Trend Micro Apex One™

Version: 2019

Administrator's Guide

For Enterprise and Medium Business

Endpoint Security

Protected Cloud

Web Security

Document Part No.: APEMS8589/190219

Release Date: March 2019

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

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

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

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

Evaluate this documentation on the following site:

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

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

To understand data privacy and protection and how data is treated within Trend Micro SaaS offerings, see:

https://www.trendmicro.com/en_us/about/legal/privacy-whitepapers.html

Table of Contents

Chapter 3: Getting Started with Data Protection

Part II: Protecting Security Agents

Chapter 4: Using Trend Micro Smart Protection

Chapter 5: Installing the Security Agent

Chapter 6: Keeping Protection Up-to-Date

Chapter 7: Scanning for Security Risks

Chapter 8: Protecting Against Unknown Threats

Chapter 9: Using Behavior Monitoring

Chapter 10: Using Device Control

Chapter 11: Using Data Loss Prevention

Chapter 12: Using Web Reputation

Chapter 13: Using the Apex One Firewall

Part III: Managing the Apex One Server and Agents

Chapter 14: Managing the Apex One Server

Chapter 15: Managing the Security Agent

Part IV: Providing Additional Protection

Chapter 16: Protecting Off-premises Agents

Chapter 17: Using Plug-in Manager

Chapter 18: Troubleshooting Resources

Chapter 19: Technical Support

Appendices

Appendix A: IPv6 Support in Apex One

Appendix B: Windows Server Core Support

Appendix C: Apex One Rollback

Appendix D: Glossary

Index

Preface

Preface

This document discusses getting started information, agent installation procedures, and Apex One server and agent management.

Topics include:

Apex One Documentation

Apex One documentation includes the following:

TABLE 1. Apex One Documentation

DOCUMENTATION	DESCRIPTION
Installation and Upgrade Guide	A PDF document that discusses requirements and procedures for installing the Apex One server, and upgrading the server and agents **Note** The Installation and Upgrade Guide may not be available for minor release versions, service packs, or patches.
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: http://esupport.trendmicro.com

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

http://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
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes

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

Terminology	Description
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".
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`	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:
	
	`C:\Program Files\Trend Micro\Security Agent`
	
	`C:\Program Files (x86)\Trend Micro\Security Agent`

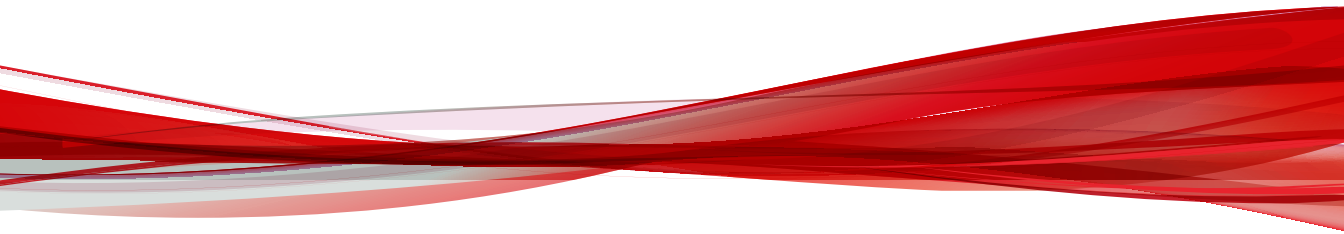
Terminology	Description

`Server installation folder`	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:
	`C:\Program Files\Trend Micro\Apex One`
	`C:\Program Files (x86)\Trend Micro\Apex One`
	For example, if a particular file is found under `\PCCSRV` on the server installation folder, the full path to the file is:
	`C:\Program Files\Trend Micro\Apex One\PCCSRV\<file_name>`.

Smart scan agent	Any Security Agent that has been configured to use smart scan
Conventional scan agent	Any Security Agent that has been configured to use conventional scan
Dual-stack	Entities that have both IPv4 and IPv6 addresses. For example: • 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

Part I

Introduction and Getting Started



Chapter 1

Introducing Apex One

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

Topics include:

About Apex One

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

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

What's New

The following tables outlines the new features and enhancements in this version of Trend Micro Apex One™ .

Item	Description
Offline Predictive Machine Learning	Predictive Machine Learning has been upgraded to provide offline protection against portable executable files. The lightweight, offline model helps protect all endpoints against unknown threats when a functional Internet connection is unavailable.
Fileless Attack Protection	Security Agent policies provide increased real-time protection against the latest fileless attack methods through enhanced memory scanning for suspicious process behaviors. Security Agents can terminate suspicious processes before any damage can be done.

Item	Description
Off-premises Security Agent Protection	Enhanced Edge Relay Server support allows for increased communication between the Apex One server and off-premises Security Agents. Security Agents can receive updated policy settings from the Apex One server even when a direct connection to the server is unavailable.
Rebranded Console	The OfficeScan server and OfficeScan agent programs have been rebranded to the Apex One server and Security Agent respectively. The new Apex One server integrates with Apex Central (formerly Trend Micro Control Manager) to provide increased protection against security risks. The all-in-one Security Agent program continues to provide superior protection against malware and data loss but also allows you implement Application Control, Endpoint Sensor, and Vulnerability Protection policies without having to install and maintain multiple agent programs.

Key Features and Benefits

Apex One provides the following features and benefits.

Table 1-1. Key Features and Benefits

Feature	Benefits
Ransomware Protection	Enhanced scan features can identify and block ransomware programs that target documents that run on endpoints by identifying common behaviors and blocking processes commonly associated with ransomware programs.

Feature	Benefits
Connected Threat Defense	Configure Apex One to subscribe to the Suspicious Object lists from the Apex Central server. Using the Apex Central console, you can create customized actions for objects detected by the Suspicious Object lists to provide custom defense against threats identified by endpoints protected by Trend Micro products specific to your environment. You can configure Security Agents to submit file objects that may contain previously unidentified threats to a Virtual Analyzer for further analysis. After assessing the objects, Virtual Analyzer adds any objects found to contain unknown threats to the Virtual Analyzer Suspicious Objects lists and distributes the lists to other Security Agents throughout the network.
Plug-in Manager and Plug-in Solutions	Plug-in Manager facilitates the installation, deployment, and management of plug-in solutions. Administrators can install two kinds of plug-in solutions: • Plug-in programs • Native Apex One features
Centralized Management	A web-based management console gives administrators transparent access to all endpoints and servers on the network. The web console coordinates automatic deployment of security policies, pattern files, and software updates on every endpoint and server. And with Outbreak Prevention Services, it shuts down infection vectors and rapidly deploys attack-specific security policies to prevent or contain outbreaks before pattern files are available. Apex One also performs real-time monitoring, provides event notification, and delivers comprehensive reporting. Administrators can perform remote administration, set customized policies for individual desktops or groups, and lock endpoint security settings.

Feature	Benefits
Antivirus / Security Risk Protection	Apex One protects computers from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak. To contain outbreaks, Apex One enforces outbreak prevention policies and isolates infected computers until they are completely risk-free. Apex One uses smart scan to make the scanning process more efficient. This technology works by off-loading a large number of signatures previously stored on the local endpoint to Smart Protection Sources. Using this approach, the system and network impact of the ever-increasing volume of signature updates to endpoint systems is significantly reduced. For information about smart scan and how to deploy it to agents, see *Scan Method Types on page 7-8*.
Damage Cleanup Services	Damage Cleanup Services™ cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, viral files) through a fully-automated process. To address the threats and nuisances posed by Trojans, Damage Cleanup Services does the following: • Detects and removes live Trojans • Kills processes that Trojans create • Repairs system files that Trojans modify • Deletes files and applications that Trojans drop Because Damage Cleanup Services runs automatically in the background, it is not necessary to configure it. Users are not even aware when it runs. However, Apex One may sometimes notify the user to restart their endpoint to complete the process of removing a Trojan.
Web Reputation	Web Reputation technology proactively protects agent endpoints within or outside the corporate network from malicious and potentially dangerous websites. Web Reputation breaks the infection chain and prevents the downloading of malicious code. Verify the credibility of websites and pages by integrating Apex One with the Smart Protection Server or the Trend Micro Smart Protection Network.

Feature	Benefits
Apex One Firewall	The Apex One Firewall protects endpoints and servers on the network using stateful inspections and high performance network virus scans. Create rules to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.
Data Loss Prevention	Data Loss Prevention safeguards an organization's digital assets against accidental or deliberate leakage. Data Loss Prevention allows administrators to: • Identify the digital assets to protect • Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email messages and external devices • Enforce compliance to established privacy standards
Device Control	Device Control regulates access to external storage devices and network resources connected to endpoints. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.
Behavior Monitoring	Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software.

The Apex One Server

The Apex One server is the central repository for all agent configurations, security risk logs, and updates.

The server performs two important functions:

- Installs, monitors, and manages Security Agents
- Downloads most of the components needed by agents. The Apex One server downloads components from the Trend Micro ActiveUpdate server and then distributes them to agents.

Note

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

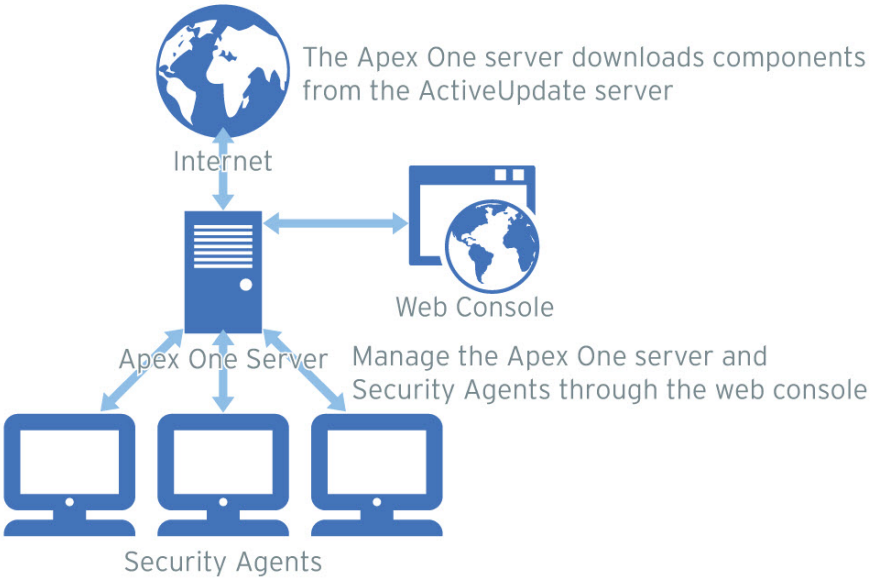


FIGURE 1-1. How the Apex One server works

The Apex One server is capable of providing real-time, bidirectional communication between the server and Security Agents. Manage the agents from a browser-based web console, which administrators can access from virtually anywhere on the network. The server communicates with the agent (and the agent with the server) through Hypertext Transfer Protocol Secure (HTTPS).

The Security Agent

Protect Windows endpoints from security risks by installing the Security Agent on each endpoint.

The Security Agent reports to the parent server from which it was installed. Configure agents to report to another server by using the Agent Mover tool. The Security Agent sends events and status information to the server in real time. Examples of events are virus/malware detection, Security Agent startup, Security Agent shutdown, start of a scan, and completion of an update.

Integration with Trend Micro Products and Services

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

TABLE 1-2. Products and Services that Integrate with Apex One

PRODUCT/ SERVICE	DESCRIPTION	VERSION
ActiveUpdate server	Provides all the components that the Security Agent needs to protect endpoints from security threats	Not applicable
Smart Protection Network	Provides File Reputation Services and Web Reputation Services to agents. Smart Protection Network is hosted by Trend Micro.	Not applicable

Product/ Service	Description	Version
Standalone Smart Protection Server	Provides the same File Reputation Services and Web Reputation Services offered by Smart Protection Network. A standalone Smart Protection Server is intended to localize the service to the corporate network to optimize efficiency. **Note** An integrated Smart Protection Server is installed with the Apex One server. It has the same functions as its standalone counterpart but has limited capacity.	• 3.3
Apex Central	A software management solution that provides the ability to control antivirus and content security programs from a central location—regardless of the platform or the physical location of the program.	• 2019
Trend Micro Control Manager		• 7.0 Patch 1
Deep Discovery Analyzer	Deep Discovery provides network-wide monitoring powered by custom sandboxing and relevant real-time intelligence to enable early attack detection, enable rapid containment, and deliver custom security updates that immediately improve protection against further attack.	5.1 and later

Chapter 2

Getting Started with Apex One

This chapter describes how to get started with Trend Micro Apex One and initial configuration settings.

Topics include:

The Web Console

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

Note

Configure the timeout settings from the web console.

For more information, see *Configuring Web Console Settings on page 14-57*.

Use the web console to do the following:

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

Note

The web console does not support Windows 8, 8.1, 10, or Windows Server 2012 in Windows UI mode.

Requirements for Opening the Web Console

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

- 300MHz Intel™ Pentium™ processor or equivalent
- 128MB of RAM
- At least 30MB of available disk space
- Monitor that supports 1366 x 768 resolution at 256 colors or higher
- Web browser support:
  - Microsoft Internet Explorer™ 10.0 or later
  - Microsoft Edge
  - Chrome

Note

Apex One only supports HTTPS traffic for viewing the web console.

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

TABLE 2-1. Apex One Web Console URLs

INSTALLATION TYPE	URL
With SSL on a default site	`https://<Apex One server FQDN or IP address>/Apex One`
With SSL on a virtual site	`https://<Apex One server FQDN or IP address>:<port number>/Apex One`

Note

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

Logon Account

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

Define user roles and set up user accounts to allow other users to access the web console without using the root account. When users log on to the console, they can use the user accounts you have set up for them. For more information, see *Role-based Administration on page 14-3*.

