



Trend Micro Apex OneTM Service Pack 1 Patch 1

Installation and Upgrade Guide

For Enterprise and Medium Business

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

<https://docs.trendmicro.com/en-us/enterprise/apex-one.aspx>

Trend Micro, the Trend Micro t-ball logo, Trend Micro Apex One, Trend Micro Apex Central, 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 © 2023. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM09525/220511

Release Date: July 2023

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

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

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

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

Evaluate this documentation on the following site:

<https://www.trendmicro.com/download/documentation/rating.asp>

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Apex One collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

<https://www.trendmicro.com/privacy>

Table of Contents

Preface

Preface	1
Apex One Documentation	2
Audience	3
Document Conventions	3
Terminology	4

Chapter 1: Planning Apex One Installation and Upgrade

Apex One Server Requirements	1-3
Operating System Support	1-3
SQL Server Requirements	1-4
Security Agent Support	1-5
Installation Verification	1-6
Apex Central Extended Feature Requirements	1-7
Apex One Application Control	1-7
Apex One Endpoint Sensor	1-11
Managed Detection and Response Service	1-15
Apex One Vulnerability Protection	1-16
Installation and Upgrade Checklist	1-19
Known Compatibility Issues	1-23
Microsoft Lockdown Tools and URLScan	1-23
Preventing URLScan Interference in Agent-Server Communication	1-23
Microsoft Exchange Server	1-23
Database Servers	1-24

Chapter 2: Installing Trend Micro Apex One

Fresh Installation Considerations	2-2
Location of the Apex One Server	2-2

Server Performance	2-3
Dedicated Server	2-3
Scan Method Deployment During Installation	2-3
Conventional Scan	2-4
Smart Scan	2-4
Scan Method Deployment	2-4
Network Traffic	2-5
Network Traffic During Component Updates	2-5
Update Agents and Network Traffic	2-6
Apex Central and Network Traffic	2-6
Third-Party Security Software	2-6
Active Directory	2-7
Silent Installation	2-7
Preparing for Silent Installation	2-7
Recording Setup Configuration to a Response File	2-7
Running Silent Installation	2-8
The Setup Program	2-9
License Agreement	2-9
Endpoint Prescan	2-9
Proxy Server	2-10
Product Activation	2-11
Product Versions	2-11
Registration Key and Activation Codes	2-11
Installation Path	2-12
Server Identification	2-12
Web Server	2-13
HTTP Port	2-13
SSL Support	2-13
Web Server Ports	2-14
Endpoint Sensor Installation	2-15
Apex One Database Setup	2-16
Apex One Security Agent Deployment	2-18
Install Integrated Smart Protection Server	2-18
Integrated Server Not Installed	2-19
Install Security Agent	2-19
Smart Feedback	2-20

Security Agent Installation	2-21
Apex One Firewall	2-22
Anti-spyware Feature	2-22
Web Reputation Services	2-23
Server Authentication Certificate	2-24
Administrator Account Password	2-24
Access the Web Console	2-25
Unload and Uninstall the Security Agent	2-25
Apex One Program Shortcuts	2-25
Installation Information	2-25
InstallShield Wizard Complete	2-25

Chapter 3: Upgrading Trend Micro Apex One

Upgrade Considerations	3-2
IPv6 Support	3-2
Trend Micro Apex One Settings and Configurations	3-3
Backing up and Restoring the Apex One Database and Configuration Files	3-3
Scan Method Deployment During Upgrade	3-5
Before Upgrading the Server and Agents	3-5
Upgrade Method 1: Disable Automatic Agent Upgrade	3-7
Part 1: Configure Update Settings on the Apex One Server	3-8
Part 2: Upgrade the Apex One Server	3-8
Part 3: Upgrade Security Agents	3-8
Upgrade Method 2: Upgrade Update Agents	3-9
Part 1: Configure Update Settings on the Apex One Server	3-10
Part 2: Upgrade the Apex One Server	3-10
Part 3: Upgrade Update Agents	3-10
Part 4: Configure Update Agent Settings	3-12
Part 5: Upgrade Security Agents	3-12
Upgrade Results	3-13
Online Agents	3-13
Offline Agents	3-14
Independent (Roaming) Agents	3-14

Upgrade Method 3: Move Agents to the Apex One Service Pack 1 Server	3-15
Part 1: Perform a fresh installation of the Apex One server and then configure update settings	3-15
Part 2: Upgrade Security Agents	3-16
Upgrade Results	3-17
Upgrade Method 4: Enable Automatic Agent Upgrade ...	3-17
Part 1: Configure Update Settings on the Apex One Server	3-17
Part 2: Upgrade the Apex One Server	3-18
Upgrade Results	3-18
Performing a Local Upgrade	3-19
License Agreement	3-19
Forensic Data	3-19
Security Agent Upgrades	3-20
Enable Enhanced Protection	3-21
Database Back Up	3-23
Endpoint Sensor Installation	3-23
Apex One Database Setup	3-24
Apex One Security Agent Deployment	3-26
Installation Information	3-26
Edge Relay Server Update	3-26
InstallShield Wizard Complete	3-27

Chapter 4: Post-installation Tasks

Verifying the Server Installation or Upgrade	4-2
Verifying Integrated Smart Protection Server Installation	
4-4	
Updating the Apex One Server	4-4
Checking Default Settings	4-5
Scan Settings	4-5
Agent Settings	4-5
Agent Privileges	4-5
Registering Apex One to Apex Central	4-6

Chapter 5: Uninstalling Apex One

Uninstallation Considerations	5-2
Before Uninstalling the Apex One Server	5-2
Moving Agents to Another Server	5-2
Backing Up and Restoring the Apex One Configuration Files	5-3
Uninstalling the Apex One Server	5-4
Uninstalling the Apex One Server Using the Uninstallation Program	5-4
Manually Uninstalling the Apex One Server	5-5
Part 1: Integrated Smart Protection Server Uninstallation	5-5
Part 2: Apex One Server Uninstallation	5-7

Chapter 6: Troubleshooting Resources

Support Intelligence System	6-2
Case Diagnostic Tool	6-2
Trend Micro Performance Tuning Tool	6-2
Identifying System-intensive Applications	6-2
Installation Logs	6-4
Server Debug Logs	6-4
Enabling Debug Logging on the Apex One Server computer	6-5
Option 1:	6-5
Option 2:	6-5
Agent Debug Logs	6-6
Enabling Debug Logging on the Security Agent	6-7

Chapter 7: Technical Support

Troubleshooting Resources	7-2
Using the Support Portal	7-2
Threat Encyclopedia	7-2

Contacting Trend Micro	7-3
Speeding Up the Support Call	7-3
Sending Suspicious Content to Trend Micro	7-4
Email Reputation Services	7-4
File Reputation Services	7-4
Web Reputation Services	7-5
Other Resources	7-5
Download Center	7-5
Documentation Feedback	7-5

Appendix A: Sample Deployment

Basic Network	A-2
Multiple Site Network	A-3
Preparing a Multiple Site Network	A-4
Head Office Deployment	A-5
Remote Site 1 Deployment	A-5
Minimizing the Impact of Component Updates Across the WAN	A-5
Remote Site 2 Deployment	A-6

Index

Index	IN-1
-------------	------

Preface

Preface

Welcome to the Trend Micro Apex One™ *Installation and Upgrade Guide*. This document discusses requirements and procedures for installing the Apex One server, and upgrading the server and Security Agents.

Topics in this chapter:

- *Apex One Documentation on page 2*
- *Audience on page 3*
- *Document Conventions on page 3*
- *Terminology on page 4*



Note

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

Apex One Documentation

Apex One documentation includes the following:

TABLE 1. Apex One Documentation

DOCUMENTATION	DESCRIPTION
Installation and Upgrade Guide	<p>A PDF document that discusses requirements and procedures for installing the Apex One server, and upgrading the server and agents</p> <p> Note The Installation and Upgrade Guide may not be available for minor release versions, service packs, or patches.</p>
System Requirements	A PDF document that outlines the minimal and recommended system requirements for installing the Apex One server, and upgrading the server and agents
Administrator's Guide	A PDF document that discusses getting started information, Security Agent installation procedures, and Apex One server and agent management
Help	HTML files compiled in WebHelp or CHM format that provide "how to's", usage advice, and field-specific information. The Help is accessible from the Apex One server and agent consoles, and from the Apex One 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: https://esupport.trendmicro.com

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

<https://docs.trendmicro.com/en-us/enterprise/apex-one.aspx>

Audience

Apex One documentation is intended for the following users:

- **Apex One Administrators:** Responsible for Apex One management, including the Apex One server and Security Agent installation and management. These users are expected to have advanced networking and server management knowledge.
- **End users:** Users who have the Security Agent installed on their endpoints. The endpoint skill level of these individuals ranges from beginner to power user.

Document Conventions

The documentation uses the following conventions.

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes

CONVENTION	DESCRIPTION
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

Terminology

The following table provides the official terminology used throughout the Apex One documentation:

TABLE 3. Apex One Terminology

TERMINOLOGY	DESCRIPTION
Security Agent	The Apex One agent program
Agent endpoint	The endpoint where the Security Agent is installed
Agent user (or user)	The person managing the Security Agent on the agent endpoint
Server	The Apex One server program
Server computer	The endpoint where the Apex One server is installed
Administrator (or Apex One administrator)	The person managing the Apex One server
Console	The user interface for configuring and managing Apex One server and agent settings The console for the Apex One server program is called "web console", while the console for the Security Agent program is called "Security Agent console".

TERMINOLOGY	DESCRIPTION
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 Apex One server installation
Apex One service	Services hosted through Microsoft Management Console (MMC). For example, ofcservice.exe, the Apex One Master Service.
Program	Includes the Security Agent and Plug-in Manager
Components	Responsible for scanning, detecting, and taking actions against security risks
Agent installation folder	<p>The folder on the endpoint that contains the Security Agent files. If you accept the default settings during installation, you will find the installation folder at any of the following locations:</p> <p>C:\Program Files\Trend Micro\Security Agent C:\Program Files (x86)\Trend Micro\Security Agent</p>
Server installation folder	<p>The folder on the endpoint that contains the Apex One server files. If you accept the default settings during installation, you will find the installation folder at any of the following locations:</p> <p>C:\Program Files\Trend Micro\Apex One C:\Program Files (x86)\Trend Micro\Apex One</p> <p>For example, if a particular file is found under \PCCSRV on the server installation folder, the full path to the file is:</p> <p>C:\Program Files\Trend Micro\Apex One\PCCSRV \<file_name>.</p>
Smart scan agent	Any Security Agent that has been configured to use smart scan

TERMINOLOGY	DESCRIPTION
Conventional scan agent	Any Security Agent that has been configured to use conventional scan
Dual-stack	<p>Entities that have both IPv4 and IPv6 addresses.</p> <p>For example:</p> <ul style="list-style-type: none">• Endpoints with both IPv4 and IPv6 addresses• Security Agents installed on dual-stack endpoints• Update Agents that distribute updates to agents• A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address
Plug-in solutions	Native Apex One features and plug-in programs delivered through Plug-in Manager

Chapter 1

Planning Apex One Installation and Upgrade

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



Important

- You cannot perform a fresh installation of the Apex One server on the server computer with Apex Central installed.
- If you are upgrading to Apex One and Control Manager is installed on the same server computer, single server computer support for Apex One and Apex Central depends on the features you enable.

For more information, go to https://success.trendmicro.com/dc/s/solution/000267022?language=en_US.

Topics in this chapter:

- *Apex One Server Requirements on page 1-3*
- *Apex Central Extended Feature Requirements on page 1-7*
- *Installation and Upgrade Checklist on page 1-19*

- *Known Compatibility Issues on page 1-23*

Apex One Server Requirements

The following topics outline some considerations you should make before installing or upgrading to the Apex One server.

- *Operating System Support on page 1-3*
- *SQL Server Requirements on page 1-4*
- *Security Agent Support on page 1-5*
- *Installation Verification on page 1-6*

Operating System Support

The following table outlines the operating system support and migration availability for the Apex One server.



