anti-malware protection.

OfficeScan client self-protection provides the following options:

- *Protect OfficeScan Client Services on page 14-13*
- *Protect Files in the OfficeScan Client Installation Folder on page 14-14*
- *Protect OfficeScan Client Registry Keys on page 14-15*
- *Protect OfficeScan Client Processes on page 14-15*

Configuring OfficeScan Client Self-protection Settings

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Client Self-protection** section.
5. Enable the following options:
   - *Protect OfficeScan Client Services on page 14-13*
   - *Protect Files in the OfficeScan Client Installation Folder on page 14-14*

- *Protect OfficeScan Client Registry Keys on page 14-15*
- *Protect OfficeScan Client Processes on page 14-15*

Note

Protection of registry keys and processes is disabled by default on Windows server platforms.

6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Protect OfficeScan Client Services

OfficeScan blocks all attempts to terminate the following OfficeScan client services:

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- OfficeScan NT Proxy Service (`TmProxy.exe`)
- OfficeScan NT Firewall (`TmPfw.exe`)
- OfficeScan Data Protection Service (`dsagent.exe`)
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

Note

If this option is enabled, OfficeScan may prevent third-party products from installing successfully on endpoints. If you encounter this issue, you can temporarily disable the option and then re-enable it after the installation of the third-party product.

Protect Files in the OfficeScan Client Installation Folder

To prevent other programs and even the user from modifying or deleting OfficeScan client files, OfficeScan locks the following files in the root <*Client installation folder*>:

- All digitally-signed files with `.exe`, `.dll`, and `.sys` extensions
- Some files without digital signatures, including:
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`
  - `msvcp80.dll`
  - `msvcr80.dll`
  - `OfceSCV.dll`
  - `OFCESCVPack.exe`
  - `patchbld.dll`
  - `patchw32.dll`
  - `patchw64.dll`

- `PiReg.exe`
- `ssleay32.dll`
- `Tmeng.dll`
- `TMNotify.dll`
- `zlibwapi.dll`

Protect OfficeScan Client Registry Keys

OfficeScan blocks all attempts to modify, delete, or add new entries under the following registry keys and subkeys:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMCSS`

Protect OfficeScan Client Processes

OfficeScan blocks all attempts to terminate the following processes:

- `TmListen.exe`: Receives commands and notifications from the OfficeScan server and facilitates communication from the OfficeScan client to the server
- `NTRtScan.exe`: Performs Real-time, Scheduled, and Manual Scan on OfficeScan clients
- `TmProxy.exe`: Scans network traffic before passing it to the target application
- `TmPfw.exe`: Provides packet level firewall, network virus scanning and intrusion detection capabilities
- `TMBMSRV.exe`: Regulates access to external storage devices and prevents unauthorized changes to registry keys and processes

- `DSAgent.exe`: Monitors the transmission of sensitive data and controls access to devices

OfficeScan Client Security

Control user access to the OfficeScan client installation directory and registry settings by selecting from two security settings.

Controlling Access to the OfficeScan Client Installation Directory and Registry Keys

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Client Security Settings** section.
5. Select from the following access permissions:
   - **High**: The OfficeScan client installation directory inherits the rights of the `Program Files` folder and the OfficeScan client's registry entries inherit permissions from the `HKLM\Software` key. For most Active Directory configurations, this automatically limits "normal" users (those without administrator privileges) to read-only access.
   - **Normal**: This permission grants all users (the user group "Everyone") full rights to the OfficeScan client program directory and OfficeScan client registry entries.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

OfficeScan Client Console Access Restriction

This setting disables OfficeScan client console access from the system tray or Windows Start menu. The only way users can access the OfficeScan client console is by clicking `PccNT.exe` from the <*Client installation folder*>. After configuring this setting, reload the OfficeScan client for the setting to take effect.

This setting does not disable the OfficeScan client. The OfficeScan client runs in the background and continues to provide protection from security risks.

Restricting Access to the OfficeScan Client Console

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Client Console Access Restriction** section.
5. Select **Do not allow users to access the client console from the system tray or Windows Start menu**.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

OfficeScan Client Unloading

The OfficeScan client unloading privilege allows users to temporarily stop the OfficeScan client with or without a password.

Granting the Client Unloading Privilege

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Unloading** section.
5. To allow client unloading without a password, select **Allow the user to unload the OfficeScan client**.
   - If a password is required, select **Require a password for the user to unload the OfficeScan client**, type the password, and then confirm it.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

OfficeScan Client Roaming Privilege

Grant certain users the OfficeScan client roaming privilege if client-server events are interfering with the users' tasks. For example, a user who frequently gives presentations can enable roaming mode before starting a presentation to prevent the OfficeScan server from deploying OfficeScan client settings and initiating scans on the OfficeScan client.

When clients are in roaming mode:

- OfficeScan clients do not send logs to the OfficeScan server, even if there is a functional connection between the server and clients.
- The OfficeScan server does not initiate tasks and deploy OfficeScan client settings to the clients, even if there is functional connection between the server and clients.
- OfficeScan clients update components if they can connect to any of their update sources. Sources include the OfficeScan server, Update Agents, or a custom update source.

  The following events trigger an update on roaming clients:

  - The user performs a manual update.
  - Automatic client update runs. You can disable automatic client update on roaming clients. For details, see *Disabling Automatic Client Update on Roaming Clients on page 14-20*.
  - Scheduled update runs. Only clients with the required privileges can run scheduled updates. You can revoke this privilege anytime. For details, see *Revoking the Scheduled Update Privilege on roaming OfficeScan Clients on page 14-21*.

Granting the Client Roaming Privilege

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Roaming Privilege** section.
5. Select **Enable roaming mode**.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Disabling Automatic Client Update on Roaming Clients

Procedure

1. Navigate to **Updates** > **Networked Computers** > **Automatic Update**.
2. Go to the **Event-triggered Update** section.
3. Disable **Include roaming and offline client(s)**.

Note

This option is automatically disabled if you disable **Initiate component update on clients immediately after the OfficeScan server downloads a new component**.

4. Click **Save**.

Revoking the Scheduled Update Privilege on roaming OfficeScan Clients

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Component Update Privileges** section.
5. Clear the **Enable scheduled update** option.
6. Click **Save**.

Client Mover

If you have more than one OfficeScan server on the network, use the Client Mover tool to transfer OfficeScan clients from one OfficeScan server to another. This is especially useful after adding a new OfficeScan server to the network and you want to transfer existing OfficeScan clients to the new server.

Note

The two servers must be of the same language version. If you use Client Mover to move an OfficeScan client running an earlier version to a server of the current version, the OfficeScan client will be upgraded automatically.

Ensure that the account you use has administrator privileges before using this tool.

Running Client Mover

Procedure

1. On the OfficeScan server, go to <*Server installation folder*>`\PCCSRV\Admin\Utility\IpXfer`.
2. Copy `IpXfer.exe` to the OfficeScan client computer. If the OfficeScan client computer runs an x64 type platform, copy `IpXfer_x64.exe` instead.
3. On the OfficeScan client computer, open a command prompt and then navigate to the folder where you copied the executable file.
4. Run Client Mover using the following syntax:

```
<executable file name> -s <server name> -p <server
listening port> -c <client listening port> -d <domain or
domain hierarchy>
```

TABLE 14-3. Client Mover Parameters

PARAMETER	EXPLANATION
`<executable file name>`	`IpXfer.exe` or `IpXfer_x64.exe`
`<server name>`	The name of the destination OfficeScan server (the server to which the OfficeScan client will transfer)
`<server listening port>`	The listening port (or trusted port) of the destination OfficeScan server. To view the listening port on the OfficeScan web console, click **Administration** > **Connection Settings** in the main menu.
`<client listening port>`	The port number used by the OfficeScan client computer to communicate with the server
`<domain or domain hierarchy>`	The client tree domain or subdomain to which the client will be grouped. The domain hierarchy should indicate the subdomain.

Examples:

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup
```

```
ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup
\Group01
```

5. To confirm the OfficeScan client now reports to the other server, do the following:

   a. On the OfficeScan client computer, right-click the OfficeScan client program icon in the system tray.

   b. Select **OfficeScan Console**.

   c. Click **Help** in the menu and select **About**.

   d. Check the OfficeScan server that the OfficeScan client reports to in the **Server name/port** field.

   Note

   If the OfficeScan client does not appear in the client tree of the new OfficeScan server managing it, restart the new server's Master Service (`ofservice.exe`).

Inactive OfficeScan Clients

When you use the OfficeScan client uninstallation program to remove the OfficeScan client program from a computer, the program automatically notifies the server. When the server receives this notification, it removes the OfficeScan client icon in the client tree to show that the client does not exist anymore.

However, if you use other methods to remove the OfficeScan client, such as reformatting the computer hard drive or deleting the OfficeScan client files manually, OfficeScan will not be aware of the removal and it will display the OfficeScan client as inactive. If a user unloads or disables the OfficeScan client for an extended period of time, the server also displays the OfficeScan client as inactive.

To have the client tree display active clients only, configure OfficeScan to automatically remove inactive clients from the client tree.

Automatically Removing Inactive Clients

Procedure

1. Navigate to **Administration** > **Inactive Clients**.
2. Select **Enable automatic removal of inactive clients**.
3. Select how many days should pass before OfficeScan considers an OfficeScan client inactive.
4. Click **Save**.

Client-Server Connection

The OfficeScan client must maintain a continuous connection with its parent server so that it can update components, receive notifications, and apply configuration changes in a timely manner. The following topics discuss how to check the OfficeScan client's connection status and resolve connection issues:

- *Client IP Addresses on page 5-9*
- *OfficeScan Client Icons on page 14-24*
- *Client-Server Connection Verification on page 14-40*
- *Connection Verification Logs on page 14-41*
- *Unreachable Clients on page 14-41*

OfficeScan Client Icons

The OfficeScan client icon in the system tray provide visual hints that indicate the current status of the OfficeScan client and prompt users to perform certain actions. At any given time, the icon will show a combination of the following visual hints.

TABLE 14-4. OfficeScan client Status as Indicated in the OfficeScan client Icon

CLIENT STATUS	DESCRIPTION	VISUAL HINT
Client connection with the OfficeScan server	Online clients are connected to the OfficeScan server. The server can initiate tasks and deploy settings to these clients	The icon contains a symbol resembling a heartbeat. The background color is a shade of blue or red, depending on the status of the Real-time Scan Service.
	Offline clients are disconnected from the OfficeScan server. The server cannot manage these clients.	The icon contains a symbol resembling the loss of a heartbeat. The background color is a shade of blue or red, depending on the status of the Real-time Scan Service. It is possible for a client to become offline even if it is connected to the network. For details about this issue, see *An OfficeScan Client is Connected to the Network but Appears Offline on page 14-37*.
	Roaming clients may or may not be able to communicate with the OfficeScan server.	The icon contains the desktop and signal symbols. The background color is a shade of blue or red, depending on the status of the Real-time Scan Service. For details about roaming clients, see *OfficeScan Client Roaming Privilege on page 14-19*.

Client Status	Description	Visual Hint
Availability of smart protection sources	Smart protection sources include Smart Protection Servers and Trend Micro Smart Protection Network. Conventional scan clients connect to smart protection sources for web reputation queries. Smart scan clients connect to smart protection sources for scan and web reputation queries.	The icon includes a check mark if a smart protection source is available.
		The icon includes a progress bar if no smart protection source is available and the client is attempting to establish connection with the sources. For details about this issue, see *Smart Protection Sources are Unavailable on page 14-38*.
		For conventional scan clients, no check mark or progress bar appears if web reputation has been disabled on the client.

Client Status	Description	Visual Hint
Real-time Scan Service status	OfficeScan uses the Real-time Scan Service not only for Real-time Scan, but also for Manual Scan and Scheduled Scan. The service must be functional or the client becomes vulnerable to security risks.	The entire icon is shaded blue if the Real-time Scan Service is functional. Two shades of blue are used to indicate the client's scan method. • For conventional scan: • For smart scan:
		The entire icon is shaded red if the Real-time Scan Service has been disabled or is not functional. Two shades of red are used to indicate the client's scan method. • For conventional scan: • For smart scan: For details about this issue, see *Real-time Scan Service Has Been Disabled or is Not Functional on page 14-37*.

Client Status	Description	Visual Hint
Real-time Scan status	Real-time Scan provides proactive protection by scanning files for security risks as they are created, modified, or retrieved.	There are no visual hints if Real-time Scan is enabled.
		The entire icon is surrounded by a red circle and contains a red diagonal line if Real-time Scan is disabled. For details about this issue, see: • *Real-time Scan was Disabled on page 14-37* • *Real-time Scan was Disabled and an OfficeScan Client is in Roaming Mode on page 14-37*
Pattern update status	Clients must update the pattern regularly to protect the client from the latest threats.	There are no visual hints if the pattern is up-to-date or is slightly out-of-date.
		The icon includes an exclamation mark if the pattern is severely outdated. This means that the pattern been not been updated for a while. For details on how to update clients, see *OfficeScan Client Updates on page 6-26*.

Smart Scan Icons

Any of the following icons displays when OfficeScan clients use smart scan.

Table 14-5. Smart Scan Icons

Icon	Connection with OfficeScan Server	Availability of Smart Protection Sources	Real-time Scan Service	Real-time Scan
	Online	Available	Functional	Enabled
	Online	Available	Functional	Disabled
	Online	Available	Disabled or not functional	Disabled or not functional
	Online	Unavailable, reconnecting to sources	Functional	Enabled
	Online	Unavailable, reconnecting to sources	Functional	Disabled
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional
	Offline	Available	Functional	Enabled
	Offline	Available	Functional	Disabled
	Offline	Available	Disabled or not functional	Disabled or not functional
	Offline	Unavailable, reconnecting to sources	Functional	Enabled
	Offline	Unavailable, reconnecting to sources	Functional	Disabled
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional
	Roaming	Available	Functional	Enabled

Icon	Connection with OfficeScan Server	Availability of Smart Protection Sources	Real-time Scan Service	Real-time Scan
	Roaming	Available	Functional	Disabled
	Roaming	Available	Disabled or not functional	Disabled or not functional
	Roaming	Unavailable, reconnecting to sources	Functional	Enabled
	Roaming	Unavailable, reconnecting to sources	Functional	Disabled
	Roaming	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional

Conventional Scan Icons

Any of the following icons displays when OfficeScan clients use conventional scan.

Table 14-6. Conventional Scan Icons

Icon	Connection with OfficeScan Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Online	Available	Functional	Enabled	Up-to-date or slightly outdated
	Online	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated

Icon	Connection with OfficeScan Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Online	Available	Functional	Enabled	Severely outdated
	Online	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated
	Online	Available	Functional	Disabled	Up-to-date or slightly outdated
	Online	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Online	Available	Functional	Disabled	Severely outdated
	Online	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated
	Online	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Online	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated

Icon	Connection with OfficeScan Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Offline	Available	Functional	Enabled	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated
	Offline	Available	Functional	Enabled	Severely outdated
	Offline	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated
	Offline	Available	Functional	Disabled	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Offline	Available	Functional	Disabled	Severely outdated
	Offline	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated
	Offline	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated

Icon	Connection with OfficeScan Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Offline	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated
	Roaming	Available	Functional	Enabled	Up-to-date or slightly outdated
	Roaming	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated
	Roaming	Available	Functional	Enabled	Severely outdated
	Roaming	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated
	Roaming	Available	Functional	Disabled	Up-to-date or slightly outdated
	Roaming	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Roaming	Available	Functional	Disabled	Severely outdated
	Roaming	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated

Icon	Connection with OfficeScan Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Roaming	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Roaming	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Roaming	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Roaming	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated
	Online	Not applicable (Web reputation feature disabled on client)	Functional	Enabled	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on client)	Functional	Enabled	Severely outdated
	Online	Not applicable (Web reputation feature disabled on client)	Functional	Disabled	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on client)	Functional	Disabled	Severely outdated

Icon	Connection with OfficeScan Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Online	Not applicable (Web reputation feature disabled on client)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on client)	Disabled or not functional	Disabled or not functional	Severely outdated
	Offline	Not applicable (Web reputation feature disabled on client)	Functional	Enabled	Up-to-date or slightly outdated
	Offline	Not applicable (Web reputation feature disabled on client)	Functional	Enabled	Severely outdated
	Offline	Not applicable (Web reputation feature disabled on client)	Functional	Disabled	Up-to-date or slightly outdated
	Offline	Not applicable (Web reputation feature disabled on client)	Functional	Disabled	Severely outdated
	Offline	Not applicable (Web reputation feature disabled on client)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated

Icon	Connection with OfficeScan Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Offline	Not applicable (Web reputation feature disabled on client)	Disabled or not functional	Disabled or not functional	Severely outdated
	Roaming	Not applicable (Web reputation feature disabled on client)	Functional	Enabled	Up-to-date or slightly outdated
	Roaming	Not applicable (Web reputation feature disabled on client)	Functional	Enabled	Severely outdated
	Roaming	Not applicable (Web reputation feature disabled on client)	Functional	Disabled	Up-to-date or slightly outdated
	Roaming	Not applicable (Web reputation feature disabled on client)	Functional	Disabled	Severely outdated
	Roaming	Not applicable (Web reputation feature disabled on client)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Roaming	Not applicable (Web reputation feature disabled on client)	Disabled or not functional	Disabled or not functional	Severely outdated

Solutions to Issues Indicated in OfficeScan Client Icons

Perform the necessary actions if the OfficeScan client icon indicates any of the following conditions:

Pattern File Has Not Been Updated for a While

OfficeScan client users need to update components. From the web console, configure component update settings in **Updates** > **Networked Computers** > **Automatic Update**, or grant users the privilege to update in **Networked Computers** > **Client Management** > **Settings** > **Privileges and Other Settings** > **Privileges** > **Component Update Privileges**.

Real-time Scan Service Has Been Disabled or is Not Functional

If the Real-time Scan Service (OfficeScan NT RealTime Scan) has been disabled or becomes non-functional, users must start the service manually from Microsoft Management Console.

Real-time Scan was Disabled

Enable Real-time Scan from the web console (**Networked Computers** > **Client Management** > **Settings** > **Scan Settings** > **Real-time Scan Settings**).

Real-time Scan was Disabled and an OfficeScan Client is in Roaming Mode

Users need to disable roaming mode first. After disabling roaming mode, enable Real-time Scan from the web console.

An OfficeScan Client is Connected to the Network but Appears Offline

Verify the connection from the web console (**Networked Computers** > **Connection Verification**) and then check connection verification logs (**Logs** > **Networked Computer Logs** > **Connection Verification**).

If the OfficeScan client is still offline after verification:

1. If the connection status on both the server and OfficeScan client is offline, check the network connection.

2. If the connection status on the OfficeScan client is offline but online on the server, the server's domain name may have been changed and the OfficeScan client connects to the server using the domain name (if you select domain name during server installation). Register the OfficeScan server's domain name to the DNS or WINS server or add the domain name and IP information into the "hosts" file in the client computer's `<Windows folder>\system32\drivers\etc` folder.

3. If the connection status on the OfficeScan client is online but offline on the server, check the OfficeScan firewall settings. The firewall may block server-to-client communication, but allow client-to-server communication.

4. If the connection status on the OfficeScan client is online but offline on the server, the OfficeScan client's IP address may have been changed but its status does not reflect on the server (for example, when the client is reloaded). Try to redeploy the OfficeScan client.

Smart Protection Sources are Unavailable

Perform these tasks if a client loses connection with smart protection sources:

1. On the web console, go to the Computer Location screen (**Networked Computers** > **Computer Location**) and check if the following computer location settings have been configured properly:

   - Reference servers and port numbers

   - Gateway IP addresses

2. On the web console, go to the Smart Protection Source screen (**Smart Protection** > **Smart Protection Sources**) and then perform the following tasks:

   a. Check if the Smart Protection Server settings on the standard or custom list of sources are correct.

   b. Test if connection to the servers can be established.

   c. Click **Notify All Clients** after configuring the list of sources.

3. Check if the following configuration files on the Smart Protection Server and OfficeScan client are synchronized:

   - `sscfg.ini`
   - `ssnotify.ini`

4. Open Registry Editor and check if a client is connected to the corporate network.

   Key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp \CurrentVersion\iCRC Scan\Scan Server`

   - If `LocationProfile=1`, the OfficeScan client is connected to the network and should be able to connect to a Smart Protection Server.
   - If `LocationProfile=2`, the OfficeScan client is not connected to the network and should connect to the Smart Protection Network. From Internet Explorer, check if the OfficeScan client computer can browse Internet web pages.

5. Check internal and external proxy settings used to connect to Smart Protection Network and Smart Protection Servers. For details, see *Internal Proxy for OfficeScan Clients on page 14-46* and *External Proxy for OfficeScan Clients on page 14-47*.

6. For conventional scan clients, verify that the OfficeScan NT Proxy Service (`TmProxy.exe`) is running. If this service stops, clients cannot connect to smart protection sources for web reputation.

Client-Server Connection Verification

The client connection status with the OfficeScan server displays on the OfficeScan web console's client tree.

FIGURE 14-2. Client tree displaying client connection status with OfficeScan server

Certain conditions may prevent the client tree from displaying the correct client connection status. For example, if you accidentally unplug the network cable of a client computer, the client will not be able to notify the server that it is now offline. This client will still appear as online in the client tree.

Verify client-server connection manually or let OfficeScan perform scheduled verification. You cannot select specific domains or clients and then verify their connection status. OfficeScan verifies the connection status of all its registered clients.

Verifying Client-Server Connections

Procedure

1. Navigate to **Networked Computers** > **Connection Verification**.
2. To verify client-server connection manually, go to the **Manual Verification** tab and click **Verify Now**.
3. To verify client-server connection automatically, go to the **Scheduled Verification** tab.

a. Select **Enable scheduled verification**.

b. Select the verification frequency and start time.

c. Click **Save** to save the verification schedule.

4. Check the client tree to verify the status or view the connection verification logs.

Connection Verification Logs

OfficeScan keeps connection verification logs to allow you to determine whether or not the OfficeScan server can communicate with all of its registered clients. OfficeScan creates a log entry each time you verify client-server connection from the web console.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 13-33*.

Viewing Connection Verification Logs

Procedure

1. Navigate to **Networked Computers** > **Connection Verification**.
2. View connection verification results by checking the **Status** column.
3. To save logs to a comma-separated value (`CSV`) file, click **Export to CSV**. Open the file or save it to a specific location.

Unreachable Clients

OfficeScan clients on unreachable networks, such as those on network segments behind a NAT gateway, are almost always offline because the server cannot establish direct connection with the clients. As a result, the server cannot notify the clients to:

- Download the latest components.

- Apply client settings configured from the web console. For example, when you change the Scheduled Scan frequency from the web console, the server will immediately notify clients to apply the new setting.

Unreachable clients therefore cannot perform these tasks in a timely manner. They only perform the tasks when they initiate connection with the server, which happens when:

- They register to the server after installation.
- They restart or reload. This event does not occur frequently and usually requires user intervention.
- Manual or scheduled update is triggered on the client. This event also does not occur frequently.

It is only during registration, restart, or reload that the server becomes "aware" of the clients' connectivity and treats them as online. However, because the server is still unable to establish connection with the clients, the server immediately changes the status to offline.

OfficeScan provides the "heartbeat" and server polling features to resolve issues regarding unreachable clients. With these features, the server stops notifying clients of component updates and setting changes. Instead, the server takes a passive role, always waiting for clients to send heartbeat or initiate polling. When the server detects any of these events, it treats the clients as online.

Note

Client-initiated events not related to heartbeat and server polling, such as manual client update and log sending, do not trigger the server to update the unreachable clients' status.

Heartbeat

OfficeScan clients send heartbeat messages to notify the server that connection from the client remains functional. Upon receiving a heartbeat message, the server treats the client as online. In the client tree, the client's status can either be:

- **Online**: For regular online clients
- **Unreachable/Online**: For online clients in the unreachable network

Note

OfficeScan clients do not update components or apply new settings when sending heartbeat messages. Regular clients perform these tasks during routine updates (see *OfficeScan Client Updates on page 6-26*). Clients in the unreachable network perform these tasks during server polling.

The heartbeat feature addresses the issue of OfficeScan clients in unreachable networks always appearing as offline even when they can connect to the server.

A setting in the web console controls how often clients send heartbeat messages. If the server did not receive a heartbeat, it does not immediately treat the client as offline. Another setting controls how much time without a heartbeat must elapse before changing the client's status to:

- **Offline**: For regular offline OfficeScan clients
- **Unreachable/Offline**: For offline OfficeScan clients in the unreachable network

When choosing a heartbeat setting, balance between the need to display the latest client status information and the need to manage system resources. The default setting is satisfactory for most situations. However, consider the following points when you customize the heartbeat setting:

TABLE 14-7. Heartbeat Recommendations

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before the server reflects the client's status on the web console.
Short-interval Heartbeats (below 60 minutes)	Short intervals present a more up-to-date client status but may be bandwidth-intensive.

Server Polling

The server polling feature addresses the issue of unreachable OfficeScan clients not receiving timely notifications about component updates and changes to client settings. This feature is independent of the heartbeat feature.

With the server polling feature:

- OfficeScan clients automatically initiate connection with the OfficeScan server at regular intervals. When the server detects that polling took place, it treats the client as "Unreachable/Online".
- OfficeScan clients connect to one or several of their update sources to download any updated components and apply new client settings. If the OfficeScan server or an Update Agent is the primary update source, clients obtain both components and new settings. If the source is not the OfficeScan server or Update Agent, clients only obtain the updated components and then connect to the OfficeScan server or Update Agent to obtain the new settings.

Configuring the Heartbeat and Server Polling Features

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**,
2. Go to the **Unreachable Network** section.
3. Configure server polling settings.

   For details about server polling, see *Server Polling on page 14-43*.

   a. If the OfficeScan server has both an IPv4 and IPv6 address, you can type an IPv4 address range and IPv6 prefix and length.

      Type an IPv4 address range if the server is pure IPv4, or an IPv6 prefix and length if the server is pure IPv6.

      When a client's IP address matches an IP address in the range, the client applies the heartbeat and server polling settings and the server treats the client as part of the unreachable network.

Note

Clients with an IPv4 address can connect to a pure IPv4 or dual-stack OfficeScan server.

Clients with an IPv6 address can connect to a pure IPv6 or dual-stack OfficeScan server.

Dual-stack clients can connect to dual-stack, pure IPv4, or pure IPv6 OfficeScan server.

b. In **Clients poll the server for updated components and settings every __ minute(s)**, specify the server polling frequency. Type a value between 1 and 129600 minutes.

Tip

Trend Micro recommends that the server polling frequency be at least three times the heartbeat sending frequency.

4. Configure heartbeat settings.

   For details about the heartbeat feature, see *Heartbeat on page 14-42*.

   a. Select **Allow clients to send heartbeat to the server**.

   b. Select **All clients** or **Only clients in the unreachable network**.

   c. In **Clients send heartbeat every __ minutes**, specify how often clients send heartbeat. Type a value between 1 and 129600 minutes.

   d. In **A client is offline if there is no heartbeat after __ minutes**, specify how much time without a heartbeat must elapse before the OfficeScan server treats a client as offline. Type a value between 1 and 129600 minutes.

5. Click **Save**.

OfficeScan Client Proxy Settings

Configure OfficeScan clients to use proxy settings when connecting to internal and external servers.

Internal Proxy for OfficeScan Clients

OfficeScan clients can use internal proxy settings to connect to the following servers on the network:

- **OfficeScan Server Computer**

  The server computer hosts the OfficeScan server and the integrated Smart Protection Server. OfficeScan clients connect to the OfficeScan server to update components, obtain configuration settings, and send logs. OfficeScan clients connect to the integrated Smart Protection Server to send scan queries.

- **Smart Protection Servers**

  Smart Protection Servers include all standalone Smart Protection Servers and the integrated Smart Protection Server of other OfficeScan servers. OfficeScan clients connect to the servers to send scan and we reputation queries.

Configuring Internal Proxy Settings

Procedure

1. Navigate to **Administration** > **Proxy Settings**.
2. Click the **Internal Proxy** tab.
3. Go to the **Client Connection with the OfficeScan Server Computer** section.
   a. Select **Use the following proxy settings when clients connect to the OfficeScan server and the Integrated Smart Protection Server**.
   b. Specify the proxy server name or IPv4/IPv6 address, and port number.

> **Note**
>
> Specify a dual-stack proxy server identified by its host name if you have IPv4 and IPv6 clients. This is because internal proxy settings are global settings. If you specify an IPv4 address, IPv6 clients cannot connect to the proxy server. The same is true for IPv4 clients.

c. If the proxy server requires authentication, type the user name and password and then confirm the password.

4. Go to the **Client Connection with Standalone Smart Protection Servers** section.

   a. Select **Use the following proxy settings when clients connect to the standalone Smart Protection Servers**.

   b. Specify the proxy server name or IPv4/IPv6 address, and port number.

   c. If the proxy server requires authentication, type the user name and password and then confirm the password.

5. Click **Save**.

External Proxy for OfficeScan Clients

The OfficeScan server and OfficeScan client can use external proxy settings when connecting to servers hosted by Trend Micro. This topic discusses external proxy settings for clients. For external proxy settings for the server, see *Proxy for OfficeScan Server Updates on page 6-17*.

OfficeScan clients use the proxy settings configured in Internet Explorer to connect to the Trend Micro Smart Protection Network. If proxy server authentication is required, clients will use proxy server authentication credentials (user ID and password).

Configuring Proxy Server Authentication Credentials

Procedure

1. Navigate to **Administration** > **Proxy Settings**.

2. Click the **External Proxy** tab.
3. Go to the **Client Connection with Trend Micro Servers** section.
4. Type the user ID and password needed for proxy server authentication. The following proxy authentication protocols are supported:
   - Basic access authentication
   - Digest access authentication
   - Integrated Windows Authentication
5. Click **Save**.

Proxy Configuration Privileges for Clients

You can grant client users the privilege to configure proxy settings. OfficeScan clients use user-configured proxy settings only on the following instances:

- When OfficeScan clients perform "Update Now".
- When users disable, or the OfficeScan client cannot detect, automatic proxy settings. See *Automatic Proxy Settings for the OfficeScan Client on page 14-49* for more information.

WARNING!

Incorrect user-configured proxy settings can cause update problems. Exercise caution when allowing users to configure their own proxy settings.

Granting Proxy Configuration Privileges

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.

3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the Proxy Setting Privileges section.
5. Select **Allow the client user to configure proxy settings**.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Automatic Proxy Settings for the OfficeScan Client

Manually configuring proxy settings may be a complicated task for many end users. Use automatic proxy settings to ensure that correct proxy settings are applied without requiring any user intervention.

When enabled, automatic proxy settings are the primary proxy settings when OfficeScan clients update components either through automatic update or Update Now. For information on automatic update and Update Now, see *OfficeScan Client Update Methods on page 6-34*.

If OfficeScan clients cannot connect using the automatic proxy settings, client users with the privilege to configure proxy settings can use user-configured proxy settings. Otherwise, connection using the automatic proxy settings will be unsuccessful.

Note

Proxy authentication is not supported.

Configuring Automatic Proxy Settings

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**,
2. Go to the **Proxy Configuration** section.
3. Select **Automatically Detect Settings** if you want OfficeScan to automatically detect the administrator-configured proxy settings by DHCP or DNS.
4. If you want OfficeScan to use the proxy auto-configuration (PAC) script set by the network administrator to detect the appropriate proxy server:
   a. Select **Use Automatic Configuration Script**.
   b. Type the address for the PAC script.
5. Click **Save**.

Viewing OfficeScan Client Information

The View Status screen displays important information about OfficeScan clients, including privileges, client software details and system events.

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Status**.
4. View status information by expanding the client computer's name. If you selected multiple clients, click **Expand All** to view status information for all the selected clients.

5. (Optional) Use the **Reset** buttons to set the security risk count back to zero.

Importing and Exporting Client Settings

OfficeScan allows you to export client tree settings applied by a particular OfficeScan client or domain to a file. You can then import the file to apply the settings to other clients and domains or to another OfficeScan server of the same version.

All client tree settings, except Update Agent settings, will be exported.

Exporting Client Settings

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Export Settings**.
4. Click any of the links to view the settings for the OfficeScan client or domain you selected.
5. Click **Export** to save the settings.

   The settings are saved in a `.dat` file.
6. Click **Save** and then specify the location to which you want to save the `.dat` file.
7. Click **Save**.

Importing Client Settings

Procedure

1. Navigate to **Networked Computers** > **Client Management**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Import Settings**.
4. Click **Browse** to locate the `.dat` file on the computer and click **Import**.

   The **Import Settings** screen appears, showing a summary of the settings.
5. Click any of the links to view details about the scan settings or privileges to import.
6. Import the settings.
   - If you clicked the root domain icon, select **Apply to all domains** and then click **Apply to Target**.
   - If you selected domains, select **Apply to all computers belonging to the selected domain(s)**, and then click **Apply to Target**.
   - If you selected several clients, click **Apply to Target**.

Security Compliance

Use Security Compliance to determine flaws, deploy solutions, and maintain the security infrastructure. This feature helps reduce the time required to secure the network environment and balance an organization's needs for security and functionality.

Enforce security compliance for two types of computers:

- **Managed**: Computers with OfficeScan clients managed by the OfficeScan server. For details, see *Security Compliance for Managed Clients on page 14-53*.
- **Unmanaged**: Includes the following:

- OfficeScan clients not managed by the OfficeScan server
- Computers without OfficeScan clients installed
- Computers that the OfficeScan server cannot reach
- Computers whose security status cannot be verified

  For details, see *Security Compliance for Unmanaged Endpoints on page 14-65*.

Security Compliance for Managed Clients

Security Compliance generates a Compliance Report to help you assess the security status of OfficeScan clients managed by the OfficeScan server. Security Compliance generates the report on demand or according to a schedule.

On-demand and scheduled reports are available on the Compliance Report screen. The screen contains the following tabs:

- **Services**: Use this tab to check if client services are functional. For details, see *Services on page 14-54*.
- **Components**: Use this tab to check if OfficeScan clients have up-to-date components. For details, see *Components on page 14-55*.
- **Scan Compliance**: Use this tab to check if OfficeScan clients are running scans regularly. For details, see *Scan Compliance on page 14-57*.
- **Settings**: Use this tab to check if client settings are consistent with the settings on the server. For details, see *Settings on page 14-59*.

Note

The **Components** tab can display OfficeScan clients running the current and earlier versions of the product. For the other tabs, only OfficeScan clients running version 10.5, 10.6, or OfficeScan clients are shown.

Notes on Compliance Report

- Security Compliance queries the OfficeScan clients' connection status before generating a Compliance Report. It includes online and offline clients in the report, but not roaming clients.
- For role-based user accounts:
  - Each web console user account has a completely independent set of Compliance Report settings. Any changes to a user account's Compliance Report settings will not affect the settings of the other user accounts.
  - The scope of the report depends on the client domain permissions for the user account. For example, if you grant a user account permissions to manage domains A and B, the user account's reports will only show data from clients belonging to domains A and B.

    For details about user accounts, see *Role-based Administration on page 13-2*.

Services

Security Compliance checks whether the following OfficeScan client services are functional:

- Antivirus
- Anti-spyware
- Firewall
- Web Reputation
- Behavior Monitoring/Device Control (also referred to as Trend Micro Unauthorized Change Prevention Service)
- Data Protection

A non-compliant client is counted at least twice in the Compliance Report.

FIGURE 14-3. Compliance Report - Services tab

- In the **Computers with Non-compliant Services** category
- In the category for which the OfficeScan client is non-compliant. For example, if the OfficeScan client's Antivirus service is not functional, the client is counted in the **Antivirus** category. If more than one service is not functional, the client is counted in each category for which it is non-compliant.

Restart non-functional services from the web console or from the OfficeScan client computer. If the services are functional after the restart, the client will no longer appear as non-compliant during the next assessment.

Components

Security Compliance determines component version inconsistencies between the OfficeScan server and OfficeScan clients. Inconsistencies typically occur when clients

cannot connect to the server to update components. If the client obtains updates from another source (such as the Trend Micro ActiveUpdate server), it is possible for a client's component version to be newer than the version on the server.

Security Compliance checks the following components:

- Smart Scan Agent Pattern
- Virus Pattern
- IntelliTrap Pattern
- IntelliTrap Exception Pattern
- Virus Scan Engine
- Spyware Pattern
- Spyware Active-monitoring Pattern
- Spyware Scan Engine
- Virus Cleanup Template
- Virus Cleanup Engine
- Common Firewall Pattern
- Common Firewall Driver
- Behavior Monitoring Driver
- Behavior Monitoring Core Service
- Behavior Monitoring Configuration Pattern
- Digital Signature Pattern
- Policy Enforcement Pattern
- Behavior Monitoring Detection Pattern
- Program Version
- C&C IP List

A non-compliant client is counted at least twice in the Compliance Report.

FIGURE 14-4. Compliance Report - Components tab

- In the **Computers with Inconsistent Component Versions** category
- In the category for which the client is non-compliant. For example, if the client's Smart Scan Agent Pattern version is not consistent with the version on the server, the client is counted in the **Smart Scan Agent Pattern** category. If more than one component version is inconsistent, the client is counted in each category for which it is non-compliant.

To resolve component version inconsistencies, update outdated components on the clients or server.

Scan Compliance

Security Compliance checks if Scan Now or Scheduled Scan are run regularly and if these scans are completed within a reasonable amount of time.

Note

Security Compliance can only report the Scheduled Scan status if Scheduled Scan is enabled on clients.

Security Compliance uses the following scan compliance criteria:

- **No Scan Now or Scheduled Scan performed for the last (x) days**: An OfficeScan client is non-compliant if it did not run Scan Now or Scheduled Scan within the specified number of days.
- **Scan Now or Scheduled Scan exceeded (x) hours**: An OfficeScan client is non-compliant if the last Scan Now or Scheduled Scan lasted more than the specified number of hours.

A non-compliant client is counted at least twice in the Compliance Report.

FIGURE 14-5. Compliance Report - Scan Compliance tab

- In the **Computers with Outdated Scanning** category

- In the category for which the client is non-compliant. For example, if the last Scheduled Scan lasted more than the specified number of hours, the client is counted in the **Scan Now or Scheduled Scan exceeded <x> hours** category. If the client satisfies more than one scan compliance criteria, it is counted in each category for which it is non-compliant.

Run Scan Now or Scheduled Scan on clients that have not performed scan tasks or were unable to complete scanning.

Settings

Security Compliance determines whether clients and their parent domains in the client tree have the same settings. The settings may not be consistent if you move a client to another domain that is applying a different set of settings, or if a client user with certain privileges manually configured settings on the OfficeScan client console.

OfficeScan verifies the following settings:

• Scan Method	• Additional Service Settings
• Manual Scan Settings	• Web Reputation
• Real-time Scan Settings	• Behavior Monitoring
• Scheduled Scan Settings	• Device Control
• Scan Now Settings	• Spyware/Grayware Approved List
• Privileges and Other Settings	• Data Loss Prevention Settings

A non-compliant client is counted at least twice in the Compliance Report.

FIGURE 14-6. Compliance Report - Settings tab

- In the **Computers with Inconsistent Configuration Settings** category
- In the category for which the client is non-compliant. For example, if the scan method settings in the client and its parent domain are not consistent, the client is counted in the **Scan Method** category. If more than one set of settings is inconsistent, the client is counted in each category for which it is non-compliant.

To resolve the setting inconsistencies, apply domain settings to the client.

On-demand Compliance Reports

Security Compliance can generate Compliance Reports on demand. Reports help you assess the security status of OfficeScan clients managed by the OfficeScan server.

For more information on Compliance Reports, see *Security Compliance for Managed Clients on page 14-53*.

Generating an On-demand Compliance Report

Procedure

1. Navigate to **Security Compliance** > **Compliance Assessment** > **Compliance Report**.
2. Go to the **Client Tree Scope** section.
3. Select the root domain or a domain and click **Assess**.
4. View Compliance Report for client services.

   For details about client services, see *Services on page 14-54*.

   a. Click the **Services** tab.

   b. Under **Computers with Non-compliant Services**, check the number of clients with non-compliant services.

   c. Click a number link to display all affected clients in the client tree.

   d. Select clients from the query result.

   e. Click **Restart OfficeScan Client** to restart the service.

   > **Note**
   >
   > After performing another assessment and the client still appears as non-compliant, manually restart the service on the client computer.

   f. To save the list of clients to a file, click **Export**.

5. View Compliance Report for client components.

   For details about client components, see *Components on page 14-55*.

   a. Click the **Components** tab.

b. Under **Computers with Inconsistent Component Versions**, check the number of clients with component versions that are inconsistent with the versions on the server.

c. Click a number link to display all affected clients in the client tree.

Note

If at least one client has a more up-to-date component than the OfficeScan server, manually update the OfficeScan server.

---

d. Select clients from the query result.

e. Click **Update Now** to force clients to download components.

Note

- To ensure that clients can upgrade the client program, disable the **Clients can update components but not upgrade the client program or deploy hot fixes** option in **Networked Computers** > **Client Management** > **Settings** > **Privileges and Other Settings**.
- Restart the computer instead of clicking **Update Now** to update the Common Firewall Driver.

---

f. To save the list of clients to a file, click **Export**.

6. View Compliance Report for scans.

For details about scans, see *Scan Compliance on page 14-57*.

a. Click the **Scan Compliance** tab.

b. Under **Computers with Outdated Scanning**, configure the following:

- Number of days a client has not performed Scan Now or Scheduled Scan
- Number of hours Scan Now or Scheduled Scan is running

> **Note**
>
> If the number of days or hours is exceeded, the client is treated as non-compliant.

c. Click **Assess** next to the **Client Tree Scope** section.

d. Under **Computers with Outdated Scanning**, check the number of clients that satisfy the scan criteria.

e. Click a number link to display all affected clients in the client tree.

f. Select clients from the query result.

g. Click **Scan Now** to initiate Scan Now on clients.

> **Note**
>
> To avoid repeating the scan, the **Scan Now** option will be disabled if Scan Now lasted more than the specified number of hours.

h. To save the list of clients to a file, click **Export**.

7. View Compliance Report for settings.

For details about settings, see *Settings on page 14-59*.

a. Click the **Settings** tab.

b. Under **Computers with Inconsistent Configuration Settings**, check the number of clients with settings inconsistent with the client tree domain settings.

c. Click a number link to display all affected clients in the client tree.

d. Select clients from the query result.

e. Click **Apply Domain Settings**.

f. To save the list of clients to a file, click **Export**.

Scheduled Compliance Reports

Security Compliance can generate Compliance Reports according to a schedule. Reports help you assess the security status of OfficeScan clients managed by the OfficeScan server.

For more information on Compliance Reports, see *Security Compliance for Managed Clients on page 14-53*.

Configuring Settings for Scheduled Compliance Reports

Procedure

1. Navigate to **Security Compliance** > **Compliance Assessment** > **Scheduled Compliance Report**.
2. Select **Enable scheduled reporting**.
3. Specify a title for the report.
4. Select one or all of the following:
   - *Services on page 14-54*
   - *Components on page 14-55*
   - *Scan Compliance on page 14-57*
   - *Settings on page 14-59*
5. Specify the email address(es) that will receive notifications about scheduled Compliance Reports.

   Note

   Configure email notification settings to ensure that email notifications can be sent successfully. For details, see *Administrator Notification Settings on page 13-29*.

6. Specify the schedule.

7. Click **Save**.

Security Compliance for Unmanaged Endpoints

Security Compliance can query unmanaged endpoints in the network to which the OfficeScan server belongs. Use Active Directory and IP addresses to query endpoints.

The security status of unmanaged endpoints can be any of the following:

TABLE 14-8. Security Status of Unmanaged Endpoints

STATUS	DESCRIPTION
Managed by another OfficeScan server	The OfficeScan clients installed on the computers are managed by another OfficeScan server. OfficeScan clients are online and run either this OfficeScan version or an earlier version.
No OfficeScan client installed	The OfficeScan client is not installed on the computer.
Unreachable	The OfficeScan server cannot connect to the computer and determine its security status.
Unresolved Active Directory Assessment	The computer belongs to an Active Directory domain but the OfficeScan server is unable to determine its security status. **Note** The OfficeScan server database contains a list of clients that the server manages. The server queries Active Directory for the computers' GUIDs and then compares them with GUIDs stored in the database. If a GUID is not in the database, the computer will fall under the Unresolved Active Directory Assessment category.

To run a security assessment, perform the following tasks:

1. Define the query scope. For details, see *Defining the Active Directory/IP Address Scope and Query on page 14-66*.
2. Check unprotected computers from the query result. For details, see *Viewing the Query Results on page 14-68*.

3. Install the OfficeScan client. For details, see *Installing with Security Compliance on page 5-59*.

4. Configure scheduled queries. For details, see *Configuring the Scheduled Query Assessment on page 14-69*.

Defining the Active Directory/IP Address Scope and Query

When querying for the first time, define the Active Directory/IP address scope, which includes Active Directory objects and IP addresses that the OfficeScan server will query on demand or periodically. After defining the scope, start the query process.

Note

To define an Active Directory scope, OfficeScan must first be integrated with Active Directory. For details about the integration, see *Active Directory Integration on page 2-32*.

Procedure

1. Navigate to **Security Compliance** > **Outside Server Management**.

2. On the **Active Directory/IP Address Scope** section, click **Define**. A new screen opens.

3. To define an Active Directory scope:

   a. Go to the **Active Directory Scope** section.

   b. Select **Use on-demand assessment** to perform real-time queries and get more accurate results. Disabling this option causes OfficeScan to query the database instead of each OfficeScan client. Querying only the database can be quicker but is less accurate.

   c. Select the objects to query. If querying for the first time, select an object with less than 1,000 accounts and then record how much time it took to complete the query. Use this data as your performance benchmark.

4. To define an IP address scope:

   a. Go to the **IP Address Scope** section.

b. Select **Enable IP Address Scope**.

c. Specify an IP address range. Click the plus or minus button to add or delete IP address ranges.

- For a pure IPv4 OfficeScan server, type an IPv4 address range.
- For a pure IPv6 OfficeScan server, type an IPv6 prefix and length.
- For a dual-stack OfficeScan server, type an IPv4 address range and/or IPv6 prefix and length.

The IPv6 address range limit is 16 bits, which is similar to the limit for IPv4 address ranges. The prefix length should therefore be between 112 and 128.

TABLE 14-9. Prefix Lengths and Number of IPv6 Addresses

LENGTH	NUMBER OF IPV6 ADDRESSES
128	2
124	16
120	256
116	4,096
112	65,536

5. Under Advanced Setting, specify ports used by OfficeScan servers to communicate with clients. Setup randomly generates the port number during OfficeScan server installation.

To view the communication port used by the OfficeScan server, go to **Networked Computers** > **Client Management** and select a domain. The port displays next to the IP address column. Trend Micro recommends keeping a record of port numbers for your reference.

a. Click **Specify ports**.

b. Type the port number and click **Add**. Repeat this step until you have all the port numbers you want to add.

c. Click **Save**.

6. To check a computer's connectivity using a particular port number, select **Declare a computer unreachable by checking port <x>**. When connection is not established, OfficeScan immediately treats the computer as unreachable. The default port number is 135.

   Enabling this setting speeds up the query. When connection to a computer cannot be established, the OfficeScan server no longer needs to perform all the other connection verification tasks before treating a computer as unreachable.

7. To save the scope and start the query, click **Save and re-assess**. To save the settings only, click **Save only**. The Outside Server Management screen displays the result of the query.

Note

The query may take a long time to complete, especially if the query scope is broad. Do not perform another query until the Outside Server Management screen displays the result. Otherwise, the current query session terminates and the query process restarts.

Viewing the Query Results

The query result appears under the Security Status section. An unmanaged endpoint will have one of the following statuses:

- Managed by another OfficeScan server
- No OfficeScan client installed
- Unreachable
- Unresolved Active Directory assessment

Recommended Tasks

1. In the **Security Status** section, click a number link to display all affected computers.
2. Use the search and advanced search functions to search and display only the computers that meet the search criteria.

If you use the advanced search function, specify the following items:

- IPv4 address range
- IPv6 prefix and length (prefix should be between 112 and 128)
- Computer name
- OfficeScan server name
- Active Directory tree
- Security status

OfficeScan will not return a result if the name is incomplete. Use the wildcard character (*) if unsure of the complete name.

3. To save the list of computers to a file, click **Export**.
4. For OfficeScan clients managed by another OfficeScan server, use the Client Mover tool to have these OfficeScan clients managed by the current OfficeScan server. For more information about this tool, see *Client Mover on page 14-21*.

Configuring the Scheduled Query Assessment

Configure the OfficeScan server to periodically query the Active Directory and IP addresses to ensure that security guidelines are implemented.

Procedure

1. Navigate to **Security Compliance** > **Outside Server Management**.
2. Click **Settings** on top of the client tree.
3. Enable scheduled query.
4. Specify the schedule.
5. Click **Save**.

Trend Micro Virtual Desktop Support

Optimize virtual desktop protection by using Trend Micro Virtual Desktop Support. This feature regulates tasks on OfficeScan clients residing in a single virtual server.

Running multiple desktops on a single server and performing on-demand scan or component updates consume significant amount of system resources. Use this feature to prohibit clients from running scans or updating components at the same time.

For example, if a VMware vCenter server has three virtual desktops running OfficeScan clients, OfficeScan can initiate Scan Now and deploy updates simultaneously to all three clients. Virtual Desktop Support recognizes that the clients are on the same physical server. Virtual Desktop Support allows a task to run on the first client and postpones the same task on the other two clients until the first client finishes the task.

Virtual Desktop Support can be used on the following platforms:

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

For more details on these platforms, refer to the VMware View, Citrix XenDesktop, or Microsoft Hyper-V websites.

Use the OfficeScan VDI Pre-Scan Template Generation Tool to optimize on-demand scan or remove GUIDs from base or golden images.

Virtual Desktop Support Installation

Virtual Desktop Support is a native OfficeScan feature but is licensed separately. After you install the OfficeScan server, this feature is available but is not functional. Installing this feature means downloading a file from the ActiveUpdate server (or a custom update source, if one has been set up). When the file has been incorporated into the OfficeScan server, you can activate Virtual Desktop Support to enable its full functionality. Installation and activation are performed from Plug-In Manager.

Note

Virtual Desktop Support is not fully supported in pure IPv6 environments. For details, see *Pure IPv6 Server Limitations on page A-3*.

Installing Virtual Desktop Support

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the **Trend Micro Virtual Desktop Support** section and click **Download**.

   The size of the package displays beside the **Download** button.

   Plug-In Manager stores the downloaded package to <*Server installation folder*> `\PCCSRV\Download\Product`.

   Note

   If Plug-In Manager is unable to download the file, it automatically re-downloads after 24 hours. To manually trigger Plug-In Manager to download the package, restart the OfficeScan Plug-In Manager service from the Microsoft Management Console.

3. Monitor the download progress. You can navigate away from the screen during the download.

   If you encounter problems downloading the package, check the server update logs on the OfficeScan product console. On the main menu, click **Logs** > **Server Update Logs**.

   After Plug-In Manager downloads the file, Virtual Desktop Support displays in a new screen.

   Note

   If Virtual Desktop Support does not display, see the reasons and solutions in *Troubleshooting Plug-In Manager on page 15-9*.

4. To install Virtual Desktop Support immediately, click **Install Now**. To install at a later time:
   a. Click **Install Later**.
   b. Open the **Plug-in Manager** screen.
   c. Go to the **Trend Micro Virtual Desktop Support** section and click **Install**.
5. Read the license agreement and accept the terms by clicking **Agree**.

   The installation starts.
6. Monitor the installation progress. After the installation, the Virtual Desktop Support version displays.

Virtual Desktop Support License

View, activate, and renew the Virtual Desktop Support license from Plug-In Manager.

Obtain the Activation Code from Trend Micro and then use it to enable the full functionality of Virtual Desktop Support.

Activating or Renewing Virtual Desktop Support

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the **Trend Micro Virtual Desktop Support** section and click **Manage Program**.
3. Click **View License Information**.
4. On the **Product License Details** screen that opens, click **New Activation Code**.
5. On the screen that opens, type the Activation Code and click **Save**.
6. Back in the Product License Details screen, click **Update Information** to refresh the screen with the new license details and the status of the feature. This screen also

provides a link to the Trend Micro website where you can view detailed information about your license.

Viewing License Information for Virtual Desktop Support

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** > **[Trend Micro Virtual Desktop Support] Manage Program** in the main menu.
2. Click **View License Information**.
3. View license details in the screen that opens.

   The Virtual Desktop Support License Details section provides the following information:

   - **Status**: Displays either "Activated", "Not Activated" or "Expired".
   - **Version**: Displays either "Full" or "Evaluation" version. If you have both full and evaluation versions, the version that displays is "Full".
   - **Expiration Date**: If Virtual Desktop Support has multiple licenses, the latest expiration date displays. For example, if the license expiration dates are 12/31/2010 and 06/30/2010, 12/31/2010 displays.
   - **Seats**: Displays how many OfficeScan clients can use Virtual Desktop Support
   - **Activation code**: Displays the activation code

   Reminders about licenses display during the following instances:

   If you have a full version license:

   - During the feature's grace period. The duration of the grace period varies by region. Please verify the grace period with your Trend Micro representative.
   - When the license expires and grace period elapses. During this time, you will not be able to obtain technical support.

   If you have an evaluation version license

- When the license expires. During this time, you will not be able to obtain technical support.

4. Click **View detailed license online** to view information about your license on the Trend Micro website.
5. To update the screen with the latest license information, click **Update Information**.

Virtual Server Connections

Optimize on-demand scan or component updates by adding VMware vCenter 4 (VMware View 4), Citrix XenServer 5.5 (Citrix XenDesktop 4), or Microsoft Hyper-V Server. OfficeScan servers communicate with the specified virtual servers to determine OfficeScan clients that are on the same physical server.

Adding Server Connections

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** > **[Trend Micro Virtual Desktop Support] Manage Program** in the main menu.
2. Select **VMware vCenter Server**, **Citrix XenServer**, or **Microsoft Hyper-V**.
3. Enable the connection to the server.
4. Specify the following information:
   - For VMware vCenter and Citrix XenServer servers:
     - IP address
     - Port
     - Connection protocol (HTTP or HTTPS)
     - Username
     - Password

- For Microsoft Hyper-V servers:
  - Host name or IP address
  - Domain\username

    Note

    The logon account must be a domain account in the Administrators group

  - Password

5. Optionally enable proxy connection for VMware vCenter or Citrix XenServer.
   a. Specify the proxy server name or IP address and port.
   b. If the proxy server requires authentication, specify the user name and password.
6. Click **Test connection** to verify that the OfficeScan server can successfully connect to the server.

   Note

   For details on troubleshooting Microsoft Hyper-V connections, see *Troubleshooting Microsoft Hyper-V Connections on page 14-77*.

7. Click **Save**.

Adding Additional Server Connections

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** > **[Trend Micro Virtual Desktop Support] Manage Program** in the main menu.
2. Click **Add new vCenter connection**, **Add new XenServer connection**, or **Add new Hyper-V connection**.
3. Repeat the steps to provide the proper server information.

4. Click **Save**.

Deleting a Connection Setting

Procedure

1. Open the OfficeScan web console and navigate to **Plug-in Manager** > **[Trend Micro Virtual Desktop Support] Manage Program** in the main menu.
2. Click **Delete this connection**.
3. Click **OK** to confirm the deletion of this setting.
4. Click **Save**.

Changing the VDI Scan Capacity

Administrators can increase the number of VDI endpoints that run concurrent scanning by modifying the `vdi.ini` file. Trend Micro recommends strictly monitoring the effect of changing the VDI capacity to ensure that system resources can handle any increased scanning.

Procedure

1. On the OfficeScan server computer, navigate to <*Server installation folder*>`PCCSRV\Private\vdi.ini`.
2. Locate the `[TaskController]` settings.

   The default TaskController settings are as follows:

   - For OfficeScan 10.5 clients:

     ```
     [TaskController]
     Controller_00_MaxConcurrentGuests=1
     Controller_01_MaxConcurrentGuests=3
     ```

Where:

- `Controller_00_MaxConcurrentGuests=1` equals the maximum number of clients that can perform scans concurrently.
- `Controller_01_MaxConcurrentGuests=3` equals the maximum number of clients that can perform updates concurrently.

- For OfficeScan 10.6 clients:

```
[TaskController]
Controller_02_MaxConcurrentGuests=1
Controller_03_MaxConcurrentGuests=3
```

Where:

- `Controller_02_MaxConcurrentGuests=1` equals the maximum number of clients that can perform scans concurrently.
- `Controller_03_MaxConcurrentGuests=3` equals the maximum number of clients that can perform updates concurrently.

3. Increase or decrease the count in each controller as necessary.

   The minimum value for all settings is 1.

   The maximum value for all settings is 65536.

4. Save and close the `vdi.ini` file.
5. Restart the OfficeScan Master Service.
6. Monitor the CPU, memory, and disk usage resources of the VDI endpoints. Modify the controller settings further to increase/decrease the number of concurrent scans to best suit the VDI environment by repeating steps 1 to 5.

Troubleshooting Microsoft Hyper-V Connections

The Microsoft Hyper-V connection uses Windows Management Instrumentation (WMI) and DCOM for client-server communication. Firewall policies may block this communication, causing an unsuccessful connection to the Hyper-V server.

The Hyper-V server listening port defaults to port 135 and then chooses a randomly configured port for further communication. If the firewall blocks WMI traffic or either of these two ports, communication with the server is unsuccessful. Administrators can modify the firewall policy to allow successful communication with the Hyper-V server.

Verify that all connection settings, including IP address, domain\username, and password are correct before performing the following firewall modifications.

Allowing WMI Communication through the Windows Firewall

Procedure

1. On the Hyper-V server, open the **Windows Firewall Allowed Programs** screen.

   On Windows 2008 R2 systems, go to **Control Panel** > **System and Security** > **Windows Firewall** > **Allow a program or feature through Windows Firewall**.

2. Select **Windows Management Instrumentation (WMI)**.

FIGURE 14-7. Windows Firewall Allowed Programs screen

3. Click **Save**.

4. Test the Hyper-V connection again.

Opening Port Communication through the Windows Firewall or a Third-party Firewall

Procedure

1. On the Hyper-V server, ensure that the firewall allows communication through port 135 and test the Hyper-V connection again.

   For details about opening ports, refer to your firewall documentation.

2. If the connection to the Hyper-V server is unsuccessful, configure WMI to use a fixed port.

   For details on *Setting Up a Fixed Port for WMI*, refer to:

   http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. Open ports 135 and the newly created fixed port (24158) for communication through the firewall.

4. Test the Hyper-V connection again.

VDI Pre-Scan Template Generation Tool

Use the OfficeScan VDI Pre-Scan Template Generation Tool to optimize on-demand scan or remove GUIDs from base or golden images. This tool scans the base or golden image and certifies the image. When scanning duplicates of this image, OfficeScan only checks parts that have changed. This ensures shorter scanning time.

Tip

Trend Micro recommends generating the pre-scan template after applying a Windows update or installing a new application.

Creating a Pre-scan Template

Procedure

1. On the OfficeScan server computer, browse to <*Server installation folder*> `\PCCSRV\Admin\Utility\TCacheGen`.

2. Choose a version of the VDI Pre-Scan Template Generation Tool. The following versions are available:

TABLE 14-10. VDI Pre-Scan Template Generation Tool Versions

FILE NAME	INSTRUCTION
TCacheGen.exe	Choose this file if you want to run the tool directly on a 32-bit platform.
TCacheGen_x64.exe	Choose this file if you want to run the tool directly on a 64-bit platform.
TCacheGenCli.exe	Choose this file if you want to run the tool from the command line interface of a 32-bit platform.
TCacheGenCli_x64.exe	Choose this file if you want to run the tool from the command line interface of a 64-bit platform.

3. Copy the version of the tool that you chose in the previous step to the <*Client installation folder*> of the base image.

4. Run the tool.

   - To run the tool directly:

     a. Double-click `TCacheGen.exe` or `TCacheGen_x64.exe`.

     b. Click **Generate Pre-Scan Template**.

   - To run the tool from the command line interface:

     a. Open a command prompt and change the directory to `<Client installation folder>`.

     b. Type the following command:

     ```
     TCacheGenCli Generate_Template
     ```

     Or

     ```
     TcacheGenCli_x64 Generate_Template
     ```

Note

The tool scans the image for security threats before generating the pre-scan template and removing the GUID.

After generating the pre-scan template, the tool unloads the OfficeScan client. Do not reload the OfficeScan client. If the OfficeScan client reloads, you will need to create the pre-scan template again.

Removing GUIDs from Templates

Procedure

1. On the OfficeScan server computer, browse to <*Server installation folder*> `\PCCSRV\Admin\Utility\TCacheGen`.

2. Choose a version of the VDI Pre-Scan Template Generation Tool. The following versions are available:

TABLE 14-11. VDI Pre-Scan Template Generation Tool Versions

FILE NAME	INSTRUCTION
TCacheGen.exe	Choose this file if you want to run the tool directly on a 32-bit platform.
TCacheGen_x64.exe	Choose this file if you want to run the tool directly on a 64-bit platform.
TCacheGenCli.exe	Choose this file if you want to run the tool from the command line interface of a 32-bit platform.
TCacheGenCli_x64.exe	Choose this file if you want to run the tool from the command line interface of a 64-bit platform.

3. Copy the version of the tool that you chose in the previous step to the <*Client installation folder*> of the base image.

4. Run the tool.

   - To run the tool directly:

a. Double-click `TCacheGen.exe` or `TCacheGen_x64.exe`.

b. Click **Remove GUID from Template**.

- To run the tool from the command line interface:

  a. Open a command prompt and change the directory to `<Client installation folder>`.

  b. Type the following command:

  ```
  TCacheGenCli Remove GUID
  ```

  Or

  ```
  TcacheGenCli_x64 Remove GUID
  ```

Global Client Settings

OfficeScan applies global client settings to all clients or only to clients with certain privileges.

Procedure

1. Navigate to **Networked Computers** > **Global Client Settings**.
2. Configure the following settings:

TABLE 14-12. Global Client Settings

SETTING	REFERENCE
Scan Settings	*Global Scan Settings on page 7-64*
Scheduled Scan Settings	*Global Scan Settings on page 7-64*
Virus/Malware Log Bandwidth Settings	*Global Scan Settings on page 7-64*
Firewall Settings	*Global Firewall Settings on page 12-24*

SETTING	REFERENCE
Firewall Log Count	*Global Firewall Settings on page 12-24*
Behavior Monitoring Settings	*Configuring Global Behavior Monitoring Settings on page 8-7*
C&C Callback Settings	*Configuring Global C&C Callback Settings on page 11-11*
Updates	*ActiveUpdate Server as the OfficeScan Client Update Source on page 6-34*
Reserved Disk Space	*Configuring Reserved Disk Space for OfficeScan Clients Updates on page 6-45*
Unreachable Network	*Unreachable Clients on page 14-41*
Alert Settings	*Configuring OfficeScan Client Update Notifications on page 6-46*
OfficeScan Service Restart	*OfficeScan Client Service Restart on page 14-11*
Proxy Configuration	*Automatic Proxy Settings for the OfficeScan Client on page 14-49*
Preferred IP Address	*Client IP Addresses on page 5-9*

3. Click **Save**.

Configuring Client Privileges and Other Settings

Grant users the privileges to modify certain settings and perform high level tasks on the OfficeScan client.

Note

Antivirus settings only appear after activating the OfficeScan Antivirus feature.

Tip

To enforce uniform settings and policies throughout the organization, grant limited privileges to users.

Procedure

1. Navigate to **Networked Computers** > **Client Management** or **Networked Computers** > **Client Management** .
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, configure the following user privileges:

TABLE 14-13. Client Privileges

CLIENT PRIVILEGES	REFERENCE
Roaming Privilege	*OfficeScan Client Roaming Privilege on page 14-19*
Scan Privileges	*Scan Type Privileges on page 7-49*
Scheduled Scan Privileges	*Scheduled Scan Privileges and Other Settings on page 7-52*
Firewall Privileges	*Firewall Privileges on page 12-22*
Behavior Monitoring Privileges	*Behavior Monitoring Privileges on page 8-10*
Mail Scan Privileges	*Mail Scan Privileges and Other Settings on page 7-58*
Toolbox Privileges	*Granting Users the Privilege to View the Toolbox Tab on page 17-6*
Proxy Setting Privileges	*Proxy Configuration Privileges for Clients on page 14-48*
Component Update Privileges	*Update Privileges and Other Settings for OfficeScan Clients on page 6-43*

Client Privileges	Reference
Uninstallation	*Granting the OfficeScan Client Uninstallation Privilege on page 5-69*
Unloading	*Granting the Client Unloading Privilege on page 14-18*

5. Click the **Other Settings** tab and configure the following settings:

Table 14-14. Other Client Settings

Setting	Reference
Update Settings	*Update Privileges and Other Settings for OfficeScan Clients on page 6-43*
Web Reputation Settings	*Web Threat Notifications for Client Users on page 11-11*
Behavior Monitoring Settings	*Behavior Monitoring Privileges on page 8-10*
C&C Contact Alert Settings	*C&C Contact Alert Notifications for Client Users on page 11-16*
Client Self-protection	*Client Self-protection on page 14-12*
Cache Settings for Scans	*Cache Settings for Scans on page 7-60*
Scheduled Scan Settings	*Granting Scheduled Scan Privileges and Displaying the Privilege Notification on page 7-53*
Client Security Settings	*OfficeScan Client Security on page 14-16*
POP3 Email Scan Settings	*Granting Mail Scan Privileges and Enabling POP3 Mail Scan on page 7-60*
Client Console Access Restriction	*OfficeScan Client Console Access Restriction on page 14-17*
Restart Notification	*Security Risk Notifications for OfficeScan Client Users on page 7-80*

6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Part IV

Providing Additional Protection

Chapter 15

Using Plug-In Manager

This chapter discusses how to set up Plug-In Manager and provides an overview of plug-in solutions delivered through Plug-In Manager.

Topics in this chapter:

- *About Plug-In Manager on page 15-2*
- *Plug-In Manager Installation on page 15-3*
- *Native OfficeScan Feature Management on page 15-4*
- *Managing Plug-in Programs on page 15-4*
- *Uninstalling Plug-In Manager on page 15-9*
- *Troubleshooting Plug-In Manager on page 15-9*

About Plug-In Manager

OfficeScan includes a framework called Plug-In Manager that integrates new solutions into the existing OfficeScan environment. To help ease the management of these solutions, Plug-In Manager provides at-a-glance data for the solutions in the form of widgets.

Note

None of the plug-in solutions currently support IPv6. The server can download these solutions but will not be able to deploy them to pure IPv6 OfficeScan clients or pure IPv6 hosts.

Plug-In Manager delivers two types of solutions:

- **Native OfficeScan Features**

  Some native OfficeScan features are licensed separately and activated through Plug-In Manager. In this release, two features fall under this category, namely, **Trend Micro Virtual Desktop Support** and **OfficeScan Data Protection**.

- **Plug-in programs**

  Plug-in programs are not part of the OfficeScan program. These programs have their own licenses and are managed mainly from their own management consoles, which are accessible from within the OfficeScan web console. Examples of plug-in programs are **Intrusion Defense Firewall**, **Trend Micro Security (for Mac)**, and **Trend Micro Mobile Security**.

This document provides a general overview of plug-in program installation and management and discusses plug-in program data available in widgets. Refer to the documentation for the specific plug-in program for details on configuring and managing the program.

Client-side Agents and Client Plug-in Manager

Some plug-in programs (such as Intrusion Defense Firewall) have a client-side agent that installs on Windows operating systems. The client-side agents can be managed through Client Plug-in Manager running under the process name `CNTAoSMgr.exe`.

`CNTAoSMgr.exe` is installed with and has the same system requirements as the OfficeScan client. The only additional requirement for `CNTAoSMgr.exe` is Microsoft XML Parser (MSXML) version 3.0 or later.

Note

Other client-side agents are not installed on Windows operating systems and are therefore not managed from Client Plug-in Manager. The Trend Micro Security (for Mac) client and Mobile Device Agent for Trend Micro Mobile Security are examples of these agents.

Widgets

Use widgets to view at-a-glance data for the individual plug-in solutions that you have deployed. Widgets are available on the OfficeScan server's Summary dashboard. A special widget, called **OfficeScan and Plug-ins Mashup**, combines data from OfficeScan clients and plug-in solutions and then presents the data in a client tree.

This Administrator's Guide provides an overview of widgets and the solutions that support widgets.

Plug-In Manager Installation

In previous Plug-In Manager versions, the Plug-In Manager installation package is downloaded from the Trend Micro ActiveUpdate server and then installed on the computer that hosts the OfficeScan server. In this version, the installation package is included in the OfficeScan server installation package.

Users who are new to OfficeScan will have both the OfficeScan server and Plug-In Manager installed after running the installation package and completing the installation. Users who are upgrading to this OfficeScan version and have used Plug-In Manager previously will need to stop the Plug-In Manager service before running the installation package.

Performing Post-installation Tasks

Perform the following after installing Plug-In Manager:

Procedure

1. Access the Plug-In Manager web console by clicking **Plug-in Manager** on the main menu of the OfficeScan web console.
2. Manage plug-in solutions.
3. Access the Summary dashboard on the OfficeScan web console to manage widgets for the plug-in solutions.

Native OfficeScan Feature Management

Native OfficeScan features are installed with OfficeScan and activated from Plug-In Manager. Some features, such as Trend Micro Virtual Desktop Support, are managed from Plug-In Manager, while others, such as OfficeScan Data Protection, are managed from the OfficeScan web console.

Managing Plug-in Programs

Install and activate plug-in programs independently of OfficeScan. Each plug-in provides its own console for product management. The management consoles are accessible from the OfficeScan web console.

Plug-in Program Installation

A plug-in program displays on the Plug-In Manager console. Use the console to download, install, and manage the program. Plug-In Manager downloads the installation package for a plug-in program from the Trend Micro ActiveUpdate server or from a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-In Manager downloads an installation package or starts the installation, Plug-In Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-In Manager does not support plug-in program installation or management from Trend Micro Control Manager's single sign-on function.

Installing a Plug-in Program

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the Plug-in Manager screen, go to the plug-in program section and click **Download**. The size of the plug-in program package displays beside the **Download** button. Plug-in Manager stores the downloaded package to `<Server installation folder>\PCCSRV\Download\Product`
3. Monitor the download progress. You can navigate away from the screen during the download.

FIGURE 15-1. Download progress for a plug-in program

After Plug-in Manager downloads the package, the plug-in program displays in a new screen.

Note

If you encounter problems downloading the package, check the server update logs on the OfficeScan product console. On the main menu, click **Logs** > **Server Update Logs**.

4. Click **Install Now** or **Install Later**.
   - If you clicked **Install Now**, check the installation progress.

- If you clicked **Install Later**, access the Plug-in Manager screen, go to the plug-in program section, click **Install**, and then check the installation progress.

After the installation, the current plug-in program version displays. You can then start managing the plug-in program.

Plug-in Program Management

Configure settings and perform program-related tasks from the plug-in program's management console, which is accessible from the OfficeScan web console. Tasks include activating the program and deploying its client-side agent to endpoints. Consult the documentation for the specific plug-in program for details on configuring and managing the program.

Managing a Plug-in Program

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager**.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.

FIGURE 15-2. Manage Program button for a plug-in program

Plug-in Program Upgrades

A new version of an installed plug-in program displays on the Plug-In Manager console. On the console, you can download the upgrade package and then upgrade the program. Plug-In Manager downloads the package from the Trend Micro ActiveUpdate server or

a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-In Manager downloads an installation package or starts the upgrade, Plug-In Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-In Manager does not support plug-in program upgrading from Trend Micro Control Manager's single sign-on function.

Upgrading a Plug-in Program

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Download**. The size of the upgrade package displays beside the **Download** button.
3. Monitor the download progress. Navigating away from the screen during the download does not affect the upgrade.

   Note

   If problems occur while downloading the package, check the server update logs on the OfficeScan web console. On the main menu, click **Logs** > **Server Update Logs**.

4. After Plug-In Manager downloads the package, a new screen displays.
5. Click **Upgrade Now** or **Upgrade Later**.
   - If you clicked **Upgrade Now**, check the upgrade progress.
   - If you clicked **Upgrade Later**, access the **Plug-in Manager** screen, go to the plug-in program section, click **Upgrade**, and then check the upgrade progress.

After the upgrade, the Plug-In Manager service may need to restart, causing the Plug-In Manager screen to be temporarily unavailable. When the screen becomes available, the current plug-in program version displays.

Plug-in Program Uninstallation

There are several ways to uninstall a plug-in program.

- Uninstall the plug-in program from the Plug-In Manager console.
- Uninstall the OfficeScan server, which uninstalls Plug-In Manager and all installed plug-in programs. For instructions on uninstalling the OfficeScan server, see the *OfficeScan Installation and Upgrade Guide*.

For plug-in programs with client-side agents:

- Consult the documentation for the plug-in program to see if uninstalling the plug-in program also uninstalls the client-side agent.
- For client-side agents installed on the same computer as the OfficeScan client, uninstalling the OfficeScan client uninstalls the client-side agents and Client Plug-in Manager (`CNTAoSMgr.exe`).

Uninstalling a Plug-in Program from the Plug-In Manager Console

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Uninstall**.

FIGURE 15-3. Uninstall button for a plug-in program

3. Monitor the uninstallation progress. You can navigate away from the screen during the uninstallation.

4. Refresh the **Plug-in Manager** screen after the uninstallation. The plug-in program is again available for installation.

Uninstalling Plug-In Manager

Uninstall the OfficeScan server to uninstall Plug-In Manager and all installed plug-in programs. For instructions on uninstalling the OfficeScan server, see the *OfficeScan Installation and Upgrade Guide*.

Troubleshooting Plug-In Manager

Check the OfficeScan server and OfficeScan client debug logs for Plug-In Manager and plug-in program debug information.

Plug-in Program Does not Display on the Plug-in Manager Console

A plug-in program available for download and installation may not display on the Plug-In Manager console for the following reasons:

Procedure

1. Plug-In Manager is still downloading the plug-in program, which may take some time if the program package size is large. Check the screen from time to time to see if the plug-in program displays.

Note

If Plug-In Manager is unable to download a plug-in program, it automatically re-downloads after 24 hours. To manually trigger Plug-In Manager to download the plug-in program, restart the OfficeScan Plug-In Manager service.

2. The server computer cannot connect to the Internet. If the server computer connects to the Internet through a proxy server, ensure that Internet connection can be established using the proxy settings.

3. The OfficeScan update source is not the ActiveUpdate server. On the OfficeScan web console, go to **Updates** > **Server** > **Update Source** and check the update source. If the update source is not the ActiveUpdate server, you have the following options:

   - Select the ActiveUpdate server as the update source.
   - If you select **Other Update Source**, select the first entry in the **Other update source** list as update source and verify that it can successfully connect to the ActiveUpdate server. Plug-In Manager only supports the first entry in the list.
   - If you select **Intranet location containing a copy of the current file**, ensure the computer in the Intranet can also connect to the ActiveUpdate server.

Client-side Agent Installation and Display Issues

Installation of a plug-in program's client-side agent may fail or the agent may not display in the OfficeScan client console for the following reasons:

Procedure

1. Client Plug-in Manager (`CNTAosMgr.exe`) is not running. In the OfficeScan client computer, open Windows Task Manager and run the `CNTAosMgr.exe` process.

2. The installation package for the client-side agent was not downloaded to the OfficeScan client computer folder located in `<Client installation folder>\AU_Data\AU_Temp\{xxx}AU_Down\Product`. Check `Tmudump.txt` located in `\AU_Data\AU_Log\` for the download failure reasons.

   Note

   If an agent successfully installs, agent information is available in `<Client installation folder>\AOSSvcInfo.xml`.

3. The agent installation was unsuccessful or requires further action. You can check the installation status from the plug-in program's management console and

perform actions such as restarting the OfficeScan client computer after installation or installing required operating system patches before installation.

The Apache Web Server Version is not Supported

Plug-In Manager handles some of the web requests using Internet Server Application Programming Interface (ISAPI). ISAPI is not compatible with Apache web server versions 2.0.56 to 2.0.59 and versions 2.2.3 to 2.2.4.

If your Apache web server runs any of the incompatible versions, you can replace it with version. 2.0.63, which is the version that OfficeScan and Plug-In Manager are using. This version is also compatible with ISAPI.

Procedure

1. Upgrade the OfficeScan server to the current version.
2. Back up the following files on the Apache2 folder on `<Server installation folder>`:
   - `httpd.conf`
   - `httpd.conf.tmbackup`
   - `httpd.default.conf`
3. Uninstall the incompatible Apache web server version from the **Add/Remove Programs** screen.
4. Install Apache web server 2.0.63.
   a. Launch `apache.msi` from `<Server installation folder>\Admin\Utility\Apache`.
   b. In the Server Information screen, type the required information.
   c. In the Destination Folder screen, change the destination folder by clicking **Change** and browsing to `<Server installation folder>`.
   d. Complete the installation.

5. Copy the backup files back to the Apache2 folder.
6. Restart the Apache web server service.

A Client-side Agent Cannot be Launched if the Automatic Configuration Script Setting on Internet Explorer Redirects to a Proxy Server

Client Plug-in Manager (`CNTAosMgr.exe`) is unable to launch a client-side agent because the agent launch command redirects to a proxy server. This problem only occurs if the proxy setting redirects the user's HTTP traffic to 127.0.0.1.

To resolve this issue, use a well-defined proxy server policy. For example, do not reroute HTTP traffic to 127.0.0.1.

If you need to use the proxy configuration that controls the 127.0.0.1 HTTP requests, perform the following tasks.

Procedure

1. Configure OfficeScan firewall settings on the OfficeScan web console.

   Note
   Perform this step only if you enables the OfficeScan firewall on OfficeScan clients.

   a. On the web console, go to **Networked Computers** > **Firewall** > **Policies** and click **Edit Exception Template**.
   b. On the Edit Exception Template screen, click **Add**.
   c. Use the following information:
      - **Name**: Your preferred name
      - **Action**: Allow network traffic
      - **Direction**: Inbound

- **Protocol**: TCP
- **Port(s)**: Any port number between 5000 and 49151

d. **IP address(es)**: Select **Single IP address** and specify your proxy server's IP address (recommended) or select **All IP addresses**.

e. Click **Save**.

f. Back on the Edit Exception Template screen, click **Save and Apply to Existing Policies**.

g. Go to **Networked Computers** > **Firewall** > **Profiles** and click **Assign Profile to Clients**.

If there is no firewall profile, create one by clicking Add. Use the following settings:

- **Name**: Your preferred name
- **Description**: Your preferred description
- **Policy**: All Access Policy

After saving the new profile, click **Assign Profile to Clients**.

2. Modify the `ofcscan.ini` file.

a. Open the `ofcscan.ini` file in `<Server installation folder>` using a text editor.

b. Search for **`[Global Setting]`** and add `FWPortNum=21212` to the next line. Change "21212" to the port number you specified in step c above.

For example:

```
[Global Setting]

FWPortNum=5000
```

c. Save the file.

3. On the web console, go to **Networked Computers** > **Global Client Settings** and click **Save**.

An Error in the System, Update Module, or Plug-in Manager Program occurred and the Error Message Provides a Certain Error Code

Plug-In Manager displays any of the following error codes in an error message. If you are unable to troubleshoot a problem after referring to the solutions provided in the table below, please contact your support provider.

TABLE 15-1. Plug-In Manager Error Codes

ERROR CODE	MESSAGE, CAUSE, AND SOLUTION
001	An error in the Plug-In Manager program occurred. The Plug-In Manager update module does not respond when querying the progress of an update task. The module or command handler may not have been not initialized. Restart the OfficeScan Plug-In Manager service and perform the task again.
002	A system error occurred. The Plug-In Manager update module is unable to open the registry key `SOFTWARE\TrendMicro\OfficeScan\service\AoS` because it may have been deleted. Perform the following steps: 1. Open Registry Editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`. Reset the value to 1.0.1000. 2. Restart the OfficeScan Plug-In Manager service. 3. Download/Uninstall the plug-in program.

Error Code	Message, Cause, and Solution
028	An update error occurred. Possible causes: • Plug-In Manager update module was unable to download a plug-in program. Verify that the network connection is functional, and then try again. • Plug-In Manager update module cannot install the plug-in program because the AU patch agent has returned an error. The AU patch agent is the program that launches installation of new plug-in programs. For the exact cause of the error, check the ActiveUpdate module debug log "`TmuDump.txt`" in `\PCCSRV\Web\Service\AU_Data\AU_Log`. Perform the following steps: 1. Open Registry Editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`. Reset the value to 1.0.1000. 2. Delete the plug-in program registry key `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_ADDON_xxxx`. 3. Restart the OfficeScan Plug-In Manager service. 4. Download and install the plug-in program.
170	A system error occurred. Plug-In Manager update module cannot process an incoming operation because it is currently handling another operation. Perform the task at a later time.
202	An error in the Plug-In Manager program occurred. The Plug-In Manager program cannot handle the task being executed on the Web console. Refresh the Web console or upgrade Plug-In Manager if an upgrade to the program is available.

Error Code	Message, Cause, and Solution
203	An error in the Plug-In Manager program occurred. The Plug-In Manager program encountered an interprocess communication (IPC) error when attempting to communicate with Plug-In Manager backend services. Restart the OfficeScan Plug-In Manager service and perform the task again.
Other error codes	A system error occurred. When downloading a new plug-in program, Plug-In Manager checks the plug-in program list from the ActiveUpdate server. Plug-In Manager was unable to obtain the list. Perform the following steps: 1. Open Registry Editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`. Reset the value to `1.0.1000`. 2. Restart the OfficeScan Plug-In Manager service. 3. Download and install the plug-in program.

Chapter 16

Using Policy Server for Cisco NAC

This chapter includes basic instructions to set up and configure Policy Server for Cisco NAC. For more information about configuring and administering Cisco Secure ACS servers and other Cisco products, see the most recent Cisco documentation available at the following website:

http://www.cisco.com/univercd/home/home.htm

Topics in this chapter:

- *About Policy Server for Cisco NAC on page 16-2*
- *Components and Terms on page 16-2*
- *Cisco NAC Architecture on page 16-6*
- *The Client Validation Sequence on page 16-7*
- *The Policy Server on page 16-9*
- *Policy Server System Requirements on page 16-19*
- *Cisco Trust Agent (CTA) Requirements on page 16-21*
- *Supported Platforms and Requirements on page 16-21*
- *Policy Server for NAC Deployment on page 16-23*

About Policy Server for Cisco NAC

Trend Micro Policy Server for Cisco Network Admission Control (NAC) evaluates the status of antivirus components on OfficeScan clients. Policy Server configuration options give you the ability to configure settings to perform actions on at-risk clients to bring them into compliance with the organization's security initiative.

These actions include the following:

- Instruct OfficeScan client computers to update their OfficeScan client components
- Enable Real-time Scan
- Perform Scan Now
- Display a notification message on OfficeScan client computers to inform users of the antivirus policy violation

For additional information on Cisco NAC technology, see the Cisco website at:

http://www.cisco.com/go/nac

Components and Terms

The following is a list of the various components and the important terms you need to become familiar with to understand and use Policy Server for Cisco NAC.

Components

The following components are necessary in the Trend Micro implementation of Policy Server for Cisco NAC:

TABLE 16-1. Policy Server for Cisco NAC Components

COMPONENT	DESCRIPTION
Cisco Trust Agent (CTA)	A program installed on a client computer that allows it to communicate with other Cisco NAC components

COMPONENT	DESCRIPTION
OfficeScan client computer	A computer with the OfficeScan client program installed. To work with Cisco NAC, the OfficeScan client computer also requires the Cisco Trust Agent.
Network Access Device	A network device that supports Cisco NAC functionality. Supported Network Access Devices include a range of Cisco routers, firewalls, and access points, as well as third-party devices with Terminal Access Controller Access Control System (TACACS+) or the Remote Dial-In User Service (RADIUS) protocol. For a list of supported devices, see *Supported Platforms and Requirements on page 16-21*.
Cisco Secure Access Control Server (ACS)	A server that receives OfficeScan client antivirus data from the client through the Network Access Device and passes it to an external user database for evaluation. Later in the process, the ACS server also passes the result of the evaluation, which may include instructions for the OfficeScan client, to the Network Access Device.
Policy Server	A program that receives and evaluates OfficeScan client antivirus data. After performing the evaluation, the Policy Server determines the actions the OfficeScan client should carry out and then notifies the OfficeScan client to perform the actions.
OfficeScan server	Reports the current Virus Pattern and Virus Scan Engine versions to the Policy Server, which uses this information to evaluate the OfficeScan client's antivirus status.

Terms

Become familiar with the following terms related to Policy Server for Cisco NAC:

TABLE 16-2. Policy Server for Cisco NAC Terms

TERM	DEFINITION
Security posture	The presence and currency of antivirus software on an OfficeScan client. In this implementation, security posture refers to whether or not the OfficeScan client program exists on client computers, the status of certain OfficeScan client settings, and whether or not the Virus Scan Engine and Virus Pattern are up-to-date.
Posture token	Created by the Policy Server after OfficeScan client validation. It includes information that tells the OfficeScan client to perform a set of specified actions, such as enabling Real-time Scan or updating antivirus components.
Client validation	The process of evaluating client security posture and returning the posture token to the OfficeScan client
Policy Server rule	Guidelines containing configurable criteria the Policy Server uses to measure OfficeScan client security posture. A rule also contains actions for the OfficeScan client and the Policy Server to carry out if the security posture information matches the criteria (see *Policy Server Policies and Rules on page 16-10* for detailed information).
Policy Server policy	A set of rules against which the Policy Server measures the security posture of OfficeScan clients. Policies also contain actions that OfficeScan clients and the Policy Server carry out if the criteria in the rules associated with the policy do not match the security posture (see *Policy Server Policies and Rules on page 16-10* for detailed information).
Authentication, Authorization, and Accounting (AAA)	Describes the three main services used to control end-user OfficeScan client access to computer resources. Authentication refers to identifying a client, usually by having the user enter a user name and password. Authorization refers to the privileges the user has to issue certain commands. Accounting refers to a measurement, usually kept in logs, of the resources utilized during a session. The Cisco Secure Access Control Server (ACS) is the Cisco implementation of an AAA server.
Certificate Authority (CA)	An authority on a network that distributes digital certificates for the purposes of performing authentication and securing connections between computers and/or servers.

Term	Definition
Digital Certificates	An attachment used for security. Most commonly, certificates authenticate clients with servers, such as a web server, and contain the following: user identity information, a public key (used for encryption), and a digital signature of a Certificate authority (CA) to verify that the certificate is valid.
Remote Authentication Dial-In User Service (RADIUS)	An authentication system requiring clients to enter a user name and password. Cisco Secure ACS servers support RADIUS.
Terminal Access Controller Access Control System (TACACS+)	A security protocol enabled through AAA commands used for authenticating end-user clients. Cisco ACS servers support TACACS+.

Cisco NAC Architecture

The following diagram illustrates a basic Cisco NAC architecture.

FIGURE 16-1. Basic Cisco NAC architecture

The OfficeScan client in this figure has a CTA installation and is only able to access the network through a Network Access Device that supports Cisco NAC. The Network Access Device is between the client and the other Cisco NAC components.

Note

The architecture of your network may differ based on the presence of proxy servers, routers, or firewalls.

The Client Validation Sequence

OfficeScan client validation refers to the process of evaluating an OfficeScan client's security posture and returning instructions for the OfficeScan client to perform if the Policy Server considers it to be at-risk. The Policy Server validates an OfficeScan client by using configurable rules and policies.

Below is the sequence of events that occurs when an OfficeScan client attempts to access the network:

1. The Cisco Network Access Device starts the validation sequence by requesting the security posture of the client when it attempts to access the network.
2. The Network Access Device then passes the security posture to the ACS server.
3. The ACS server passes the security posture to the Policy Server, which performs the evaluation.
4. In a separate process, the Policy Server periodically polls the OfficeScan server for Virus Pattern and Virus Scan Engine version information to keep its data current. It then uses a policy you configure to perform a comparison of this information with the OfficeScan client security posture data.
5. Following that, the Policy Server creates a posture token, and passes it back to the OfficeScan client.

6. The OfficeScan client performs the actions configured in the posture token.

FIGURE 16-2. Network access validation sequence

The Policy Server

The Policy Server is responsible for evaluating the OfficeScan client's security posture and for creating the posture token. It compares the security posture with the latest versions of the Virus Pattern and Virus Scan Engine received from the OfficeScan server to which the OfficeScan client is a member. It returns the posture token to the Cisco Secure ACS server, which in turn passes it to the OfficeScan client from the Cisco Network Access Device.

Installing additional Policy Servers on a single network can improve performance when a large number of clients simultaneously attempt to access the network. These Policy Servers can also act as a backup if a Policy Server becomes inoperable. If there are multiple OfficeScan servers on a network, the Policy Server handles requests for all OfficeScan servers registered to it. Likewise, multiple Policy Servers can handle requests for a single OfficeScan server registered to all the Policy Servers. The following figure illustrates the relationship of multiple OfficeScan servers and Policy Servers.

FIGURE 16-3. Multiple Policy Server/OfficeScan server relationship

You can also install the Policy Server on the same computer as the OfficeScan server.

Policy Server Policies and Rules

Policy Servers use configurable rules and policies to help enforce your organization's security guidelines.

Rules include specific criteria that Policy Servers use to compare with the security posture of OfficeScan clients. If the client security posture matches the criteria you configure in a rule, the client and server carry out the actions you specify in the rule (see *Policy Server and OfficeScan Client Actions on page 16-12*).

Policies include one or more rules. Assign one policy to each registered OfficeScan server on the network for both outbreak mode and normal mode (see *Security Risk Outbreaks on page 7-94*for more information on network modes).

If the OfficeScan client security posture matches the criteria in a rule that belongs to the policy, the OfficeScan client carries out the actions you configure in the rule. However, if the OfficeScan client security posture does not match any of the criteria in any of the rules associated with the policy, you can still configure default actions in the policy for the OfficeScan client and server to carry out (see *Policy Server and OfficeScan Client Actions on page 16-12*).

Tip

If you want certain OfficeScan clients in an OfficeScan domain to have different outbreak and normal mode policies from other OfficeScan clients in the same domain, Trend Micro suggests restructuring the domains to group OfficeScan clients with similar requirement (see *OfficeScan Domains on page 2-48*).

Rule Composition

Rules include security posture criteria, default responses associated with OfficeScan clients, and actions that OfficeScan clients and the Policy Server perform.

Security Posture Criteria

Rules include the following security posture criteria:

- **Client machine state**: If the OfficeScan client computer is in the booting state or not
- **Client Real-time Scan status**: If Real-time Scan is enabled or disabled
- **Client scan engine version currency**: If the Virus Scan Engine is up-to-date
- **Client virus pattern file status**: How up-to-date the Virus Pattern is. The Policy Server determines this by checking one of the following:
  - If the Virus Pattern is a certain number of versions older than the Policy Server version
  - If the Virus Pattern became available a certain number of days prior to the validation

Default Responses for Rules

Responses help you understand the condition of OfficeScan clients on the network when OfficeScan client validation occurs. The responses, which appear in the Policy Server client validation logs, correspond to posture tokens. Choose from the following default responses:

- **Healthy**: The OfficeScan client computer conforms to the security policies and is not infected.
- **Checkup**: The OfficeScan client needs to update its antivirus components.
- **Infected**: The OfficeScan client computer is infected or is at risk of infection.
- **Transition**: The OfficeScan client computer is in the booting state.
- **Quarantine**: The OfficeScan client computer is at high risk of infection and requires quarantine.
- **Unknown**: Any other condition

Note

You cannot add, delete, or modify responses.

Policy Server and OfficeScan Client Actions

If the OfficeScan client security posture matches the rule criteria, the Policy Server can create an entry in a Policy Server client validation log (see *Client Validation Logs on page 16-42* for more information).

If the OfficeScan client security posture matches the rule criteria, the OfficeScan client can carry out the following actions:

- Enable client Real-time Scan so the OfficeScan client can scan all opened or saved files (see *Real-time Scan on page 7-14* for more information)
- Update all OfficeScan components (see *OfficeScan Components and Programs on page 6-2* for more information)
- Scan the OfficeScan client (Scan Now) after enabling Real-time Scan or after an update
- Display a notification message on the OfficeScan client computer

Default Rules

Policy Server provides default rules to give you a basis for configuring settings. The rules cover common and recommended security posture conditions and actions. The following rules are available by default:

TABLE 16-3. Default Rules

RULE NAME	MATCHING CRITERIA	RESPONSE IF CRITERIA MATCHED	SERVER ACTION	OFFICESCAN CLIENT ACTION
Healthy	Real-time Scan status is enabled and Virus Scan Engine and Virus Pattern are up-to-date.	Healthy	None	None

Rule Name	Matching Criteria	Response if Criteria Matched	Server Action	OfficeScan client Action
Checkup	Virus Pattern version is at least one version older than the version on the OfficeScan server to which the OfficeScan client is registered.	Checkup	Create entry in client validation log	• Update components • Perform automatic Cleanup Now on the OfficeScan client after enabling Real-time Scan or after an update • Display notification message on the OfficeScan client computer **Tip** If you use this rule, use automatic deployment. This helps ensure that OfficeScan clients receive the latest Virus Pattern immediately after the OfficeScan downloads new components.
Transition	OfficeScan client computer is in the booting state.	Transition	None	None

Rule Name	Matching Criteria	Response if Criteria Matched	Server Action	OfficeScan client Action
Quarantine	Virus Pattern version is at least five versions older than the version on the OfficeScan server to which the OfficeScan client is registered.	Quarantine	Create entry in client validation log	• Update components • Perform automatic Cleanup Now and Scan Now on the OfficeScan client after enabling Real-time Scan or after an update • Display notification message on the OfficeScan client computer
Not protected	Real-time Scan status is disabled.	Infected	Create entry in client validation log	• Enable OfficeScan client Real-time Scan • Display notification message on the OfficeScan client computer

Policy Composition

Policies include of any number of rules and default responses and actions.

- **Rule Enforcement**

  Policy Server enforces rules in a specific order, which allows you to prioritize rules. Change the order of rules, add new ones, and remove existing ones from a policy.

- **Default Responses for Policies**

  As with rules, policies include default responses to help you understand the condition of OfficeScan clients on the network when client validation occurs. However, the default responses are associated with clients only when client security posture does NOT match any rules in the policy.

The responses for policies are the same as those for rules (see *Default Responses for Rules on page 16-11* for the list of responses).

- **Policy Server and OfficeScan client Actions**

  The Policy Server enforces rules to clients by subjecting OfficeScan client posture information to each of the rules associated with a policy. Rules are applied top-down based on the rules in use specified on the web console. If the OfficeScan client posture matches any of the rules, the action corresponding to the rule is deployed to the OfficeScan client. If no rules match, the default rule applies and the action corresponding to the default rule is deployed to clients.

  Default Outbreak Mode Policy evaluates OfficeScan clients using the "Healthy" rule. It forces all OfficeScan clients that do not match this rule to immediately implement the actions for the "Infected" response.

  Default Normal Mode Policy evaluates OfficeScan clients using all the non-"Healthy" rules (Transition, Not Protected, Quarantine, CheckUp). It classifies all OfficeScan clients that do not match any of these rules as "healthy" and applies the actions for the "Healthy" rule.

Default Policies

Policy Server provides default policies to give you a basis for configuring settings. Two policies are available, one for normal mode and one for outbreak mode.

TABLE 16-4. Default Policies

POLICY NAME	DESCRIPTION
Default Normal Mode Policy	• Default rules associated with policy: Transition, Not protected, Quarantine, and Checkup • Response if none of the rules match: Healthy • Server action: None • OfficeScan client action: None

Policy Name	Description

Default Outbreak Mode Policy	• Default rules associated with policy: Healthy
	• Response if none of the rules match: Infected
	• Server action: Create entry in client validation log
	• OfficeScan client action:
	  • Enable client Real-time Scan
	  • Update components
	  • Perform Scan Now on the OfficeScan client after enabling Real-time Scan or after an update
	  • Display a notification message on the OfficeScan client computer

Synchronization

Regularly synchronize the Policy Server with registered OfficeScan servers to keep the Policy Server versions of the Virus Pattern, Virus Scan Engine, and server outbreak status (normal mode or outbreak mode) up-to-date with those on the OfficeScan server. Use the following methods to perform synchronization:

- **Manually**: Perform synchronization at any time on the Summary screen (see *Summary Information for a Policy Server on page 16-40*).
- **By schedule**: Set a synchronization schedule (see *Administrative Tasks on page 16-43*).

Certificates

Cisco NAC technology uses the following digital certificates to establish successful communication between various components:

TABLE 16-5. Cisco NAC Certificates

CERTIFICATE	DESCRIPTION
ACS certificate	Establishes trusted communication between the ACS server and the Certificate Authority (CA) server. The Certificate Authority server signs the ACS certificate before you save it on the ACS server.
CA certificate	Authenticates OfficeScan clients with the Cisco ACS server. The OfficeScan server deploys the CA certificate to both the ACS server and to OfficeScan clients (packaged with the Cisco Trust Agent).
Policy Server SSL certificate	Establishes secure HTTPS communication between the Policy Server and ACS server. The Policy Server installer automatically generates the Policy Server SSL certificate during Policy Server installation. The Policy Server SSL certificate is optional. However, use it to ensure that only encrypted data transmits between the Policy Server and ACS server.

The figure below illustrates the steps involved in creating and deploying ACS and CA certificates:

FIGURE 16-4. ACS and CA certificate creation and deployment

1. After the ACS server issues a certificate signing request to the CA server, the CA issues a certificated called ACS certificate. The ACS certificate then installs on the ACS server. See *Cisco Secure ACS Server Enrolment on page 16-24* for more information.

2. A CA certificate is exported from the CA server and installed on the ACS server. See *CA Certificate Installation on page 16-24* for detailed instructions.

3. A copy of the same CA certificate is saved on the OfficeScan server.

4. The OfficeScan server deploys the CA certificate to OfficeScan clients with the CTA. See *Cisco Trust Agent Deployment on page 16-27* for detailed instructions.

The CA Certificate

OfficeScan clients with CTA installations authenticate with the ACS server before communicating client security posture. Several methods are available for authentication (see the Cisco Secure ACS documentation for details). For example, you may already have enabled computer authentication for Cisco Secure ACS using Windows Active Directory, which you can configure to automatically produce an end user client certificate when adding a new computer in Active Directory. For instructions, see Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows.

For users with their own Certificate Authority (CA) server, but whose end user clients do not yet have certificates, OfficeScan provides a mechanism to distribute a root certificate to OfficeScan clients. Distribute the certificate during OfficeScan installation or from the OfficeScan web console. OfficeScan distributes the certificate when it deploys the Cisco Trust Agent to OfficeScan clients (see *Cisco Trust Agent Deployment on page 16-27*).

Note

If you already acquired a certificate from a Certificate Authority or produced your own certificate and distributed it to end user OfficeScan clients, it is not necessary to do so again.

Before distributing the certificate to OfficeScan clients, enroll the ACS server with the CA server and then prepare the certificate (see *Cisco Secure ACS Server Enrolment on page 16-24* for details).

Policy Server System Requirements

Before installing Policy Server, check if the computer meets the following requirements:

TABLE 16-6. Policy Server System Requirements

HARDWARE/ SOFTWARE	REQUIREMENTS
Operating System	• Windows 2000 Professional with Service Pack 4 • Windows 2000 Server with Service Pack 4 • Windows 2000 Advanced Server with Service Pack 4 • Windows XP Professional with Service Pack 3 or later, 32-bit and 64-bit • Windows Server 2003 (Standard and Enterprise Editions) with Service Pack 2 or later, 32-bit and 64-bit
Hardware	• 300MHz Intel Pentium II processor or equivalent • 128MB of RAM • 300MB of available disk space • Monitor that supports 800 x 600 resolution at 256 colors or higher
Web Server	• Microsoft Internet Information Server (IIS) versions 5.0 or 6.0 • Apache web server 2.0 or later (for Windows 2000/XP/Server 2003 only)
Web Console	To use the OfficeScan server web console, the following are required: • 133MHz Intel Pentium processor or equivalent • 64MB of RAM • 30MB of available disk space • Monitor that supports 800 x 600 resolution at 256 colors or higher • Microsoft Internet Explorer 5.5 or later

Cisco Trust Agent (CTA) Requirements

Before deploying Cisco Trust Agent to client computers, check if the computers meet the following requirements:

Note

Cisco Trust Agent does not support IPv6. You cannot deploy the agent to pure IPv6 endpoints.

TABLE 16-7. Cisco Trust Agent (CTA) Requirements

HARDWARE/ SOFTWARE	REQUIREMENTS
Operating System	• Windows 2000 Professional and Server with Service Pack 4 • Windows XP Professional with Service Pack 3 or later, 32-bit • Windows Server 2003 (Standard and Enterprise Editions) with Service Pack 2 or later, 32-bit
Hardware	• 200MHz single or multiple Intel Pentium processors • 128MB of RAM for Windows 2000 • 256MB of RAM for Windows XP and Windows Server 2003 • 5MB of available disk space (20MB recommended)
Others	• Windows Installer 2.0 or later

Supported Platforms and Requirements

The following platforms support the Cisco NAC functionality:

TABLE 16-8. Supported Platforms and Requirements

SUPPORTED PLATFORM	MODELS	IOS IMAGES	MINIMUM MEMORY/ FLASH
Routers			
Cisco 830, 870 series	831, 836, 837	IOS 12.3(8) or later	48MB/8MB
Cisco 1700 series	1701, 1711, 1712, 1721, 1751, 1751-V, 1760	IOS 12.3(8) or later	64MB/16MB
Cisco 1800 series	1841	IOS 12.3(8) or later	128MB/32MB
Cisco 2600 series	2600XM, 2691	IOS 12.3(8) or later	96MB/32MB
Cisco 2800 series	2801, 2811, 2821, 2851	IOS 12.3(8) or later	128MB/64MB
Cisco 3600 series	3640/3640A, 3660-ENT series	IOS 12.3(8) or later	48MB/16MB
Cisco 3700 series	3745, 3725	IOS 12.3(8) or later	128MB/32MB
Cisco 3800 series	3845, 3825	IOS 12.3(8) or later	256MB/64MB
Cisco 7200 series	720x, 75xx	IOS 12.3(8) or later	128MB/48MB
VPN Concentrators			
Cisco VPN 3000 Series	3005 - 3080	V4.7 or later	N/A
Switches			
Cisco Catalyst 2900	2950, 2970	IOS 12.1(22)EA5	N/A
Cisco Catalyst 3x00	3550, 3560, 3750	IOS 12.2(25)SEC	N/A
Cisco Catalyst 4x00	Supervisor 2+ or higher	IOS 12.2(25)EWA	N/A

Supported Platform	Models	IOS Images	Minimum Memory/ Flash
Cisco Catalyst 6500	6503, 6509, Supervisor 2 or higher	CatOS 8.5 or later	Sup2 - 128MB, Sup32 - 256MB, Sup720 - 512MB
Wireless Access Points			
Cisco AP1200 Series	1230	N/A	N/A

Policy Server for NAC Deployment

The following procedures are for reference only and may be subject to change depending on updates to either the Microsoft and/or Cisco interfaces.

Before performing any of the tasks, verify that the Network Access Device(s) on the network are able to support Cisco NAC (see *Supported Platforms and Requirements on page 16-21*). See the device documentation for set up and configuration instructions. Also, install the ACS server on the network. See the Cisco Secure ACS documentation for instructions.

1. Install the OfficeScan server on the network (see the *Installation and Upgrade Guide*).

2. Install the OfficeScan client program on all clients whose antivirus protection you want Policy Server to evaluate.

3. Enroll the Cisco Secure ACS server. Establish a trusted relationship between the ACS server and a Certificate Authority (CA) server by having the ACS server issue a certificate signing request. Then save the CA-signed certificate (called the ACS certificate) on the ACS server (see *Cisco Secure ACS Server Enrolment on page 16-24* for details).

4. Export the CA certificate to the ACS server and store a copy on the OfficeScan server. This step is only necessary if you have not deployed a certificate to clients and the ACS server (see *CA Certificate Installation on page 16-24*).