The Web Console Banner

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

- **<account name>**: Click the account name (for example, root) to modify details for the account, such as the password.
- **Log Off**: Logs user off from the web console

Getting Help

The **Help** menu provides access to the following support information:

- **Contents & Index**: Opens the Online Help
- **Support**: Displays the Trend Micro support web page, where you can submit questions and find answers to common questions about Trend Micro products

- **Threat Encyclopedia**: Displays the Threat Encyclopedia website which is the Trend Micro repository of malware-related information. Trend Micro threat experts regularly publish detections for malware, spam, malicious URLs, and vulnerabilities. The Threat Encyclopedia also explains high-profile web attacks and provides correlated information.
- **Contact Trend Micro**: Displays the Trend Micro **Contact Us** website with information about offices worldwide.
- **About**: Provides an overview of the product, instructions to check component version details, and a link to the Support Intelligence System.

  For details, see *Support Intelligence System on page 18-2*.

The Dashboard

The **Dashboard** appears when you open the Apex One web console or click **Dashboard** in the main menu.

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

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

For details about user accounts, see *Role-based Administration on page 14-3*.

The **Dashboard** screen contains the following:

- Product License Status section
- Widgets
- Tabs

Product License Status Section

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

Reminders about the license status display during the following instances:

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

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

Product Information Bars

Apex One displays a variety of messages at the top of the **Dashboard** screen that provide additional information for administrators.

The information displayed includes:

- Latest service packs or patches available for Apex One

Note

Click **More Information** to download the patch from the Trend Micro Download Center (http://downloadcenter.trendmicro.com).

- New widgets available
- Maintenance agreement notifications when an agreement is close to the expiry date
- Assessment mode notifications
- Authenticity notifications

Note

If the license used for Apex One is not genuine, an informational message displays. If you do not obtain a genuine license, Apex One displays a warning and stops performing updates.

Tabs and Widgets

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

The information that widgets display comes from:

- Apex One server and agents
- Plug-in solutions and their agents
- Trend Micro Smart Protection Network

Note

Enable Smart Feedback to display data from Smart Protection Network. For details about Smart Feedback, see *Smart Feedback on page 14-61*.

Tabs provide a container for widgets. The **Dashboard** supports up to 30 tabs.

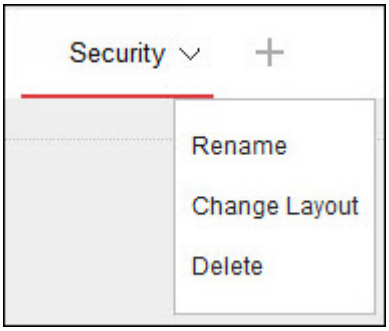
Working with Tabs

Manage tabs by adding, renaming, changing the layout, deleting, and automatically switching between tab views.

Procedure

1. Go to **Dashboard**.
2. To add a new tab:
   a. Click the add icon.

   b. Type a name for the new tab.
3. To rename a tab:
   a. Hover over the tab name and click the down arrow.



   b. Click **Rename** and type the new tab name.
4. To change the layout of the widgets for a tab:
   a. Hover over the tab name and click the down arrow.

b. Click **Change Layout**.

c. Select the new layout from the screen that appears.

d. Click **Save**.

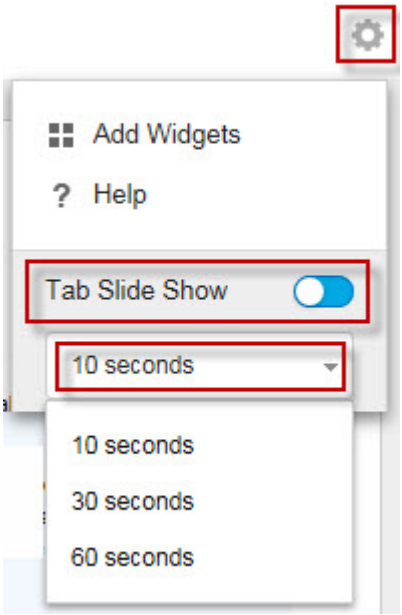
5. To delete a tab:

a. Hover over the tab name and click the down arrow.

b. Click **Delete** and confirm.

6. To play a tab slide show:

a. Click the **Settings** button to the right of the tab display.



b. Enable the **Tab Slide Show** control.

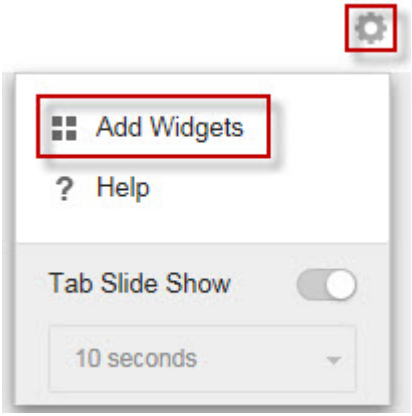
c. Select the length of time each tab displays before switching to the next tab.

Working with Widgets

Manage widgets by adding, moving, resizing, renaming, and deleting items.

Procedure

1. Go to **Dashboard**.
2. Click a tab.
3. To add a widget:
   a. Click the **Settings** button to the right of the tab display.



   b. Click **Add Widgets**.
   c. Select the widgets to add.
      - In the drop-down on top of the widgets, select a category to narrow down the selections.

- Use the search text box on top of the screen to search for a specific widget.

d. Click **Add**.

4. To move a widget to a new location on the same tab, drag-and-drop a widget to a new location.

5. Resize widgets on a multi-column tab by pointing the cursor to the right edge of the widget and then moving the cursor to the left or right.

6. To rename a widget:

   a. Click the settings icon (>).

   b. Type the new title.

   Note

   For some widgets, such as the **Apex One and Plug-ins Mashup**, you can modify widget-related items.

   c. Click **Save**.

7. To delete a widget, click the delete icon (>).

Summary Tab Widgets

The **Summary** tab provides an overview of the security status of all the Security Agents on your network.

Note

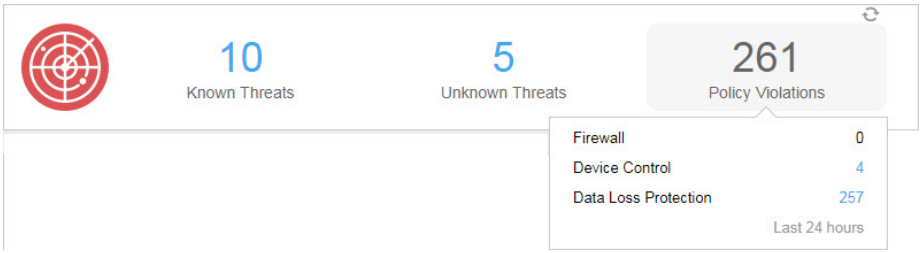
You cannot add, delete, or modify the widgets that display on the **Summary** tab.

Available widgets:

- *Overall Threat Detections and Policy Violations Widget on page 2-12*

- *Endpoint Status Widget on page 2-13*
- *Ransomware Summary Widget on page 2-15*
- *Top Ransomware Detections Widget on page 2-18*
- *Security Risk Detections Over Time Widget on page 2-19*

Overall Threat Detections and Policy Violations Widget



This widget provides an overview of all the threat detections and policy violations across the network over the last 24 hours.

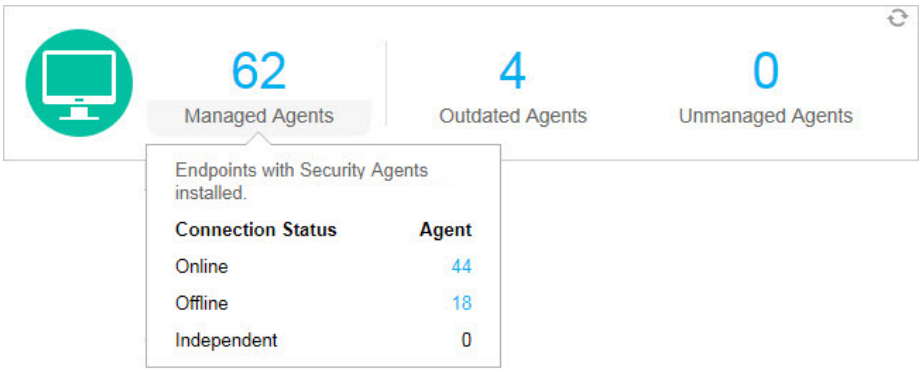
Hover over the threat or violation count to view a breakdown of the specific types of detections that occurred for each group. To view the logs for a specific feature, click the count to the right.

TABLE 2-2. Detection Categories

CATEGORY	DESCRIPTION
Known Threats	Displays all the features that detect security threats confirmed by Trend Micro • Virus/Malware • Spyware/Grayware • Web Reputation

Category	Description
Unknown Threats	Displays all the features that detect potential threats using advanced heuristics, analysis, or feature modeling • Predictive Machine Learning • Behavior Monitoring • Suspicious Connections • Suspicious File Objects
Policy Violations	Displays all the features that contain policy violations that are specific to your corporate security standards • Firewall • Device Control • Data Loss Prevention

Endpoint Status Widget



This widget provides an overview of the connection and update status of Security Agents on your network, and the latest security compliance count of unmanaged endpoints that do not report to the Apex One server.

Hover over a count to view a breakdown of the different statuses. To view the logs for a specific status, click the count to the right.

TABLE 2-3. Agent/Endpoint Groups

GROUP	DESCRIPTION
Managed Agents	Displays the last reported connection status of the Security Agents on your network • Online • Offline • Independent
Outdated Agents	Displays a list of component categories and the count of Security Agents with an outdated component in each category
Unmanaged Endpoints	Displays a list of all endpoints that the Apex One can detect, but that do not have the Security Agent program installed or do not report to the Apex One server **Note** To ensure that the Apex One server updates the unmanaged endpoint count regularly: 1. Define the Active Directory / IP address scope for an assessment. For more information, see *Active Directory Integration on page 2-32*. 2. Configure a Scheduled Assessment. For more information, see *Security Compliance for Unmanaged Endpoints on page 15-71*.

Ransomware Summary Widget

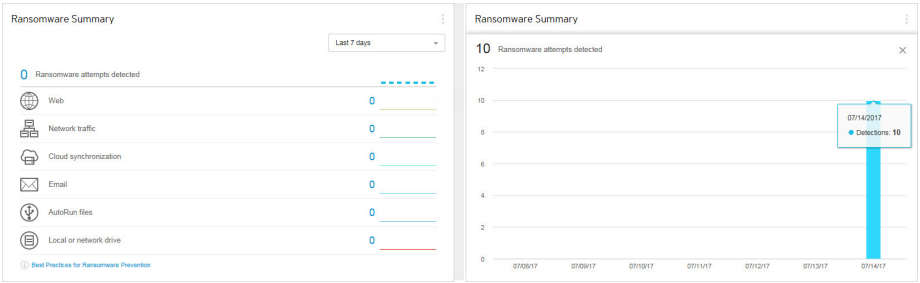


FIGURE 2-1. Default view displaying all ransomware data and enlarged view of the "Ransomware attempts detected" bar chart

This widget provides an overview of all the attempted ransomware attacks for a specified time range.

The default view displays a summary of all the ransomware detections and further categorizes the attempts based on the infection channel.

- Click the ransomware detection count on the default view to open the **Security Risks - Ransomware** logs screen that lists the ransomware detection details.

Click any of the charts on the right side of the widget to display an enlarged view of the chart data.

- Hover over the node(s) for any particular day to view the total number of detections for the displayed detection category. Click a node to redirect to the **Security Risks - Ransomware** logs screen, which lists the ransomware detection details for that particular day.

TABLE 2-4. Ransomware Detection Channels

CHANNEL	DESCRIPTION	DETECTED BY
Web	Files downloaded using a web client (for example, browser or FTP client)	• Web Reputation • Real-time Scan • Behavior Monitoring
Network traffic	Ransomware detected by the Suspicious Connections feature	• Suspicious Connections
Cloud synchronization	Files synchronized to the local sync folder by the following supported cloud storage services: • Microsoft™ OneDrive™	• Real-time Scan • Behavior Monitoring • Predictive Machine Learning
Email	Email attachments opened using Microsoft Outlook **Note** Apex One classifies all attachments opened using other email client applications in the **Local or network drive** channel.	• Real-time Scan • Behavior Monitoring
AutoRun files	Programs located on removable storage drives and executed by an autorun file **Note** Apex One classifies all other files/ programs not executed by the autorun program on removable storage devices in the **Local or network drive** channel.	• Real-time Scan • Behavior Monitoring

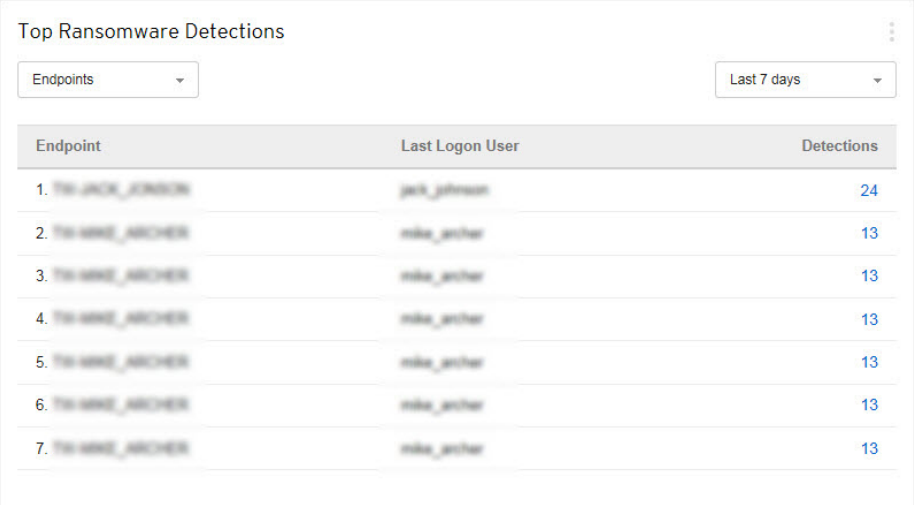
Channel	Description	Detected By
Local or network drive	Ransomware detected on local or network drives including: • Email attachments opened using email clients other than Microsoft Outlook • Files on removable storage devices not executed by the autorun program	• Real-time Scan • Manual Scan • Scheduled Scan • Scan Now • Behavior Monitoring

Security Threats - Ransomware Logs

The Security Threats - Ransomware logs provide an overview of all the ransomware threats detected on your network, regardless of the type of scan that detected the threat.