Tip

Trend Micro recommends that you perform a complete Windows Update on the target server computer before installing or upgrading to the Apex One server

OPERATING SYSTEM	APEX ONE	APEX ONE SERVICE PACK 1
Windows Server 2012	Yes	Yes
Windows Server 2012 R2	Yes	Yes
Windows Server 2016	Yes	Yes
Windows Server 2019	Yes	Yes
Windows Server 2022	-	Yes



Important

Apex One completely discontinues support of the Apache server.

SQL Server Requirements

Apex One discontinues support of the older Codebase database model used by previous OfficeScan versions. You can prepare your own SQL Server before installation or allow the Apex One Setup program to install SQL Server 2016 SP1 Express during the server installation process.



Important

After upgrading to Apex One, the older **Database Backup** screen used to back up the older Codebase database no longer appears on the Apex One web console.

The following table outlines the database support and migration availability for the Apex One server.

DATABASE	APEX ONE	APEX ONE WITH ENDPOINT SENSOR
Codebase	-	-
SQL Server 2014	Yes	-
SQL Server 2016	Yes	-
SQL Server 2016 SP1	Yes	Yes
SQL Server 2016 Express SP1	Yes	-
SQL Server 2017	Yes	Yes
SQL Server 2019	Yes	Yes
SQL Server 2022	Yes	Yes

**Note**

When installing or upgrading to Apex One with the Endpoint Sensor feature, you must enable **Full-Text and Semantic Extractions for Search** on a supported SQL Server version before beginning the installation process.

For more information about the Endpoint Sensor requirements, see [Apex One Endpoint Sensor on page 1-11](#).

Security Agent Support

The following table outlines Security Agent requirements and recommended settings.

**Important**

Resource spikes may occur if a large number of applications are running simultaneously on an endpoint. If the target endpoint is already running low on memory or disk space, Trend Micro recommends upgrading the necessary hardware components prior to Apex One Security Agent installation or upgrade.

Trend Micro recommends allocating the minimum system requirements listed as dedicated resources for the Security Agent program to ensure adequate performance during extensive scanning operations.

ITEM	DESCRIPTION
HTTPS support	<p>HTTPS communication between the Apex One server and the Security Agent is required.</p> <p>Important</p> <p>You cannot upgrade to the Apex One Service Pack 1 server if you do not select to allow HTTPS communication during the upgrade procedure.</p>

ITEM	DESCRIPTION
Server-Agent communication	Trend Micro recommends enabling AES-256 encryption for communication between the Apex One server and Security Agents on the Global Agent Settings screen after installation completes.
Operating system support	<p>Apex One only supports endpoints running specific Windows operating systems.</p> <p>For a complete list of Apex One server and Security Agent requirements, see the <i>System Requirements</i> documents.</p> <p>During an upgrade installation, the Setup program verifies that all endpoints that report to the server run a supported operating system. If the Setup program detects an unsupported operating system, the upgrade cannot continue.</p> <p>Before upgrading to the Apex One server, move all agents installed on unsupported operating systems to an older OfficeScan server or uninstall the agent program.</p>

Installation Verification

The following table outlines how to verify the successful completion of the Apex One server and Security Agent.

ITEM	DESCRIPTION
Apex One server	<p>Check that the following services are running:</p> <ul style="list-style-type: none"> Apex One Master Service (OfcService.exe) Apex One Plug-in Manager (OfcAoSMgr.exe) Apex One Active Directory Service (OSCEIntegrationService.exe) Apex One Log Receiver Service (OfcLogReceiverSvc.exe) Apex One Deep Discovery Service (OfcDdaSvr.exe) Apex One database process (DbServer.exe)

ITEM	DESCRIPTION
Security Agent	<p>Check that the following services are running:</p> <ul style="list-style-type: none"> • For desktop platforms: <ul style="list-style-type: none"> • Apex One Common Client Solution Framework Service (TmCCSF.exe) • Apex One NT Listener (Tmlisten.exe) • Apex One NT RealTimeScan (Nrttscan.exe) • Apex One NT Firewall (Tmpfw.exe) • Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe) • For server platforms: <ul style="list-style-type: none"> • Apex One Common Client Solution Framework Service (TmCCSF.exe) • Apex One NT Listener (Tmlisten.exe) • Apex One NT RealTimeScan (Nrttscan.exe)

Apex Central Extended Feature Requirements

If you plan to deploy the additional security features available through integration with the Apex Central web console, ensure that you understand the effect that the additional features have on the Apex One system requirements. The following topics outline system requirements, installation and upgrade information, and any additional information related to the enhanced product features.

- *Apex One Application Control on page 1-7*
- *Apex One Endpoint Sensor on page 1-11*
- *Managed Detection and Response Service on page 1-15*
- *Apex One Vulnerability Protection on page 1-16*

Apex One Application Control

- *Prerequisites on page 1-8*

- *Fresh Installation Information on page 1-9*
- *Upgrade Notes on page 1-9*
- *Installation Verification on page 1-10*
- *Post Installation Configuration on page 1-11*

TABLE 1-1. Prerequisites

ITEM	REQUIREMENTS
System requirements	Same as Apex One server and Security Agent
License	<ul style="list-style-type: none"> • Included in the Apex One Full Feature for Windows and Mac license • An existing Trend Micro Endpoint Application Control license (activated in Apex Central)
Apex Central registration	Required for licensing and Security Agent policy deployment
Compatibility with Trend Micro Endpoint Application Control	<ul style="list-style-type: none"> • Server: The Apex One server with Application Control can exist on the same server with Trend Micro Endpoint Application Control (not recommended). <p> Important Trend Micro Endpoint Application Control server settings are not compatible with the Apex One Application Control feature. You must manually configure all policies using the Apex Central web console.</p> <ul style="list-style-type: none"> • Agent: Once you deploy an Application Control policy to the Apex One Security Agent, the Security Agent automatically uninstalls any existing Trend Micro Endpoint Application Control agent before applying the Apex One Application Control settings.

TABLE 1-2. Fresh Installation Information

TYPE	DESCRIPTION
Server	<p>The Apex One Setup program installs the Application Control feature automatically during normal Apex One server installation.</p> <p>After verifying that the Activation Code includes Application Control, Apex One starts the Trend Micro Application Control Service on the Apex One server computer.</p>
Agent	<p>The Security Agent program includes but does not immediately install the Application Control Service during normal Security Agent installation. To install the Apex One Application Control feature on the Security Agent, you must enable and deploy an Application Control policy from the Apex Central web console.</p> <p>Once the Security Agent receives the Application Control settings, the Security Agent installs the Application Control feature.</p>

TABLE 1-3. Upgrade Notes

TYPE	DESCRIPTION
OfficeScan server	<p>The Apex One license only includes the Application Control activation for fresh installations. If you upgrade from a previous version of the OfficeScan server, you must contact your sales representative to obtain a new license that activates the Application Control feature.</p> <p>The Apex One Setup program installs the Apex One Application Control feature automatically during normal Apex One server installation.</p>
Trend Micro Endpoint Application Control server	<p>Apex One does not support any upgrade or settings migration from the standalone Trend Micro Endpoint Application Control server to the Apex One Application Control feature.</p> <p>Important  Trend Micro Endpoint Application Control server settings are not compatible with the Apex One Application Control feature. You must manually configure all policies using the Apex Central web console.</p>

TYPE	DESCRIPTION
Trend Micro Endpoint Application Control agent	<p>Apex One does not support upgrading the Trend Micro Endpoint Application Control agent program to the Apex One Security Agent. If you install the Apex One Security Agent on an endpoint with the Trend Micro Endpoint Application Control agent installed and deploy an Application Control policy from the Apex Central console, the Security Agent automatically uninstalls the Trend Micro Endpoint Application Control agent and installs the Apex One Application Control feature.</p>

TABLE 1-4. Installation Verification

TYPE	DESCRIPTION
Apex One server	<p>After installing the Apex One server with a valid license for the feature, you can verify the following:</p> <ul style="list-style-type: none"> • The Trend Micro Application Control Service is running on the Apex One server computer. • The Application Control Service folder exists on the Apex One server computer in the following location: <code><Server installation folder>/iServiceSrv/iAC</code> • The Application Control Service installation log exists on the Apex One server computer in the following location: <code>%windir%/OFCMAS.LOG</code>
Security Agent endpoint	<p>After installing the Security Agent and deploying an Application Control policy from Apex Central, you can verify the following:</p> <ul style="list-style-type: none"> • The Trend Micro Application Control Service (Agent) is running on the Security Agent endpoint. • The Application Control Service folder exists on the endpoint in the following location: <code><Security Agent installation folder>/iService/iAC</code>

TABLE 1-5. Post Installation Configuration

SETTINGS	DESCRIPTION
Server	On the Apex Central web console, go to Administration > Updates > Manual Update and ensure that you download the Certified Safe Software Pattern .
Security Agent endpoint	On the Apex Central web console, go to Policies > Policy Management and add or modify the Application Control Settings for the Apex One Security Agent policies as required.

Apex One Endpoint Sensor

Endpoint Sensor is available to customers who have purchased the Apex One™: Endpoint Sensor license and integrate with Apex Central. You can only configure Endpoint Sensor policy settings using the Apex Central web console.

Before installing the Apex One server, ensure that you have access to the correct version of SQL Server. If you want to use the Endpoint Sensor feature, you must install and prepare specific SQL Server versions.



Note

If you do not install the Endpoint Sensor Service and select a supported SQL Server with **Full-Text and Semantic Extractions for Search** enabled, the only way to use Endpoint Sensor later is to go to the **Uninstall or change a program** screen of Windows **Control Panel**.

Select the Apex One server and click **Change**.

- *Prerequisites on page 1-12*
- *Fresh Installation Information on page 1-14*
- *Upgrade Notes on page 1-14*

TABLE 1-6. Prerequisites

ITEM	REQUIREMENTS
System requirements	<p>Server: Same operating system requirements as the Apex One server (SQL Server requirements differ)</p> <p>Endpoints: Same system requirements as the Apex One Security Agent</p> <p>Important  This feature is only officially supported on the following platforms: <ul style="list-style-type: none"> • Windows 7 SP1 • Windows 8.1 • Windows 10 </p>
License	<ul style="list-style-type: none"> • Apex One Endpoint Sensor license (activated in Apex Central) • An existing Trend Micro Endpoint Sensor license (activated in Apex Central)
Apex Central registration	Required for licensing and Security Agent policy deployment

ITEM	REQUIREMENTS
Compatibility with Trend Micro Endpoint Sensor	<ul style="list-style-type: none"> Server: If you install the Apex One server with the Apex One Endpoint Sensor feature on the same server with the standalone Trend Micro Endpoint Sensor server (not recommended): <ul style="list-style-type: none"> The standalone Trend Micro Endpoint Sensor server is disabled. The standalone Trend Micro Endpoint Sensor files and database continue to reside on the server computer and may cause a performance impact. <p>Important</p>  <p>Standalone Trend Micro Endpoint Sensor server settings are not compatible with the Apex One Endpoint Sensor feature. You must manually configure all policies using the Apex Central web console.</p> <ul style="list-style-type: none"> Agent: Once you deploy an Endpoint Sensor policy to the Apex One Security Agent, the Security Agent automatically uninstalls any existing standalone Trend Micro Endpoint Sensor agent before applying the Apex One Endpoint Sensor settings.
Redis service	<p>The Apex One server computer cannot have an existing Redis service installed. You must uninstall any existing Redis service and allow the Setup program to install a new service.</p> <p>Verification</p> <p>After clicking Next on the Endpoint Sensor Installation screen</p>
SQL Server version	<ul style="list-style-type: none"> SQL Server 2017 SQL Server 2016 SP1 <p>Note</p>  <p>This feature does not support SQL Server Express versions.</p> <p>Verification</p> <p>After clicking Next on the Apex One Database Setup screen</p>

ITEM	REQUIREMENTS
Database configuration	<p>Full-Text and Semantic Extractions for Search enabled</p> <p>For more information on enabling Full-Text and Semantic Extractions for Search, see your SQL Server documentation.</p> <p>Verification</p> <p>After clicking Next on the Apex One Database Setup screen</p>
	<p>Access rights to the tempdb database for database maintenance functions</p> <p>Verification</p> <p>None</p>

TABLE 1-7. Fresh Installation Information

TYPE	DESCRIPTION
Server	The Apex One Setup program provides the option of installing the Apex One Endpoint Sensor feature during normal Apex One server installation.
Agent	<p>The Security Agent program includes but does not immediately install the Endpoint Sensor Service during normal Security Agent installation. To install the Endpoint Sensor Service on the Security Agent, you must enable and deploy an Endpoint Sensor policy from the Apex Central web console.</p> <p>Once the Security Agent receives the Endpoint Sensor settings, the Security Agent installs the Endpoint Sensor Service.</p>

TABLE 1-8. Upgrade Notes

TYPE	DESCRIPTION
OfficeScan server	The Apex One Setup program provides the option of installing the Apex One Endpoint Sensor feature during normal Apex One server upgrades.