5. Deploy the Cisco Trust Agent and the CA certificate to all OfficeScan clients so clients can submit security posture information to the Policy server (see *Cisco Trust Agent Deployment on page 16-27*).

6. Install the Policy Server for Cisco NAC to handle requests from the ACS server (see *Policy Server for Cisco NAC Installation on page 16-32*).

7. Export an SSL certificate from the Policy Server to the Cisco ACS server to establish secure SSL communications between the two servers (see *Policy Server for Cisco NAC Installation on page 16-32*).

8. Configure the ACS server to forward posture validation requests to the Policy Server (see *ACS Server Configuration on page 16-37*).

9. Configure the Policy Server for NAC. Create and modify Policy Server rules and policies to enforce your organization's security strategy for OfficeScan clients (see *Policy Server for Cisco NAC Configuration on page 16-38*).

Cisco Secure ACS Server Enrolment

Enroll the Cisco Secure ACS server with the Certificate Authority (CA) server to establish a trust relationship between the two servers. The following procedure is for users running a Windows Certification Authority server to manage certificates on the network. Refer to the vendor documentation if using another CA application or service and see the ACS server documentation for instructions on how to enroll a certificate.

CA Certificate Installation

The OfficeScan client authenticates with the ACS server before it sends security posture data. The CA certificate is necessary for this authentication to take place. First, export the CA certificate from the CA server to both the ACS server and the OfficeScan server, then create the CTA agent deployment package. The package includes the CA certificate (see *The CA Certificate on page 16-19* and *Cisco Trust Agent Deployment on page 16-27*).

Perform the following to export and install the CA certificate:

- Export the CA certificate from the Certificate Authority server

- Install it on the Cisco Secure ACS server
- Store a copy on the OfficeScan server

Note

The following procedure is for users running a Windows Certification Authority server to manage certificates on the network. Refer to the vendor documentation if you use another Certification Authority application or service.

Exporting and Installing the CA Certificate for Distribution

Procedure

1. Export the certificate from the Certification Authority (CA) server:

   a. On the CA server, click **Start** > **Run**.

      The Run screen opens.

   b. Type `mmc` in the **Open** box.

      A new management console screen opens.

   c. Click **File** > **Add/Remove Snap-in**.

      The **Add/Remove Snap-in** screen appears.

   d. Click **Certificates** and click **Add**.

      The **Certificates snap-in** screen opens.

   e. Click **Computer Account** and click **Next**.

      The **Select Computer** screen opens.

   f. Click **Local Computer** and click **Finish**.

   g. Click **Close** to close the **Add Standalone Snap-in** screen.

   h. Click **OK** to close the **Add/remove Snap-in** screen.

i. In the tree view of the console, click **Certificates** > **Trusted Root** > **Certificates**.

j. Select the certificate to distribute to clients and the ACS server from the list.

k. Click **Action** > **All Tasks** > **Export...**.

The **Certificate Export Wizard** opens.

l. Click **Next**.

m. Click **DER encoded binary x.509** and click **Next**.

n. Enter a file name and browse to a directory to which to export the certificate.

o. Click **Next**.

p. Click **Finish**.

A confirmation window displays.

q. Click **OK**.

2. Install the certificate on Cisco Secure ACS.

a. Click **System Configuration** > **ACS Certificate Setup** > **ACS Certification Authority Setup**.

b. Type the full path and file name of the certificate in the **CA certificate file** field.

c. Click **Submit**. Cisco Secure ACS prompts you to restart the service.

d. Click **System Configuration** > **Service Control**.

e. Click **Restart**. Cisco Secure ACS restarts.

f. Click **System Configuration** > **ACS Certificate Management** > **Edit Certificate Trust List**. The **Edit Certificate Trust List** screen appears.

g. Select the check box that corresponds to the certificate you imported in step b and click **Submit**. Cisco Secure ACS prompts you to restart the service.

h. Click **System Configuration** > **Service Control**.

i. Click **Restart**. Cisco Secure ACS restarts.

3. Copy the certificate (.cer file) to the OfficeScan server computer to deploy it to the client with the CTA (see for more information).

Note

Store the certificate on a local drive and not on mapped drives.

Cisco Trust Agent Deployment

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

Note

Cisco Trust Agent does not support IPv6. You cannot deploy the agent to pure IPv6 endpoints.

Deploying CTA During OfficeScan Server Installation

If you already prepared a CA certificate before installing the OfficeScan server, deploy CTA during OfficeScan server installation. The option to deploy CTA is on the **Install Other OfficeScan Programs** screen of Setup. For instructions on installing the OfficeScan server, see the *Installation and Upgrade Guide*.

Procedure

1. On the **Install Other OfficeScan Programs** screen, select **Cisco Trust Agent for Cisco NAC**.
2. If you have already distributed certificates to Cisco Secure NAC end user clients, click **Next**, otherwise perform the following to distribute the certificates:
   a. Click **Import Certificate**.
   b. Locate and select the prepared certificate file and click **OK**.

      For instructions on preparing a certificate file, see *CA Certificate Installation on page 16-24*.

c. Click **Next**.

3. Continue with OfficeScan server installation.

Deploying CTA from the OfficeScan Web Console

If you did not select the option to install/upgrade CTA during server installation, you can do so from the web console. Before installing/upgrading CTA, deploy the client certificate to OfficeScan clients.

Note

A Certificate Authority (CA) server generates the client certificate file. Request a certificate file from your Trend Micro representative.

When you are ready to install/upgrade, check the version of the CTA to be installed in **Cisco NAC** > **Agent Management**, then install CTA to OfficeScan clients in **Cisco NAC** > **Agent Deployment**. The Agent Deployment screen also gives you the option to uninstall CTA.

Install Windows Installer 2.0 for NT 4.0 on OfficeScan clients running Windows 2000/XP before deploying CTA.

Importing the Client Certificate

The client (or CA) certificate authenticates end-user OfficeScan clients with the Cisco ACS server. The OfficeScan server deploys the CA certificate to OfficeScan clients along with the Cisco Trust Agent (CTA). Therefore, import the certificate to the OfficeScan server before deploying CTA.

Procedure

1. Open the OfficeScan server web console and click **Cisco NAC** > **Client Certificate**.

2. Type the exact file path of the certificate.

3. Type the full path and file name of the prepared CA certificate stored on the server (for example: `C:\CiscoNAC\certificate.cer`). For instructions on preparing a CA certificate, see *CA Certificate Installation on page 16-24*.

4. Click **Import**.

   To clear the field, click **Reset**.

Cisco Trust Agent Version

Before installing CTA to clients, check the CTA version (Cisco Trust Agent or Cisco Trust Agent Supplicant) to install. The only difference between these two versions is that the Supplicant package provides layer 2 authentication for the computer and end user.

If the Cisco NAC Access Control Server (ACS) is version 4.0 or later, upgrade the Cisco Trust Agent on the clients to version 2.0 or later.

Checking the CTA Version

Procedure

1. Open the OfficeScan server web console and click **Cisco NAC** > **Agent Management**.

2. Click **Use <CTA version>**.

   The OfficeScan server starts to use the new version.

Manually Replacing the CTA Package

Manually replace the CTA package on the OfficeScan server if there is a specific version you want to use.

Procedure

1. In the CTA version you want to use, copy the CTA `.msi` file to one of the following folders:

- <*Server installation folder*>\PCCSRV\Admin\Utility\CTA\CTA-Package
- <Server installation folder>\PCCSRV\Admin\Utility\CTA\CTA-Supplicant-Package

2. Copy the following files to <Server installation folder>\ PCCSRV \Admin\Utility\CTA\PosturePlugin: TmabPP.dll, tmabpp.inf and TmAbPpAct.exe.
3. In the web console, go to **Cisco NAC** > **Agent Management** and click **Use <CTA version>**.

After agent upgrade, the files will be zipped to PostureAgent.zip as a CTA deployment package under <Server installation folder>\PCCSRV\download\Product.

Deploying the Cisco Trust Agent

Deploy the Cisco Trust Agent to enable the OfficeScan client to report antivirus information to Cisco ACS.

Procedure

1. Navigate to **Cisco NAC** > **Agent Deployment**.
2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.
3. Click **Deploy Agent**.
4. If you did not accept the terms of the Cisco License Agreement during the installation of the OfficeScan server, the license information appears. Read the license agreement and click **Yes** to agree to the terms.
5. Select **Install/Upgrade Cisco Trust Agent**.
6. (Optional) Select **Uninstall Cisco Trust Agent when OfficeScan client is uninstalled**.

Note

Also use this screen to uninstall or preserve CTA status on clients.

Preserving the CTA status means preventing an installation from overwriting CTA if one is already installed. Unless you are upgrading or are certain that you have never installed CTA on any of the clients you selected, you may want to use this option, otherwise the server will reinstall CTA and your settings will be lost.

7. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Note

If the OfficeScan client to which you deploy the agent is not online when you click **Install Cisco Trust Agent**, OfficeScan automatically fulfills the task request when the OfficeScan client becomes online.

Cisco Trust Agent Installation Verification

After deploying the CTA to OfficeScan clients, verify successful installation by viewing the client tree. The client tree contains a column titled **CTA Program**, which is visible in the **Update**, **View All**, or **Antivirus** views. Successful CTA installations contain a version number for the CTA program.

Also check if the following processes are running on the client computer:

- `ctapsd.exe`
- `ctaEoU.exe`
- `ctatransapt.exe`

- `ctalogd.exe`

Policy Server for Cisco NAC Installation

There are two ways to install Policy Server:

- The Policy Server installer located on the Enterprise DVD
- The OfficeScan server's master installer (this installs both OfficeScan server and the Policy Server on the same computer)

Note

The master installer installs both the OfficeScan server and Policy Server web console on an IIS or Apache web server. If the installer does not find an Apache server on the system, or if an existing Apache server installation is not version 2.0, the installer automatically installs Apache version 2.0.

The ACS server, Policy Server, and OfficeScan server must be on the same network segment to ensure effective communication.

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

http://www.apache.org

Installing the Policy Server Using the Policy Server Installer

Procedure

1. Log on to the computer to which you will install Policy Server for Cisco NAC.
2. Locate the Policy Server for Cisco NAC installer package on the Enterprise CD.
3. Double-click `setup.exe` to run the installer.
4. Follow the installation instructions.

You can install the Policy Server to the OfficeScan server computer.

Installing Policy Server for Cisco NAC from the OfficeScan Server Master Installer

Procedure

1. In the **Install Other OfficeScan Programs** screen of the OfficeScan server master installer, select **Policy Server for Cisco NAC**.
2. Click **Next**.
3. Continue with OfficeScan server installation until the **Welcome screen for Trend Micro Policy Server for Cisco NAC** appears.
4. Click **Next**.

   The **Policy Server for Cisco NAC License Agreement** screen appears.
5. Read the agreement and click **Yes** to continue.

   The **Choose Destination Location** screen appears.
6. Modify the default destination location if necessary by clicking **Browse...** and selecting a new destination for the Policy Server installation.
7. Click **Next**.

   The **Web Server** screen appears.
8. Choose the web server for the Policy Server:
   - **IIS server**: Click to install on an existing IIS web server installation
   - **Apache 2.0 Web server**: Click to install on an Apache 2.0 web server
9. Click **Next**.

   The **Web Server Configuration** screen appears.
10. Configure the following information:
    a. If you selected to install Policy Server on an IIS server, select one of the following:
       - **IIS default Web site**: Click to install as an IIS default website

- **IIS virtual Web site**: Click to install as an IIS virtual website

b. Next to **Port**, type a port that will serve as the server listening port.

When the Policy Server and OfficeScan server are on the same computer and uses the same web server, the port numbers are as follows:

- **Apache Web server/IIS Web server on default Web site**: Policy Server and OfficeScan server share the same port
- **Both on IIS Web server on virtual Web site**: Policy Server default listening port is 8081 and the SSL port is 4344. The OfficeScan server default listening port is 8080 and the SSL port is 4343.

c. If you selected to install Policy Server on an IIS server, you can use Secured Socket Layer (SSL). Type the SSL port number and the number of years to keep the SSL certificate valid (the default is 3 years).

If you enable SSL, this port number will serve as the server's listening port. The Policy Server's address is as follows:

- `http://<Policy Server name>:<port number>`
- `https://<Policy Server name>:<port number>` (if you enable SSL)

11. Click **Next**.
12. Specify the Policy Server console password and click **Next**.
13. Specify the ACS Server authentication password and click **Next**.
14. Review the installation settings. If satisfied with the settings, click **Next** to start the installation. Otherwise, click **Back** to go to the previous screens.
15. When the installation completes, click **Finish**.

The OfficeScan server master installer will continue with the rest of the OfficeScan server installation.

Policy Server SSL Certificate Preparation

To establish a secure SSL connection between the ACS server and the Policy Server, prepare a certificate especially for use with SSL. Setup automatically generates the SSL certificate.

Preparing the IIS Policy Server SSL Certificate

Procedure

1. Export the certificate from the Certification Store on mmc.
   a. On the Policy Server, click **Start** > **Run**.

      The Run screen opens.

   b. Type `mmc` in the **Open** box.

      A new management console screen opens.

   c. Click **Console** > **Add/Remove Snap-in**.

      The Add/Remove Snap-in screen appears.

   d. Click **Add**.

      The **Add Standalone Snap-ins** screen appears.

   e. Click **Certificates** and click **Add**.

      The **Certificates snap-in** screen opens.

   f. Click **Computer Account** and click **Next**.

      The **Select Computer** screen opens.

   g. Click **Local Computer** and click **Finish**.

   h. Click **Close** to close the **Add Standalone Snap-in** screen.

   i. Click **OK** to close the **Add/remove Snap-in** screen.

j. In the tree view of the console, click **Certificates (Local Computer)** > **Trusted Root Certification Authorities** > **Certificates**.

k. Select the certificate from the list.

> **Note**
>
> Check the certificate thumbprint by double-clicking the certificate and selecting Properties. The thumbprint should be the same as the thumbprint for the certificate located in the IIS console.
>
> To verify this, open the IIS console and right click either **virtual Web site** or **default Web site** (depending on the website on which you installed Policy Server) and then select **Properties**. Click **Directory Security** and then click **View Certificate** to view the certificate details, including the thumbprint.

l. Click **Action** > **All Tasks** > **Export...**. The **Certificate Export Wizard** opens.

m. Click **Next**.

n. Click **DER encoded binary x.509** or **Base 64 encoded X.509** and click **Next**.

o. Enter a file name and browse to a directory to which to export the certificate.

p. Click **Next**.

q. Click **Finish**. A confirmation window displays.

r. Click **OK**.

2. Install the certificate on Cisco Secure ACS.

   a. On the ACS web console, click **System Configuration** > **ACS Certificate Setup** > **ACS Certification Authority Setup**.

   b. Type the full path and file name of the certificate in the **CA certificate file** field.

   c. Click **Submit**. Cisco Secure ACS prompts you to restart the service.

   d. Click **System Configuration** > **Service Control**.

   e. Click **Restart**. Cisco Secure ACS restarts.

Preparing the Apache Policy Server SSL Certificate

Procedure

1. Export the certificate from the Certification Store on mmc.
   a. Obtain the certificate file `server.cer`. The location of the file depends on which server, the OfficeScan server or the Policy Server, you installed first:
      - If you installed OfficeScan server before installing Policy Server, the file is in the following directory: <*Server installation folder*>`\PCCSRV\Private\certificate`
      - If you installed Policy Server before installing OfficeScan server, the file is in the following directory: `<Server installation folder>\PolicyServer\Private\certificate`
   b. Copy the certificate file to the ACS server.
2. Install the certificate on Cisco Secure ACS.
   a. On the ACS web console, click **System Configuration** > **ACS Certificate Setup** > **ACS Certification Authority Setup**.
   b. Type the full path and file name of the certificate in the **CA certificate file** field.
   c. Click **Submit**.

      Cisco Secure ACS prompts you to restart the service.
   d. Click **System Configuration** > **Service Control**.
   e. Click **Restart**.

      Cisco Secure ACS restarts.

ACS Server Configuration

To allow Cisco Secure ACS to pass authentication requests to the Policy Server for Cisco NAC, add the Policy Server for Cisco NAC in External Policies for the external

user database to use for authentication. See the ACS server documentation for instructions on how to add the policy server in a new external policy.

Note

Configure the ACS server to perform tasks such as blocking client access to the network. These ACS functions are beyond the scope of the Trend Micro Policy Server for Cisco NAC implementation and are not in this document. See the ACS documentation for details on configuring other ACS functions.

Policy Server for Cisco NAC Configuration

After installing OfficeScan and the Policy Server, and deploying both the OfficeScan client and the Cisco Trust Agent, configure the Policy Server for Cisco NAC. To configure a Policy Server, access the Policy Server web console from the OfficeScan web console by going to **Cisco NAC** > **Policy Servers** and clicking the Policy Server link.

This section describes the following aspects of Policy Server configuration:

- *Policy Server Configuration from OfficeScan on page 16-39* describes how to manage Policy Servers on the OfficeScan web console.
- *Summary Information for a Policy Server on page 16-40* shows you how to get an overview of Policy Servers on the network.
- *Policy Server Registration on page 16-41* is the first step in configuring Policy Servers.
- *Rules on page 16-42* shows you how to create and edit rules that comprise policies.
- *Policies on page 16-42* shows you how to create and edit policies that ultimately determine how Policy Server measures client security posture.
- *Client Validation Logs on page 16-42* gives an overview of how to use logs to understand the security posture status of clients on the network.
- *Client Log Maintenance on page 16-43* gives an overview on how to maintain client validation log size.

- *Administrative Tasks on page 16-43* describes how to change the Policy Server password and set a schedule for synchronization.

Policy Server Configuration from OfficeScan

The first step in configuring Policy Servers is to add the installed Policy Servers to the OfficeScan server. This allows you to open the Policy Server web console from the OfficeScan web console.

Adding a Policy Server from OfficeScan

Procedure

1. On the main menu of the OfficeScan web console, click **Cisco NAC** > **Policy Servers**.

   The Policy Servers screen appears displaying a list of all Policy Servers.

2. Click **Add**.

   The **Policy Server** screen displays.

3. Type the full Policy Server address and port number the server uses for HTTPS communication (for example: `https://policy-server:4343/`). Also type an optional description for the server.

4. Type a password to use when logging in the Policy Server web console.

5. Click **Add**.

Deleting a Policy Server from OfficeScan

Procedure

1. On the main menu of the OfficeScan web console, click **Cisco NAC** > **Policy Servers**.

   The **Policy Servers** screen appears displaying a list of all Policy Servers.

2. Select the check box next to the Policy Server to delete.
3. Click **Delete**.

> **Note**
> To validate all clients on the network, add all OfficeScan servers to at least one Policy Server.

Summary Information for a Policy Server

The **Summary** screen contains information about the Policy Server including configuration settings for policies and rules, client validation logs, and OfficeScan servers registered to a Policy Server.

The IP address and port number of the Policy Server for Cisco NAC appears at the top of the **Summary** screen.

The **Configuration Summary** table displays the number of OfficeScan servers registered to the Policy Server, the Policy Server policies, and the rules that compose the policies.

Viewing and Modifying Configuration Summary Details for a Policy Server

Procedure

1. On the main menu of the OfficeScan web console, click **Cisco NAC** > **Policy Servers**.

   The **Policy Servers** screen appears displaying a list of all Policy Servers.

2. Click the server name of the Policy Server whose details you want to view.

   The **Summary** screen appears showing the **Configuration Summary** table.

3. Click the link next to the item whose configuration settings you want to view:

   - **Registered OfficeScan server(s)**: The OfficeScan servers currently on the network

- **Policies**: The Policy Server policies registered OfficeScan servers can use
- **Rule(s)**: The Policy Server rules that comprise policies

Tip

If you want multiple Policy Servers on the network to have the same settings, including the same rules and policies, export and then import settings from one server to another. Trend Micro recommends configuring the same settings on all Policy Servers on the network to maintain a consistent antivirus policy.

Synchronizing the Policy Server with Registered OfficeScan Servers

Procedure

1. In the **Summary** screen, click **Synchronize with OfficeScan**. The **Summary - Synchronization Results** screen appears showing the following read-only information:
   - **OfficeScan server name**: The host name or IP address and port number of the registered OfficeScan servers
   - **Synchronization Result**: Indicates if the synchronization was successful or not
   - **Last Synchronized**: The date of the last successful synchronization

For more information on synchronization, see *Synchronization on page 16-16*.

Policy Server Registration

Register the Policy Server with at least one OfficeScan server so the Policy Server can obtain Virus Pattern and Virus Scan Engine version information. See *The Client Validation Sequence on page 16-7* for information on the role the OfficeScan server performs in the validation process.

Note

For Policy Server to validate all clients on the network, add all OfficeScan servers to at least one Policy Server.

Add a new OfficeScan server or edit the settings of an existing one from the OfficeScan servers screen, which you can access by going to the Policy Server web console and clicking **Configurations** > **OfficeScan servers**.

Rules

Rules are the building blocks of policies and comprise policies. Configure rules as the next step in Policy Server configuration. See *Rule Composition on page 16-10* for more information.

To access the web console screens for Cisco ACS rules, go to the Policy Server web console and click **Configurations** > **Rules** on the main menu.

Policies

After configuring new rules or ensuring that the default rules are suitable for your security enforcement needs, configure policies registered OfficeScan servers can use. See *Policy Composition on page 16-14* for more information.

Add a new Cisco NAC policy or edit an existing one to determine the rules currently enforced and to take action on clients when client security posture does not match any rules.

To access the web console screens for Cisco ACS policies, go to the Policy Server web console and click **Configurations** > **Policies** on the main menu.

Client Validation Logs

Use the client validation logs to view detailed information about clients when they validate with the Policy Server. Validation occurs when the ACS server retrieves client security posture data and sends it to the Policy Server, which compares the data to policies and rules (see *The Client Validation Sequence on page 16-7*).

Note

To generate client validation logs, when adding or editing a new rule or policy, select the check box under Server-side actions.

To access the web console screens for Cisco ACS logs, go to the Policy Server web console and click **Logs** > **View Client Validation Logs** on the main menu.

Client Log Maintenance

The Policy Server archives client validation logs when they reach a size you specify. It can also delete log files after a specified number of log files accumulates. Specify the way Policy Server maintains client validation logs by clicking **Logs** > **Log Maintenance** on the Policy Server web console.

Administrative Tasks

Perform the following administrative tasks on the Policy Server:

- **Change password**: Change the password configured when adding the Policy Server (see *Policy Server Configuration from OfficeScan on page 16-39*)
- **Configure a synchronization schedule**: The Policy Server needs to periodically obtain the version of the Virus Pattern and Virus Scan Engine on the OfficeScan server to evaluate OfficeScan client security posture. Therefore, you cannot enable or disable scheduled synchronization. By default, the Policy Server synchronizes with the OfficeScan server(s) every five minutes (see *Synchronization on page 16-16* for more information).

  Note

  Manually synchronize the Policy Server with the OfficeScan server at any time on the Summary screen (see *Summary Information for a Policy Server on page 16-40*).

To access the web console screens for Cisco ACS administration tasks, go to the Policy Server web console and click Administration on the main menu.

Chapter 17

Configuring OfficeScan with Third-party Software

This chapter describes OfficeScan integration with third-party software.

Topics in this chapter:

- *Overview of Check Point Architecture and Configuration on page 17-2*
- *Configuring the Secure Configuration Verification File for OfficeScan on page 17-4*
- *SecureClient Support Installation on page 17-5*

Overview of Check Point Architecture and Configuration

Integrate OfficeScan installations with Check Point™ SecureClient™ using Secure Configuration Verification (SCV) within the Open Platform for Security (OPSEC) framework. Refer to the Check Point SecureClient OPSEC documentation before reading this section. Documentation for OPSEC can be found at:

http://www.opsec.com

Check Point SecureClient has the capability to confirm the security configuration of computers connected to the network using Secure Configuration Verification (SCV) checks. SCV checks are a set of conditions that define a securely configured client system. Third-party software can communicate the value of these conditions to Check Point SecureClient. Check Point SecureClient then compares these conditions with conditions in the SCV file to determine if the client is considered secure.

SCV checks are regularly performed to ensure that only securely configured systems are allowed to connect to the network.

SecureClient uses Policy Servers to propagate SCV checks to all clients registered with the system. The administrator sets the SCV checks on the Policy Servers using the SCV Editor.

The SCV Editor is a tool provided by Check Point that allows you to modify SCV files for propagation to client installation. To run the SCV Editor, locate and run the file `SCVeditor.exe` on the Policy Server. In the SCV Editor, open the file `local.scv` in the folder `C:\FW1\NG\Conf` (replace `C:\FW1` with the installation path for the Check Point firewall if different from the default).

For specific instructions on opening and modifying an `SCV` file with the SCV Editor, see *OfficeScan Integration on page 17-2*.

OfficeScan Integration

The OfficeScan client periodically passes the Virus Pattern number and Virus Scan Engine number to SecureClient for verification. SecureClient then compares these values with values in the client `local.scv` file.

This is what the `local.scv` file looks like if you open it in a text editor:

```
(SCVObject
:SCVNames (
: (OfceSCV
:type (plugin)
:parameters (
:CheckType (OfceVersionCheck)
:LatestPatternVersion (701)
:LatestEngineVersion (7.1)
:PatternCompareOp (">=")
:EngineCompareOp (">=")
)
)
)
:SCVPolicy (
: (OfceSCV)
)
:SCVGlobalParams (
:block_connections_on_unverified (true)
:scv_policy_timeout_hours (24)
)
)
```

In this example, the `SCV` check will allow connections through the firewall if the pattern file version is 701 or later, and the scan engine number is 7.1 or later. If the scan engine

or pattern file is earlier, all connections through the Check Point firewall get blocked. Modify these values using the SCV Editor on the `local.scv` file on the Policy Server.

Note

Check Point does not automatically update the pattern file and scan engine version numbers in the `SCV` file. Whenever OfficeScan updates the scan engine or pattern file, you need to manually change the value of the conditions in the `local.scv` file to keep them current. If you do not update the scan engine and pattern versions, Check Point will authorize traffic from clients with earlier pattern files or scan engines, creating a potential for new viruses to infiltrate the system.

Configuring the Secure Configuration Verification File for OfficeScan

To modify the `local.scv` file, you need to download and run the SCV Editor (`SCVeditor.exe`).

Procedure

1. Download `SCVeditor.exe` from the Check Point download site.

   The SCV Editor is part of the OPSEC SDK package.

2. Run `SCVeditor.exe` on the Policy Server.

   The SCV Editor console opens.

3. Expand the `Products` folder and select `user_policy_scv`.

4. Click **Edit** > **Product** > **Modify**, and then type `OfceSCV` in the **Modify** box. Click **OK**.

   Note

   If the `local.scv` file already contains product policies for other third-party software, create a new policy by clicking **Edit** > **Product** > **Add**, and then typing `OfceSCV` in the **Add** box.

5. Add a parameter by clicking **Edit** > **Parameters** > **Add**, and then typing a **Name** and **Value** in the corresponding boxes.

   The following table lists the parameter names and values. Parameter names and values are case-sensitive. Type them in the order given in the table.

   TABLE 17-1. SCV File Parameter Names and Values

NAME	VALUE
CheckType	OfceVersionCheck
LatestPatternVersion	<current pattern file number>
LatestEngineVersion	<current scan engine number>
LatestPatternDate	<current pattern file release date>
PatternCompareOp	>=
EngineCompareOp	>=
PatternMismatchMessage	
EngineMismatchMessage	

   Type the most current pattern file number and scan engine number in place of the text in curly braces. View the latest virus pattern and scan engine versions for clients by clicking **Update & Upgrade** on the main menu of the OfficeScan web console. The pattern version number will appear to the right of the pie chart representing the percentage of OfficeScan clients protected.

6. Select **Block connections on SCV unverified**.

7. Click **Edit** > **Product** > **Enforce**.

8. Click **File** > **Generate Policy File** to create the file. Select the existing `local.scv` file to overwrite it.

SecureClient Support Installation

If users connect to the office network from a Virtual Private Network (VPN), and they have both Check Point SecureClient and the OfficeScan client installed on their

computers, instruct them to install SecureClient support. This module allows SecureClient to perform SCV checks on VPN clients, ensuring that only securely configured systems are allowed to connect to the network. Users can verify that they have Check Point SecureClient installed on their computers by checking for the ( ) icon in the system tray. Users can also check for an item named **Check Point SecureClient** on the **Add/Remove Programs** screen of Windows.

Users launch the installation from the OfficeScan client console's **Toolbox** tab. This tab only appears if users have the necessary privileges and if the OfficeScan client computer's operating system is Windows XP or Windows Server 2003.

FIGURE 17-1. Toolbox tab on the OfficeScan client console

Granting Users the Privilege to View the Toolbox Tab

Procedure

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

2. In the client tree, click the root domain icon ( ) to include all clients or select specific domains or clients.

> **Note**
> Check Point SecureClient Support does not support IPv6. You cannot deploy this module to pure IPv6 endpoints.

3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Toolbox Privileges** section.
5. Select **Display the Toolbox tab on the client console and allow users to install Check Point SecureClient Support**.
6. If you selected domain(s) or client(s) in the client tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Installing SecureClient Support

Procedure

1. Open the OfficeScan client console.
2. Click the **Toolbox** tab.
3. Under **Check Point SecureClient Support**, click **Install/Upgrade SecureClient support**.

   A confirmation screen appears.
4. Click **Yes**.

The OfficeScan client connects to the server and downloads the module. OfficeScan displays a message when the download is complete.

5. Click **OK**.

Chapter 18

Getting Help

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

Topics in this chapter:

- *Troubleshooting Resources on page 18-2*
- *Contacting Technical Support on page 18-24*

Troubleshooting Resources

This section provides a list of resources you can use to troubleshoot OfficeScan server and OfficeScan client issues.

- *Support Intelligence System on page 18-2*
- *Case Diagnostic Tool on page 18-2*
- *OfficeScan Server Logs on page 18-3*
- *OfficeScan Client Logs on page 18-15*

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.

Run the tool on all platforms that OfficeScan supports. 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, available from the Trend Micro Knowledge Base, 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 Behavior Monitoring and Device Control.

For details, visit http://esupport.trendmicro.com/solution/en-us/1056425.aspx.

OfficeScan Server Logs

Aside from logs available on the web console, you can use other types of logs (such as debug logs) to troubleshoot product issues.

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 you need to conserve disk space.

Server Debug Logs Using LogServer.exe

Use `LogServer.exe` to collect debug logs for the following:

- OfficeScan server basic logs
- Trend Micro Vulnerability Scanner
- Active Directory integration logs
- Client grouping logs
- Security compliance logs
- Role-based administration
- Smart scan
- Policy Server

Enabling Debug Logging

Procedure

1. Log on to the web console.
2. On the banner of the web console, click the first "O" in "OfficeScan".
3. Specify debug log settings.
4. Click **Save**.
5. Check the log file (`ofcdebug.log`) in the default location: <*Server installation folder*>`\PCCSRV\Log`.

Disabling Debug Logging

Procedure

1. Log on to the web console.
2. On the banner of the web console, click the first "O" in "OfficeScan".
3. Clear **Enable debug log**.
4. Click **Save**.

Enabling Debug Logging for Server Installation and Upgrade

Enable debug logging before performing the following tasks:

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

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, upgrade to a new server version, or perform remote installation/upgrade).
5. Check ofcdebug.log in `C:\LogServer`.

Installation Logs

- Local Installation/Upgrade Logs

  File name: `OFCMAS.LOG`

  Location: `%windir%`

- Remote Installation/Upgrade Logs
  - On the computer where you launched Setup:

    File name: `ofcmasr.log`

    Location: `%windir%`

- On the target computer:

  File name: `OFCMAS.LOG`

  Location: `%windir%`

Active Directory Logs

- **File name**: `ofcdebug.log`
- **File name**: `ofcserver.ini`

  Location: <*Server installation folder*>`\PCCSRV\Private\`
- **File names**:
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbADPredefinedScope.cdx`
  - `dbADPredefinedScope.dbf`
  - `dbCredential.cdx`
  - `dbCredential.dbf`

  Location: `<Server installation folder>\PCCSRV\HTTPDB\`

Role-based Administration Logs

To get detailed role-based administration information, do one of the following:

- Run the Trend Micro Case Diagnostics Tool. For information, see *Case Diagnostic Tool on page 18-2*.
- Gather the following logs:
  - All files in the <*Server installation folder*>`\PCCSRV\Private\AuthorStore` folder.

- *OfficeScan Server Logs on page 18-3*

OfficeScan Client Grouping Logs

- **File name**: `ofcdebug.log`
- **File name**: `ofcserver.ini`

  Location: <*Server installation folder*>`\PCCSRV\Private\`
- **File name**: `SortingRule.xml`

  Location: `<Server installation folder>\PCCSRV\Private\SortingRuleStore\`
- **File names**:
  - `dbADScope.cdx`
  - `dbADScope.dbf`

  Location: `<Server installation folder>\HTTPDB\`

Component Update Logs

File name: `TmuDump.txt`

Location: <*Server installation folder*>`\PCCSRV\Web\Service\AU_Data\AU_Log`

Getting Detailed Server Update Information

Procedure

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

```
[Debug]
level=-1
[Downloader]
```

```
ProxyCache=0
```

2. Save the file to <*Server installation folder*>`\PCCSRV\Web\Service`.
3. Restart the OfficeScan Master Service.

Stopping the Collection of Detailed Server Update Information

Procedure

1. Delete `aucfg.ini`.
2. Restart the OfficeScan Master Service.

Apache Server Logs

File names:

- `install.log`
- `error.log`
- `access.log`

Location: <*Server installation folder*>`\PCCSRV\Apache2`

Client Packager Logs

Enabling Logging for Client Packager Creation

Procedure

1. Modify `ClnExtor.ini` in <*Server installation folder*>`\PCCSRV\Admin\Utility\ClientPackager` as follows:

```
[Common]

DebugMode=1
```

2. Check `ClnPack.log` in `C:\`.

Disabling Logging for Client Packager Creation

Procedure

1. Open `ClnExtor.ini`.
2. Change the "DebugMode" value from 1 to 0.

Security Compliance Report Logs

To get detailed Security Compliance information, gather the following:

- **File name**: `RBAUserProfile.ini`

  Location: <*Server installation folder*>`\PCCSRV\Private\AuthorStore\`

- All files in the `<Server installation folder>\PCCSRV\Log\Security Compliance Report` folder.
- *OfficeScan Server Logs on page 18-3*

Outside Server Management Logs

- **File name**: `ofcdebug.log`
- **File name**: `ofcserver.ini`

  Location: <*Server installation folder*>`\PCCSRV\Private\`

- All files in the `<Server installation folder>\PCCSRV\Log\Outside Server Management Report\` folder.
- **File names**:
  - `dbADScope.cdx`
  - `dbADScope.dbf`

- `dbClientInfo.cdx`
- `dbclientInfo.dbf`

Location: `<Server installation folder>\HTTPDB\`

Device Control Exception Logs

To get detailed Device Control Exception information, gather the following:

- **File name**: `ofcscan.ini`

  Location: <*Server installation folder*>\
- **File name**: `dbClientExtra.dbf`

  Location: `<Server installation folder>\HTTPDB\`
- Device Control Exception List from the OfficeScan web console.

Web Reputation Logs

File name: `diagnostic.log`

Location: <*Server installation folder*>`\PCCSRV\LWCS\`

ServerProtect Normal Server Migration Tool Logs

Enabling Debug Logging for ServerProtect Normal Server Migration Tool

Procedure

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

```
[Debug]
DebugLog=C:\ofcdebug.log
DebugLevel=9
```

2. Save the file to `C:\`.
3. Check `ofcdebug.log` in `C:\`.

Note

To disable debug logging, delete the `ofcdebug.ini` file.

VSEncrypt Logs

OfficeScan automatically creates the debug log (`VSEncrypt.log`) in the user account's temporary folder. For example, `C:\Documents and Settings\<User name>\Local Settings\Temp`.

Control Manager MCP Agent Logs

Debug Files on the <*Server installation folder*>`\PCCSRV\CMAgent` folder

- `Agent.ini`
- `Product.ini`
- The screenshot of the Control Manager Settings page
- `ProductUI.zip`

Enabling Debug Logging for the MCP Agent

Procedure

1. Modify `product.ini` in <*Server installation folder*>`\PCCSRV\CmAgent` as follows:

```
[Debug]

debugmode = 3

debuglevel= 3
```

```
debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Restart the OfficeScan Control Manager Agent service from Microsoft Management Console.
3. Check `CMAgent_debug.log` in `C:\`.

Disabling Debug Logging for the MCP Agent

Procedure

1. Open `product.ini` and delete the following:

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Restart the OfficeScan Control Manager service.

Virus Scan Engine Logs

Enabling Debug Logging for the Virus Scan Engine

Procedure

1. Open Registry Editor (`regedit.exe`).
2. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`.

3. Change the value of "`DebugLogFlags`" to "`00003eff`".
4. Perform the steps that led to the scanning issue you encountered.
5. Check `TMFilter.log` in `%windir%`.

Note

Disable debug logging by restoring the value of "`DebugLogFlags`" to "`00000000`".

Virus/Malware Logs

File name:

- `dbVirusLog.dbf`
- `dbVirusLog.cdx`

Location: <*Server installation folder*>`\PCCSRV\HTTPDB\`

Spyware/Grayware Logs

File name:

- `dbSpywareLog.dbf`
- `dbSpywareLog.cdx`

Location: <*Server installation folder*>`\PCCSRV\HTTPDB\`

Outbreak Logs

Current Firewall Violation Outbreak Logs

File name: `Cfw_Outbreak_Current.log`

Location: <*Server installation folder*>`\PCCSRV\Log\`

Last Firewall Violation Outbreak Logs

File name: `Cfw_Outbreak_Last.log`

Location: <*Server installation folder*>`\PCCSRV\Log\`

Current Virus /Malware Outbreak Logs

File name: `Outbreak_Current.log`

Location: <*Server installation folder*>`\PCCSRV\Log\`

Last Virus /Malware Outbreak Logs

File name: `Outbreak_Last.log`

Location: <*Server installation folder*>`\PCCSRV\Log\`

Current Spyware/Grayware Outbreak Logs

File name: `Spyware_Outbreak_Current.log`

Location: <*Server installation folder*>`\PCCSRV\Log\`

Last Spyware/Grayware Outbreak Logs

File name: `Spyware_Outbreak_Last.log`

Location: <*Server installation folder*>`\PCCSRV\Log\`

Virtual Desktop Support Logs

- **File name**: `vdi_list.ini`

  Location: <*Server installation folder*>`\PCCSRV\TEMP\`

- **File name**: `vdi.ini`

  Location: `<Server installation folder>\PCCSRV\Private\`

- **File name**: `ofcdebug.txt`

  Location: `<Server installation folder>\PCCSRV\`

To generate `ofcdebug.txt`, enable debug logging. For instructions on enabling debug logging, see *Enabling Debug Logging on page 18-4*.

OfficeScan Client Logs

Use OfficeScan client logs (such as debug logs) to troubleshoot OfficeScan client issues.

WARNING!

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

OfficeScan Client Debug Logs Using LogServer.exe

Enabling Debug Logging for the OfficeScan Client

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 client users, instructing them to save the file to `C:\`.

Note

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

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

Note

Disable debug logging for the OfficeScan client by deleting `ofcdebug.ini`.

Fresh Installation Logs

File name: `OFCNT.LOG`

Locations:

- `%windir%` for all installation methods except MSI package
- `%temp%` for the MSI package installation method

Upgrade/Hot Fix Logs

File name: `upgrade_yyyymmddhhmmss.log`

Location: <*Client installation folder*>

Damage Cleanup Services Logs

Enabling Debug Logging for Damage Cleanup Services

Procedure

1. Open `TSC.ini` in <*Client installation folder*>.

2. Modify the following line as follows:

   `DebugInfoLevel=3`

3. Check `TSCDebug.log` in `<Client installation folder>\debug`.

Disabling Debug Logging for Damage Cleanup Services

Open `TSC.ini` and change the "`DebugInfoLevel`" value from 3 to 0.

Cleanup Log

File name: `yyyymmdd.log`

Location: <*Client installation folder*>`\report\`

Mail Scan Logs

File name: `SmolDbg.txt`

Location: <*Client installation folder*>

ActiveUpdate Logs

- **File name**: `Update.ini`

  Location: <*Client installation folder*>

- **File name**: `TmuDump.txt`

  Location: `<Client installation folder>\AU_Log\`

OfficeScan Client Connection Logs

File name: `Conn_YYYYMMDD.log`

Location: <*Client installation folder*>`\ConnLog`

OfficeScan Client Update Logs

File name: `Tmudump.txt`

Location: <*Client installation folder*>`\AU_Data\AU_Log`

Getting Detailed OfficeScan Client Update Information

Procedure

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

```
[Debug]
level=-1
[Downloader]
ProxyCache=0
```

2. Save the file to <*Client installation folder*>.
3. Reload the OfficeScan client.

Note

Stop collecting detailed client update information by deleting the `aucfg.ini` file and reloading the OfficeScan client.

Outbreak Prevention Logs

File name: `OPPLogs.log`

Location: <*Client installation folder*>`\OppLog`

Outbreak Prevention Restore Logs

File names:

- `TmOPP.ini`

- `TmOPPRestore.ini`

Location: <*Client installation folder*>\

OfficeScan Firewall Logs

Enabling Debug Logging for the Common Firewall Driver on Windows Vista/Server 2008/7/Server 2012/8 Computers

Procedure

1. Modify the following registry values:

Registry Key	Values
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters`	**Type**: `DWORD` value `(REG_DWORD)` **Name**: `DebugCtrl` **Value**: `0x00001111`
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters`	**Type**: `DWORD` value `(REG_DWORD)` **Name**: `DebugCtrl` **Value**: `0x00001111`

2. Restart the computer.
3. Check `wfp_log.txt` and `lwf_log.txt` in `C:\`.

Enabling Debug Logging for the Common Firewall Driver on Windows XP and Windows Server 2003 Computers

Procedure

1. Add the following data in `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters`:
   - Type: `DWORD` value `(REG_DWORD)`

- **Name**: `DebugCtrl`
- **Value**: `0x00001111`

2. Restart the computer.
3. Check `cfw_log.txt` in `C:\`.

Disabling Debug Logging for the Common Firewall Driver (all operating systems)

Procedure

1. Delete "`DebugCtrl`" in the registry key.
2. Restart the computer.

Enabling Debug Logging for the OfficeScan NT Firewall Service

Procedure

1. Edit `TmPfw.ini` located in <*Client installation folder*> as follows:

```
[ServiceSession]
Enable=1
```

2. Reload the client.
3. Check `ddmmyyyy_NSC_TmPfw.log` in `C:\temp`.

Disabling Debug Logging for the OfficeScan NT Firewall Service

Procedure

1. Open `TmPfw.ini` and change the "`Enable`" value from 1 to 0.

2. Reload the OfficeScan client.

Web Reputation and POP3 Mail Scan Logs

Enabling Debug Logging for the Web Reputation and POP3 Mail Scan Features

Procedure

1. Edit `TmProxy.ini` located in <*Client installation folder*> as follows:

   ```
   [ServiceSession]
   Enable=1
   LogFolder=C:\temp
   ```

2. Reload the OfficeScan client.
3. Check the `ddmmyyyy_NSC_TmProxy.log` in `C:\temp`.

Disabling Debug Logging for the Web Reputation and POP3 Mail Scan Features

Procedure

1. Open `TmProxy.ini` and change the "`Enable`" value from 1 to 0.
2. Reload the OfficeScan client.

Device Control Exception List Logs

File name: `DAC_ELIST`

Location: <*Client installation folder*>\

Data Protection Debug Logs

Enabling Debug Logging for the Data Protection Module

Procedure

1. Obtain the `logger.cfg` file from your support provider.
2. Add the following data in `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`:
   - **Type**: `String`
   - **Name**: `debugcfg`
   - **Value**: `C:\Log\logger.cfg`
3. Create a folder named "Log" in the `C:\ directory`.
4. Copy `logger.cfg` to the "Log" folder.
5. Deploy Data Loss Prevention and Device Control settings from the web console to start collecting logs.

Note

Disable debug logging for the Data Protection module by deleting `debugcfg` in the registry key and restarting the computer.

Windows Event Logs

Windows Event Viewer records successful application events such as logging on or changing account settings.

Procedure

1. Do one of the following:

- Click **Start** > **Control Panel** > **Performance and Maintenance** > **Administrative Tools** > **Computer Management**.
- Open the MMC containing the Event Viewer snap-in.

2. Click **Event Viewer**.

Transport Driver Interface (TDI) Logs

Enabling Debug Logging for TDI

Procedure

1. Add the following data in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters`:

PARAMETER	VALUES
Key 1	**Type**: `DWORD` value `(REG_DWORD)` **Name**: `Debug` **Value**: `1111 (Hexadecimal)`
Key 2	**Type**: `String value (REG_SZ)` **Name**: `LogFile` **Value**: `C:\tmtdi.log`

2. Restart the computer.
3. Check `tmtdi.log` in `C:\`.

Note

Disable debug logging for TDI by deleting `Debug` and `LogFile` in the registry key and restarting the computer.

Contacting Technical Support

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

Worldwide support offices:

http://www.trendmicro.com/support

Trend Micro product documentation:

http://docs.trendmicro.com/en-us/home.aspx

Contact Information

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

Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main) Fax: +1 (408) 257-2003

Web address: www.trendmicro.com

Email: support@trendmicro.com

Speeding Up Your Support Call

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

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Amount of memory and free hard disk space on your computer

- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

The Trend Micro Knowledge Base

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

http://esupport.trendmicro.com/en-us/enterprise/default.aspx

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

TrendLabs

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

You can rely on the following post-sales service:

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

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

Comprehensive security information is available at the Trend Micro website:

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

Documentation Feedback

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

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

Appendix A

IPv6 Support in OfficeScan

This appendix is required reading for users who plan to deploy OfficeScan in an environment that supports IPv6 addressing. This appendix contains information on the extent of IPv6 support in OfficeScan.

Trend Micro assumes that the reader is familiar with IPv6 concepts and the tasks involved in setting up a network that supports IPv6 addressing.

IPv6 Support for OfficeScan Server and Clients

IPv6 support for OfficeScan started in this version 10.6. Earlier OfficeScan versions do not support IPv6 addressing. IPv6 support is automatically enabled after installing or upgrading the OfficeScan server and OfficeScan clients that satisfy the IPv6 requirements.

OfficeScan Server Requirements

The IPv6 requirements for the OfficeScan server are as follows:

- The 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 OfficeScan clients, it must have both IPv4 and IPv6 addresses and must be identified by its host name. If a server is identified by its IPv4 address, IPv6 OfficeScan clients cannot connect to the server. The same issue occurs if pure IPv4 clients connect to a server identified by its IPv6 address.
- If the server will manage only IPv6 clients, the minimum requirement is an IPv6 address. The server can be identified by its host name or IPv6 address. When the server is identified by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.

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

OfficeScan Client Requirements

The OfficeScan client must be installed on:

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows 8
- Windows Server 2012

It cannot be installed on Windows Server 2003 and Windows XP because these operating systems only support IPv6 addressing partially.

It is preferable for an OfficeScan client to have both IPv4 and IPv6 addresses as some of the entities to which it connects only support IPv4 addressing.

Pure IPv6 Server Limitations

The following table lists the limitations when the OfficeScan server only has an IPv6 address.

TABLE A-1. Pure IPv6 Server Limitations

ITEM	LIMITATION
Client management	A pure IPv6 server cannot: • Deploy OfficeScan clients to pure IPv4 endpoints. • Manage pure IPv4 OfficeScan clients.

ITEM	LIMITATION
Updates and centralized management	A pure IPv6 server cannot update from pure IPv4 update sources, such as: • Trend Micro ActiveUpdate Server • Control Manager 5.5 • Control Manager 5.0 **Note** IPv6 support for Control Manager starts in version 5.5 SP1. • Any pure IPv4 custom update source
Product registration, activation, and renewal	A pure IPv6 server cannot connect to the Trend Micro Online Registration Server to register the product, obtain the license, and activate/renew the license.
Proxy connection	A pure IPv6 server cannot connect through a pure IPv4 proxy server.
Plug-in solutions	A pure IPv6 server will have Plug-In Manager but will not be able to deploy any of the plug-in solutions to: • Pure IPv4 OfficeScan clients or pure IPv4 hosts (because of the absence of a direct connection) • Pure IPv6 OfficeScan clients or pure IPv6 hosts because none of the plug-in solutions support IPv6.

Most of these limitations can be overcome by setting 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 entities to which it connects or the entities that it serves.

Pure IPv6 OfficeScan Client Limitations

The following table lists the limitations when the OfficeScan client only has an IPv6 address.

TABLE A-2. Pure IPv6 OfficeScan client Limitations

ITEM	LIMITATION
Parent OfficeScan server	Pure IPv6 OfficeScan clients cannot be managed by a pure IPv4 OfficeScan server.
Updates	A pure IPv6 OfficeScan client cannot update from pure IPv4 update sources, such as: • Trend Micro ActiveUpdate Server • A pure IPv4 OfficeScan server • A pure IPv4 Update Agent • Any pure IPv4 custom update source
Scan queries, web reputation queries, and Smart Feedback	A pure IPv6 OfficeScan client cannot send queries to smart protection sources, such as: • Smart Protection Server 2.0 (integrated or standalone) **Note** IPv6 support for Smart Protection Server starts in version 2.5. • Trend Micro Smart Protection Network (also for Smart Feedback)
Software safety	Pure IPv6 OfficeScan clients cannot connect to the Trend Micro-hosted Certified Safe Software Service.
Plug-in solutions	Pure IPv6 OfficeScan clients cannot install plug-in solutions because none of the plug-in solutions support IPv6.
Programs	Pure IPv6 OfficeScan clients cannot install the following programs because they do not support IPv6: • Cisco Trust Agent • Check Point SecureClient Support
Proxy connection	A pure IPv6 OfficeScan client cannot connect through a pure IPv4 proxy server.

Most of these limitations can be overcome by setting up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the OfficeScan clients and the entities to which they connect.

Configuring IPv6 Addresses

The web console allows you to configure an IPv6 address or an IPv6 address range. The following are some configuration guidelines.

- OfficeScan accepts standard IPv6 address presentations.

  For example:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- OfficeScan also accepts link-local IPv6 addresses, such as:

  `fe80::210:5aff:feaa:20a2`

  WARNING!

  Exercise caution when specifying a link-local IPv6 address because even though OfficeScan can accept the address, it might not work as expected under certain circumstances. For example, OfficeScan clients cannot update from an update source if the source is on another network segment and is identified by its link-local IPv6 address.

- When the IPv6 address is part of a URL, enclose the address in square brackets ([]).
- For IPv6 address ranges, a prefix and prefix length are usually required. For configurations that require the server to query IP addresses, prefix length restrictions apply to prevent performance issues that may occur when the server queries a significant number of IP addresses. For example, for the Outside Server Management feature, the prefix length can only be between 112 (65,536 IP addresses) and 128 (2 IP addresses).

- Some settings that involve IPv6 addresses or address ranges will be deployed to OfficeScan clients but OfficeScan clients will ignore them. For example, if you configured the smart protection source list and included a Smart Protection Server identified by its IPv6 address, pure IPv4 OfficeScan clients will ignore the server and connect to the other smart protection sources.