Item	Description
Date/Time	The time the detection occurred
Security Threat	The name of the security threat
Category	The type of scan that detected the threat
File Path / URL	The location where the threat detection occurred or the list used to detect the malicious website
Action	The action taken on the threat
Infection Channel	The channel the threat originated from
Endpoint	The endpoint on which the detection occurred

Top Ransomware Detections Widget



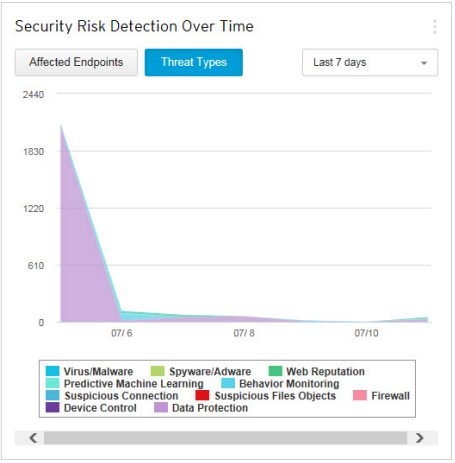
This widget provides an overview of the top ransomware detections for a specified time range.

Use the drop-down to select the type of ransomware data to display.

View	Description
Endpoints	Displays the endpoints with the greatest number of ransomware detections on your network Click the ransomware detection count to open the **Security Risks - Ransomware** logs screen that lists the ransomware detection details.
Ransomware Types	Displays the types of ransomware with the greatest number of detections on your network Click the **Threat Name** link to open the Trend Micro Threat Encyclopedia for further information regarding the specific threat type.

View	Description
Domains	Displays the ransomware domains with the greatest number of detections on your network Click the **Threat Name** link to open the Trend Micro Threat Encyclopedia for further information regarding the specific domain.

Security Risk Detections Over Time Widget



This widget provides an overview of the endpoints on your network with threat detections and the types of threats that affected your network for a specific time range.

Click the **Affected Endpoints** or **Threat Types** button to switch between the different views.

View	Description
Affected Endpoints	Displays the daily trend of endpoints with threat detections or policy violations for the specified time range

View	Description
Threat Types	Displays a graph that outlines the number of threats and policy violations logged for the specified time range • Click the threat type names at the bottom of the graph to show/hide detection information on the graph. • Hover over the node(s) for any particular day to view the total number of detections for the displayed threat types. Click a node to redirect to the logs screen for the threat type highlighted in the list.

Tip

You can add this widget multiple times to display both views.

Data Protection Widgets

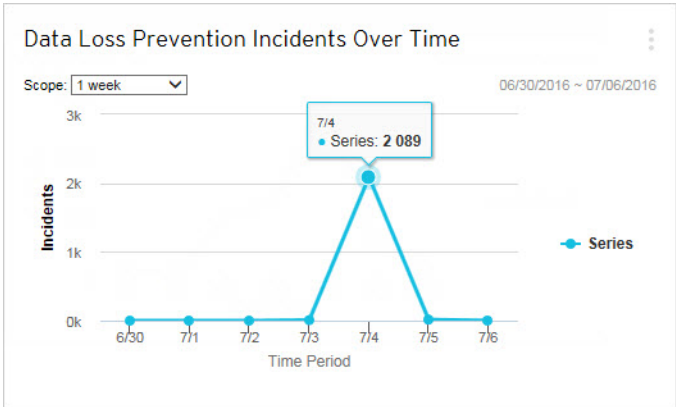
Note

The Data Protection widgets are available after activating Apex One Data Protection.

Available widgets:

- *Data Loss Prevention Incidents Over Time Widget on page 2-21*
- *Top Data Loss Preventions Incidents Widget on page 2-22*

Data Loss Prevention Incidents Over Time Widget

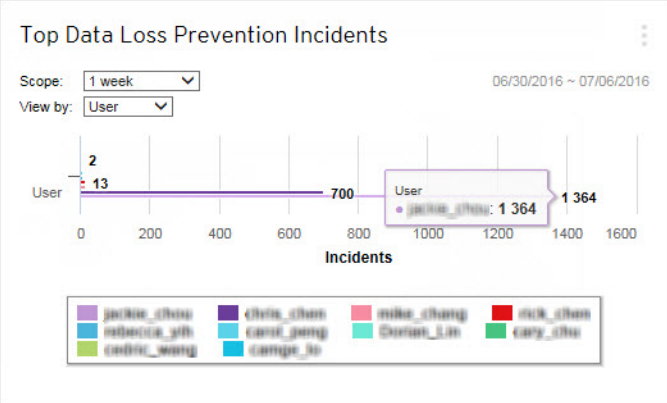


This widget displays the overall number of Data Loss Prevention incidents for a specific time range.

Note

The detections include all Data Loss Prevention incidents regardless of the action taken (“Block” or “Pass”).

Top Data Loss Preventions Incidents Widget



This widget displays the top Users, Channels, Templates, or Endpoints that triggered Data Loss Prevention incidents for a specified time range.

Note

- This widget displays a maximum of 10 users, channels, templates, or endpoints.
- The detections include all Data Loss Prevention incidents regardless of the action taken ("Block" or "Pass").

Select the type of Data Loss Prevention data that displays using the **View by** drop-down.

TABLE 2-5. Data Loss Prevention Views

VIEW	DESCRIPTION
User	Users that transmitted the greatest number of digital assets • Click the user names at the bottom of the graph to show/hide detection information on the graph. • Hover over the detection bars to view the user name and number of Data Loss Prevention incidents for that user.
Channel	Channels most often used to transmit digital assets • Click the channel names at the bottom of the graph to show/hide detection information on the graph. • Hover over the detection bars to view the channel name and number of Data Loss Prevention incidents for that channel.
Template	Digital asset templates that triggered the most detections • Click the template names at the bottom of the graph to show/hide detection information on the graph. • Hover over the detection bars to view the template name and number of Data Loss Prevention incidents for that template.
Endpoints	Endpoints that transmitted the greatest number of digital assets • Click the endpoint names at the bottom of the graph to show/hide detection information on the graph. • Hover over the detection bars to view the endpoint name and number of Data Loss Prevention incidents for that endpoint.

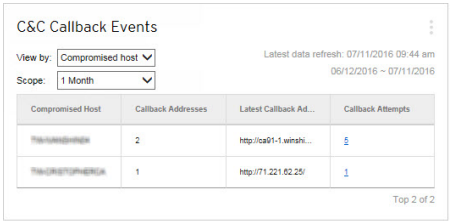
Apex One Widgets

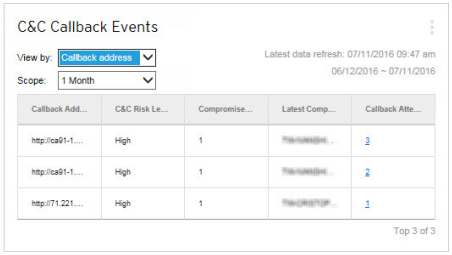
The Apex One widgets provide a quick reference for Security Agent security statuses and detections, plug-in program information, and outbreak incidents.

Available widgets:

- *C&C Callback Events Widget on page 2-24*

C&C Callback Events Widget





This widget displays all C&C callback event information including the target of the attack and the source callback address.

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

Use the **View by** drop-down to select the type of C&C callback data that displays:

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

TABLE 2-6. Compromised Host Information

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

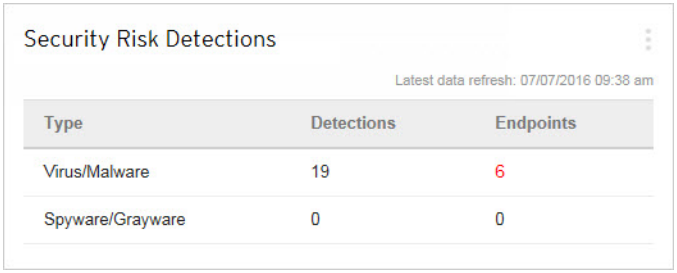
- **Callback address**: Displays the most recent C&C information per C&C callback address

TABLE 2-7. C&C Address Information

COLUMN	DESCRIPTION
Callback Address	The address of C&C callbacks originating from the network
C&C Risk Level	The risk level of the callback address determined by either the Global Intelligence or Virtual Analyzer list
Compromised Hosts	The number of endpoints that the callback address targeted
Latest Compromised Host	The name of the endpoint that last attempted to contact the C&C callback address

Column	Description
Callbacks Attempts	The number of attempted callbacks made to the address from the network **Note** Click the hyperlink to open the **C&C Callback Logs** screen and view more detailed information.

Security Risk Detections Widget



This widget displays the number of security risks detected and number of affected endpoints.

Click the endpoint count to open the **Agent Management** screen that lists the affected Security Agents in the agent tree.

Apex One and Plug-ins Mashup Widget

This widget combines data from Security Agents and installed plug-in programs and then presents the data in the agent tree. This widget helps you quickly assess the protection coverage on agents and reduces the overhead required to manage the individual plug-in programs.

This widget displays data from the following plug-in programs:

- Trend Micro Virtual Desktop Support

Important

You must activate a supported plug-in program before the mashup widget can display the corresponding data. Upgrade the plug-in programs if newer versions are available.

To select the columns that display in the agent tree, click the **More Options** button on the top right corner of the widget and click the **Widget Settings** button.

Click the data under any column to open the corresponding plug-in program console or the Apex One **Agent Management** screen. The screen that displays depends on the type of data that you clicked.

Antivirus Agent Connectivity Widget

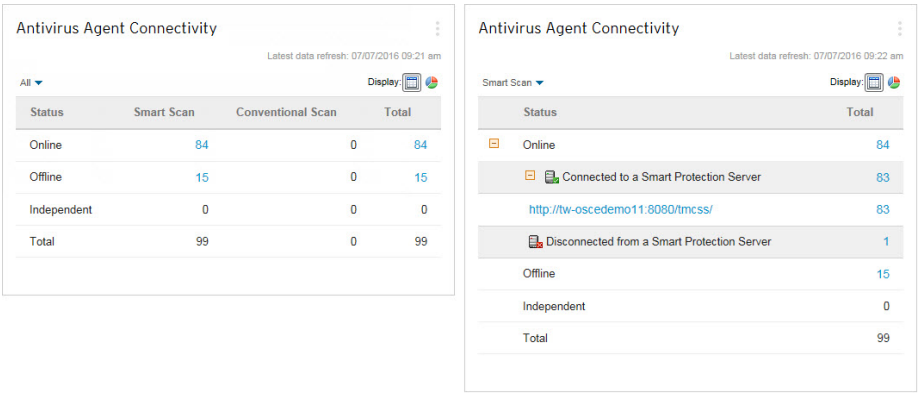


FIGURE 2-2. Default view displaying all Smart Scan and Conventional Scan agents and expanded Smart Scan agent view with Smart Protection Servers

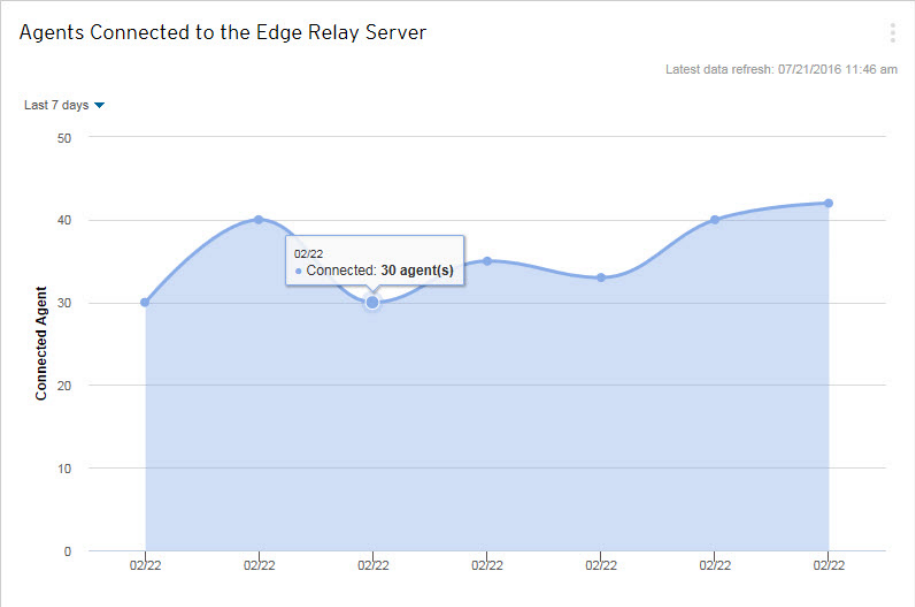
This widget displays the connection status of Security Agents to the Apex One server in relation to the configured scan method (Smart Scan and Conventional Scan).

You can choose to display the data in a table or pie chart by clicking the display icons ( ).

Use the drop-down list above the table/graph to change the type of data that displays. Click the count for any status to open the **Agent Management** screen that lists the related Security Agents in the agent tree.

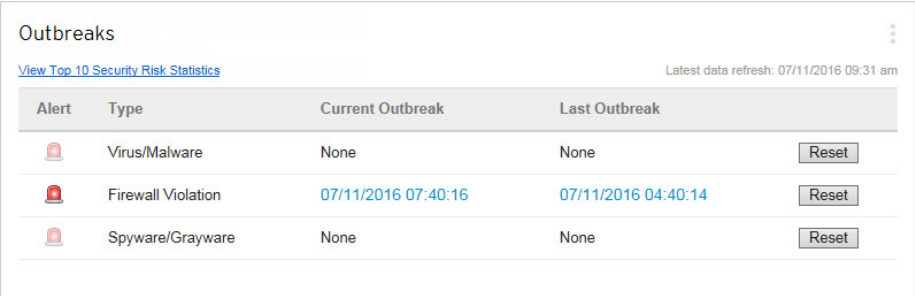
VIEW	DESCRIPTION
All	Displays the connection status of all Security Agents for both scan methods
Conventional Scan	Displays the connection status of all Security Agents that use the Conventional Scan method
Smart Scan	Displays the connection status of all Security Agents that use the Smart Scan method When viewing the agent connection status in a table: • Expand the "Online" agent information to view the connection status of agents with a Smart Protection Server. • Click the URL to open the Smart Protection Server management console. **Note** Only online agents (reporting to the Apex One server) can report their connection status with Smart Protection Servers. To restore an offline agent connection with a Smart Protection Server, see *Solutions to Issues Indicated in Security Agent Icons on page 15-41*.