TYPE	DESCRIPTION
Trend Micro Endpoint Sensor server	<p>Apex One does not support any upgrade or settings migration from the standalone Trend Micro Endpoint Sensor server to the Apex One Endpoint Sensor feature.</p> <p>Important</p>  <p>Standalone Trend Micro Endpoint Sensor server settings are not compatible with the Apex One Endpoint Sensor feature. You must manually configure all policies using the Apex Central web console.</p>
Trend Micro Endpoint Sensor agent	<p>Apex One does not support upgrading the Trend Micro Endpoint Sensor agent program to the Apex One Security Agent.</p> <p>If you install the Apex One Security Agent on an endpoint with the standalone Trend Micro Endpoint Sensor agent installed and deploy an Endpoint Sensor policy from the Apex Central console, the Security Agent automatically uninstalls the Trend Micro Endpoint Sensor agent and installs the Apex One Endpoint Sensor feature.</p>

Managed Detection and Response Service

The Managed Detection and Response (MDR) Service is only available if you purchased the Endpoint Sensor service and subscribed to the MDR service through a sales representative. The MDR service system requirements, deployment, and upgrade all follow the Endpoint Sensor service except for the following additional task requirements.

TASK	ADDITIONAL DISK SPACE REQUIREMENTS
Assessment task	When the MDR service begins an assessment task, an additional 20 GB of disk space (per 100 endpoints) is required on the Apex One server to handle the additional log information.
Trend Micro Investigation Kit (TMIK)	When the MDR service deploys the TMIK, an additional 40 GB of disk space (per 100 endpoints) is required on the Apex One server to handle the additional log information.

Apex One Vulnerability Protection

- *Prerequisites on page 1-16*
- *Fresh Installation Information on page 1-17*
- *Upgrade Notes on page 1-17*
- *Installation Verification on page 1-18*
- *Post Installation Configuration on page 1-19*

TABLE 1-9. Prerequisites

ITEM	REQUIREMENTS
System requirements	Same as Apex One server and Security Agent
License	<ul style="list-style-type: none"> • Included in the Apex One Full Feature for Windows and Mac license • An existing Trend Micro Vulnerability Protection license (activated in Apex Central)
Apex Central registration	Required for licensing and Security Agent policy deployment
Compatibility with Trend Micro Vulnerability Protection	<ul style="list-style-type: none"> • Server: The Apex One server with Vulnerability Protection can exist on the same server with Trend Micro Vulnerability Protection (not recommended). • Agent: Once you deploy a Vulnerability Protection policy to the Apex One Security Agent, the Security Agent automatically uninstalls any existing Trend Micro Vulnerability Protection agent before applying the Apex One Vulnerability Protection settings.
Compatibility with other Trend Micro products	<p>The following Trend Micro products are not compatible with the Apex One Vulnerability Protection feature:</p> <ul style="list-style-type: none"> • Deep Security Agent • Intrusion Defense Firewall agent <p>You cannot activate the Apex One Vulnerability Protection feature on Security Agents installed on endpoints with an incompatible agent program installed. You must uninstall the conflicting program before activating the Apex One Vulnerability Protection feature.</p>

TABLE 1-10. Fresh Installation Information

TYPE	DESCRIPTION
Server	<p>The Apex One Setup program installs the Apex One Vulnerability Protection feature automatically during normal Apex One server installation.</p> <p>After verifying that the Activation Code includes Vulnerability Protection, Apex One starts the Trend Micro Vulnerability Protection Service on the Apex One server computer.</p>
Agent	<p>The Security Agent program includes but does not immediately install the Apex One Vulnerability Protection feature during normal Security Agent installation. To install the Vulnerability Protection feature on the Security Agent, you must enable and deploy a Vulnerability Protection policy from the Apex Central web console.</p> <p>Once the Security Agent receives the Vulnerability Protection settings, the Security Agent installs the Vulnerability Protection feature.</p>

TABLE 1-11. Upgrade Notes

TYPE	DESCRIPTION
OfficeScan server	<p>The Apex One license only includes the Vulnerability Protection activation for fresh installations. If you upgrade from a previous version of the OfficeScan server, you must contact your sales representative to obtain a new license that activates the Vulnerability Protection feature.</p> <p>The Apex One Setup program installs the Apex One Vulnerability Protection feature automatically during normal Apex One server installation.</p>
Trend Micro Vulnerability Protection server	Apex One does not support any upgrade or settings migration from the standalone Trend Micro Vulnerability Protection server to the Apex One Vulnerability Protection feature.

TYPE	DESCRIPTION
Trend Micro Vulnerability Protection agent	<p>Apex One does not support upgrading the Trend Micro Vulnerability Protection agent program to the Apex One Security Agent.</p> <p>If you install the Apex One Security Agent on an endpoint with the Trend Micro Vulnerability Protection agent installed and deploy a Vulnerability Protection policy from the Apex Central console, the Security Agent automatically uninstalls the Trend Micro Vulnerability Protection agent and installs the Apex One Vulnerability Protection feature.</p>

TABLE 1-12. Installation Verification

TYPE	DESCRIPTION
Apex One server	<p>After installing the Apex One server with a valid license for the feature, you can verify the following:</p> <ul style="list-style-type: none"> • The Trend Micro Vulnerability Protection Service is running on the Apex One server computer. • The Vulnerability Protection Service folder exists on the Apex One server computer in the following location: <p style="padding-left: 20px;"><code><Server installation folder>/iServiceSrv/iVP</code></p> <ul style="list-style-type: none"> • The Vulnerability Protection Service installation log exists on the Apex One server computer in the following location: <p style="padding-left: 20px;"><code><Server installation folder>/iServiceSrv/iVP/install.log</code></p>
Security Agent endpoint	<p>After installing the Security Agent and deploying a Vulnerability Protection policy from Apex Central, you can verify the following:</p> <ul style="list-style-type: none"> • The Trend Micro Vulnerability Protection Service (Agent) is running on the Security Agent endpoint. • The Vulnerability Protection Service folder exists on the endpoint in the following location: <p style="padding-left: 20px;"><code><Security Agent installation folder>/iService/iVP</code></p>

TABLE 1-13. Post Installation Configuration

SETTINGS	DESCRIPTION
Server	On the Apex Central web console, go to Administration > Updates > Scheduled Update and ensure that you schedule automatic updates of the Vulnerability Protection Pattern .
Security Agent endpoint	On the Apex Central web console, go to Policies > Policy Management and add or modify the Vulnerability Protection Settings for the Apex One Security Agent policies as required.

Installation and Upgrade Checklist

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

TABLE 1-14. Installation and Upgrade Checklist

INSTALLATION INFORMATION	INFORMATION NEEDED DURING	
	FRESH INSTALL	UPGRADE
Apex One Installation path The default server installation path is: <ul style="list-style-type: none"> • C:\Program Files\Trend Micro\Apex One • C:\Program Files (x86)\Trend Micro\Apex One (for x64 type platforms) Identify the installation path or use the default path. If the path does not exist, Setup creates it automatically.	Yes	No

INSTALLATION INFORMATION	INFORMATION NEEDED DURING	
	FRESH INSTALL	UPGRADE
<p>Proxy server settings</p> <p>If the Apex One server connects to the Internet through a proxy server, specify the following:</p> <ul style="list-style-type: none"> • Proxy type (HTTP or SOCKS 4) • Server name or IP address • Port • Proxy authentication credentials 	Yes	No
<p>Web server settings</p> <p>The web server runs web console CGIs and accepts commands from agents. Specify the following:</p> <ul style="list-style-type: none"> • HTTP port: The default port is 8080. If you are using the IIS default web site, check the HTTP server's TCP port. <hr/> <p>WARNING!</p>  <p>Many hacker and virus/malware attacks delivered over HTTP use ports 80 and/or 8080. Most organizations use these port numbers as the default TCP port for HTTP communications. Use other port numbers if the default port numbers are currently in use.</p>	Yes	No
<p>If enabling secure connections:</p> <ul style="list-style-type: none"> • SSL certificate validity period • SSL port (Default: 4343) 		

INSTALLATION INFORMATION	INFORMATION NEEDED DURING	
	FRESH INSTALL	UPGRADE
Registration Register the product to receive the Activation Codes. The following information is necessary to register the product: <ul style="list-style-type: none"> For returning users: <ul style="list-style-type: none"> Online registration account (logon name and password) For users without an account: <ul style="list-style-type: none"> Registration Key 	Yes	Yes
Activation Obtain the Activation Code	Yes	Yes
Integrated Smart Protection Server installation When installing the integrated server, specify the following: <ul style="list-style-type: none"> SSL certificate validity period SSL port 	Yes	Yes
Install the Security Agent	Yes	No
Administrator account password Setup creates a root account for web console logon. Specify the following: <ul style="list-style-type: none"> Root account password Prevent unauthorized uninstallation or unloading of the Security Agent by specifying the following: <ul style="list-style-type: none"> Security Agent uninstallation/unloading password 	Yes	No

INSTALLATION INFORMATION	INFORMATION NEEDED DURING	
	FRESH INSTALL	UPGRADE
Security Agent installation path Specify the directory on the agent endpoint where the Security Agent installation occurs. Specify the following: <ul style="list-style-type: none"> • Installation path: The default agent installation path is C:\Program Files\Trend Micro\Security Agent or C:\Program Files (x86)\Trend Micro\Security Agent. Identify the installation path or use the default path. If the path does not exist, Setup creates it during agent installation. • Security Agent communication port number 	Yes	No
Database back up Specify a location on the server computer to back up the Apex One server for rollback purposes.	No	Yes
 Note The backup package requires at least 300MB of free disk space and may take some time to complete.		
Server Authentication Certificate Apex One attempts to detect preexisting authentication certificates during installation. If Apex One does not detect a certificate, specify the backup password for the new certificate.	Yes	Yes
Program folder shortcut The shortcut to the Apex One server installation folder displays from the Windows Start menu. The default shortcut name is Trend Micro Apex One Server-<Server_name>. Identify a different name or use the default name.	Yes	No

Known Compatibility Issues

This section explains compatibility issues when installing Apex One server on the same endpoint with certain third-party applications. Refer to the documentation of third-party applications for details.

Microsoft Lockdown Tools and URLScan

When using the Microsoft IIS Lockdown Tool or URLScan, lockdown of the following Apex One files may block Security Agent and server communication:

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

Preventing URLScan Interference in Agent-Server Communication

Procedure

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

Microsoft Exchange Server

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

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

[https://technet.microsoft.com/en-us/library/bb332342\(EXCHG.80\).aspx](https://technet.microsoft.com/en-us/library/bb332342(EXCHG.80).aspx)

Database Servers

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

Chapter 2

Installing Trend Micro Apex One

This chapter describes the steps in installing Trend Micro Apex OneTM.

Topics in this chapter:

- *Fresh Installation Considerations on page 2-2*
- *Silent Installation on page 2-7*
- *The Setup Program on page 2-9*

Fresh Installation Considerations



Important

You cannot perform a fresh installation of the Apex One server on the server computer with Apex Central installed.