Screens That Display IP Addresses

This topic enumerates places in the web console where IP addresses are shown.

- Client Tree

  Whenever the client tree displays, the IPv6 addresses of pure IPv6 OfficeScan clients display under the **IP address** column. For dual-stack OfficeScan clients, their IPv6 addresses display if they used their IPv6 address to register to the server.

  Note

  The IP address that dual-stack OfficeScan clients use when registering to the server can be controlled from **Networked Computers** > **Global Client Settings** > **Preferred IP Address**.

  When you export client tree settings to a file, the IPv6 addresses also display in the exported file.

- Client Status

  Detailed client information is available when you navigate to **Networked Computers** > **Client Management** > **Status**. In this screen, you will see the IPv6 addresses of pure IPv6 OfficeScan clients and dual-stack OfficeScan clients that used their IPv6 addresses to register to the server.

- Logs

  The IPv6 addresses of dual-stack and pure IPv6 OfficeScan clients display on the following logs:

  - Virus/Malware logs
  - Spyware/Grayware logs

- Firewall logs
- Connection verification logs

- Control Manager Console

The following table lists which of the OfficeScan server and OfficeScan clients' IP addresses display on the Control Manager console.

TABLE A-3. OfficeScan Server and OfficeScan client IP Addresses that Display on the Control Manager Console

OFFICESCAN	CONTROL MANAGERVERSION		
	5.5 SP1	**5.5**	**5.0**
Dual-stack server	IPv4 and IPv6	IPv4	IPv4
Pure IPv4 server	IPv4	IPv4	IPv4
Pure IPv6 server	IPv6	Not supported	Not supported
Dual-stack OfficeScan client	The IP address used when the OfficeScan client registered to the OfficeScan server	The IP address used when the OfficeScan client registered to the OfficeScan server	The IP address used when the OfficeScan client registered to the OfficeScan server
Pure IPv4 OfficeScan client	IPv4	IPv4	IPv4
Pure IPv6 OfficeScan client	IPv6	IPv6	IPv6

Appendix B

Windows Server Core 2008/2012 Support

This appendix discusses OfficeScan support for Windows Server Core 2008/2012.

Windows Server Core 2008/2012 Support

Windows Server Core 2008/2012 are "minimal" installations of Windows Server 2008/2012. In a Server Core:

- Many of the Windows Server 2008/2012 options and features are removed.
- The server runs a much thinner core operating system.
- Tasks are performed mostly from the command line interface.
- The operating system runs fewer services and requires less resources during startup.

The OfficeScan client supports Server Core. This section contains information on the extent of support for Server Core.

The OfficeScan server does not support Server Core.

Installation Methods for Windows Server Core

The following installation methods are not or are partially supported:

- **Web install page:** This method is not supported because Server Core does not have Internet Explorer.
- **Trend Micro Vulnerability Scanner:** The Vulnerability Scanner tool cannot be run locally on the Server Core. Run the tool from the OfficeScan server or another computer.

The following installation methods are supported:

- Remote installation. For details, see *Installing Remotely from the OfficeScan Web Console on page 5-19*.
- Login Script Setup
- Client Packager

Installing the OfficeScan Client Using Login Script Setup

Procedure

1. Open a command prompt.
2. Map the location of `AutoPcc.exe` file by typing the following command:

   ```
   net use <mapped drive letter> \\<OfficeScan server host name or IP address>\ofcscan
   ```

   For example:

   ```
   net use P: \\10.1.1.1\ofcscan
   ```

   A message appears, informing you if the location of AutoPcc.exe was mapped successfully.
3. Change to the location of `AutoPcc.exe` by typing the mapped drive letter and a colon. For example:

   ```
   P:
   ```
4. Type the following to launch the installation:

   ```
   AutoPcc.exe
   ```

The following image shows the commands and results on the command prompt.

```
C:\WINDOWS>net use P: \\10.1.1.1\ofcscan
The command completed successfully.

C:\WINDOWS>P:

P:\>AutoPcc.exe
AutoPcc.exe

 |-----------------------------------------|
 |        Trend Micro OfficeScan           |
 |       Auto Setup Program V10.6          |
 |      Copyright Trend Micro, Inc.        |
 |              1998-2011                  |
 |-----------------------------------------|

P:\>
```

FIGURE B-1. Command prompt showing how to install the OfficeScan client using Login Script Setup

Installing the OfficeScan Client Using an OfficeScan Client Package

Procedure

1. Create the package.

   For details, see *Installing with Client Packager on page 5-23*.

2. Open a command prompt.

3. Map the location of the OfficeScan client package by typing the following command:

   ```
   net use <mapped drive letter> \\<Location of the client package>
   ```

   For example:

```
net use P: \\10.1.1.1\Package
```

A message appears, informing you if the location of the OfficeScan client package was mapped successfully.

4. Change to the location of the OfficeScan client package by typing the mapped drive letter and a colon. For example:

```
P:
```

5. Copy the OfficeScan client package to a local directory on the Server Core computer by typing the following command:

```
copy <package file name> <directory on the Server Core
computer where you want to copy the package>
```

For example:

```
copy officescan.msi C:\Client Package
```

A message appears, informing you if the OfficeScan client package was copied successfully.

6. Change to the local directory. For example:

```
C:
```

```
cd C:\Client Package
```

7. Type the package file name to launch the installation. For example:

```
officescan.msi
```

The following image shows the commands and results on the command prompt.

```
C:\WINDOWS>net use P: \\10.1.1.1\Package
The command completed successfully.

C:\WINDOWS>P:

P:\>copy officescan.msi C:\Client Package
        1 file(s) copied.

P:\>C:

C:\WINDOWS>cd C:\Client Package

C:\Client Package>officescan.msi
```

FIGURE B-2. Command prompt showing how to install the OfficeScan client using a client package

OfficeScan Client Features on Windows Server Core

Most OfficeScan client features available on Windows Server 2008/2012 work on Server Core. The only feature that is not supported is roaming mode.

For a list of features available on Windows Server 2008/2012, see *OfficeScan Client Features on page 5-3*.

The OfficeScan client console is only accessible from the command line interface.

Note

Some OfficeScan client console screens include a Help button, which, when clicked, opens context-sensitive, HTML-based Help. Because Windows Server Core 2008/2012 lack a browser, the Help will not be available to the user. To view the Help, the user must install a browser.

Windows Server Core Commands

Launch the OfficeScan client console and other OfficeScan client tasks by issuing commands from the command line interface.

To run the commands, navigate to the location of `PccNTMon.exe`. This process is responsible for starting the OfficeScan client console. This process is found under the <*Client installation folder*>.

The following table lists the available commands.

TABLE B-1. Windows Server Core Commands

COMMAND	ACTION
`pccntmon`	Opens the OfficeScan client console
`pccnt`	
`pccnt <drive or folder path>`	Scans the specified drive or folder for security risks Guidelines: • If the folder path contains a space, enclose the entire path in quotes. • Scanning of individual files is not supported. Correct commands: • `pccnt C:\` • `pccnt D:\Files` • `pccnt "C:\Documents and Settings"` Incorrect commands: • `pccnt C:\Documents and Settings` • `pccnt D:\Files\example.doc`
`pccntmon -r`	Opens Real-time Monitor
`pccntmon -v`	Opens a screen with a list of client components and their versions

COMMAND	ACTION
`pccntmon -u`	Opens a screen where "Update Now" (manual client update) is launched If "Update Now" cannot be launched, the following message displays on the command prompt: Disabled or Not Functional
`pccntmon -n`	Opens a popup window where a password is specified to unload the client If a password is not required to unload the OfficeScan client, OfficeScan client unloading starts. To reload the OfficeScan client, type the following command: `pccntmon`
`pccntmon -m`	Opens a popup window where a password is specified to uninstall the OfficeScan client If a password is not required to uninstall the OfficeScan client, OfficeScan client uninstallation starts.

COMMAND	ACTION

`pccntmon -c`	Shows the following information in the command line:
	• Scan method
	  • Smart scan
	  • Conventional scan
	• Pattern status
	  • Updated
	  • Outdated
	• Real-time scan service
	  • Functional
	  • Disabled or Not Functional
	• Client connection status
	  • Online
	  • Roaming
	  • Offline
	• Web Reputation Services
	  • Available
	  • Reconnecting
	• File Reputation Services
	  • Available
	  • Reconnecting

`pccntmon -h`	Shows all the available commands

Appendix C

Windows 8 and Windows Server 2012 Support

This appendix discusses OfficeScan support for Windows 8 and Windows Server 2012.

About Windows 8 and Windows Server 2012

Windows 8 and Windows Server 2012 provide users with two types of operating modes: desktop mode and Windows UI mode. The desktop mode is similar to the classic Windows **Start** screen.

The Windows UI provides users with a new user interface experience similar to that used on Windows phones. New features include a scrolling touch screen interface, tiles, and toast notifications.

TABLE C-1. Tiles and Toast Notifications

CONTROL	DESCRIPTION
Tiles	Tiles are similar to the desktop icons used in previous Windows releases. Users click or tap on a tile to launch the application associated with the tile. Live tiles provide users application-specific information that dynamically updates. Applications can post information to tiles even when the application is not running
Toast notifications	Toast notifications are similar to a popup message. These notifications provide time-sensitive information about events that occur while an application is running. Toast notifications appear in the foreground whether Windows is currently in desktop mode, displaying the lock screen, or running another application. **Note** Depending on the application, toast notifications may not appear on all screens or in each mode.

OfficeScan in Windows UI Mode

The following table describes how OfficeScan supports the tiles and toast notifications in Windows UI mode.

TABLE C-2. OfficeScan Support for Tiles and Toast Notifications

CONTROL	OFFICESCAN SUPPORT
Tiles	OfficeScan provides users with a tile that links to the OfficeScan client program. When users click the tile, Windows switches to desktop mode and the OfficeScan client program displays. **Note** OfficeScan does not support live tiles.
Toast notifications	OfficeScan provides the following toast notifications: • Suspicious Program Detected • Scheduled Scan • Threat Resolved • Computer Restart Required • USB Storage Device Detected • Outbreak Detected **Note** OfficeScan only displays toast notifications in Windows UI mode.

Enabling Toast Notifications

Users can choose to receive toast notifications by modifying **PC Settings** on the OfficeScan client computer. OfficeScan requires that users enable toast notifications.

Procedure

1. Move the mouse pointer to the bottom right corner of the screen to display the **Charms** bar.
2. Click **Settings** > **Change PC Settings**.

The **PC settings** screen appears.

3. Click **Notifications**.
4. Under the **Notifications** section, set the following settings to **On**:
   - **Show app notifications**
   - **Show app notifications on the lock screen** (optional)
   - **Play notification sounds** (optional)

Internet Explorer 10

Internet Explorer (IE) 10 is the default browser in Windows 8 and Windows Server 2012. Internet Explorer 10 comes in two different versions: one for the Windows UI and one for the desktop mode.

Internet Explorer 10 for the Windows UI provides a plug-in free browsing experience. Plug-in programs for web browsing previously followed no set standards and consequently, the quality of the code employed by these plug-in programs is variable. Plug-ins also require the use of more system resources and increase the risk of malware infection.

Microsoft has developed Internet Explorer 10 for the Windows UI to follow new standards-based technologies to replace the previously used plug-in solutions. The following table lists the technologies that Internet Explorer 10 uses instead of older plug-in technology.

TABLE C-3. Comparison of Standards-based Technologies to Plug-in Programs

CAPABILITY	WORLD WIDE WEB (W3C) STANDARD TECHNOLOGY	EXAMPLE PLUG-IN EQUIVALENTS
Video and audio	HTML5 video and audio	• Flash • Apple QuickTime • Silverlight

Capability	World Wide Web (W3C) Standard Technology	Example Plug-in Equivalents
Graphics	• HTML5 canvas • Scalable Vector Graphics (SVG) • Cascading Style Sheets, Level 3 (CSS3) Transitions and Animations • CSS Transforms	• Flash • Apple QuickTime • Silverlight • Java applets
Offline storage	• Web storage • File API • IndexedDB • Application cache API	• Flash • Java applets • Google Gears
Network communication, resource sharing, file uploading	• HTML Web Messaging • Cross-origin resource sharing (CORS)	• Flash • Java applets

Microsoft has also developed a plug-in compatible Internet Explorer 10 version solely for the desktop mode. If users in Windows UI mode encounter a website that requires the use of additional plug-in programs, a notification displays in Internet Explorer 10 prompting users to switch to desktop mode. Once in desktop mode, users can view websites requiring the use or installation of third-party plug-in programs.

OfficeScan Feature Support in Internet Explorer 10

The mode in which users operate Windows 8 or Windows Server 2012 affects the Internet Explorer 10 version used and hence the level of support that different OfficeScan features provide. The following table lists the support level for different OfficeScan features in desktop mode and Windows UI mode.

Note

Features not listed provide full support in both Windows operating modes.

TABLE C-4. OfficeScan Feature Support by UI Mode

FEATURE	DESKTOP MODE	WINDOWS UI
Web server console	Full support	Not supported
Web reputation	Full support	Limited support • HTTPS scanning disabled
Firewall	Full support	Limited support • Application filtering disabled

Appendix D

OfficeScan Rollback

This appendix discusses OfficeScan server and client rollback support.

Rolling Back the OfficeScan Server and OfficeScan Clients

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

Important

- Administrators can only roll back the OfficeScan server and clients using the following procedure if the administrator chose to back up the server during the installation process. If the server backup file are not available, refer to the OfficeScan 10.6, 10.6 SP1, or 10.6 SP2 *Installation and Upgrade Guide* for manual rollback procedures.
- This version of OfficeScan only supports rollbacks to the following OfficeScan versions:
  - OfficeScan 10.6
  - OfficeScan 10.6 SP1
  - OfficeScan 10.6 SP2
  - OfficeScan 10.6 SP2 DLP Enhancement Patch
  - OfficeScan 10.6 SP2 Custom Defense Pack
  - OfficeScan 10.6 SP2 Custom Defense Pack Scan Enhancement

Rolling Back the OfficeScan Clients

Procedure

1. Ensure that OfficeScan clients can upgrade the client program.
   a. On the OfficeScan 10.6 SP3 web console, navigate to **Networked Computers** > **Client Management**.
   b. Select the OfficeScan clients to be rolled back.
   c. Click the **Settings** > **Privileges and Other Settings** > **Other Settings** tab.

d. Enable the **Clients can update components but not upgrade the client program or deploy hot fixes** option.

2. On the OfficeScan 10.6 SP3 web console, navigate to **Updates** > **Networked Computers** > **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 clients 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 Clients**.

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

Tip

Administrators can speed up the rollback process by initiating a Manual Update on clients. For details, see *Updating OfficeScan Clients Manually on page 6-41*.

---

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

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

Note

After rolling back the OfficeScan client, 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 client cannot update components. Administrators must change the update source of the rolled-back OfficeScan client to the standard update source to receive further component updates.

Rolling Back the OfficeScan Server

The rollback procedure for the OfficeScan server requires that administrators manually stop Windows services, update the system registry, and replace OfficeScan server files in the OfficeScan installation directory.

Procedure

1. 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)
2. Copy and replace all files and directories from the <*Server installation folder*>`\PCCSRV\Backup\ServicePack3_<build_number>\` directory to the <*Server installation folder*>`\PCCSRV\` directory.
3. Click **Start**, type `regedit`, and press ENTER.

The **Registry Editor** screen appears.