Agents Connected to the Edge Relay Server Widget



This widget displays the number of Security Agents connected to the Apex One Edge Relay server for a specific time range.

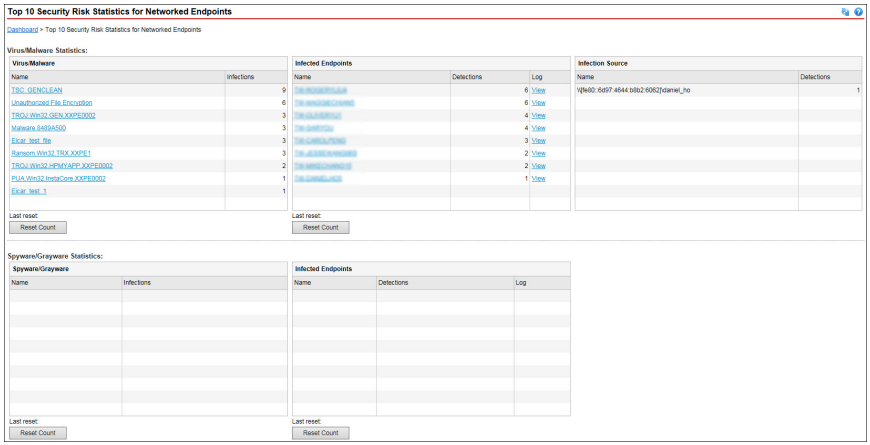
Outbreaks Widget



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

- Click the date/time link of the alert to view more details about the outbreak.
- **Reset** the status of the outbreak alert information and immediately enforce outbreak prevention measures when Apex One detects an outbreak.

  For details on enforcing outbreak prevention measures, see *Outbreak Prevention Policies on page 7-108*.
- Click **View Top 10 Security Risk Statistics** to view the most prevalent security risks, the endpoints with the greatest number of security risks, and the top infection sources.



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

- View detailed information about a security risk by clicking the security risk name.
- View the overall status of a particular endpoint by clicking the endpoint name.

- View security risk logs for the endpoint by clicking **View** corresponding to the endpoint name.
- Reset the statistics in each table by clicking **Reset Count**.

Agent Updates Widget

This widget displays components and programs that protect Security Agents from security risks.

Click the "Outdated" count to open the **Agent Management** screen that lists the Security Agents that require updates in the agent tree.

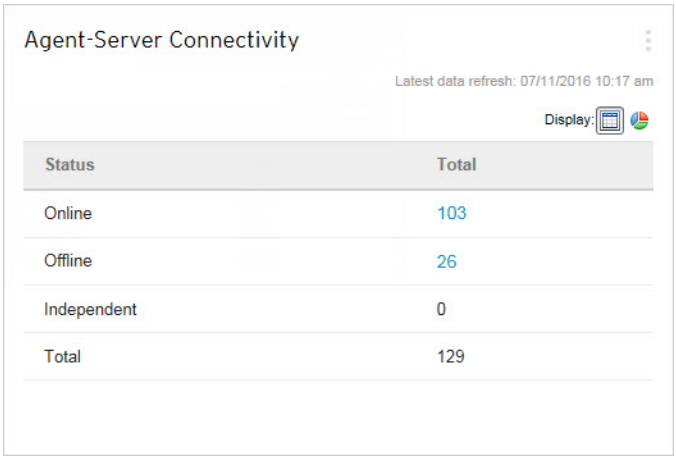
Management Widget

The management widget displays the connection status of Security Agents with the Apex One server.

Available widgets:

- *Agent-Server Connectivity Widget on page 2-31*

Agent-Server Connectivity Widget



This widget shows the connection status of all agents with the Apex One server.

You can switch between the table and pie chart by clicking the display icons ().

Click the count for any status to open the **Agent Management** screen that lists the related Security Agents in the agent tree.

Active Directory Integration

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

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

- **Custom agent groups**: Use Active Directory or IP addresses to manually group agents and map them to domains in the Apex One agent tree.

  For details, see *Automatic Agent Grouping on page 2-51*.

- **Unmanaged endpoints**: Ensure that endpoints in the network that are not managed by the Apex One server comply with your company's security guidelines.

  For details, see *Security Compliance for Unmanaged Endpoints on page 15-71*.

Manually or periodically synchronize the Active Directory structure with the Apex One server to ensure data consistency.

For details, see *Synchronizing Data with Active Directory Domains on page 2-34*.

Integrating Active Directory with Apex One

Procedure

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

c. Specify a file to which to save the encryption key. You can choose a popular file format, such as `.txt`. Type the file's full path and name, such as `C:\AD_Encryption\EncryptionKey.txt`.

WARNING!

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

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

Synchronizing Data with Active Directory Domains

Synchronize data with Active Directory domains regularly to keep the Apex One agent tree structure up-to-date and to query unmanaged agents.

Manually Synchronizing Data with Active Directory Domains

Procedure

1. Go to **Administration** > **Active Directory** > **Active Directory Integration**.
2. Verify that the domain credentials and encryption settings have not changed.

3. Click **Save and Synchronize**.

Automatically Synchronizing Data with Active Directory Domains

Procedure

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

   Note

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

4. Click **Save**.

The Apex One Agent Tree

The Apex One agent tree displays all the agents grouped into domains that the server currently manages. Agents are grouped into domains so you can simultaneously configure, manage, and apply the same configuration to all domain members.

Agent Connection Status

The Security Agent connection status depends on the way in which the Apex One server communicates with the Security Agent. The following table outlines the different connection statuses available for the Security Agent.

TABLE 2-8. Office Agent Connection Status

STATUS	DESCRIPTION
Online	The Security Agent can connect to the Apex One server for bidirectional communication of the following: • Policy settings • Updates • Scan commands • Suspicious Object list synchronization • Sample submission • Log submission
Offline	The Security Agent has no functional connection with the Apex One server or an Edge Relay server.
Independent	The Security Agent can connect to the server but communication is limited. While in Independent mode: • The Security Agent does not accept policy settings from the server • The Security Agent does not initiate scan commands from the server • The Security Agent does not send logs to the server You can configure Independent agents with privileges to allow or block component updates if a functional connection to the Apex One server is available. End users can manually initiate scans and updates on agents in Independent mode.

Status	Description
Off-premises	The Security Agent is outside of the corporate network and cannot connect to the Apex One server directly. The Security Agent can, however, connect to an Edge Relay server for the following: • Suspicious Object list synchronization • Sample submission • Log submission **Note** The **Connection Status** for an off-premises agent displays as "Offline" in the agent tree because the Apex One server has no direct connection with the Security Agent.

Agent Tree Icons

The Apex One agent tree icons provide visual hints that indicate the type of endpoint and the status of Security Agents that Apex One manages.

Table 2-9. Apex One Agent Tree Icons

Icon	Description
	Domain
	Root
	Update agent
	Conventional scan agent
	Smart scan available Security Agent

Icon	Description
	Smart scan unavailable Security Agent
	Smart scan available update agent
	Smart scan unavailable update agent

Searching the Agent Tree

Use the search and view features above the Agent Tree (**Agents** > **Agent Management**) to locate specific endpoints managed by Apex One.

Procedure

- Search for any agent to manage by specifying the agent name in the **Search for endpoints** text box.

  A list of results appears in the agent tree. For more search options, click **Advanced Search**.

  Note

  You must use the Advanced Search feature to locate endpoints using IPv4 or IPv6 addresses.

  For details, see *Advanced Search Options on page 2-39*.

- After selecting a domain, the agent tree table expands to show the agents belonging to the domain and all the columns containing relevant information for each agent. To view only a set of related columns, select an item in the agent tree view.

  - **View all**: Shows all columns
  - **Update view**: Shows all the components and programs

- **Antivirus view**: Shows antivirus components
- **Anti-spyware view**: Shows anti-spyware components
- **Data protection view**: Shows the status of the Data Protection module on agents
- **Firewall view**: Shows firewall components
- **Smart protection view**: Shows the scan method used by agents (conventional or smart scan) and smart protection components
- **Update Agent view**: Shows information for all Update Agents managed by the Apex One server
- **Off-premises agent view**: Shows information for all agents reporting to the Edge Relay Server

Advanced Search Options

Search for agents based on the following criteria:

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

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

Agent Tree Specific Tasks

The agent tree displays when you access certain screens on the web console. Above the agent tree are menu items specific to the screen you have accessed. These menu items allow you to perform specific tasks, such as configuring agent settings or initiating agent tasks. To perform any of the tasks, first select the task target and then select a menu item.

The following screens display the agent tree:

- *Agent Management Screen on page 2-40*
- *Outbreak Prevention Screen on page 2-44*
- *Agent Selection Screen on page 2-45*
- *Rollback Screen on page 2-46*
- *Security Risk Logs Screen on page 2-47*

Agent Management Screen

To view this screen, go to **Agents** > **Agent Management**.

Manage general agent settings and view status information about specific agents (for example, **Logon User**, **IP Address**, and **Connection Status**) on the **Agent Management** screen.

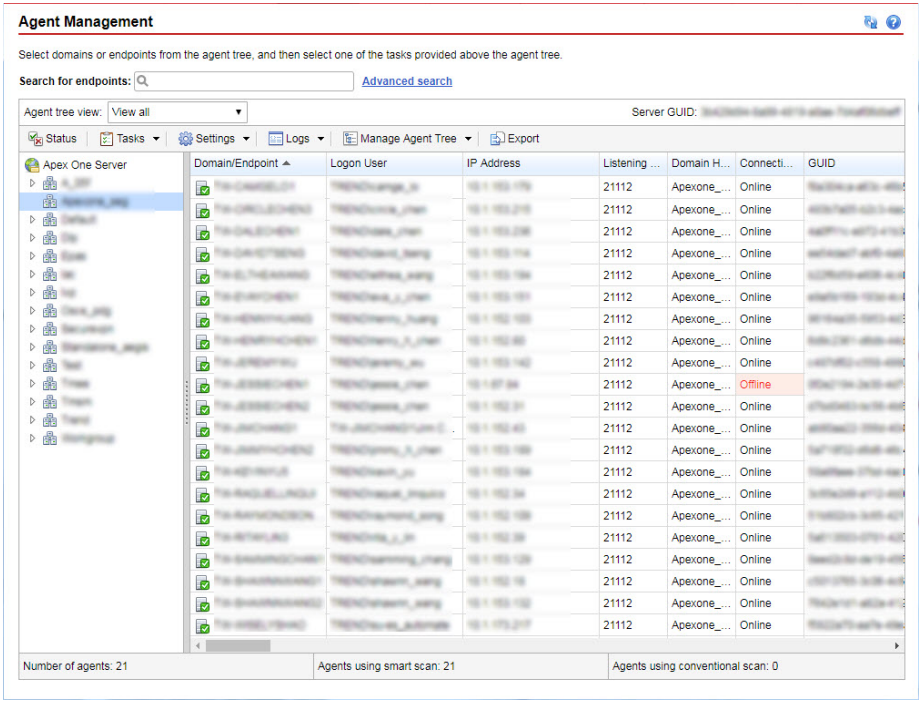


FIGURE 2-3. Agent Management screen

The following table lists the tasks you can perform:

TABLE 2-10. Agent Management Tasks

MENU BUTTON	TASK
Status	View detailed agent information. For details, see *Viewing Security Agent Information on page 15-55*.

Menu Button	Task
Tasks	• Run Scan Now on agent endpoints. For details, see *Initiating Scan Now on page 7-25*. • Uninstall the agent. For details, see *Uninstalling the Security Agent from the Web Console on page 5-61*. • Restore suspicious file detections. For details see *Restoring Quarantined Files on page 7-44*. • Restore spyware/grayware components. For details, see *Restoring Spyware/Grayware on page 7-52*.

Menu Button	Task

Settings	• Configure scan settings. For details, see the following topics:
	  • *Scan Method Types on page 7-8*
	  • *Manual Scan on page 7-18*
	  • *Real-time Scan on page 7-15*
	  • *Scheduled Scan on page 7-20*
	  • *Scan Now on page 7-22*
	• Configure Web Reputation settings. For details, see *Web Reputation Policies on page 12-5*.
	• Configure Predictive Machine Learning Settings. For details, see *Configuring Predictive Machine Learning Settings on page 8-3*.
	• Configure Suspicious Connection Settings. For details, see *Configuring Suspicious Connection Settings on page 8-7*.
	• Configure Behavior Monitoring settings. For details, see *Behavior Monitoring on page 9-2*.
	• Configure Device Control settings. For details, see *Device Control on page 10-2*.
	• Configure Data Loss Prevention policies. For details, see *Data Loss Prevention Policy Configuration on page 11-47*.
	• Configure Sample Submission settings. For details, see *Configuring Sample Submission on page 8-10*.
	• Assign agents as Update Agents. For details, see *Update Agent Configuration on page 6-54*.
	• Configure agent privileges and other settings. For details, see *Configuring Agent Privileges and Other Settings on page 15-92*.
	• Enable or disable Security Agent services. For details, see *Security Agent Services on page 15-6*.
	• Configure the spyware/grayware approved list. For details, see *Spyware/Grayware Approved List on page 7-50*.
	• Configure the Trusted Program List. For details, see *Configuring the Trusted Programs List on page 7-54*.
	• Import and export agent settings. For details, see *Importing and Exporting Agent Settings on page 15-56*.