Consider the following when performing a fresh installation of the Apex One server:

- *Location of the Apex One Server on page 2-2*
- *Server Performance on page 2-3*
- *Scan Method Deployment During Installation on page 2-3*
- *Network Traffic on page 2-5*
- *Third-Party Security Software on page 2-6*
- *Active Directory on page 2-7*

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

<http://docs.trendmicro.com/en-us/home.aspx>

Location of the Apex One Server

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

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

**Important**

Due to security concerns, Trend Micro recommends installing the Apex One server within the company intranet. If you need to manage endpoints that leave the local intranet, Trend Micro recommends installing the Apex One Edge Relay Server in the DMZ.

Server Performance

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

**Tip**

Trend Micro recommends at least 2 GHz dual processors and over 3 GB of RAM for the Apex One server.

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

Dedicated Server

When selecting the endpoint to host the Apex One server, consider the following:

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

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

Scan Method Deployment During Installation

In this Apex One version, you can configure agents to use either Smart Scan or Conventional Scan.

Conventional Scan

Conventional Scan is the scan method used in all earlier Apex One versions. A Conventional Scan agent stores all Apex One components on the agent endpoint and scans all files locally.

Smart Scan

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

Smart Scan provides the following features and benefits:

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

Scan Method Deployment

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

- If you did not change the scan method after installing the server, all agents that you install use Smart Scan.
- If you want to use Conventional Scan on all agents, change the root level scan method to Conventional Scan after installing the server.

- If you want to use both Conventional Scan and Smart Scan, Trend Micro recommends retaining smart scan as the root level scan method and then changing the scan method on domains that you want to apply Conventional Scan.

Network Traffic

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

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

The Security Agent generates traffic when it does the following:

- Starts up
- Updates components
- Updates settings and installs a hot fix
- Scans for security risks
- Switches between “Independent” mode and “Normal” mode
- Switches between Conventional Scan and Smart Scan

Network Traffic During Component Updates

Apex One generates significant network traffic when it updates a component. To reduce network traffic generated during component updates, Apex One performs component duplication. Instead of downloading an updated full pattern file, Apex One only downloads the “incremental” patterns (smaller versions of the full pattern file) and merges them with the old pattern file after the download.

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

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

Update Agents and Network Traffic

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

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

Apex Central and Network Traffic

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

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

For details, see the Apex Central documentation.

Third-Party Security Software

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

**Note**

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

Active Directory

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

Silent Installation

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

Preparing for Silent Installation

Procedure

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

**Important**

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

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

Recording Setup Configuration to a Response File

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

Procedure

1. Download the ApexOne.exe file and extract the contents.
2. Open a command prompt and type the directory of the Apex One setup.exe file.

For example, "CD C:\Apex One Installer\setup.exe".

3. Type the following:

```
setup.exe -r
```

The -r parameter triggers Setup to launch and record the installation details to a response file.

4. Perform the installation steps in Setup.
 5. After completing the steps, check the response file setup.iss in %windir%.
-

Running Silent Installation

Procedure

1. Copy the installation package and setup.iss to the target endpoint.
2. In the target endpoint, open a command prompt and type the directory of the installation package.
3. Type the following:

```
setup.exe -s <-f1path>setup.iss <-f2path>setup.log.
```

For example: C:\setup.exe -s -f1C:\setup.iss -f2C:\setup.log

Where:

- -s: Triggers Setup to perform a silent installation
- <-f1path>setup.iss: Location of the response file. If the path contains spaces, enclose the path with quotes (""). For example, -f1"C:\osce script\setup.iss".

- <-f2path>setup.log: Location of the log file that Setup will create after installation. If the path contains spaces, enclose the path with quotes (""). For example, -f2"C:\osce log\setup.log".
4. Press ENTER.
- Setup silently installs the server to the endpoint.
5. To determine if installation was successful:
- Check the Apex One program shortcuts on the target endpoint. If the shortcuts are not available, retry the installation.
 - Log on to the Apex One web console.
-

The Setup Program

Execute the Setup program when you are ready to begin installing the Apex One server.

Before you begin a fresh installation of the Apex One server, ensure that you have properly prepared your environment. For more information about fresh installation considerations, see:

- *Fresh Installation Considerations on page 2-2*
- *Apex Central Extended Feature Requirements on page 1-7*

When you are sure you are ready to begin, follow the on screen instructions to install the Apex One server.

License Agreement

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

Endpoint Prescan

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

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

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

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



Important

During a local upgrade installation, the setup program prompts you to update your ransomware protection settings in order to receive optimized protection against ransomware threats.

Applying the updated settings only changes the settings on agents that already have Behavior Monitoring enabled.

Proxy Server

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

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

Product Activation

Specify the case-sensitive Activation Code you received to activate all Apex One features.

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

Product Versions

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

TABLE 2-1. Version Comparison

VERSION	DESCRIPTION
Full Version	The full version includes all the product features and technical support, and provides a grace period (usually 30 days) after the license expires. After the grace period expires, technical support and component updates are not available. The scan engines continue to scan endpoints using out-of-date components. These out-of-date components may not be able to protect endpoints completely from the latest security risks. Renew the license before or after it expires by purchasing a maintenance renewal.
Trial Version	The trial version includes all the product features. Upgrade a trial version to the full version at any time. If not upgraded at the end of the trial period, Apex One disables component updates, scanning, and all agent features.

Registration Key and Activation Codes

During installation, specify the Activation Code to activate all features.

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

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

Contact a Trend Micro sales representative to obtain the Registration Key or Activation Codes, if neither is available at the time of installation.

For more information, see [Contacting Trend Micro on page 7-3](#).



Note

For questions about registration, refer to:

<https://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326>.

Installation Path

Accept the default installation path or specify a new one.

Server Identification

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

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

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

**Tip**

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

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

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

Web Server

The Apex One web server hosts the web console, allows the administrator to run console Common Gateway Interfaces (CGIs), and accepts commands from Security Agents. The web server converts these commands to Security Agent CGIs and forwards them to the Apex One Master Service.

HTTP Port

The web server listens for Security Agent requests on the HTTP port and forwards these requests to the Apex One Master Service. This service returns information to Security Agents at the designated Security Agent communication port.

SSL Support

Apex One uses Secure Sockets Layer (SSL) for secure communication between the web console and the server. SSL provides an extra layer of protection against hackers. Although Apex One encrypts the passwords specified on the web console before sending them to the Apex One server,

hackers can still sniff the packet and, without decrypting the packet, "replay" it to gain access to the console. SSL tunneling prevents hackers from sniffing packets traversing the network.

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

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

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

How communication through SSL works:

1. The administrator sends information from the web console to the web server through SSL connection.
2. The web server responds to the web console with the required certificate.
3. The browser performs key exchange using RSA encryption.
4. The web console sends data to the web server using RC4 encryption.

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

Web Server Ports

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

TABLE 2-2. Port Numbers for the Apex One Web Server

WEB SERVER AND SETTINGS	PORTS	
	HTTP	HTTPS (SSL)
IIS default website with SSL enabled	80 (not configurable)	443 (not configurable)

WEB SERVER AND SETTINGS	PORTS	
	HTTP	HTTPS (SSL)
IIS virtual website with SSL enabled	8080 (configurable)	4343 (configurable)

Endpoint Sensor Installation

If you integrate with Apex Central and have purchased the Endpoint Sensor license, select **Install Endpoint Sensor** to ensure that all required Endpoint Sensor Services are available for Security Agents.



Note

This feature is only officially supported on the following platforms:

- Windows 7 SP1
- Windows 8.1
- Windows10

The following table outlines the minimum requirements necessary for installing the Endpoint Sensor Service.

ITEM	REQUIREMENTS	VERIFICATION
Redis service	The Apex One server computer cannot have an existing Redis service installed. You must uninstall any existing Redis service and allow the Setup program to install a new service.	After clicking Next on the Endpoint Sensor Installation screen
SQL Server version	<ul style="list-style-type: none"> • SQL Server 2017 • SQL Server 2016 SP1 <p> Note This feature does not support SQL Server Express versions.</p>	After clicking Next on the Apex One Database Setup screen

ITEM	REQUIREMENTS	VERIFICATION
Database configuration	Full-Text and Semantic Extractions for Search enabled For more information on enabling Full-Text and Semantic Extractions for Search , see your SQL Server documentation.	After clicking Next on the Apex One Database Setup screen
	Access rights to the tempdb database for database maintenance functions	None



Note

If you do not install the Endpoint Sensor Service and select a supported SQL Server with **Full-Text and Semantic Extractions for Search** enabled, the only way to use Endpoint Sensor later is to go to the **Uninstall or change a program** screen of Windows **Control Panel**.

Select the Apex One server and click **Change**.

Apex One Database Setup



Important

If you are planning to use the Endpoint Sensor feature, you must create a database on a properly prepared and supported version of SQL Server.

For more information, see [Apex One Endpoint Sensor on page 1-11](#).

Procedure

1. Choose the location of the Apex One database:

- **Install/Create a new SQL Server Express instance:** Choose to install SQL Server 2016 SP2 Express and create the “\OFFICESCAN” database instance

**Important**

This option is not available if you chose to install the Endpoint Sensor feature.

- **SQL Server:** Select the preexisting SQL Server installation and the database instance that Apex One should use.

2. Select the **Database Authentication** method.

When using the **Windows Account** to log on to the server, Apex One applies the **User name** of the currently logged on user.

**Important**

The user account must belong to the local administrator group or Active Directory (AD) built-in administrator and you must configure the following User Rights Assignment policies using the Windows **Local Security Policy** or **Group Policy Management** console:

- Log on as a service
- Log on as a batch job
- Allow log on locally

The user account must also have the following database roles:

- dbcreator

**Note**

Only required if you are creating a new database instance using the Setup program.

- bulkadmin
- db_owner

3. In the **Database Name** section, specify the name of the database instance on the SQL Server to use for the required **Apex One** database(s).

**Note**

- The **Endpoint Sensor** option only displays if you chose to install the Endpoint Sensor feature.
 - The Setup program automatically creates a new database instance if the specified database does not exist on the SQL Server. The configured authentication account must have the dbcreator permission to create a new database.
-

Apex One Security Agent Deployment

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

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

**Note**

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

Install Integrated Smart Protection Server

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

**Important**

This version of Apex One only supports HTTPS communication for File Reputation and Web Reputation queries.

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

**Tip**

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

Integrated Server Not Installed

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

- Conventional scan becomes the default scan method.
- When enabling web reputation policies in a separate installation screen (for details, see *Web Reputation Services on page 2-23*), agents cannot send web reputation queries because Apex One assumes that no Smart Protection Server installation occurred.

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

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

Install Security Agent

Choose to install the Security Agent on the target server.

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

**Note**

Install the Security Agent to other endpoints on the network after server installation.

For more information, see the *Administrator's Guide*.

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

Smart Feedback

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

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

Samples of information sent to Trend Micro:

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

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

**Tip**

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

For more information on the Smart Protection Network, visit:

<http://www.smartprotectionnetwork.com>

Security Agent Installation

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

**Tip**

Trend Micro recommends using the default settings.

If specifying a different installation path, type a static path or use variables. If the specified path includes a directory that does not exist on the Security Agent, Setup creates the directory automatically during Security Agent installation.

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

**Note**

Modification of the Security Agent installation path is not possible after installation of the Apex One server completes. All installed Security Agents use the same installation path.

When specifying variables for the Security Agent installation path, use the following:

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

Also on this screen, configure the following:

- **Port number:** The Apex One server uses the specified port to communicate with agents. Accept the default or type a new value.

Apex One Firewall

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

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

Optionally enable the Apex One Firewall on server platforms. When upgrading with the Apex One Firewall already enabled on server platforms, select **Enable the Apex One Firewall (on Server platforms)** so that Apex One does not disable the Apex One Firewall after the upgrade.

Anti-spyware Feature

When in assessment mode, all agents managed by the server log spyware/grayware detected during Manual Scan, Scheduled Scan, Real-Time Scan,

and Scan Now but do not clean spyware/grayware components. Cleaning terminates processes or deletes registries, files, cookies, and shortcuts.

Trend Micro provides assessment mode to allow for the evaluation of items that Trend Micro detects as spyware/grayware. Administrators can then configure the appropriate action. For example, add spyware/grayware detected as a security risk to the spyware/grayware approved list.