4. 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`
5. Go to **File** > **Import...**.
6. Select the `RegBak_ServicePack3_<build_number>.reg` file located in the <*Server installation folder*>`\PCCSRV\Backup\` directory.
7. Click **Yes** to restore all of the previous OfficeScan version keys.
8. Open a command line editor (click **Start** and type `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
```

9. 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)

10. 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 OfficeScan server has been restored to the previously installed version.

Tip

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

11. After confirming that OfficeScan rolled back successfully, delete the following in the `<Server installation folder>\PCCSRV\Backup\` directory:

    - Folder: `ServicePack3_<SP3_build_number>`
    - File: `RegBak_ServicePack3_<SP3_build_number>.reg`

Appendix E

Glossary

The terms contained in this glossary provide further information about commonly referenced computer terms, as well as Trend Micro products and technologies.

ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides up-to-date downloads of pattern files, scan engines, programs, and other Trend Micro component files through the Internet.

Compressed File

A single file containing one or more separate files plus information for extraction by a suitable program, such as WinZip.

Cookie

A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in the web browser for later use. The next time you access a website for which your browser has a cookie, the browser sends the cookie to the web server, which the web server can then use to present you with customized web pages. For example, you might enter a website that welcomes you by name.

Denial of Service Attack

A Denial of Service (DoS) attack refers to an attack on a computer or network that causes a loss of "service", namely a network connection. Typically, DoS attacks negatively affect network bandwidth or overload system resources such as the computer's memory.

DHCP

Dynamic Host control Protocol (DHCP) is a protocol for assigning dynamic IP addresses to devices in a network. With dynamic addressing, a device can have a

different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

DNS

Domain Name system (DNS) is a general-purpose data query service chiefly used in the Internet for translating host names into IP addresses.

When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data in a machine in the current zone. Client software in the remote server queries the resolver, which answers the request from its database files.

Domain Name

The full name of a system, consisting of its local host name and its domain name, for example, `tellsitall.com`. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).

Dynamic IP Address

A Dynamic IP address is an IP address assigned by a DHCP server. The MAC address of a computer will remain the same, however, the DHCP server may assign a new IP address to the computer depending on availability.

ESMTP

Enhanced Simple Mail Transport Protocol (ESMTP) includes security, authentication and other devices to save bandwidth and protect servers.

End User License Agreement

An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product.

Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.

False Positive

A false positive occurs when a file is incorrectly detected by security software as infected.

FTP

File Transfer Protocol (FTP) is a standard protocol used for transporting files from a server to a client over the Internet. Refer to Network Working Group RFC 959 for more information.

GeneriClean

GeneriClean, also known as referential cleaning, is a new technology for cleaning viruses/malware even without the availability of virus cleanup components. Using a

detected file as basis, GeneriClean determines if the detected file has a corresponding process/service in memory and a registry entry, and then removes them altogether.

Hot Fix

A hot fix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes do not (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).

By default, the OfficeScan clients can install hot fixes. If you do not want OfficeScan clients to install hot fixes, change client update settings in the web console by going to **Networked Computers** > **Client Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings** tab.

If you unsuccessfully attempt to deploy a hot fix on the OfficeScan server, use the Touch Tool to change the time stamp of the hot fix. This causes OfficeScan to interpret the hot fix file as new, which makes the server attempt to automatically deploy the hot fix again. For details about this tool, see *Running the Touch Tool for OfficeScan Client Hot Fixes on page 6-49*.

HTTP

Hypertext Transfer Protocol (HTTP) is a standard protocol used for transporting web pages (including graphics and multimedia content) from a server to a client over the Internet.

HTTPS

Hypertext Transfer Protocol using Secure Socket Layer (SSL). HTTPS is a variant of HTTP used for handling secure transactions.

ICMP

Occasionally a gateway or destination host uses Internet Control Message Protocol (ICMP) to communicate with a source host, for example, to report an error in datagram processing. ICMP uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and implemented by every IP module. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.

IntelliScan

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

Using IntelliScan provides the following benefits:

- Performance optimization: IntelliScan does not affect applications on the client because it uses minimal system resources.
- Shorter scanning period: Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

IntelliTrap

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics. Because IntelliTrap identifies such files as security risks and may

incorrectly block safe files, consider quarantining (not deleting or cleaning) files when you enable IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap.

IntelliTrap uses the following components:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

IP

"The internet protocol (IP) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)

Java File

Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets". An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet transfers its code to your computer and the browser's Java Virtual Machine executes the applet.

LDAP

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP.

Listening Port

A listening port is utilized for client connection requests for data exchange.

MCP Agent

Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP replaces Trend Micro Management Infrastructure (TMI) as the way Control Manager communicates with OfficeScan. MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and two-way communication support
- Single sign-on (SSO) support
- Cluster node support

Mixed Threat Attack

Mixed threat attacks take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the "Nimda" or "Code Red" threats.

NAT

Network Address Translation (NAT) is a standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows trusted networks with privately assigned IP addresses to have access to the Internet. This also

means that you do not have to get a registered IP address for every machine in the network.

NetBIOS

Network Basic Input Output System (NetBIOS) is an application program interface (API) that adds functionality such as network capabilities to disk operating system (DOS) basic input/output system (BIOS).

One-way Communication

NAT traversal has become an increasingly more significant issue in the current real-world network environment. To address this issue, MCP uses one-way communication. One-way communication has the MCP agent initiating the connection to, and polling of commands from, the server. Each request is a CGI-like command query or log transmission. To reduce the network impact, the MCP agent keeps connection alive and open as much as possible. A subsequent request uses an existing open connection. If the connection breaks, all SSL connections to the same host benefit from session ID cache that drastically reduces re-connection time.

Patch

A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program, while non-Windows patches commonly have a setup script.

Phish Attack

Phish, or phishing, is a rapidly growing form of fraud that seeks to fool web users into divulging private information by mimicking a legitimate website.

In a typical scenario, unsuspecting users get an urgent sounding (and authentic looking) email telling them there is a problem with their account that they must immediately fix

to avoid account termination. The email will include a URL to a website that looks exactly like the real thing. It is simple to copy a legitimate email and a legitimate website but then change the so-called backend, which receives the collected data.

The email tells the user to log on to the site and confirm some account information. A hacker receives data a user provides, such as a logon name, password, credit card number, or social security number.

Phish fraud is fast, cheap, and easy to perpetuate. It is also potentially quite lucrative for those criminals who practice it. Phish is hard for even computer-savvy users to detect. And it is hard for law enforcement to track down. Worse, it is almost impossible to prosecute.

Please report to Trend Micro any website you suspect to be a phishing site.

Ping

Ping is a utility that sends an ICMP echo request to an IP address and waits for a response. The Ping utility can determine if the computer with the specified IP address is online or not.

POP3

Post Office Protocol 3 (POP3) is a standard protocol for storing and transporting email messages from a server to a client email application.

Proxy Server

A proxy server is a World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.

RPC

Remote procedure call (RPC) is a network protocol that allows a computer program running on one host to cause code to be executed on another host.

Security Patch

A security patch focuses on security issues suitable for deployment to all customers. Windows security patches include a Setup program, while non-Windows patches commonly have a setup script.

Service Pack

A service pack is a consolidation of hot fixes, patches, and feature enhancements significant enough to be a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

SMTP

Simple Mail Transport Protocol (SMTP) is a standard protocol used to transport email messages from server to server, and client to server, over the internet.

SNMP

Simple Network Management Protocol (SNMP) is a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.

SNMP Trap

A Small Network Management Protocol (SNMP) trap is a method of sending notifications to network administrators that use management consoles that support this protocol.

OfficeScan can store notification in Management Information Bases (MIBs). You can use the MIBs browser to view SNMP trap notification.

SOCKS 4

SOCKS 4 is a TCP protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model.

SSL

Secure Socket Layer (SSL) is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

SSL Certificate

This digital certificate establishes secure HTTPS communication.

TCP

Transmission Control Protocol (TCP) is a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols that support multi-network

applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.

Telnet

Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.

Trojan Port

Trojan ports are commonly used by Trojan horse programs to connect to a computer. During an outbreak, OfficeScan blocks the following port numbers that Trojan programs may use.

TABLE E-1. Trojan Ports

PORT NUMBER	TROJAN HORSE PROGRAM	PORT NUMBER	TROJAN HORSE PROGRAM
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM

Port Number	Trojan Horse Program	Port Number	Trojan Horse Program
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Trusted Port

The server and the OfficeScan client use trusted ports to communicate with each other.

If you block the trusted ports and then restore network settings to normal after an outbreak, OfficeScan clients will not immediately resume communication with the server. Client-server communication will only be restored after the number of hours you have specified in the Outbreak Prevention Settings screen elapses.

OfficeScan uses the HTTP port (by default, 8080) as the trusted port on the server. During installation, you may enter a different port number. To block this trusted port and the trusted port on the OfficeScan client, select the Block trusted ports check box on the Port Blocking screen.

The master installer randomly generates the OfficeScan client trusted port during installation.

Determining the Trusted Ports

Procedure

1. Access <*Server installation folder*>`\PCCSRV`.
2. Open the `ofcscan.ini` file using a text editor such as Notepad.
3. For the server trusted port, search for the string "Master_DomainPort" and then check the value next to it.

   For example, if the string appears as `Master_DomainPort=80`, this means that the trusted port on the server is port 80.
4. For the client trusted port, search for the string "Client_LocalServer_Port" and then check the value next to it.

   For example, if the string appears as `Client_LocalServer_Port=41375`, this means that the trusted port on the client is port 41375.

Two-way Communication

Two-way communication is an alternative to one-way communication. Based on one-way communication but with an extra HTTP-based channel that receives server notifications, two-way communication can improve real time dispatching and processing of commands from the server by the MCP agent.

UDP

User Datagram Protocol (UDP) is a connectionless communication protocol used with IP for application programs to send messages to other programs. Refer to DARPA Internet Program RFC 768 for information.

Uncleanable File

The Virus Scan Engine is unable to clean the following files:

- Files infected with Trojans
- Files infected with Worms
- Write-protected infected files
- Password-protected files
- Backup files
- Infected files in the Recycle Bin
- Infected files in Windows Temp Folder or Internet Explorer Temporary Folder

Files Infected with Trojans

Trojans are programs that perform unexpected or unauthorized, usually malicious, actions such as displaying messages, erasing files, or formatting disks. Trojans do not infect files, thus cleaning is not necessary.

Solution: OfficeScan uses the Virus Cleanup Engine and Virus Cleanup Template to remove Trojans.

Files Infected with Worms

A computer worm is a self-contained program (or set of programs) able to spread functional copies of itself or its segments to other computer systems. The propagation

usually takes place through network connections or email attachments. Worms are uncleanable because the file is a self-contained program.

Solution: Trend Micro recommends deleting worms.

Write-protected Infected Files

Solution: Remove the write-protection to allow OfficeScan to clean the file.

Password-protected Files

Includes password-protected compressed files or password-protected Microsoft Office files.

Solution: Remove the password protection for OfficeScan to clean these files.

Backup Files

Files with the RB0~RB9 extensions are backup copies of infected files. OfficeScan creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.

Solution: If OfficeScan successfully cleans the infected file, you do not need to keep the backup copy. If the computer functions normally, you can delete the backup file.

Index

A

Access Control Server (ACS), 16-3
ACS certificate, 16-17
action on monitored system events, 8-4
actions
    Data Loss Prevention, 10-34
ActiveAction, 7-36
Active Directory, 2-32–2-34, 2-49, 2-53, 5-13, 5-30
    client grouping, 2-49
    credentials, 2-33
    custom client groups, 2-32
    duplicate structure, 2-53
    integration, 2-32
    outside server management, 2-32
    role-based administration, 2-32
    scope and query, 14-66
    synchronization, 2-34
ActiveSync, 10-33
ActiveX malicious code, 7-3
Additional Service Settings, 14-6
advanced permissions
    configuring, 9-11
    storage devices, 9-5, 9-6
application filtering, 12-3
approved list, 7-46
approved programs list, 8-6
assessment mode, 7-70
Authentication, Authorization, and Accounting (AAA), 16-4
automatic client grouping, 2-49, 2-50
AutoPcc.exe, 5-11, 5-12, 5-21, 5-22

B

Behavior Monitoring, 8-12
    action on system events, 8-4
    exception list, 8-5
    logs, 8-12
Behavior Monitoring Configuration Pattern, 6-8
Behavior Monitoring Core Service, 6-8
Behavior Monitoring Detection Pattern, 6-7
Behavior Monitoring Driver, 6-8
blocked programs list, 8-6
boot sector virus, 7-3

C

C&C callbacks
    global settings, 11-11
    widgets, 2-24
CA certificate, 16-17, 16-19
cache settings for scans, 7-60
Case Diagnostic Tool, 18-2
Certificate Authority (CA), 16-4
certificates, 16-16
    CA, 16-19
    SSL, 16-35, 16-37
Certified Safe Software List, 12-3
Certified Safe Software Service, 8-8
Check Point SecureClient, 5-30
Cisco NAC
    architecture, 16-6
    components and terms, 16-2
    policy server deployment, 16-23
Cisco Trust Agent, 6-9, 16-2
client console
    access restriction, 14-17
client disk image, 5-13, 5-36
client grouping, 2-49, 2-50, 2-52, 2-54–2-57

Active Directory, 2-49, 2-52
adding a domain, 2-55
automatic, 2-49, 2-50
custom groups, 2-49
deleting a domain or client, 2-56
DNS, 2-49
IP addresses, 2-54
manual, 2-49
methods, 2-49
moving a client, 2-57
NetBIOS, 2-49
renaming a domain, 2-57
tasks, 2-55
client installation, 5-2, 5-21
browser-based, 5-17
Client Packager, 5-23
from the web console, 5-19
from the web install page, 5-15
Login Script Setup, 5-21
post-installation, 5-65
system requirements, 5-2
using client disk image, 5-36
using Security Compliance, 5-59
using Vulnerability Scanner, 5-37
client logs
ActiveUpdate logs, 18-17
client connection logs, 18-17
client update logs, 18-18
Damage Cleanup Services logs, 18-16
Data Protection debug logs, 10-55, 18-22
debug logs, 18-15
fresh installation logs, 18-16
Mail Scan logs, 18-17
OfficeScan firewall debug logs, 18-19
Outbreak Prevention debug logs, 18-18
TDI debug logs, 18-23
upgrade/hot fix logs, 18-16
web reputation debug logs, 18-21
client mover, 14-21
Client Packager, 5-12, 5-23–5-25, 5-30, 5-32
deployment, 5-26
settings, 5-26
clients, 2-49, 2-56, 2-57, 4-30, 5-2
connection, 4-30
deleting, 2-56
features, 5-3
grouping, 2-49
installation, 5-2
locations, 4-30
moving, 2-57
proxy settings, 4-30
client security level, 14-16
client self-protection, 14-12
client tree, 2-35, 2-37–2-40, 2-43–2-46, 2-48
about, 2-35
advanced search, 2-38, 2-39
filters, 2-38
general tasks, 2-37
specific tasks, 2-39, 2-40, 2-43–2-46, 2-48
Cisco NAC agent deployment, 2-48
client management, 2-40
manual component updates, 2-44
outbreak prevention, 2-43
rollback component updates, 2-45
security risk logs, 2-46
views, 2-38
client uninstallation, 5-68
client update
automatic, 6-35
customized source, 6-30
event-triggered, 6-35

from the ActiveUpdate server, 6-43
manual, 6-41
privileges, 6-43
scheduled update, 6-37, 6-43
scheduled update with NAT, 6-39
standard source, 6-28
client upgrade
disable, 6-44
client validation, 16-4
COM file infector, 7-3
Common Firewall Driver, 6-6, 6-7, 18-19
Common Firewall Pattern, 7-3
Compliance Report, 14-53
component duplication, 6-19, 6-56
components, 2-19, 5-67, 6-2
on the client, 6-26
on the OfficeScan server, 6-14
on the Update Agent, 6-50
update privileges and settings, 6-43
update summary, 6-59
compressed files, 7-27, 7-65, 7-68
condition statements, 10-20
Conflicted ARP, 12-4
connection verification, 14-40
contacting, 18-24–18-26
documentation feedback, 18-26
Knowledge Base, 18-25
technical support, 18-24
Trend Micro, 18-24–18-26
continuity of protection, 4-10
Control Manager
integration with OfficeScan, 13-22
MCP Agent logs, 18-11
conventional scan, 7-8, 7-9
switching to smart scan, 7-9
cookie scanning, 7-71
CPU usage, 7-28
criteria
customized expressions, 10-7
keywords, 10-15, 10-16
custom client groups, 2-32, 2-49
customized expressions, 10-6, 10-7, 10-9
criteria, 10-7
importing, 10-9
customized keywords, 10-14
criteria, 10-15, 10-16
importing, 10-18
customized templates, 10-19
creating, 10-21
importing, 10-22

D

Damage Cleanup Services, 1-15, 5-3, 5-5
dashboards
Summary, 2-5–2-7, 2-10
database backup, 13-39
database scanning, 7-66
data identifiers, 10-4
expressions, 10-4
file attributes, 10-4
keywords, 10-4
Data Loss Prevention, 10-2–10-4
actions, 10-34
channels, 10-23
data identifiers, 10-4
expressions, 10-5–10-7, 10-9
file attributes, 10-10–10-12
keywords, 10-12–10-16, 10-18
network channels, 10-23–10-27, 10-29, 10-30, 10-35
policies, 10-40
policy, 10-3

system and application channels, 10-30–10-34
templates, 10-18–10-22
widgets, 2-21
Data Loss Prevention:decompression rules;decompression rules;compressed files:decompression rules, 10-36
Data Loss Prevention:system and application channels;system and application channels;system and application channels:PGP encryption, 10-32
Data Protection
deployment, 3-5
installation, 3-2
license, 3-4
status, 3-7
uninstallation, 3-14
debug logs
clients, 18-15
server, 18-3
device control, 9-2, 9-3, 9-5–9-12, 9-14
advanced permissions, 9-11
configuring, 9-11
approved list, 9-12
Digital Signature Provider, 9-7
external devices, 9-10, 9-14
managing access, 9-10, 9-14
non-storage devices, 9-10
permissions, 9-3, 9-5, 9-6, 9-8, 9-10
program path and name, 9-8
requirements, 9-2
storage devices, 9-3, 9-5, 9-6
USB devices, 9-12
wildcards, 9-9
Device Control, 1-16
logs, 9-17, 18-10
notifications, 9-16
device control;device control list;device control list:adding programs, 9-15
Device List Tool, 9-13
DHCP settings, 5-45
Digital Asset Control
widgets, 2-23
digital certificates, 16-5
digital signature cache, 7-61
Digital Signature Pattern, 6-8, 7-61
Digital Signature Provider, 9-7
specifying, 9-7
documentation, x
documentation feedback, 18-26
domains, 2-48, 2-49, 2-55–2-57
adding, 2-55
client grouping, 2-49
deleting, 2-56
renaming, 2-57
DSP, 9-7

E

EICAR test script, 5-67, 7-3
email domains, 10-24
encrypted files, 7-41
End User License Agreement (EULA), E-4
evaluation version, 13-36
Event Monitoring, 8-2
exception list, 8-5
Behavior Monitoring, 8-5
EXE file infector, 7-3
export settings, 14-51
expressions, 10-4, 10-5
customized, 10-6, 10-9
criteria, 10-7
predefined, 10-5
external device protection, 6-8

external devices
managing access, 9-10, 9-14

F

FakeAV, 7-40
file attributes, 10-4, 10-10–10-12
creating, 10-11
importing, 10-12
wildcards, 10-11
file reputation, 4-3
firewall, 5-3, 5-5, 12-2
benefits, 12-2
default policy exceptions, 12-14
disabling, 12-6
outbreak monitor, 12-5
policies, 12-8
policy exceptions, 12-13
privileges, 12-5, 12-22
profiles, 12-4, 12-17
tasks, 12-8
testing, 12-30
firewall log count, 12-25
Fragmented IGMP, 12-5
FTP, 10-25

G

gateway IP address, 14-3
gateway settings importer, 14-4

H

hot fixes, 6-9, 6-49
HTML virus, 7-4
HTTP and HTTPS, 10-26

I

IDS, 12-4
IM applications, 10-26
import settings, 14-51
inactive clients, 14-23
incremental pattern, 6-19
installation, 5-2
client, 5-2
Data Protection, 3-2
Plug-in Manager, 15-3
plug-in program, 15-4
Policy Server, 16-32
Security Compliance, 5-59
integrated server, 4-6
integrated Smart Protection Server, 4-17
ptngrowth.ini, 4-17
update, 4-17, 4-19
components, 4-19
Web Blocking List, 4-19
IntelliScan, 7-26
IntelliTrap Exception Pattern, 6-5
IntelliTrap Pattern, 6-5
intranet, 4-11
Intrusion Detection System, 12-4
IPv6, 4-23
support, 4-23
IPv6 support, A-2
displaying IPv6 addresses, A-7
limitations, A-3, A-4
IpXfer.exe, 14-21

J

Java malicious code, 7-3
JavaScript virus, 7-4
joke program, 7-2

K

keywords, 10-4, 10-12
customized, 10-14–10-16, 10-18
predefined, 10-13
Knowledge Base, 18-25

L

LAND Attack, 12-5
licenses, 13-36
    Data Protection, 3-4
    status, 2-6
location awareness, 14-2
locations, 4-30
    awareness, 4-30
logical operators, 10-20
Login Script Setup, 5-11, 5-12, 5-21, 5-22
logs, 13-33
    about, 13-33
    Behavior Monitoring, 8-12
    client update logs, 6-47
    connection verification logs, 14-41
    Device Control logs, 9-17
    firewall logs, 12-23, 12-24, 12-27
    scan logs, 7-93
    security risk logs, 7-83
    spyware/grayware logs, 7-90
    spyware/grayware restore logs, 7-92
    system event logs, 13-32
    virus/malware logs, 7-73, 7-83
    web reputation logs, 11-18
LogServer.exe, 18-3, 18-15

M

MAC address, 14-3
macro virus, 7-3
mail scan, 5-4, 5-6, 5-29, 7-58
Malware Behavior Blocking, 8-2
manual client grouping, 2-49
Manual Scan, 7-17
    shortcut, 7-66
Microsoft Exchange Server scanning, 7-67
Microsoft SMS, 5-13, 5-32
migration
    from ServerProtect Normal Servers, 5-62
    from third-party security software, 5-61
monitored email domains, 10-24
monitored system events, 8-3
monitored targets, 10-28, 10-29
MSI package, 5-13, 5-30, 5-32

N

NetBIOS, 2-49
Network Access Device, 16-3
network channels, 10-23–10-27, 10-29, 10-30, 10-35
    email clients, 10-24
    FTP, 10-25
    HTTP and HTTPS, 10-26
    IM applications, 10-26
    monitored targets, 10-30, 10-35
    non-monitored targets, 10-30, 10-35
    SMB protocol, 10-26
    transmission scope, 10-30
        all transmissions, 10-27
        conflicts, 10-30
        external transmissions, 10-29
    transmission scope and targets, 10-27
    webmail, 10-27
network virus, 7-3, 12-3
Network VirusWall Enforcer, 4-30
new features, 1-2, 1-6, 1-8
non-monitored email domains, 10-24
non-monitored targets, 10-28, 10-29
non-storage devices
    permissions, 9-10
notifications
    C&C callback detections, 11-16
    client update, 6-46
    computer restart, 6-47

Device Control, 9-16
firewall violations, 12-26
for administrators, 10-46, 13-29
for client users, 7-80, 10-49
outbreaks, 7-94, 11-16, 12-29
outdated Virus Pattern, 6-47
spyware/grayware detection, 7-45
virus/malware detection, 7-41
web threat detection, 11-11

O

OfficeScan
about, 1-2
client, 1-18
client services, 14-11
components, 2-19, 6-2
component update, 5-67
database backup, 13-39
database scanning, 7-66
documentation, x
key features and benefits, 1-14
licenses, 13-36
logs, 13-33
programs, 2-19
SecureClient integration, 17-2
terminology, xii
web console, 2-2
web server, 13-41
OfficeScan client
connection with OfficeScan server, 14-24, 14-37
connection with Smart Protection Server, 14-38
detailed client information, 14-50
files, 14-14
import and export settings, 14-51
inactive clients, 14-23
installation methods, 5-10
processes, 14-15
registry keys, 14-15
reserved disk space, 6-45
uninstallation, 5-68
OfficeScan server, 1-17
functions, 1-17
OfficeScan update, 6-11
on-demand scan cache, 7-62
outbreak criteria, 7-94, 11-16, 12-29
outbreak prevention, 2-17
disabling, 7-103
policies, 7-99
outbreak prevention policy
block ports, 7-100
deny write access, 7-102
limit/deny access to shared folders, 7-99
outside server management, 2-32, 14-65
logs, 18-9
query results, 14-68
scheduled query, 14-69
Overlapping Fragment, 12-5

P

packer, 7-3
password, 13-42
patches, 6-9
pattern files
smart protection, 4-7
Smart Scan Agent Pattern, 4-7
Smart Scan Pattern, 4-8
Web Blocking List, 4-8
PCRE, 10-6
performance control, 7-28
Performance Tuning Tool, 18-2
Perle Compatible Regular Expressions, 10-6
permissions

advanced, 9-11
non-storage devices, 9-10
program path and name, 9-8
storage devices, 9-3
phishing, E-9
Ping of Death, 12-4
Plug-in Manager, 1-14, 5-4, 5-7, 15-2
installation, 15-3
managing native OfficeScan features, 15-4
troubleshooting, 15-9
uninstallation, 15-9
plug-in program
installation, 15-4
policies
Data Loss Prevention, 10-40
firewall, 12-4, 12-8
web reputation, 11-5
policy, 10-3
Policy Enforcement Pattern, 6-8
Policy Server for Cisco NAC, 16-3
CA certificate, 16-19
certificates, 16-16
client validation process, 16-7
default policies, 16-15
default rules, 16-12
deployment overview, 16-23
policies, 16-42
policies and rules, 16-10
policy composition, 16-14
Policy Server installation, 16-32
rule composition, 16-10
rules, 16-42
SSL certificate, 16-17
synchronization, 16-43
system requirements, 16-19
port blocking, 7-100
posture token, 16-4
predefined expressions, 10-5
viewing, 10-5
predefined keywords
distance, 10-13
number of keywords, 10-13
predefined tabs, 2-10
predefined templates, 10-19
predefined widgets, 2-10
pre-installation tasks, 5-16, 5-19, 5-59
privileges
firewall privileges, 12-22, 12-24
mail scan privileges, 7-58
proxy configuration privileges, 14-48
roaming privilege, 14-19
scan privileges, 7-49
Scheduled Scan privileges, 7-52
unload privilege, 14-18
probable virus/malware, 7-2, 7-86
programs, 2-19, 6-2
proxy settings, 4-30
automatic proxy settings, 14-49
clients, 4-30
for external connection, 14-47
for internal connection, 14-46
for server component update, 6-17
privileges, 14-48
ptngrowth.ini, 4-16, 4-17

Q

quarantine directory, 7-38, 7-42
quarantine manager, 13-43

R

Real-time Scan, 7-14
Real-time Scan service, 14-37

reference server, 13-27
Remote Authentication Dial-In User Service (RADIUS), 16-5
remote installation, 5-12
roaming clients, 5-5, 5-7
role-based administration, 2-32, 13-2
    user accounts, 13-17
    user roles, 13-2
rootkit detection, 6-8

S

scan actions, 7-34
    spyware/grayware, 7-45
    virus/malware, 7-68
scan cache, 7-60
scan criteria
    CPU usage, 7-28
    file compression, 7-27
    files to scan, 7-26
    schedule, 7-29
    user activity on files, 7-26
scan exclusions, 7-29, 7-30
    directories, 7-31
    file extensions, 7-33
    files, 7-33
scan method, 5-26
    default, 7-7
Scan Now, 7-21
scan privileges, 7-49
scan types, 5-3, 5-5, 7-13
scheduled assessments, 14-64
Scheduled Scan, 7-19
    postpone, 7-72
    reminder, 7-72
    resume, 7-73
    skip and stop, 7-52, 7-72
    stop automatically, 7-72
SCV Editor, 17-2
SecureClient, 5-5, 5-7, 17-2
    integrating with OfficeScan, 17-2
    Policy Servers, 17-2
    SCV Editor, 17-2
Secure Configuration Verification, 17-2
Security Compliance, 14-52
    components, 14-55
    enforcing, 14-65
    enforcing update, 6-48
    installation, 5-59
    logs, 18-9
    outside server management, 2-32, 14-65
    scan, 14-57
    scheduled assessments, 14-64
    services, 14-54
    settings, 14-59
Security Information Center, 18-26
security patches, 6-9
security posture, 16-4
security risks, 7-2, 7-4–7-6
    phish attacks, E-9
    protection from, 1-15
    spyware/grayware, 7-4–7-6
server logs
    Active Directory logs, 18-6
    Apache server logs, 18-8
    client grouping logs, 18-7
    Client Packager logs, 18-8
    component update logs, 18-7
    Control Manager MCP Agent logs, 18-11
    debug logs, 18-3
    Device Control logs, 18-10
    local installation/upgrade logs, 18-5
    outside server management logs, 18-9

remote installation/upgrade logs, 18-5
role-based administration logs, 18-6
Security Compliance logs, 18-9
ServerProtect Migration Tool debug logs, 18-10
Virtual Desktop Support logs, 18-14
Virus Scan Engine debug logs, 18-12
VSEncrypt debug logs, 18-11
web reputation logs, 18-10
ServerProtect, 5-62
Server Tuner, 13-44
server update
component duplication, 6-19
logs, 6-25
manual update, 6-24
proxy settings, 6-17
scheduled update, 6-24
update methods, 6-23
service restart, 14-11
Smart Feedback, 4-3
smart protectection, 4-12
smart protection, 4-2–4-4, 4-6–4-9, 4-23
environment, 4-12
File Reputation Services, 4-3
pattern files, 4-7–4-9
Smart Scan Agent Pattern, 4-7
Smart Scan Pattern, 4-8
update process, 4-9
Web Blocking List, 4-8
Smart Feedback, 4-3
Smart Protection Network, 4-6
Smart Protection Server, 4-6
source, 4-6, 4-7
sources, 4-23
comparison, 4-6
IPv6 support, 4-23
locations, 4-23
protocols, 4-7
volume of threats, 4-2
Web Reputation Services, 4-3, 4-4
Smart Protection Network, 1-2, 4-6
Smart Protection Server, 4-6, 4-12, 4-16, 4-17, 4-19
best practices, 4-16
installation, 4-12
integrated, 4-6, 4-17, 4-19
standalone, 4-6, 4-16
update, 6-13, 6-26
smart scan, 6-3, 7-8, 7-9
switching from conventional scan, 7-9
Smart Scan Agent Pattern, 4-7, 6-3
Smart Scan Pattern, 4-8, 6-3
SMB protocol, 10-26
spyware/grayware, 7-4–7-6
adware, 7-4
dialers, 7-4
guarding against, 7-6
hacking tools, 7-5
joke programs, 7-4
password cracking applications, 7-5
potential threats, 7-5
remote access tools, 7-5
restoring, 7-48
spyware, 7-4
spyware/grayware scan
actions, 7-45
approved list, 7-46
results, 7-91
Spyware Active-monitoring Pattern, 6-6
Spyware Pattern, 6-6
Spyware Scan Engine, 6-6
SSL Certificate, 16-35, 16-37

standalone server, 4-6
standalone Smart Protection Server, 4-16
    ptngrowth.ini, 4-16
storage devices
    advanced permissions, 9-5, 9-6
    permissions, 9-3
summary
    dashboard, 2-5–2-7, 2-10
    updates, 6-59
summary dashboard
    components and programs, 2-19
Summary dashboard, 2-5–2-7, 2-10
    predefined tabs, 2-10
    predefined widgets, 2-10
    product license status, 2-6
    tabs, 2-7
    user accounts, 2-5
    widgets, 2-7
Support Intelligence System, 2-5, 18-2
synchronization, 16-43
SYN Flood, 12-4
system and application channels, 10-23, 10-30–10-34
    CD/DVD, 10-30
    peer-to-peer (P2P), 10-31
    printer, 10-32
    removable storage, 10-32
    synchronization software, 10-33
    Windows clipboard, 10-34
system requirements
    Policy Server, 16-19
    Update Agent, 6-50

T

tabs, 2-7
Teardrop, 12-5
technical support, 18-24
templates, 10-18–10-22
    condition statements, 10-20
    customized, 10-19, 10-21, 10-22
    logical operators, 10-20
    predefined, 10-19
Terminal Access Controller Access Control System (TACACS+), 16-5
test scan, 5-67
test virus, 7-3
third-party security software, 5-60
Tiny Fragment Attack, 12-5
TMPerftool, 18-2
TMTouch.exe, 6-49
token variable, 7-97
Too Big Fragment, 12-4
Top 10 Security Risk Statistics, 2-18
touch tool, 6-49
TrendLabs, 18-25
Trend Micro
    contact information, 18-24
    Knowledge Base, 18-25
    Security Information Center, 18-26
    TrendLabs, 18-25
Trojan horse program, 1-15, 6-5, 7-2
troubleshooting
    Plug-in Manager, 15-9
troubleshooting resources, 18-2

U

uninstallation, 5-68
    Data Protection, 3-14
    from the web console, 5-68
    Plug-in Manager, 15-9
    using the uninstallation program, 5-69
unreachable clients, 14-41
update
    Smart Protection Server, 6-13, 6-26

Update Agent, 5-3, 5-5, 5-28, 6-50
analytical report, 6-57
assigning, 6-51
component duplication, 6-56
standard update source, 6-53
system requirements, 6-50
update methods, 6-57
update methods
clients, 6-34
OfficeScan server, 6-23
Update Agent, 6-57
Update Now, 6-43
updates, 4-17, 4-19
clients, 6-26
enforcing, 6-48
integrated Smart Protection Server, 4-17, 4-19
OfficeScan server, 6-14
Update Agent, 6-50
update source
clients, 6-28
OfficeScan server, 6-16
Update Agents, 6-52
URL Filtering Engine, 6-7
USB devices
approved list, 9-12
configuring, 9-12
user accounts, 2-5
Summary dashboard, 2-5
user role
administrator, 13-10
guest user, 13-10
Trend Power User, 13-11

V

VBScript virus, 7-4
VDI, 14-70
logs, 18-14
VDI Pre-scan Template Generation Tool, 14-80
Virtual Desktop Support, 14-70
virus/malware, 7-2–7-4
ActiveX malicious code, 7-3
boot sector virus, 7-3
COM and EXE file infector, 7-3
Java malicious code, 7-3
joke program, 7-2
macro virus, 7-3
packer, 7-3
probable virus/malware, 7-2
test virus, 7-3
Trojan horse program, 7-2
types, 7-2–7-4
VBScript, JavaScript or HTML virus, 7-4
worm, 7-4
virus/malware scan
global settings, 7-64
results, 7-84
Virus Cleanup Engine, 6-5
Virus Cleanup Template, 6-5
Virus Encyclopedia, 7-2
Virus Pattern, 6-3, 6-47, 6-48
Virus Scan Driver, 6-4
Virus Scan Engine, 6-3
Vulnerability Scanner, 5-14, 5-37
computer description retrieval, 5-54
DHCP settings, 5-45
effectiveness, 5-37
ping settings, 5-56
product query, 5-50
supported protocols, 5-52

W

Web Blocking List, 4-8, 4-19
web console, 1-14, 2-2–2-4
about, 2-2
banner, 2-4
logon account, 2-4
password, 2-4
requirements, 2-3
URL, 2-3
web install page, 5-10, 5-15
webmail, 10-27
web reputation, 1-16, 4-3, 4-4, 5-3, 5-5, 11-4
logs, 18-10
policies, 11-5
web server information, 13-41
web threats, 11-2
widgets, 2-7, 2-10, 2-13, 2-16, 2-17, 2-19–2-21, 2-23, 2-24, 2-27–2-29, 15-3
available, 2-10
C&C Callback Events, 2-24
Client Connectivity, 2-13
Client Updates, 2-19
Digital Asset Control - Detections Over Time, 2-23
File Reputation Threat Map, 2-29
OfficeScan and Plug-ins Mashup, 2-20
Outbreaks, 2-17
Security Risk Detections, 2-16
Top Data Loss Prevention Incidents, 2-21
Web Reputation Top Threatened Users, 2-28
Web Reputation Top Threat Sources, 2-27
wildcards, 10-11
device control, 9-9
file attributes, 10-11
Windows clipboard, 10-34
Windows Server Core, B-2
available client features, B-6
commands, B-7
supported installation methods, B-2
worm, 7-4

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: OSEM105883/130313