Menu Button	Task
Logs	View the following logs: • Virus/Malware logs (for details, see *Viewing Virus/Malware Logs on page 7-89*) • Spyware/Grayware logs (for details, see *Viewing Spyware/Grayware Logs on page 7-96*) • Firewall logs (for details, see *Firewall Logs on page 13-28*) • Web Reputation logs (for details, see *Web Threat Logs on page 12-20*) • Suspicious Connection logs (for details, see *Viewing Suspicious Connection Logs on page 8-14*) • Suspicious Files logs (for details, see *Viewing Suspicious File Logs on page 7-100*) • C&C Callback logs (for details, see *Viewing C&C Callback Logs on page 12-21*.) • Behavior Monitoring logs (for details, see *Behavior Monitoring Logs on page 9-22*) • Predictive Machine Learning logs (for details, see *Viewing Predictive Machine Learning Logs on page 8-11*) • Device Control logs (for details, see *Device Control Logs on page 10-18*) • DLP logs (for details, see *Data Loss Prevention Logs on page 11-56*) • Scan Operation logs (for details see *Viewing Scan Operation Logs on page 7-101*) Delete logs. For details, see *Log Management on page 14-42*.
Manage Agent Tree	Manage the agent tree. For details, see *Agent Grouping Tasks on page 2-55*.
Export	Export a list of agents to a comma-separated value (`.csv`) file.

Outbreak Prevention Screen

To view this screen, go to **Agents** > **Outbreak Prevention**.

Specify and activate outbreak prevention settings in the **Outbreak Prevention** screen. For details, see *Configuring Security Risk Outbreak Prevention on page 7-106*.

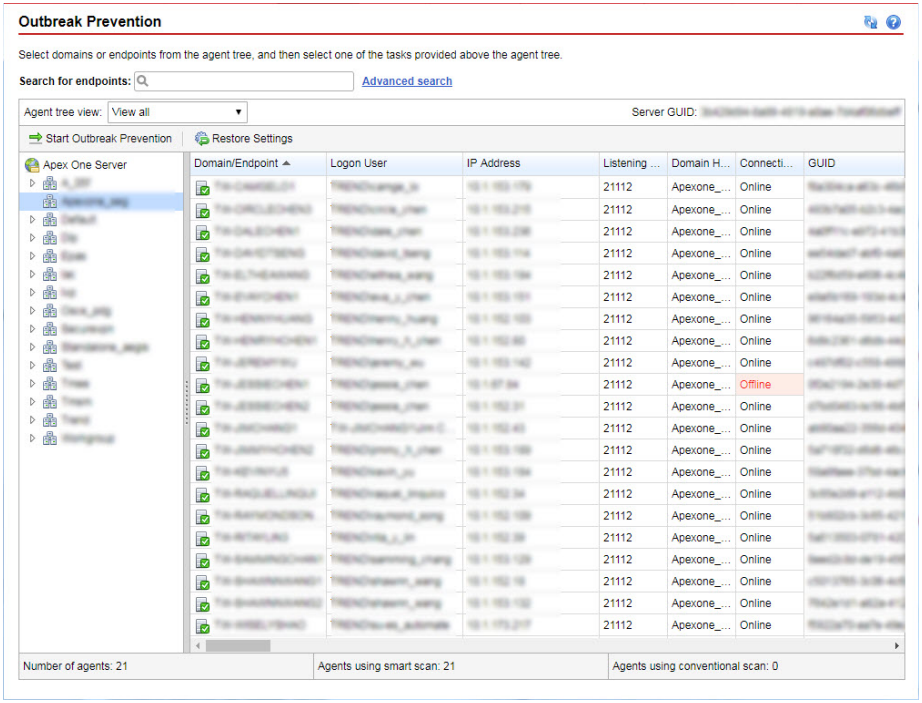


FIGURE 2-4. Outbreak Prevention screen

Agent Selection Screen

To view this screen, go to **Updates** > **Agents** > **Manual Update**. Select **Manually select agents** and click **Select**.

Initiate manual update in the **Agent Selection** screen. For details, see *Security Agent Manual Updates on page 6-44*.

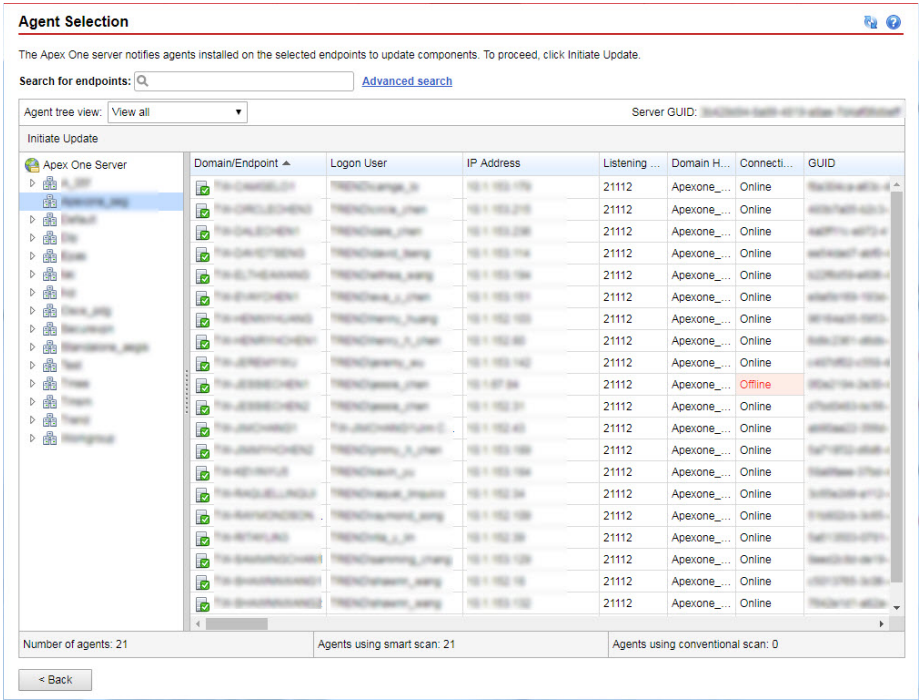


FIGURE 2-5. Agent Selection screen

Rollback Screen

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

Roll back agent components in the **Rollback** screen. For details, see *Rolling Back Components for Security Agents on page 6-51*.

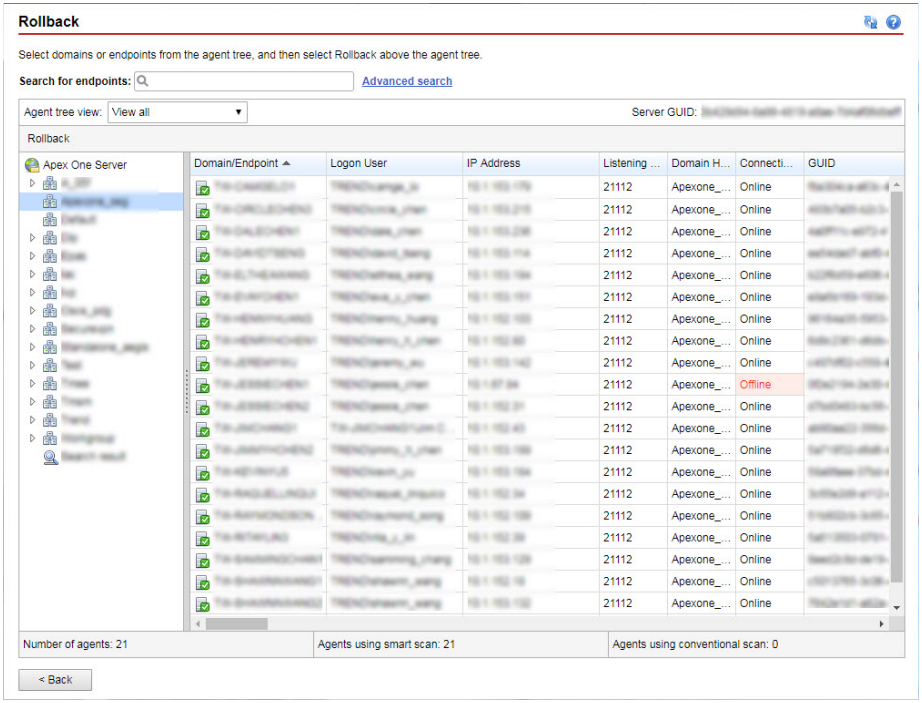


FIGURE 2-6. Rollback screen

Security Risk Logs Screen

To view this screen, go to **Logs** > **Agents** > **Security Risks**.

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

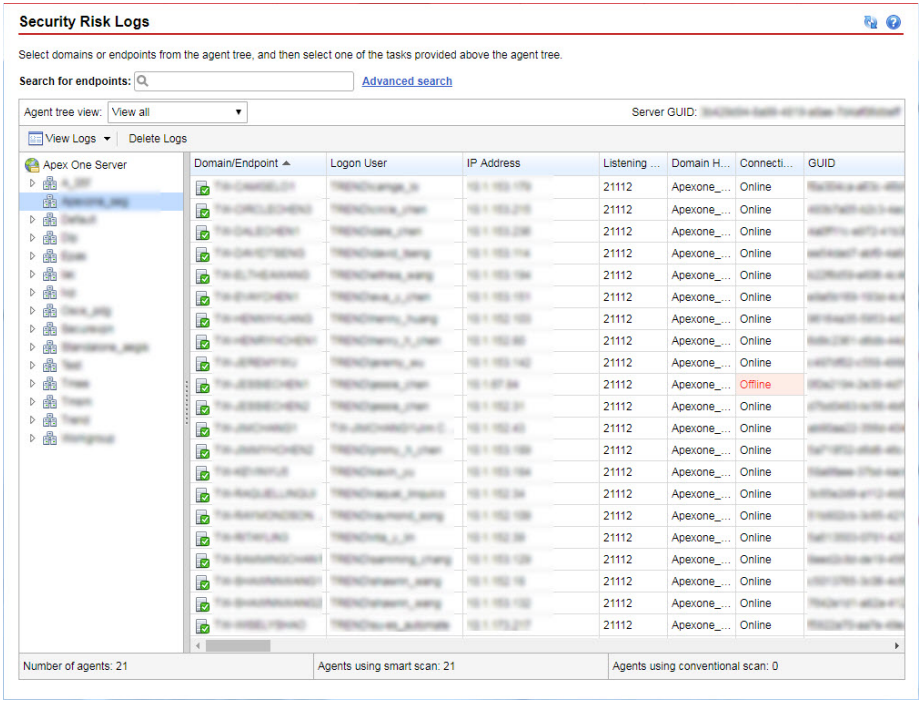


FIGURE 2-7. Security Risk Logs screen

Perform the following tasks:

1. View logs that agents send to the server. For details, see:
   - *Viewing Virus/Malware Logs on page 7-89*
   - *Viewing Spyware/Grayware Logs on page 7-96*
   - *Viewing Firewall Logs on page 13-28*
   - *Viewing Web Reputation Logs on page 12-20*
   - *Viewing Suspicious Connection Logs on page 8-14*

- *Viewing Suspicious File Logs on page 7-100*
- *Viewing C&C Callback Logs on page 12-21*
- *Viewing Behavior Monitoring Logs on page 9-23*
- *Viewing Predictive Machine Learning Logs on page 8-11*
- *Viewing Device Control Logs on page 10-19*
- *Viewing Data Loss Prevention Logs on page 11-57*
- *Viewing Scan Operation Logs on page 7-101*

2. Delete logs. For details, see *Log Management on page 14-42*.

Apex One Domains

A domain in Apex One is a group of agents that share the same configuration and run the same tasks. By grouping agents into domains, you can configure, manage, and apply the same configuration to all domain members.

For more information on agent grouping, see *Agent Grouping on page 2-49*.

Agent Grouping

Use Agent Grouping to manually or automatically create and manage domains on the Apex One agent tree.

There are two ways to group Security Agents into domains.

TABLE 2-11. Agent Grouping Methods

METHOD	AGENT GROUPING	DESCRIPTION
Manual	• NetBIOS domain • Active Directory domain • DNS domain	Manual agent grouping defines the domain to which a newly installed agent should belong. When the agent appears in the agent tree, you can move it to another domain or to another Apex One server. Manual agent grouping also allows you to create, manage, and remove domains in the agent tree. For details, see *Manual Agent Grouping on page 2-50*.
Automatic	Custom agent groups	Automatic agent grouping uses rules to sort agents in the agent tree. After you define the rules, you can access the agent tree to manually sort the agents or allow Apex One to automatically sort them when specific events occur. For details, see *Automatic Agent Grouping on page 2-51*.

Manual Agent Grouping

Apex One uses this setting only during fresh agent installations. The installation program checks the network domain to which a target endpoint belongs. If the domain name already exists in the agent tree, Apex One groups the agent on the target endpoint under that domain and will apply the settings configured for the domain. If the domain name does not exist, Apex One adds the domain to the agent tree, groups the agent under that domain, and then applies the root settings to the domain and agent.

Configuring Manual Agent Grouping

Procedure

1. Go to **Agents** > **Agent Grouping**.
2. Specify the agent grouping method:
   - NetBIOS domain

- Active Directory domain
- DNS domain

3. Click **Save**.

What to do next

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

- Add a domain
- Delete a domain or agent
- Rename a domain
- Move a single agent to another domain

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

Automatic Agent Grouping

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

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

Configuring Automatic Agent Grouping

Procedure

1. Go to **Agents** > **Agent Grouping**
2. Go to the **Agent Grouping** section and select **Create custom agent groups for existing Security Agents**.

3. Go to the **Automatic Agent Grouping** section.
4. To start creating rules, click **Add** and then select either **Active Directory** or **IP Address**.
   - If you selected **Active Directory**, see the configuration instructions in *Defining Agent Grouping Rules by Active Directory Domains on page 2-53*.
   - If you selected **IP Address**, see the configuration instructions in *Defining Agent Grouping Rules by IP Addresses on page 2-54*.
5. If you created more than one rule, prioritize the rules by performing these steps:
   a. Select a rule.
   b. Click an arrow under the **Group Priority** column to move the rule up or down the list. The ID number of the rule changes to reflect the new position.
6. To use the rules during agent sorting:
   a. Select the check boxes for the rules that you want to use.
   b. Enable the rules by switching the **Status** control to **On**.

Note

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

7. Specify a sorting schedule in the **Scheduled Domain Creation** section.
   a. Select **Enable scheduled domain creation**.
   b. Specify the schedule under **Scheduled Domain Creation**.
8. Choose from the following options:
   - **Save and Create Domain Now**: Choose this option if you specified new domains in *Defining Agent Grouping Rules by IP Addresses on page*

2-54, step 7 or in *Defining Agent Grouping Rules by Active Directory Domains on page 2-53*, step 7.