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

Configure assessment mode to take effect only for a certain period of time by specifying the number of weeks in this screen. After the installation, change assessment mode settings from the web console (**Agents > Global Agent Settings**, on the **Security Settings** tab in the **Spyware/Grayware Scan Settings Only** section).

Web Reputation Services

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

Selecting **Enable Web Reputation Services (on desktop platforms)** enables policies for internal and external agents installed on desktop platforms.

Select **Enable Web Reputation Services (on Server platforms)** if server platforms require the same level of web threat protection as desktop platforms.

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

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

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

When enabling web reputation policies, be sure to install Smart Protection Servers (integrated or standalone) and add them to the smart protection source list on the Apex One web console. Security Agents send web

reputation queries to the servers to verify the safety of websites that users are accessing.

**Note**

The integrated server installs with the Apex One server. For details, see [Install Integrated Smart Protection Server on page 2-18](#). The standalone server installs separately.

Server Authentication Certificate

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

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

**Note**

Apex One does not authenticate communications that agents initiate on the server.

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

Administrator Account Password

Specify passwords to access the web console and unload and uninstall the Security Agent.

Access the Web Console

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

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

Unload and Uninstall the Security Agent

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

Apex One Program Shortcuts

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

Installation Information

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

InstallShield Wizard Complete

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

Restore the forensic folder and database you have backed up to the following location:

<Apex One server installation folder>\PCCSRV\Private\

Administrators can launch the web console to start configuring Apex One settings.

Chapter 3

Upgrading Trend Micro Apex One

This chapter describes the steps in upgrading Trend Micro Apex OneTM.

Topics in this chapter:

- *Upgrade Considerations on page 3-2*
- *Before Upgrading the Server and Agents on page 3-5*
- *Performing a Local Upgrade on page 3-19*

Upgrade Considerations



Important

If you are upgrading to Apex One and Control Manager is installed on the same server computer, single server computer support for Apex One and Apex Central depends on the features you enable.

For more information, go to https://success.trendmicro.com/dc/s/solution/000267022?language=en_US.

This version of Apex One Service Pack 1 supports upgrades from Apex One.



Note

Trend Micro highly recommends applying all available patches and hotfixes to your current Apex One server before performing an upgrade.

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

<https://docs.trendmicro.com/en-us/home.aspx>

Consider the following when upgrading the Apex One server and Security Agents:

- *IPv6 Support on page 3-2*
- *Trend Micro Apex One Settings and Configurations on page 3-3*
- *Scan Method Deployment During Upgrade on page 3-5*

IPv6 Support

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

- The server must already be using an IIS web server.
- Assign an IPv6 address to the server. In addition, the server must be identified by its host name, preferably its fully qualified domain name

(FQDN). If the server is identified by its IPv6 address, all agents currently managed by the server lose connection with the server. If the server is identified by its IPv4 address, it cannot deploy the agent to pure IPv6 endpoints.

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

Trend Micro Apex One Settings and Configurations

Back up the Trend Micro Apex One database and important configuration files before upgrading the Trend Micro Apex One server.



Tip

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

Backing up and Restoring the Apex One Database and Configuration Files

Procedure

1. Stop the Apex One Master Service from the Microsoft Management Console.
2. Stop the Apex One Apex Central Agent Service.
3. Stop the Apex One Plug-in Manager Service.
4. Stop the World Wide Web Publishing Service.
5. Manually back up the following database files found under <Server installation folder>\PCCSRV\Admin\Utility\SQL:
 - libSQLDatabaseUpgrade.dll
 - oscedbt.exe
6. Manually back up the following files and folders found under <Server installation folder>\PCCSRV:

**Note**

Back up these files and folders to roll back Apex One only if you encounter upgrade issues.

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

7. Upgrade the Apex One server.

**Note**

If you encounter upgrade issues, copy the backup files from step 6 to the `<Server installation folder>\PCCSRV` folder on the target endpoint and restart the following services:

- World Wide Web Publishing Service
 - Apex One Plug-in Manager Service
 - Apex One Apex Central Agent Service
 - Apex One Master Service
-

Scan Method Deployment During Upgrade

In this Apex One version, administrators can configure Security Agents to use either Smart Scan or Conventional Scan.

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

- When planning to upgrade the Apex One server directly on the server computer, it is not necessary to make scan method changes from the web console because agents retain their scan method settings after they upgrade.
- When planning to upgrade Security Agents by moving them to the Apex One Service Pack 1 server:
 - In the Apex One Service Pack 1 server, choose manual agent grouping. This agent grouping method allows for the creation of new domains.



Note

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

- Duplicate the domain structure and scan method settings in an earlier version of Apex One server into the Apex One Service Pack 1 server. If the domain structure and scan method settings on the two servers are not identical, some Security Agents that move to the Apex One Service Pack 1 server may not apply their original scan method settings.

Before Upgrading the Server and Agents

Before upgrading the Apex One server and agent, take note of the following:

1. On the Apex One server, manually create a backup of the following forensic folder and database for Data Loss Prevention:

- <Apex One server installation folder>\PCCSRV\Private\DLPForensicData
- <Apex One server installation folder>\PCCSRV\Private\DLPForensicDataTracker.db

**Important**

Take note of the file location. After the upgrade process is complete, restore the forensic folder and database to the same location.

-
2. The installation package includes updates to the firewall drivers. If you have enabled the Apex One firewall in your current server version, deploying the package may cause the following agent endpoint disruptions:
 - When Common Firewall Driver update starts, agent endpoints are temporarily disconnected from the network. Users are not notified before disconnection.
An option on the Apex One web console, which is enabled by default, postpones the Common Firewall Driver update until the agent endpoint is restarted. To avoid the disconnection issue, ensure that this option is enabled.
To check the status of this option:
 - a. Go to **Agents > Global Agent Settings** and click the **Security Settings** tab.
 - b. Go to the **Firewall Settings** section. The option is **Update the Apex One firewall driver only after a system restart**. - After deploying the package, the TDI driver's previous version still exists on the agent endpoint and the new version is not loaded until the endpoint is restarted. Users are likely to encounter problems with the Security Agent if they do not restart immediately.
If the option to display the restart notification message is enabled on the web console, users are prompted to restart. However, users who decide to postpone the restart are not prompted again. If the option is disabled, users are not notified at all.

The option to display the restart notification message is enabled by default. To check the status of this option:

- a. Go to **Agents > Global Agent Settings** and click the **Agent Control** tab.
 - b. Go to the **Alert Settings** section. The option is **Display a notification message if the endpoint needs to restart to load a kernel mode driver**.
3. The Apex One server cannot upgrade to this version if:
- The agent is running Login Script (AutoPcc.exe) at the time of server upgrade. Ensure that no agent is running Login Script before upgrading the server.
 - The server is performing database-related tasks. Before upgrading, check the status of the server database (DbServer.exe). For example, open Windows Task Manager and verify that CPU usage for DbServer.exe is 00. If CPU usage is higher, wait until usage is 00, which signals that database-related tasks have been completed. If you run an upgrade and encounter upgrade problems, it is possible that database files have been locked. In this case, restart the server computer to unlock the files and then run another upgrade.

Use one of following upgrade methods:

- *Upgrade Method 1: Disable Automatic Agent Upgrade on page 3-7*
- *Upgrade Method 2: Upgrade Update Agents on page 3-9*
- *Upgrade Method 3: Move Agents to the Apex One Service Pack 1 Server on page 3-15*
- *Upgrade Method 4: Enable Automatic Agent Upgrade on page 3-17*

Upgrade Method 1: Disable Automatic Agent Upgrade

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

Part 1: Configure Update Settings on the Apex One Server

Procedure

1. Go to **Agents > Agent Management**.
2. On the agent tree, click the root domain icon (🌐) to select all agents.
3. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
4. In the **Security Agents only update the following components** dropdown, select **Pattern Files**.
5. Click **Apply to All Agents**.

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

Part 2: Upgrade the Apex One Server

See [Performing a Local Upgrade on page 3-19](#) for details on upgrading the Apex One server.

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

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

Part 3: Upgrade Security Agents

Procedure

1. Go to **Updates > Agents > Automatic Update**, and ensure that the following options are enabled:
 - **Initiate component update on agents immediately after the Apex One server downloads a new component**

- **Let agents initiate component update after restarting and connecting to the Apex One server (Independent agents excluded)**
2. Go to **Agents > Agent Management**.
 3. On the agent tree, select the agents that you want to upgrade. You can select one or several domains, or individual/all agents within a domain.
 4. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
 5. In the **Security Agents only update the following components** dropdown, select **All components (including hotfixes and the agent program)**.
 6. Click **Save**.
 7. Check the upgrade results.
 - *Online Agents on page 3-13*
 - *Offline Agents on page 3-14*
 - *Independent (Roaming) Agents on page 3-14*
 8. Restart the agent endpoints to finish upgrading the agents.
 9. Repeat step 2 to step 8 until all agents have been upgraded.

Upgrade Method 2: Upgrade Update Agents

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

Security Agents that do not update from Update Agents will upgrade from the Apex One server.

Part 1: Configure Update Settings on the Apex One Server

Procedure

1. Go to **Agents > Agent Management**.
2. On the agent tree, click the root domain icon (globe) to select all agents.
3. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
4. In the **Security Agents only update the following components** dropdown, select **Pattern Files**.
5. Click **Apply to All Agents**.

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

Part 2: Upgrade the Apex One Server

See [Performing a Local Upgrade on page 3-19](#) for details on upgrading the Apex One server.

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

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

Part 3: Upgrade Update Agents

Procedure

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

**Tip**

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

3. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
4. In the **Security Agents only update the following components** drop-down, select **All components (including hotfixes and the agent program)**.
5. Click **Save**.
6. Go to **Updates > Agents > Manual Update**.
7. Select the **Manually select agents** option and click **Select**.
8. In the agent tree that opens, choose the Update Agents to upgrade.

**Tip**

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

9. Click **Initiate Update** on top of the agent tree.
10. Check the upgrade results.
 - Online Update Agents upgrade immediately after initiating component update.
 - Offline Update Agents upgrade when they become online.
 - Independent (formerly roaming) Update Agents upgrade when they become online or, if the Update Agent has scheduled update privileges, when scheduled update runs.
11. Restart the Update Agents' endpoints to finish upgrading the agents.
12. Repeat step 1 to step 11 until all Update Agents have been upgraded.

Part 4: Configure Update Agent Settings

Procedure

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



Tip

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

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

Part 5: Upgrade Security Agents

Procedure

1. Go to **Updates > Agents > Automatic Update**, and ensure that the following options are enabled:
 - **Initiate component update on agents immediately after the Apex One server downloads a new component**

- **Let agents initiate component update after restarting and connecting to the Apex One server (Independent agents excluded)**
2. Go to **Agents > Agent Management**.
 3. On the agent tree, select the agents that you want to upgrade. You can select one or several domains, or individual/all agents within a domain.
 4. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
 5. In the **Security Agents only update the following components** dropdown, select **All components (including hotfixes and the agent program)**.
 6. Click **Save**.
 7. Check the upgrade results.
 - *Online Agents on page 3-13*
 - *Offline Agents on page 3-14*
 - *Independent (Roaming) Agents on page 3-14*
 8. Restart the agent endpoints to finish upgrading the agents.
 9. Repeat step 2 to step 8 until all agents have been upgraded.

Upgrade Results

Online Agents



Note

Restart the agent endpoints after the upgrade.

- Automatic Upgrade

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

- The Apex One server downloads a new component and notifies agents to update.

- The agent reloads.
 - The agent restarts and then connects to the Apex One server.
 - Schedule update runs on the agent endpoint (only for agents with scheduled update privileges).
- Manual Upgrade

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

- Create and deploy an EXE or MSI Security Agent package.



Note

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

- Instruct users to run **Update Now** on the agent endpoint.
- Right-click `AutoPcc.exe`, and select **Run as administrator**.
- Initiate manual agent update.

To initiate manual update:

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

Offline Agents

Offline agents upgrade when they become online.

Independent (Roaming) Agents

Independent agents (previously referred to as Roaming agents) upgrade when they become online or, if the agent has scheduled update privileges, when scheduled update runs.