- **Save**: Choose this option if you did not specify new domains or want to create the new domains only when agent sorting runs.

Note

Agent sorting will not start after completing this step.

Defining Agent Grouping Rules by Active Directory Domains

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

Procedure

1. Go to **Agents** > **Agent Grouping**.
2. Go to the **Agent Grouping** section and select **Create custom agent groups for existing Security Agents**.
3. Go to the **Automatic Agent Grouping** section.
4. Click **Add** and then select **Active Directory**.

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

a. Mouseover on a particular Apex One domain and click the add domain icon (+).

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

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

9. (Optional) Select **Duplicate Active Directory structure into the agent tree**. This option duplicates the hierarchy of the selected Active Directory domains to the selected Apex One domain.

10. Click **Save**.

Defining Agent Grouping Rules by IP Addresses

Create custom agent groups using network IP addresses to sort agents in the Apex One agent tree. The feature can help administrators arrange the Apex One agent tree structure before the agent registers to the Apex One server.

Procedure

1. Go to **Agents** > **Agent Grouping**.
2. Go to the **Agent Grouping** section and select **Create custom agent groups for existing Security Agents**.
3. Go to the **Automatic Agent Grouping** section.
4. Click **Add** and then select **IP Address**.

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

- An IPv4 address range
- An IPv6 prefix and length

Note

If a dual-stack agent's IPv4 and IPv6 addresses belong to two separate agent groups, the agent will be grouped under the IPv6 group. If IPv6 is disabled on the agent's host machine, the agent will move to the IPv4 group.

8. Select the Apex One domain to which the IP address or IP address ranges maps. If the domain does not exist, do the following:

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

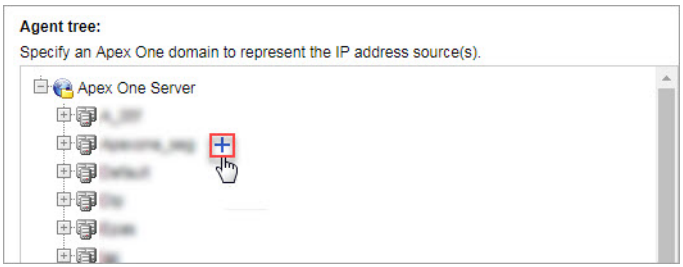


FIGURE 2-8. Add domain icon

   b. Type the domain in the text box provided.

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

9. Click **Save**.

Agent Grouping Tasks

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

- Add a domain. See *Adding a Domain on page 2-56* for details.
- Delete a domain or agent. See *Deleting a Domain or Agent on page 2-56* for details.
- Rename a domain. See *Renaming a Domain on page 2-57* for details.
- Move a single agent to another domain or another Apex One server. See *Moving Security Agents to Another Domain or Server on page 2-58* for details.

Adding a Domain

Procedure

1. Navigate to **Agents** > **Agent Management**.
2. Click **Manage Agent Tree** > **Add Domain**.
3. Type a name for the domain you want to add.
4. Click **Add**.

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

Deleting a Domain or Agent

Procedure

1. Navigate to **Agents** > **Agent Management**.
2. In the agent tree, select:

- One or several domains
- One, several, or all agents belonging to a domain

3. Click **Manage Agent Tree** > **Remove Domain/Agent**.
4. To delete an empty domain, click **Remove Domain/Agent**. If the domain has agents and you click **Remove Domain/Agent**, the Apex One server will re-create the domain and group all agents under that domain the next time agents connect to the Apex One server. You can perform the following tasks before deleting the domain:
   a. Move agents to other domains. To move agents to other domains, drag and drop agents to the destination domains.
   b. Delete all agents.
5. To delete a single agent, click **Remove Domain/Agent**.

Note

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

Renaming a Domain

Procedure

1. Navigate to **Agents** > **Agent Management**.
2. Select a domain in the agent tree.
3. Click **Manage Agent Tree** > **Rename Domain**.
4. Type a new name for the domain.
5. Click **Rename**.

The new domain name appears in the agent tree.

Moving Security Agents to Another Domain or Server

Procedure

1. Navigate to **Agents** > **Agent Management**.
2. In the agent tree, select one, several, or all agents.
3. Click **Manage Agent Tree** > **Move Agent**.
4. To move agents to another domain:
   - Select **Move selected agent(s) to another domain**.
   - Select the domain.
   - (Optional) Apply the settings of the new domain to the agents.

   Tip

   You can also drag and drop agents to another domain in the agent tree.
5. To move agents to another server:
   - Select **Move selected agent(s) to another server**.
   - Type the server name or IPv4/IPv6 address and HTTP or SSL (443) port number.

     Note

     If you are moving Security Agents to Apex One as a Service, you can obtain the Apex One as a Service server information by accessing the Apex Central console. Go to **Directories** > **Product Servers** and, in the **Server Type** drop-down, select **Apex One**.
6. Click **Move**.

Chapter 3

Getting Started with Data Protection

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

Topics include:

Data Protection Installation

The Data Protection module includes the following features:

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

Note

Apex One out-of-the-box has a Device Control feature that regulates access to commonly used devices such as USB storage devices. Device Control that is part of the Data Protection module expands the range of monitored devices. For a list of monitored devices, see *Device Control on page 10-2*.

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

Installing Data Protection

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the **Apex One Data Protection** section and click **Download**.

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

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

Note

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

3. Monitor the download progress.

   You can navigate away from the screen during the download.

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

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

Note

If Apex One Data Protection does not display, see the reasons and solutions in *Troubleshooting Plug-in Manager on page 17-12*.

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

   a. Click **Install Later**.

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

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

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

   The installation starts.

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

Data Protection License

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

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

Activating the Plug-in Program License

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.

   The **Product License New Activation Code** screen appears.
3. Type or copy-and-paste the Activation Code into the text fields.
4. Click **Save**.

   The plug-in console appears.

Viewing and Renewing the License Information

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.
3. Click **View License Information** to view information about the current license on the Trend Micro website.
4. View the following license details in the screen that opens.

Option	Description
Status	Displays either "Activated", "Not Activated" or "Expired"
Version	Displays either "Full" or "Trial" version **Note** Activation of both the full and trial versions displays only as "Full".
Seats	Displays how many endpoints the plug-in program can manage
License expires on	If the plug-in program has multiple licenses, the latest expiration date displays. For example, if the license expiration dates are 12/31/2011 and 06/30/2011, 12/31/2011 displays.
Activation Code	Displays the Activation Code
Reminders	Depending on the current license version, the plug-in displays reminders about the license expiration date either during the grace period (full versions only), or when the license expires

Note

The duration of the grace period varies by region. Verify the grace period of a plug-in program with a Trend Micro representative.

5. To update the screen with the latest license information, click **Update Information**.

6. Click **New Activation Code** to open the **Product License New Activation Code** screen.

   For details, see *Activating the Plug-in Program License on page 3-4*.

Deployment of Data Protection to Security Agents

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

Important

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

  You can enable or disable the module from the web console. For details, see *Security Agent Services on page 15-6*.

- If the Trend Micro Data Loss Prevention software already exists on the endpoint, Apex One will not replace it with the Data Protection module.
- Online agents install the Data Protection module immediately. Offline and Independent agents install the module after reconnecting to the Apex One server.
- Users must restart their computers to finish installing Data Loss Prevention drivers. Inform users about the restart ahead of time.
- Trend Micro recommends enabling debug logging to help you troubleshoot deployment issues. For details, see *Enabling Debug Logging for the Data Protection Module on page 11-62*.

Deploying the Data Protection Module to Security Agents

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, you can:
   - Click the root domain icon ( ) to deploy the module to all existing and future agents.

- Select a specific domain to deploy the module to all existing and future agents under the domain.
- Select a specific agent to deploy the module only to that agent.

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

   Note

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

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

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

   Note

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

   Security Agents start to download the module from the server.

5. Check if the module was deployed to agents.
   a. In the agent tree, select a domain.
   b. In the agent tree view, select **Data protection view** or **View all**.
   c. Check the **Data Protection Status** column. The deployment status can be any of the following:

- **Running**: The module was deployed successfully and its features have been enabled.
- **Requires restart**: Data Loss Prevention drivers have not been installed because users have not restarted their computers. If the drivers are not installed, Data Loss Prevention will not be functional.
- **Stopped**: The service for the module has not been started or the target endpoint has been shut down normally. To start the Data Protection service, go to **Agents** > **Agent Management** > **Settings** > **Additional Service Settings** and enable Data Protection Services.
- **Cannot install**: There was a problem deploying the module to the agent. You will need to re-deploy the module from the agent tree.
- **Cannot install (Data Loss Prevention already exists)**: The Trend Micro Data Loss Prevention software already exists on the endpoint. Apex One will not replace it with the Data Protection module.
- **Not installed**: The module has not been deployed to the agent. This status displays if you chose not to deploy the module to the agent or if the status of the agent is Offline or Independent during deployment.

Forensic Folder and DLP Database

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

Important

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

Modifying the Forensic Folder and Database Settings

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

WARNING!

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

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

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

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

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

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

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

The following table outlines the Security Agent settings available in the <*Server installation folder*>\PCCSRV\ofcscan.ini file located on the Apex One server.

TABLE 3-2. Forensic File Agent Settings in PCCSRV\ofcscan.ini

OBJECTIVE	INI SETTING	VALUES
Enabling the uploading of forensic data files to the server	`UploadForensicDataEnable`	0: Disable 1: Enable (default)
Configuring the maximum size of files that the Security Agent uploads to the server	`UploadForensicDataSizeLimitInMb` **Note** The Security Agent only sends files that are less than this size to the server.	Default value (in MB): 10 Minimum value: 1 Maximum value: 20
Configuring the length of time to store forensic data files on the Security Agent	`ForensicDataKeepDays` **Note** The Security Agent deletes forensic data files that have passed the expiry date specified once per day based on the previous day's purge time.	Default value (in days): 180 Minimum value: 1 Maximum value: 3650
Configuring the frequency in which the Security Agent checks for server connectivity	`ForensicDataDelayUploadFrequenceInMinutes` **Note** Security Agents that are unable to upload forensic files to the server automatically try to resend the files using the specified time interval.	Default value (in minutes): 5 Minimum value: 5 Maximum value: 60

Creating a Backup of Forensic Data

Depending on the company's security policy, the length of time necessary to store the forensic data information may vary greatly. In order to free disk

space on the server, Trend Micro recommends performing a manual backup of the forensic folder data and forensic database.

Procedure

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

Uninstalling Data Protection

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

- All Data Loss Prevention configurations, settings, and logs are removed from the Apex One server.
- All Device Control configurations and settings provided by the Data Protection module are removed from the server.
- The Data Protection module is removed from agents. Agent endpoints must be restarted to remove Data Protection completely.
- Data Loss Prevention policies will no longer be enforced on agents.
- Device Control will no longer monitor access to the following devices:
  - Bluetooth adapters

- COM and LPT ports
- IEEE 1394 interface
- Imaging devices
- Infrared devices
- Modems
- PCMCIA card
- Print screen key
- Wireless NICs

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

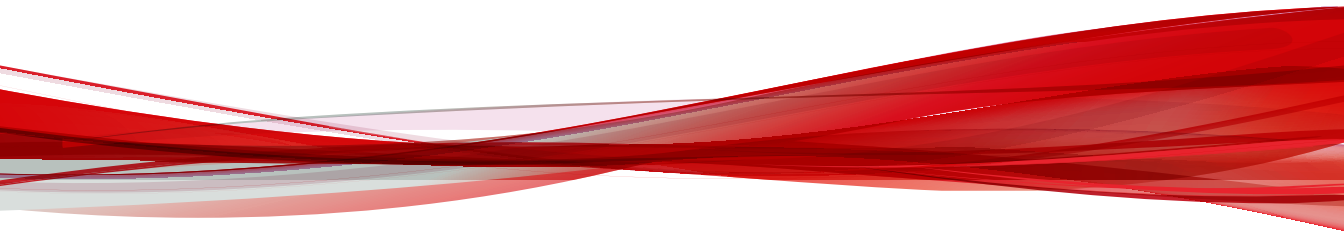
Uninstalling Data Protection from Plug-in Manager

Procedure

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

Part II

Protecting Security Agents



Chapter 4

Using Trend Micro Smart Protection

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

Topics include:

About Trend Micro Smart Protection

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

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

The Need for a New Solution

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

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

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

Smart Protection Services

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

Smart protection services include:

- **File Reputation Services**: File Reputation Services off-loads a large number of anti-malware signatures that were previously stored on agent computers to smart protection sources.

  For details, see *File Reputation Services on page 4-3*.

- **Web Reputation Services**: Web Reputation Services allows local smart protection sources to host URL reputation data that were previously hosted solely by Trend Micro. Both technologies ensure smaller bandwidth consumption when updating patterns or checking a URL's validity.

  For details, see *Web Reputation Services on page 4-4*.

- **Smart Feedback**: Trend Micro continues to harvest information anonymously sent from Trend Micro products worldwide to proactively determine each new threat.

  For details, see *Smart Feedback on page 4-4*.

File Reputation Services

File Reputation Services checks the reputation of each file against an extensive in-the-cloud database. Since the malware information is stored in

the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-agent architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall agent footprint.

Agents must be in smart scan mode to use File Reputation Services. These agents are referred to as smart scan agents in this document. Agents that are not in smart scan mode do not use File Reputation Services and are called conventional scan agents. Apex One administrators can configure all or several agents to be in smart scan mode.

Web Reputation Services

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

Security Agents subject to web reputation policies use Web Reputation Services. Apex One administrators can subject all or several agents to web reputation policies.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and its 24/7 threat research centers and technologies. Each new threat identified through every single customer's routine

reputation check automatically updates all Trend Micro threat databases, blocking any subsequent customer encounters of a given threat.

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

Samples of information sent to Trend Micro:

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

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

Tip

You do not need to participate in Smart Feedback to protect your 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

Smart Protection Sources

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

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

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

The smart protection source to which the agent connects depends on the agent location. Agents can connect to either Trend Micro Smart Protection Network or Smart Protection Server.

Trend Micro™ Smart Protection Network™

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

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Smart Protection Server

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

There are two types of Smart Protection Servers:

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

Smart Protection Sources Compared

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

TABLE 4-1. Smart Protection Sources Compared

BASIS OF COMPARISON	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Availability	Available for internal agents, which are agents that meet the location criteria specified on the Apex One web console	Available mainly for external agents, which are agents that do not meet the location criteria specified on the Apex One web console

Basis of Comparison	Smart Protection Server	Trend Micro Smart Protection Network
Purpose	Designed and intended to localize smart protection services to the corporate network to optimize efficiency	A globally scaled, Internet-based infrastructure that provides smart protection services to agents who do not have immediate access to their corporate network
Administration	Apex One administrators install and manage these smart protection sources	Trend Micro maintains this source
Pattern update source	Trend Micro ActiveUpdate server	Trend Micro ActiveUpdate server
Agent connection protocols	HTTP and HTTPS	HTTPS

Smart Protection Pattern Files

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

Smart Scan Agent Pattern

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

Note

Smart scan agents are Security Agents that administrators have configured to use File Reputation Services. Agents that do not use File Reputation Services are called conventional scan agents.

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

Smart Scan Pattern

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

Web Blocking List

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

Note

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

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

Smart Protection Pattern Update Process

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

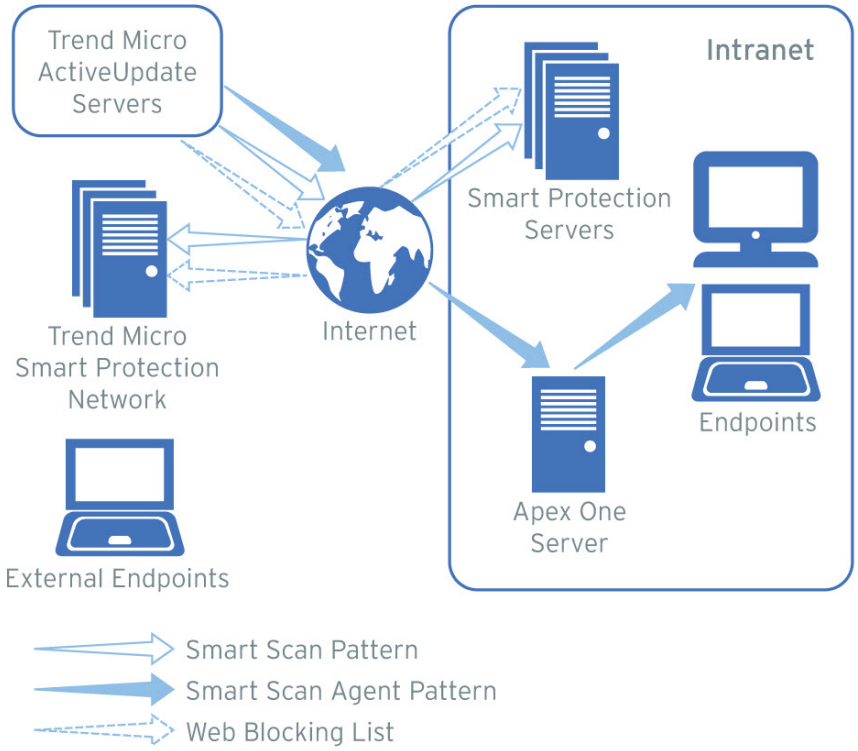


FIGURE 4-1. Pattern update process

Usage of Smart Protection Patterns

The Security Agent uses the Smart Scan Agent Pattern to scan for security risks and only queries the Smart Scan Pattern if the Smart Scan Agent

Pattern cannot determine the risk of a file. The agent queries the Web Blocking List when a user attempts to access a website. Advanced filtering technology enables the agent to "cache" the query results. This eliminates the need to send the same query more than once.

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

Tip

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

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

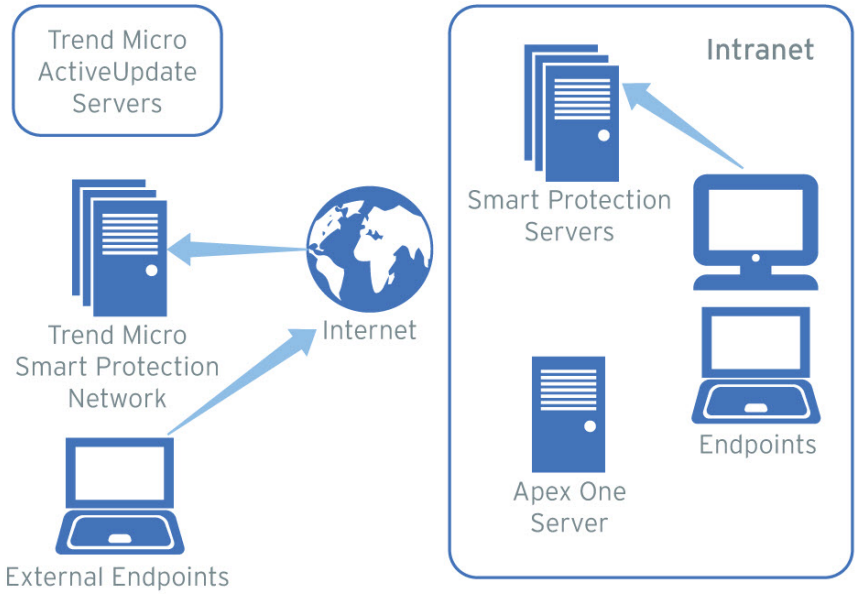


FIGURE 4-2. Query process

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

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

TABLE 4-2. Protection Behaviors Based on Location

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

Setting Up Smart Protection Services

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

- *Smart Protection Server Installation on page 4-14*
- *Integrated Smart Protection Server Management on page 4-19*
- *Smart Protection Source List on page 4-23*
- *Agent Connection Proxy Settings on page 4-30*

- *Endpoint Location Settings on page 4-31*
- *Trend Micro Network VirusWall Installations on page 4-31*

Smart Protection Server Installation

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

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

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

Standalone Smart Protection Server Installation

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

Integrated Smart Protection Server Installation

If you installed the integrated server during Apex One server installation:

- Enable the integrated server and configure settings for the server. For details, see *Integrated Smart Protection Server Management on page 4-19*.
- If the integrated server and Security Agent exist on the same server computer, consider disabling the Apex One firewall. The Apex One firewall is intended for agent endpoint use and may affect performance when enabled on servers. For instructions on disabling the firewall, see *Enabling or Disabling the Apex One Firewall on page 13-6*.

Note

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

Tip

Install the integrated Smart Protection Server after completing the Apex One installation by using the *Integrated Smart Protection Server Tool on page 4-15*.

Integrated Smart Protection Server Tool

The Trend Micro Integrated Smart Protection Tool helps administrators to install or uninstall an Integrated Smart Protection Server after the Apex One server installation is completed. The Apex One web console does not permit administrators to install/remove an Integrated Smart Protection Server once the Apex One server installation is complete.

Procedure

1. Open a command prompt and go to the <*Server installation folder*>`\PCCSRV\Admin\Utility\ISPSInstaller` directory where `ISPSInstaller.exe` is located.
2. Run `ISPSInstaller.exe` using one of the following commands:

TABLE 4-3. Installer Options

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

Command	Description
`ISPSInstaller.exe /i /f:[port number] /s:[port number] /w:[port number]`	Installs the integrated Smart Protection Server using the ports specified. **Note** You can only configure the ports when using an Apache web server. Where: • `/f:[port number]` represents the HTTP file reputation port • `/s:[port number]` represents the HTTPS file reputation port • `/w:[port number]` represents the web reputation port **Note** An unspecified port is automatically assigned the default value.
`ISPSInstaller.exe /u`	Uninstalls the integrated Smart Protection Server

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

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

Web Server and Settings	Ports for File Reputation Services		HTTP Port for Web Reputation Services
	HTTP	HTTPS (SSL)	
IIS virtual website with SSL disabled	8080	4343 (configurable)	8080 (configurable)

3. After the installation completes, open the Apex One web console and verify the following:

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

Smart Protection Server Best Practices

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

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

Customizing ptngrowth.ini for the Standalone Server

Procedure

1. Open the `ptngrowth.ini` file in `/var/tmcss/conf/`.
2. Modify the `ptngrowth.ini` file using the recommended values below:
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Save the `ptngrowth.ini` file.
4. Restart the `lighttpd` service by typing the following command from the Command Line Interface (CLI):
   - `service lighttpd restart`

Customizing ptngrowth.ini for the Integrated Server

Procedure

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

4. Restart the `Trend Micro Smart Protection Server` service.

Integrated Smart Protection Server Management

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

- Enabling the integrated server's File Reputation Services and Web Reputation Services
- Recording the integrated server's addresses
- Updating the integrated server's components
- Configuring the integrated server's Approved/Blocked URL List

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-22*.

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

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

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

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

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-22*.

Recording the Integrated Server's Addresses

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

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

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

Tip

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

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-22*.

Updating the Integrated Server's Components

The integrated server updates the following components:

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

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

Note

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

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-22*.

Integrated Server's Approved/Blocked URL List Configuration

Agents maintain their own approved/blocked URL list. Configure the list for agents when you set up web reputation policies (see *Web Reputation Policies on page 12-5* for details). Any URL in the agent's list will automatically be allowed or blocked.

The integrated server has its own approved/blocked URL list. If a URL is not in the agent's list, the agent sends a web reputation query to the integrated server (if the integrated server has been assigned as a smart protection source). If the URL is found in the integrated server's approved/blocked URL list, the integrated server notifies the agent to allow or block the URL.

Note

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

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

For details, see *Configuring Integrated Smart Protection Server Settings on page 4-22*.

Configuring Integrated Smart Protection Server Settings

Procedure

1. Go to **Administration** > **Smart Protection** > **Integrated Server**.
2. Select **Enable File Reputation Services**.
3. Select the protocol (HTTP or HTTPS) that agents will use when sending scan queries to the integrated server.
4. Select **Enable Web Reputation Services**.
5. Record the integrated server's addresses found under the **Server Address** column.
6. To update the integrated server's components:
   - View the current versions of the Smart Scan Pattern and Web Blocking List. If an update is available, click **Update Now**. The update result displays on top of the screen.
   - To update the pattern automatically:
     a. Select **Enable scheduled updates**.
     b. Choose whether to update hourly or every 15 minutes.
     c. Select an update source under **File Reputation Services**. The Smart Scan Pattern will be updated from this source.
     d. Select an update source under **Web Reputation Services**. The Web Blocking List will be updated from this source.

Note

- If you choose the ActiveUpdate server as the update source, ensure that the server has Internet connection and, if you are using a proxy server, test if Internet connection can be established using the proxy settings. See *Proxy for Apex One Server Updates on page 6-18* for details.
- If you choose a custom update source, set up the appropriate environment and update resources for this update source. Also ensure that there is a functional connection between the server computer and this update source. If you need assistance setting up an update source, contact your support provider.

7. To configure the integrated server's Approved/Blocked List:
   a. Click **Import** to populate the list with URLs from a pre-formatted `.csv` file. You can obtain the `.csv` file from a standalone Smart Protection Server.
   b. If you have an existing list, click **Export** to save the list to a `.csv` file.
8. Click **Save**.

Smart Protection Source List

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

IPv6 Support for Smart Protection Sources

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

- Trend Micro Smart Protection Network

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

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

Smart Protection Sources and Endpoint Location

The smart protection source to which the agent connects depends on the agent endpoint's location.

For details on configuring location settings, see *Endpoint Location on page 15-2*.

TABLE 4-5. Smart Protection Sources by Location

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

Configuring the Standard List of Smart Protection Sources

Procedure

1. Go to **Administration** > **Smart Protection** > **Smart Protection Sources**.

2. Click the **Internal Agents** tab.
3. Select **Use the standard list (for all internal agents)**.
4. Click the **standard list** link.

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

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

   Note

   Specify the host name if there are IPv4 and IPv6 agents connecting to the Smart Protection Server.
7. Select **File Reputation Services**. Agents send scan queries using the HTTP or HTTPS protocol. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

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

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

   Tip

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

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

   For the standalone server, open the standalone server's console and go to the **Summary** screen.
8. Select **Web Reputation Services**. Agents send web reputation queries using the HTTP protocol. HTTPS is not supported.

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

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

9. Click **Save**.

   The screen closes.

10. Add more servers by repeating the previous steps.

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

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

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 computer, assign a standalone Smart Protection Server as the primary smart protection source and the integrated server as a backup source.

12. Perform miscellaneous tasks on the screen.

    - If you have exported a list from another server and want to import it to this screen, click **Import** and locate the `.dat` file. The list loads on the screen.
    - To export the list to a `.dat` file, click **Export** and then click **Save**.
    - To refresh the service status of servers, click **Refresh**.
    - Click the server name to do one of the following:
      - To view or edit server information.
      - View the full server address for Web Reputation Services or File Reputation Services.

- To open the console of a Smart Protection Server, click **Launch console**.
  - For the integrated Smart Protection Server, the server's configuration screen displays.
  - For standalone Smart Protection Servers and the integrated Smart Protection Server of another Apex One server, the console logon screen displays.
- To delete an entry, select the check box for the server and click **Delete**.

13. Click **Save**.

    The screen closes.

14. Click **Notify All Agents**.

Configuring Custom Lists of Smart Protection Sources

Procedure

1. Go to **Administration** > **Smart Protection** > **Smart Protection Sources**.
2. Click the **Internal Agents** tab.
3. Select **Use custom lists based on agent IP address**.
4. (Optional) Select **Use the standard list when all servers on the custom lists are unavailable**.

   Tip

   Trend Micro recommends enabling this feature to ensure that agents can connect to a smart protection source if the custom sources become unavailable.

5. Click **Add**.

   A new screen opens.

6. In the **IP Range** section, specify an IPv4 or IPv6 address range, or both.

   Note

   Agents with an IPv4 address can connect to pure IPv4 or dual-stack Smart Protection Servers. Agents with an IPv6 address can connect to pure IPv6 or dual-stack Smart Protection Servers. Agents with both IPv4 and IPv6 addresses can connect to any Smart Protection Server.