Upgrade Method 3: Move Agents to the Apex One Service Pack 1 Server

Perform a fresh installation of the Apex One Service Pack 1 server and then move agents to this server. When you move the agents, they automatically upgrade to Apex One Service Pack 1.

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

Procedure

1. Perform a fresh installation of the Apex One Service Pack 1 server.
For details, see [The Setup Program on page 2-9](#).
2. Log on to the web console.
3. Go to **Updates > Agents > Automatic Update**, and ensure that the following options are enabled:
 - **Initiate component update on agents immediately after the Apex One server downloads a new component**
 - **Let agents initiate component update after restarting and connecting to the Apex One server (Independent agents excluded)**
4. Go to **Agents > Agent Management**.
5. On the agent tree, click the root domain icon () to select all agents.
6. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
7. In the **Security Agents only update the following components** dropdown, select **All components (including hotfixes and the agent program)**.
8. Click **Apply to All Agents**.
9. Record the following Apex One Service Pack 1 server information. Specify this information on the previous Apex One server when moving agents:

- Endpoint name or IP address
- Server listening port

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

Part 2: Upgrade Security Agents

Procedure

1. On the web console of the previous server, go to **Updates > Summary**.
2. Click **Cancel Notification**. This function clears the server notification queue, which will prevent problems moving clients/agents to the Apex One server.



WARNING!

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

3. Go to **Agents > Agent Management**.
 4. On the agent tree, select the agents that you want to upgrade. Select only online agents because offline and roaming agents cannot be moved.
 5. Move agents as follows:
 - a. Click **Manage Agent Tree > Move Agent**.
 - b. Specify the Apex One server computer name/IP address and server listening port under **Move selected agent(s) online to another Apex One server**.
 6. Click **Move**.
-

Upgrade Results

- Online agents start to move and upgrade.
- Tips for managing offline and independent (formerly roaming) agents:
 - Disable independent (formerly roaming) mode on agents in order to upgrade them.
 - For offline agents, instruct users to connect to the network so that the agents can become online. For agents that are offline for an extended period of time, instruct users to uninstall the agent from the endpoint and then use a suitable agent installation method (such as agent packager) discussed in the *Administrator's Guide* to install the Security Agent.



Note

Restart the agent endpoints to finish upgrading the agents.

Upgrade Method 4: Enable Automatic Agent Upgrade

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

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

Part 1: Configure Update Settings on the Apex One Server

Procedure

1. Go to **Updates > Agents > Automatic Update** and ensure that the following options are enabled:
 - **Initiate component update on agents immediately after the Apex One server downloads a new component.**
 - **Let agents initiate component update after restarting and connecting to the Apex One server (Independent agents excluded)**

2. Go to **Agents > Agent Management**.
3. On the agent tree, click the root domain icon (earth) to select all agents.
4. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
5. In the **Security Agents only update the following components** dropdown, select **Pattern Files**.
6. Click **Apply to All Agents**.

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

Part 2: Upgrade the Apex One Server

See *Performing a Local Upgrade on page 3-19* for details on upgrading the Apex One server.



Note

To speed up the upgrade process, unload the Security Agent before upgrading any Apex One server running Windows Server 2008 Standard 64-bit.

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

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

Upgrade Results

- Online agents upgrade immediately after server upgrade is complete.
- Offline agents upgrade when they become online.

- Independent (formerly roaming) agents upgrade when they become online or, if the agent has scheduled update privileges, when scheduled update runs.

**Note**

Restart the agent endpoints to finish upgrading the agents.

Performing a Local Upgrade

During a local upgrade, Apex One applies the settings used by the previous Apex One server version. A limited subset of screens display that allow you to configure the new features offered by Apex One Service Pack 1.

**Important**

Before upgrading the Apex One server, create a backup of the following forensic folder and database for Data Loss Prevention:

- <Apex One server installation folder>\PCCSRV\Private\DLPMforensicData
- <Apex One server installation folder>\PCCSRV\Private\DLPMforensicDataTracker.db

Take note of the file location. After the upgrade process is complete, restore the forensic folder and database to the same location.

License Agreement

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

Forensic Data

On the Apex One server, manually create a backup of the following forensic folder and database for Data Loss Prevention:

- <Apex One server installation folder>\PCCSRV\Private\DLPMforensicData
 - <Apex One server installation folder>\PCCSRV\Private\DLPMforensicDataTracker.db
-

**Important**

Take note of the file location. After the upgrade process is complete, restore the forensic folder and database to the same location.

Security Agent Upgrades

The Setup program assesses the target endpoint resources. During upgrade scenarios, a warning screen appears if a previous version of the Security Agent program exists on the target endpoint.

Enable Enhanced Protection

Trend Micro Apex One Setup Program

Enable Enhanced Protection



To maximize your protection against network and ransomware attacks, Trend Micro recommends enabling the following Security Agent settings:

Protect against ransomware (Behavior Monitoring)

- Enable Malware Behavior Blocking for "Known and potential threats"
- Enable "Protect documents against unauthorized encryption or modification"
- Enable program inspection to detect and block compromised executable files

Protect against network attacks (Suspicious Connection Service and Settings)

- Enable the "Suspicious Connection Service" for Windows desktops
- Enable "Detect connections made to addresses in the Global C&C IP list" and set to "Block"
- Enable "Detect connections using malware network fingerprinting" and set to "Block"

InstallShield

[Help](#) [< Back](#) [Next >](#) [Cancel](#)

Trend Micro recommends enabling ransomware and network attack protection on all Security Agents.

The following table outlines the Apex One web console features enabled for each setting.

Setting	Web Console Location	Features
Protect against ransomware	Agents > Agent Management > Settings > Behavior Monitoring Settings > Rules > Malware Behavior Blocking section	<ul style="list-style-type: none"> Enable Malware Behavior Blocking <ul style="list-style-type: none"> Threats to block: Known and potential threats Protect documents against unauthorized encryption or modification Enable program inspection to detect and block compromised executable files <p>Important</p>  <p>Enabling Protect against ransomware does not automatically enable the Unauthorized Change Prevention Service. If you disabled the service, you must manually enable the Unauthorized Change Prevention Service before Security Agents can protect against ransomware attacks.</p>
Protect against network attacks	Agents > Agent Management > Settings > Additional Service Settings > Suspicious Connection Service section	Enables the Suspicious Connection Service on Windows desktops
	Agents > Agent Management > Settings > Suspicious Connection Settings	<ul style="list-style-type: none"> Detect network connections made to addresses in the Global C&C IP list: Block Detect connections using malware network fingerprinting: Block

Database Back Up

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



Note

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

Endpoint Sensor Installation

If you integrate with Apex Central and have purchased the Endpoint Sensor license, select **Install Endpoint Sensor** to ensure that all required Endpoint Sensor Services are available for Security Agents.



Note

This feature is only officially supported on the following platforms:

- Windows 7 SP1
- Windows 8.1
- Windows10

The following table outlines the minimum requirements necessary for installing the Endpoint Sensor Service.

ITEM	REQUIREMENTS	VERIFICATION
Redis service	The Apex One server computer cannot have an existing Redis service installed. You must uninstall any existing Redis service and allow the Setup program to install a new service.	After clicking Next on the Endpoint Sensor Installation screen

ITEM	REQUIREMENTS	VERIFICATION
SQL Server version	<ul style="list-style-type: none"> • SQL Server 2017 • SQL Server 2016 SP1 <hr/>  Note This feature does not support SQL Server Express versions.	After clicking Next on the Apex One Database Setup screen
Database configuration	Full-Text and Semantic Extractions for Search enabled For more information on enabling Full-Text and Semantic Extractions for Search , see your SQL Server documentation.	After clicking Next on the Apex One Database Setup screen
	Access rights to the tempdb database for database maintenance functions	None


Note

If you do not install the Endpoint Sensor Service and select a supported SQL Server with **Full-Text and Semantic Extractions for Search** enabled, the only way to use Endpoint Sensor later is to go to the **Uninstall or change a program** screen of Windows **Control Panel**.

Select the Apex One server and click **Change**.

Apex One Database Setup


Important

If you are planning to use the Endpoint Sensor feature, you must select a database on a properly prepared and supported version of SQL Server.

For more information, see [Apex One Endpoint Sensor on page 1-11](#).

Procedure

1. Beside **SQL Server**, select the preexisting SQL Server installation and the database instance that Apex One should use.
2. Select the database authentication method.

When using the **Windows Account** to log on to the server, Apex One applies the **User name** of the currently logged on user.

domain_name\user_name or user_name



Important

The user account must belong to the local administrator group or Active Directory (AD) built-in administrator and you must configure the following User Rights Assignment policies using the Windows **Local Security Policy** or **Group Policy Management** console:

- Log on as a service
- Log on as a batch job
- Allow log on locally

The user account must also have the following database roles:

- dbcreator
- bulkadmin
- db_owner

-
3. Specify the Apex One **Database name** on the SQL Server.
 4. Click **Next**.

**Important**

If you selected to install Endpoint Sensor Services, the Setup program immediately evaluates whether the selected SQL Server database is properly configured and meets the minimum requirements. If the SQL Server database does not meet the requirements, you must select another SQL Server database or go back and choose to not install Endpoint Sensor.

Apex One Security Agent Deployment

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

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

**Note**

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

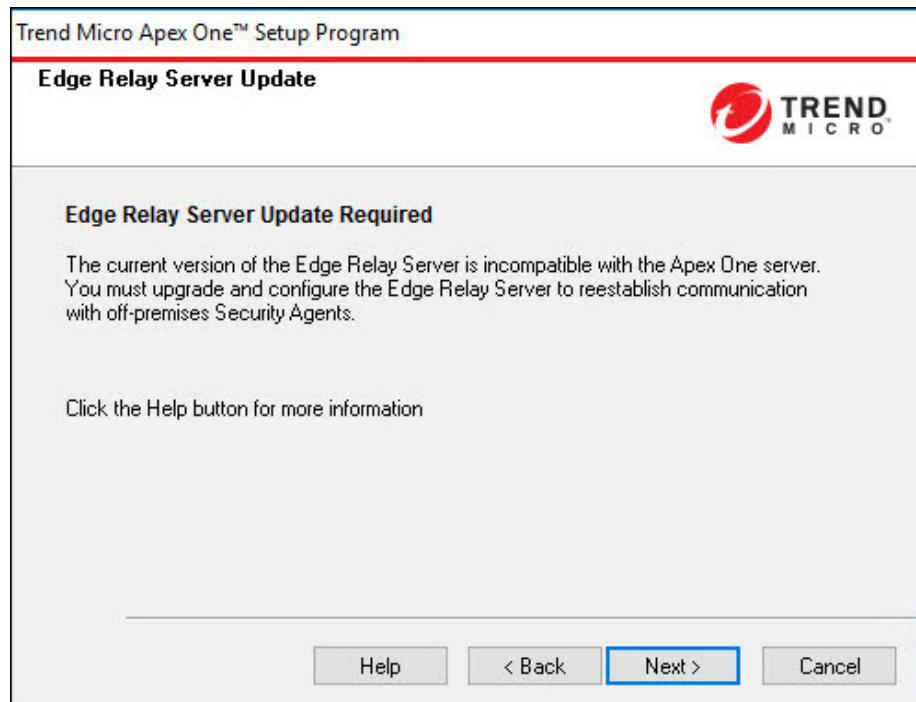
Installation Information

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

Edge Relay Server Update

**Important**

Only displays if the previous Apex One server had a registered Edge Relay Server.



Apex One does not support the older OfficeScan versions of the Edge Relay Server. You must install a new Edge Relay Server or upgrade your existing Edge Relay Server to protect off-premises Security Agents.

After installing or upgrading the Edge Relay Server, all Security Agents that you want to manage using the Edge Relay Server must connect directly to the Apex One server to obtain the latest Edge Relay Server settings.

For more information about Edge Relay Server installation or upgrade, refer to the *Apex One Administrator's Guide*.

InstallShield Wizard Complete

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

Restore the forensic folder and database you have backed up to the following location:

<Apex One server installation folder>\PCCSRV\Private\

Administrators can launch the web console to start configuring Apex One settings.

Chapter 4

Post-installation Tasks

Perform the following tasks after the Apex One server installation completes.

Topics in this chapter:

- *Verifying the Server Installation or Upgrade on page 4-2*
- *Updating the Apex One Server on page 4-4*
- *Checking Default Settings on page 4-5*
- *Registering Apex One to Apex Central on page 4-6*

Verifying the Server Installation or Upgrade

After completing the installation or upgrade, verify the following:

TABLE 4-1. Items to Verify After Installing Apex One

ITEM TO VERIFY	DETAILS
Apex One server shortcuts	The Trend Micro Apex One server shortcuts appear on the Windows Start menu on the server computer.
Programs list	Trend Micro Apex One Server is listed on the Add/Remove Programs list on the server computer's Control Panel.
Apex One web console	Type the following URL in the Internet Explorer browser: <ul style="list-style-type: none">HTTPS connection: <code>https://<Apex One server name>:<port number>/officescan</code> Where <Apex One server name> is the name or IP address of the Apex One server. The web console logon screen displays.

ITEM TO VERIFY	DETAILS
Apex One server services	<p>The following Apex One server services display on the Microsoft Management Console:</p> <ul style="list-style-type: none"> Apex One Active Directory Integration Service: This service displays if the Active Directory integration and Role-based Administration features work properly. Apex One Apex Central Agent: The status for this service should be "Started" if the Apex One server has been registered to Apex Central. Apex One Deep Discovery Service: The status for this service should be "Started". Apex One Master Service: The status for this service should be "Started". Apex One Log Receiver Service: The status for this service should be "Started". Apex One Plug-in Manager: The status for this service should be "Started". Trend Micro Smart Protection Query Handler: The status for this service should be "Started". Trend Micro Smart Protection Server: The status for this service should be "Started". Trend Micro Local Web Classification Server: The status for this service should be "Started" if Web Reputation Services was enabled during installation.
Apex One server processes	When you open Windows Task Manager, DBServer.exe is running.
Server installation log	The server installation log, OFCMAS.LOG, exists in %windir%.

ITEM TO VERIFY	DETAILS
Registry keys	<p>The following registry key exists:</p> <ul style="list-style-type: none">• For 32-bit platforms: HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan• For 64-bit platforms: HKEY_LOCAL_MACHINE\Software\Wow6432Node\TrendMicro\OfficeScan
Program folder	The Apex One server files are found under the <Server installation folder>.

Verifying Integrated Smart Protection Server Installation

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

Procedure

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

Connection with the integrated server should be successful.

Updating the Apex One Server

After installing Apex One, update components on the server.



Note

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

Procedure

1. Log on to the web console.
2. On the main menu, click **Updates > Server > Manual Update**.

The **Manual Update** screen appears, showing the current components, their version numbers, and the most recent update dates.

3. Select the components to update.
 4. Click **Update**. The server checks the update server for updated components. The update progress and status display.
-

Checking Default Settings

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

Scan Settings

Apex One provides several types of scans to protect endpoints from security risks. Modify the scan settings from the web console by going to **Agents > Agent Management** and clicking **Settings > {Scan Type}**.

Agent Settings

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

Agent Privileges

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

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

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

Registering Apex One to Apex Central

When a Apex Central server manages newly installed Apex One servers, register Apex One to Apex Central after installation.



Note

Apex Central registration only applies to newly installed Apex One servers.

On the Apex One web console, go to **Administration > Settings > Apex Central**.

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

Chapter 5

Uninstalling Apex One

This chapter describes the steps for uninstalling the Apex One server.

Topics in this chapter:

- *Uninstallation Considerations on page 5-2*
- *Before Uninstalling the Apex One Server on page 5-2*
- *Uninstalling the Apex One Server on page 5-4*

Uninstallation Considerations

When experiencing problems with Apex One, use the uninstallation program to safely remove the Apex One server from the endpoint. Before uninstalling the server, move the agents it manages to another Apex One server.

Before Uninstalling the Apex One Server

Use the uninstallation program to safely remove the Apex One server.

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

Moving Agents to Another Server

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

Procedure

1. Record the following information for the other server. This information is necessary when moving the agents.
 - Endpoint name or IP address
 - Server listening portTo view the server listening port, go to **Administration > Settings > Agent Connection**. The port number displays on the screen.
2. On the web console of the server to uninstall, go to **Agents > Agent Management**.
3. On the agent tree, select the agents to move and then click **Manage Agent Tree > Move Agent**.
4. Under **Move selected agent(s) to another Apex One server**, specify the server computer name/IP address and server listening port of the other Apex One server.

5. Click **Move**.

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

Backing Up and Restoring the Apex One Configuration Files

Back up important configuration files before uninstalling the Apex One server.



Note

During the uninstallation process, Apex One does give you the option of not deleting the SQL database.

Procedure

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

For more information, see [Uninstalling the Apex One Server on page 5-4](#).

4. Perform a fresh installation.
For more information, see [The Setup Program on page 2-9](#).
 5. After Setup finishes, open the Microsoft Management Console (`services.msc`).
 6. Right-click **Apex One Master Service** and then click **Stop**.
 7. Copy the backup files to the <Server installation folder>\PCCSRV folder on the target endpoint.
 8. Restart the Apex One Master Service.
-

Uninstalling the Apex One Server

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

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



Note

For Security Agent uninstallation instructions, see the *Administrator's Guide*.

Uninstalling the Apex One Server Using the Uninstallation Program

Procedure

1. Run the uninstallation program. There are two ways to access the uninstallation program.
 - Method A
 - a. On the Apex One server computer, click **Start** > **Programs** > **Trend Micro Apex One Server** > **Uninstall Apex One**. A confirmation screen appears.

- b. Click **Yes**. The server uninstallation program prompts you for the administrator password.
 - c. Type the administrator password and click **OK**. The server uninstallation program starts removing the server files. A confirmation message appears.
 - d. Click **OK** to close the uninstallation program.
- Method B
- a. Double-click the Apex One server program on the **Windows Add/Remove Programs** screen.
 - b. Click **Control Panel > Add or Remove Programs**. Locate and double-click "Trend Micro Apex One Server". Follow the on-screen instructions until you are prompted for the administrator password.
 - c. Type the administrator password and click **OK**. The server uninstallation program starts removing the server files. A confirmation message appears.
 - d. Click **OK** to close the uninstallation program.

Manually Uninstalling the Apex One Server

Part 1: Integrated Smart Protection Server Uninstallation

Procedure

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

```
SVRSVCSETUP.EXE -uninstall
```

This command uninstalls Apex One-related services but does not remove configuration files or the Apex One database.

4. Go to <Server installation folder>\PCCSRV\private and open ofcserver.ini.
5. Modify the following settings:

TABLE 5-1. ofcserver.ini Settings

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

6. Navigate to <Server installation folder>\PCCSRV and open OfUninst.ini. Delete the following lines:

[WSS_WEB_SERVER]

ServerPort=8082

IIS_VhostName=Smart Protection Server (Integrated)

IIS_VHostIdx=5



Note

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

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

[WSS_SSL]

SSLPorT=<SSL port>

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

8. Run the following commands:

```
Svrsvcsetup -install  
Svrsvcsetup -enablessl  
Svrsvcsetup -setprivilege
```

9. Verify that the following items were removed:

- Trend Micro Smart Protection Server service from the Microsoft Management Console
- Smart Protection Server performance counters
- Smart Protection Server (Integrated) website

Part 2: Apex One Server Uninstallation

Procedure

1. Open Registry Editor and perform the following steps:



WARNING!

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

-
- a. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\.**
 - b. Verify that the ofcservice hive has been deleted.**
 - c. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\ and delete the OfficeScan hive.**
- For 64-bit endpoints, the path is HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\.**

- d. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\. Delete the OfficeScan Management Console-<Server Name> folder.**
 - 2. Go to <Server installation folder>\PCCSRV folder and unshare the PCCSRV folder.**
 - 3. Restart the server computer.**
 - 4. Go to <Server installation folder>\PCCSRV and delete the PCCSRV folder.**
 - 5. Delete the Apex One website from the Internet Information Services (IIS) console.**
 - a. Open the IIS console.**
 - b. Expand ServerName.**
 - c. If you installed Apex One on a separate website, go to the Web Sites folder and then delete Apex One.**
 - d. If you installed Apex One virtual directories under the default website, go to Default Web Site and then delete the Apex One virtual directory.**
-

Chapter 6

Troubleshooting Resources

This chapter describes resources you can use to troubleshoot possible issues with this version of Apex One.

Topics in this chapter:

- *Support Intelligence System on page 6-2*
- *Case Diagnostic Tool on page 6-2*
- *Trend Micro Performance Tuning Tool on page 6-2*
- *Installation Logs on page 6-4*
- *Server Debug Logs on page 6-4*
- *Agent Debug Logs on page 6-6*

Support Intelligence System

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

Case Diagnostic Tool

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

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

Trend Micro Performance Tuning Tool

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



Note

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

Identifying System-intensive Applications

Procedure

1. Contact Trend Micro Technical Support to obtain a copy of the Trend Micro Performance Tuning Tool.

2. Unzip TMPerfTool.zip to extract TMPerfTool.exe.
3. Place TMPerfTool.exe in the <Client installation folder> or in the same folder as TMBMCLI.dll.
4. Right-click TMPerfTool.exe and select **Run as administrator**.
5. Read and accept the end user agreement and then click **OK**.
6. Click **Analyze**. The tool starts to monitor CPU usage and event loading. A system-intensive process is highlighted in red.

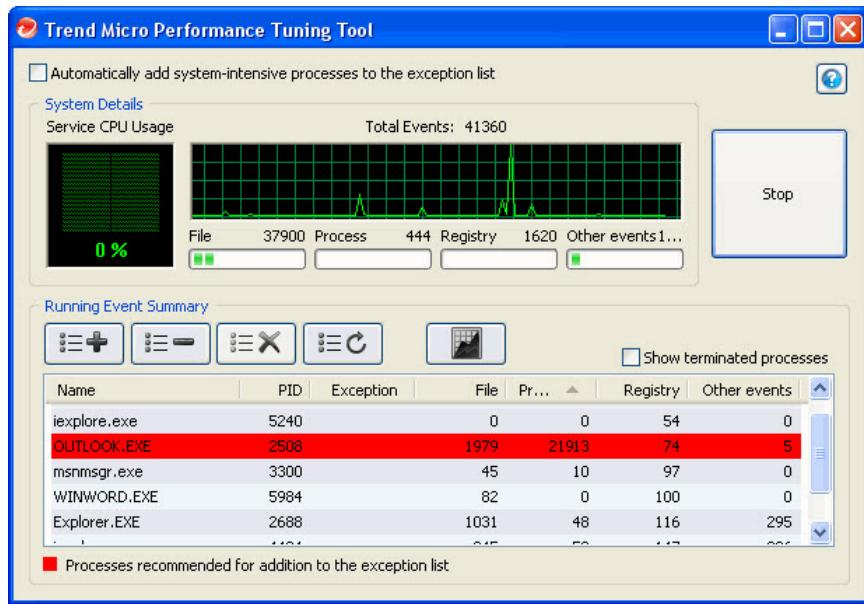


FIGURE 6-1. System-intensive process highlighted

7. Select a system-intensive process and click the **Add to the exception list (allow)** button ().
8. Check if the system or application performance improves.

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

Installation Logs

Use the installation log files Apex One automatically generates to troubleshoot installation problems.

TABLE 6-1. Installation Log Files

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

Server Debug Logs

Enable debug logging before performing the following server tasks:

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

**WARNING!**

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

Enabling Debug Logging on the Apex One Server computer

Option 1:

Procedure

1. Log on to the web console.
2. On the banner of the web console, click the "A" in "Apex". This opens the **Debug Log Setting** screen.
3. Specify debug log settings.
4. Click **Save**.
5. Check the log file (ofcdebug.log) in the default location: <Server installation folder>\PCCSRV\Log.

Option 2:

Procedure

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

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

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

3. Save `ofcdebug.ini` to `C:\LogServer`.
4. Perform the appropriate task (that is, reinstall the server, upgrade to a new server version, or perform a remote installation/upgrade).
5. Check `ofcdebug.log` in `C:\LogServer`.

**Note**

If the Security Agent is present on the Apex One server, then the agent also outputs its debug logs in the server's debug logs.

Agent Debug Logs

Enable debug logging before installing the Security Agent.

**WARNING!**

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

Enabling Debug Logging on the Security Agent

Procedure

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

```
[Debug]  
DebugLog=C:\ofcdebug.log  
DebugLevel=9  
DebugLevel_new=D  
DebugSplitSize=10485760  
DebugSplitPeriod=12  
DebugRemoveAfterSplit=1
```

2. Send `ofcdebug.ini` to agent users, instructing them to save the file to `C:\.`
LogServer.exe automatically runs each time the agent endpoint starts.
 3. To start debug logging, reload the Security Agent or restart the endpoint.
Instruct users NOT to close the LogServer.exe command window that opens when the endpoint starts as this prompts Apex One to stop debug logging. If users close the command window, they can start debug logging again by running LogServer.exe located in `\Security Agent\Temp`.
 4. For each agent endpoint, check `ofcdebug.log` in `C:\.`.
 5. To disable debug logging for the Security Agent, delete `ofcdebug.ini`.
-

Chapter 7

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 7-2*
- *Contacting Trend Micro on page 7-3*
- *Sending Suspicious Content to Trend Micro on page 7-4*
- *Other Resources on page 7-5*

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to <https://success.trendmicro.com>.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.



Tip

To submit a support case online, visit the following URL:

<https://success.trendmicro.com/smb-new-request>

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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware> to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

<https://www.trendmicro.com/us/about-us/contact/index.html>

- Trend Micro product documentation:

<https://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem

- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

<https://servicecentral.trendmicro.com/en-us/ers/>

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

<https://success.trendmicro.com/solution/1112106>

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

<https://success.trendmicro.com/solution/1059565>

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

<https://global.sitesafety.trendmicro.com/>

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

<https://www.trendmicro.com/download/>

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

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:

<https://docs.trendmicro.com/en-us/survey.aspx>

Appendix A

Sample Deployment

This section illustrates how to deploy Apex One based on network topology and available network resources. Use this as a reference when planning Apex One deployment in your organization.

Basic Network

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

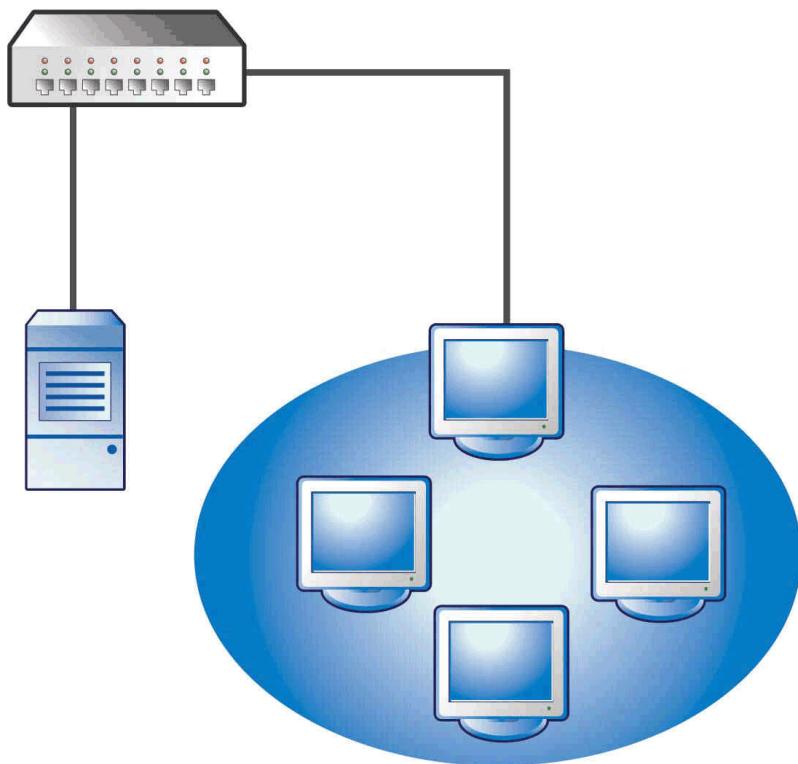


FIGURE A-1. Basic network topology

Multiple Site Network

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

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

This presents a clearer picture as to how best to deploy Apex One. Figure 1 illustrates a multiple site network topology.

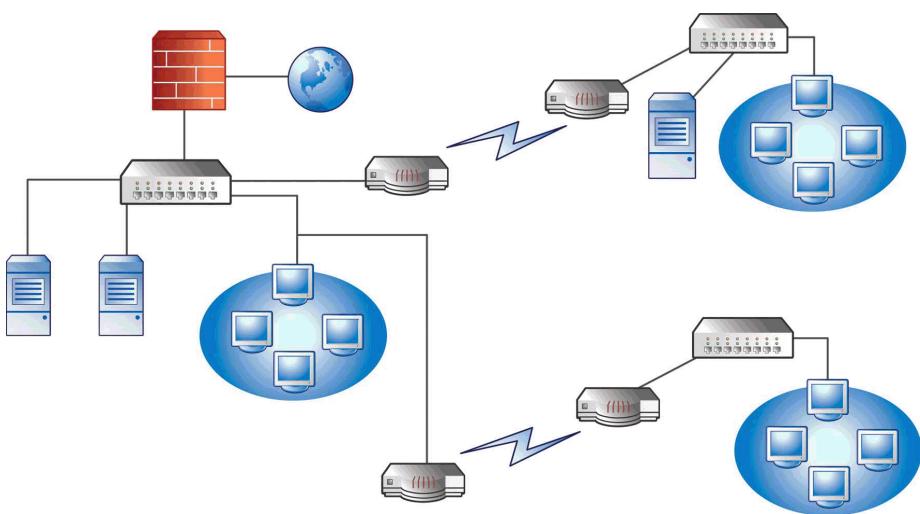


FIGURE A-2. Multiple site network topology

Network information:

- Remote Site 1 WAN link averages around 70 percent utilization during business hours. There are 35 agent endpoints on this site.
- Remote Site 2 WAN link averages around 40 percent utilization during business hours. There are 9 agent endpoints on this site.

- Server 3 only functions as a file and print server for the group at Remote Site 1. This endpoint is a possible candidate for installing the Apex One server, but may not be worth the extra management overhead. All servers run Windows Server 2012. The network uses Active Directory, but mainly for network authentication.
- All agent endpoints in Head Office, Remote Site 1, and Remote Site 2 run Windows Server 2012 or Windows 7.

Preparing a Multiple Site Network

Procedure

1. Identify the endpoint on which to install the Apex One server.
2. Identify the available agent installation methods and eliminate methods that do not fit the requirement. See the *Administrator's Guide* for more information on the agent installation methods.

Possible installation methods:

- Login Script Setup

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

- Remote installation from the web console

This method is valid for all the LAN-connected endpoints at the head office. Because these endpoints all run Windows Server 2012, it is simple to deploy the package to the endpoints.

Due to the low link speed between the two remote sites, this deployment method may impact available bandwidth if Apex One deployment occurs during business hours. Use the whole link capacity to deploy Apex One during non-business hours when most people are no longer at work. However, if users turn off their endpoints, Apex One deployment to these endpoints is not successful.

- Security Agent package deployment

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

Head Office Deployment

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

Remote Site 1 Deployment

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

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

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

Minimizing the Impact of Component Updates Across the WAN

Procedure

1. Designate one agent to act as an Update Agent on Remote Site 1.
 - a. Log on to the web console and navigate to **Agents > Agent Management**.

- b.** In the agent tree, select the agent to act as the Update Agent and click **Settings > Update Agent Settings**.
 - 2.** Select the agents in Remote Site 1 that update components from the Update Agent.
 - a.** Navigate to **Updates > Server > Update Source**.
 - b.** Select **Customized Update Source** and click **Add**.
 - c.** In the screen that displays, type the IP address range of the endpoints in Remote Site 1.
 - d.** Select **Update source** and then select the designated Update Agent from the drop-down list.
-

Remote Site 2 Deployment

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

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

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

Use another Active Directory policy, but again, not specifying the DFS share as the source.

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

To minimize the impact of component updates across the WAN, designate one agent to act as an Update Agent. See *Remote Site 1 Deployment on page A-5* for more information.

Index

A

activation, 1-21
Activation Code, 2-11
Active Directory, 2-7, A-5
agent installation path, 1-22, 2-21
Agent Mover, 5-2
Apex Central, 2-6
Apex One
 Apex Central management, 2-6
 documentation, 2
Apex One firewall, 2-22
Apex One server
 default settings, 4-5
 installation logs, 4-3
 manual update, 4-4
 master service, 4-3
 processes, 4-3
 registry keys, 4-4
 services, 4-3
assessment mode, 2-22
automatic agent upgrade, 3-7, 3-13, 3-17

B

backup
 Apex One server files and folders, 5-3
 OfficeScan database, 5-3

C

Case Diagnostic Tool, 6-2
Client Packager, A-5
compatibility issues, 1-23
component duplication, 2-5
components, 4-4

component updates, 2-5

considerations
 fresh installation, 2-2
 upgrade, 3-2

Conventional Scan, 2-4

D

database backup, 3-3, 5-3
database back up, 1-22
debug logs
 server, 6-4
default settings
 agent privileges, 4-5
 global agent settings, 4-5
 scan settings, 4-5
Distributed File System (DFS), A-5
documentation, 2
documentation feedback, 7-5

E

Endpoint Sensor
 SQL Server, 1-11
Exceptions
 performance tuning tool, 6-2

F

firewall, 2-22
fresh installation
 checklist, 1-19
 considerations, 2-2
 summary, 2-25, 3-26
 verification, 4-2
full version, 2-11

H

HTTP port, 1-20, 2-13

I

incremental pattern, 2-5

installation

logs, 6-4

post-installation tasks, 4-1

installation path

agent, 1-22, 2-21

server, 1-19, 2-12

integrated Smart Protection Server, 2-4, 5-4

installation, 2-18

uninstallation, 5-5

L

Login Script Setup, A-4

M

manual agent upgrade, 3-14

manual update, 4-4

Microsoft Exchange Server, 1-23

MSI package deployment, A-5

N

network traffic, 2-5

O

OfficeScan server

debug logs, 6-4

functions, 2-3

location, 2-2

performance, 2-3

P

passwords, 1-21, 2-24

Performance Tuning Tool, 6-2

port

agent communication port, 1-22, 2-22

HTTP port, 1-20, 2-13

proxy server port, 1-20

server listening port, 3-16

SSL port, 1-20

post-installation, 4-1

prescan, 2-9

program folder shortcut, 1-22, 2-25, 4-2

program settings, 5-3

proxy server, 1-20

R

readme file, 2-25, 3-27

registration, 1-21

Registration Key, 2-11

remote installation, A-4

response file, 2-7

root account, 1-21, 2-25

RSA encryption, 2-14

S

scan method, 2-3

Security Agent

unload, 2-25

server

identification, 2-12

installation summary, 2-25, 3-26

master service, 2-13

product services, 2-11

server authentication certificate, 1-22

Smart Protection Server, 2-4, 2-18, 5-4, 5-5
Smart Scan, 2-4
SQL server, 1-24
SQL Server, 1-11
SSL port, 1-20, 2-13
SSL tunneling, 2-14
support
 resolve issues faster, 7-3
Support Intelligence System, 6-2

T

terminology, 4
third-party security software, 2-6
TMPerftool, 6-2
trial version, 2-11
troubleshooting, 6-1

U

uninstallation
 using the uninstallation program, 5-4
Update Agent, 2-6
updates, 2-5
upgrade
 agents, 3-13, 3-17
 checklist, 1-19
 considerations, 3-2
 summary, 2-25, 3-26
 verification, 4-2

W

web console, 2-25, 3-27, 4-2
web server, 1-20, 2-13

**TREND MICRO INCORPORATED**

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM09726/230508