7. In the **Proxy Setting** section, specify proxy settings agents will use to connect to the Smart Protection Servers.

   a. Select **Use a proxy server for agent and Smart Protection Server communication**.

   b. Specify the proxy server name or IPv4/IPv6 address, and port number.

   c. If the proxy server requires authentication, type the user name and password.

8. In the **Custom Smart Protection Server List**, add the Smart Protection Servers.

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

      Note

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

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

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

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

Tip

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

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

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

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

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

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

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

e. Add more servers by repeating the previous steps.

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

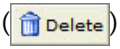
   - **Order**: Agents pick servers in the order in which they appear on the list. If you select **Order**, use the arrows under the **Order** column to move servers up and down the list.
   - **Random**: Agents pick servers randomly.

Tip

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

g. Perform miscellaneous tasks in the screen.

   - To refresh the service status of servers, click **Refresh**.

- To open the console of a Smart Protection Server, click **Launch console**.
  - For the integrated Smart Protection Server, the server's configuration screen displays.
  - For standalone Smart Protection Servers and the integrated Smart Protection Server of another Apex One server, the console logon screen displays.
- To delete an entry, click **Delete** (

).

9. Click **Save**.

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

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

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

12. Click **Notify All Agents**.

Agent Connection Proxy Settings

If connection to the Smart Protection Network requires proxy authentication, specify authentication credentials.

Configure internal proxy settings that agents use when connecting to a Smart Protection Server.

For more information, see *Security Agent Proxy Settings on page 15-50*.

Endpoint Location Settings

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

To configure location settings, see *Endpoint Location on page 15-2*.

Trend Micro Network VirusWall Installations

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

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

Using Smart Protection Services

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

Note

For instructions on setting up the smart protection environment, see *Setting Up Smart Protection Services on page 4-13*.

To benefit from protection provided by File Reputation Services, agents must use the scan method called smart scan. For details about smart scan and how to enable smart scan on agents, see *Scan Method Types on page 7-8*.

To allow Security Agents to use Web Reputation Services, configure web reputation policies. For details, see *Web Reputation Policies on page 12-5*.

Note

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

For instructions on configuring Smart Feedback, see *Smart Feedback on page 14-61*.

Chapter 5

Installing the Security Agent

This chapter describes Trend Micro Apex One system requirements and Security Agent installation procedures.

For details on upgrading the Security Agent, see the *Apex One Installation and Upgrade Guide*.

Topics include:

Security Agent Fresh Installations

The Security Agent can be installed on computers running Microsoft Windows platforms. Apex One is also compatible with various third-party products.

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

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

Installation Considerations

Before installing Security Agents, consider the following:

TABLE 5-1. Security Agent Installation Considerations

CONSIDERATION	DESCRIPTION
Windows feature support	Some Security Agent features are not available on certain Windows platforms.
IPv6 support	The Security Agent can be installed on dual-stack or pure IPv6 endpoints. However: • Some of the Windows operating systems to which the Security Agent can be installed do not support IPv6 addressing. • For some of the installation methods, there are special requirements to install the Security Agent successfully.
Security Agent IP addresses	For Security Agents with both IPv4 and IPv6 addresses, you can choose which IP address will be used when the Security Agent registers to the server.

Consideration	Description
Exception lists	Ensure that exception lists for the following features have been configured properly: • **Behavior Monitoring**: Add critical endpoint applications to the Approved Programs list to prevent the Security Agent from blocking these applications. For more information, see *Behavior Monitoring Exception List on page 9-9*. • **Web Reputation**: Add websites that you consider safe to the Approved URL List to prevent the Security Agent from blocking access to the websites. For more information, see *Web Reputation Policies on page 12-5*.

Security Agent Features

The Security Agent features available on the endpoint depend on the operating system.

Table 5-2. Security Agent Features on Server Platforms

Feature	Windows Operating System			
	Server 2008 R2/ Server Core 2008 R2	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016	Server 2019/ Server Core 2019
Manual Scan, Real-time Scan, and Scheduled Scan	Yes	Yes	Yes	Yes
Component update (manual and scheduled update)	Yes	Yes	Yes	Yes
Update Agent	Yes	Yes	Yes	Yes

Feature	Windows Operating System			
	Server 2008 R2/ Server Core 2008 R2	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016	Server 2019/ Server Core 2019
Web Reputation	Yes but disabled by default during server installation	Yes but disabled by default during server installation	Yes but disabled by default during server installation	Yes but disabled by default during server installation
Damage Cleanup Services	Yes	Yes	Yes	Yes
Apex One Firewall	Yes but disabled by default during server installation	Yes but disabled by default during server installation	Yes but disabled by default during server installation	Yes but disabled by default during server installation
Behavior Monitoring	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default
Agent Self-protection for: • Registry keys • Processes	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default
Agent Self-protection for: • Services • File protection	Yes	Yes	Yes	Yes
Device Control (Unauthorized Change Prevention service)	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default

Feature	Windows Operating System			
	Server 2008 R2/ Server Core 2008 R2	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016	Server 2019/ Server Core 2019
Data Protection (including Data Protection for Device Control)	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default	Yes (64-bit) but disabled by default
Suspicious Connection settings	Yes	Yes	Yes	Yes
Sample submission	Yes	Yes	Yes	Yes
POP3 mail scan	Yes	Yes	Yes	Yes
Predictive Machine Learning	Yes	Yes	Yes	Yes
Agent Plug-in Manager	Yes	Yes	Yes	Yes
Independent mode	Yes (Server) No (Server Core)	Yes	Yes	Yes
Smart Feedback	Yes	Yes	Yes	Yes

Table 5-3. Security Agent Features on Desktop Platforms

Feature	Windows Operating System		
	Windows 7	Windows 8.1	Windows 10
Manual Scan, Real-time Scan, and Scheduled Scan	Yes	Yes	Yes
Component update (manual and scheduled update)	Yes	Yes	Yes

Feature	Windows Operating System		
	Windows 7	Windows 8.1	Windows 10
Update Agent	Yes	Yes	Yes
Web Reputation	Yes	Yes but only limited support for Windows UI mode	Yes
Damage Cleanup Services	Yes	Yes	Yes
Apex One Firewall	Yes	Yes	Yes
Behavior Monitoring	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)
	Yes (64-bit)	Yes (64-bit)	Yes (64-bit)
Agent Self-protection for: • Registry keys • Processes	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)
	Yes (64-bit)	Yes (64-bit)	Yes (64-bit)
Agent Self-protection for: • Services • File protection	Yes	Yes	Yes
Device Control (Unauthorized Change Prevention service)	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)
	Yes (64-bit)	Yes (64-bit)	Yes (64-bit)
Data Protection (including Data Protection for Device Control)	Yes (32-bit)	Yes (32-bit)	Yes (32-bit)
	Yes (64-bit)	Yes (64-bit) in desktop mode	Yes (64-bit)
Suspicious Connection settings	Yes	Yes	Yes
Sample submission	Yes	Yes	Yes
POP3 mail scan	Yes	Yes	Yes

Feature	Windows Operating System		
	Windows 7	Windows 8.1	Windows 10
Predictive Machine Learning	Yes	Yes	Yes
Agent Plug-in Manager	Yes	Yes	Yes
Independent mode	Yes	Yes	Yes
Smart Feedback	Yes	Yes	Yes

Security Agent Installation and IPv6 Support

This topic discusses considerations when installing the Security Agent to dual-stack or pure IPv6 endpoints.

Installation Methods

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

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

TABLE 5-4. Installation Methods and IPv6 Support

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

Agent IP Addresses

Apex One servers installed in an environment that supports IPv6 addressing can manage the following Security Agents:

- Apex One servers installed on pure IPv6 host machines can manage pure IPv6 agents.
- Apex One servers installed on dual-stack host machines and have been assigned both IPv4 and IPv6 addresses can manage pure IPv6, dual-stack, and pure IPv4 agents.

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

- Pure IPv6 agents register using their IPv6 address.
- Pure IPv4 agents register using their IPv4 address.

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

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

This setting is only available on dual-stack Apex One servers and is applied only by dual-stack agents.

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **Network** tab.
3. Go to the **Preferred IP Address** section.
4. Choose from the following options:
   - **IPv4 only**: Agents use their IPv4 address.
   - **IPv4 first, then IPv6**: Agents use their IPv4 address first. If the agent cannot register using its IPv4 address, it uses its IPv6 address. If registration is unsuccessful using both IP addresses, the agent retries using the IP address priority for this selection.
   - **IPv6 first, then IPv4**: Agents use their IPv6 address first. If the agent cannot register using its IPv6 address, it uses its IPv4 address. If registration is unsuccessful using both IP addresses, the agent retries using the IP address priority for this selection.
5. Click **Save**.

Deployment Considerations

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

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

TABLE 5-5. Deployment Considerations for Installation

Installation Method/ Operating System Support	Deployment Considerations					
	WAN Deployment	Centrally Managed	Requires User Intervention	Requires IT Resource	Mass deployment	Bandwidth Consumed
Web install page Not supported on Windows Server Core platforms	No	No	Yes	No	No	High
Email Link installation Not supported on Windows Server Core platforms	No	No	Yes	Yes	No	High, if installations start at the same time
UNC-based installations Supported on all operating systems	No	No	Yes	Yes	No	High, if installations start at the same time
Remote installations Supported on all operating systems except: • Windows 7 Home Basic/ Home Premium • Windows 8.1 (basic versions) • Windows 10 Home Edition	No	Yes	No	Yes	No	High

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

Installation Method/ Operating System Support	Deployment Considerations					
	WAN Deployment	Centrally Managed	Requires User Intervention	Requires IT Resource	Mass deployment	Bandwidth Consumed
Trend Micro Vulnerability Scanner (TMVS) Supported on all operating systems except: • Windows 8.1 (basic versions) • Windows 10 Home Edition	No	Yes	No	Yes	No	High
Security Compliance installations Supported on all operating systems except: • Windows 7 Home Basic/ Home Premium • Windows 8.1 (basic versions) • Windows 10 Home Edition	No	Yes	No	Yes	No	High

Installing from the Web Install Page

Procedure

1. Open a supported web browser window and type the following:

   `https://<Apex One server name>:<port>/officescan`

2. Click the **installer** link on the logon page to download the 32-bit or 64-bit MSI package (depending on your operating system).

3. After the installation completes, the Security Agent icon appears in the Windows system tray.

Note

For a list of icons that display on the system tray, see *Security Agent Icons on page 15-28*.

Email Link Installation

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

Before you install Security Agents:

- Check the Security Agent installation requirements.
- Identify which computers on the network currently do not have protection against security risks. Perform the following tasks:
  - Run the \Trend Micro Vulnerability Scanner. This tool analyzes endpoints for installed antivirus software based on an IP address range you specify.

    For more information, see *Vulnerability Scanner Usage on page 5-32*.
  - Run Security Compliance.

    For more information, see *Security Compliance for Unmanaged Endpoints on page 15-71*.

Sending an Email Link

If you are installing to a pure IPv6 agent, the server must be dual-stack or pure IPv6 and its host name or IPv6 address must be part of the URL.

For dual-stack agents, the IPv6 address that displays in the installation status screen depends on the option selected in the **Preferred IP Address** section of **Agents** > **Global Agent Settings** on the **Network** tab.

For more information, see *Agent IP Addresses on page 5-8*.

Procedure

1. Go to **Agents** > **Agent Installation** > **Email Link**.
2. Modify the subject line of the email message if necessary.
3. Click **Create Email.**

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

Performing a UNC-based Installation

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

Procedure

1. Go to **Agents** > **Agent Installation** > **UNC-based**.
   - To install the Security Agent to an unprotected endpoint using `AutoPcc.exe`:
     a. Connect to the server computer. Go to the UNC path:

        ```
        \\<server computer name>\ofcscan
        ```

     b. Right-click `AutoPcc.exe` and select **Run as administrator**.
   - For remote desktop installations using `AutoPcc.exe`:

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

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

Installing Remotely from the Apex One Web Console

Install the Security Agent remotely to one or several endpoints connected to the network. Ensure you have administrator rights to the target endpoints to perform remote installation. Remote installation does not install the Security Agent on endpoints already running the Apex One server.

Note

This installation method cannot be used on endpoints running Windows 7 Home Basic and Home Premium Editions (32-bit and 64-bit versions), Windows 8.1 (32-bit and 64-bit basic versions), or Windows 10 Home Edition. A pure IPv6 server cannot install the Security Agent on pure IPv4 agents. Similarly, a pure IPv4 server cannot install the Security Agent on pure IPv6 agents.

Procedure

1. Perform the following pre-installation tasks.

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

   b. Go to **Start** > **Programs** > **Administrative Tools** > **Windows Firewall with Advanced Security**.

   c. Enable **File and Printer Sharing** rules for "Domain", "Private", and/or "Public" depending on your network environment.

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

2. On the web console, go to **Agents** > **Agent Installation** > **Remote**.
3. Select the target endpoints.
   - The **Domains and Endpoints** list displays all the Windows domains on the network. To display endpoints under a domain, double-click the domain name. Select any endpoint, and then click **Add**.
   - If you have a specific endpoint name in mind, type the endpoint name in the **Search for endpoints** field on top of the page and press ENTER.

   Apex One prompts you for the target endpoint user name and password. Use an administrator account user name and password to continue.
4. Type the user name and password, and then click **Log in**.

   The target endpoint appears in the **Selected Endpoints** table.
5. Repeat steps 3 and 4 to add more endpoints.
6. Click **Install** when you are ready to install the Security Agent to target endpoints.

   A confirmation box appears.
7. Click **Yes** to confirm that you want to install the Security Agent to the target endpoints.

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

When Apex One completes the installation to a target endpoint, the endpoint name disappears in the **Selected Endpoints** list and appears in the **Domains and Endpoints** list with a red check mark.

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

Note

If you install to multiple endpoints, Apex One records any unsuccessful installation in the logs (for details, see *Fresh Installation Logs on page 18-14*), but it will not postpone the other installations. You do not have to supervise the installation after you click **Install**. Check the logs later to see the installation results.

Installing with Login Script Setup

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

`AutoPcc.exe` installs the Security Agent to unmanaged endpoints and updates program files and components. Endpoints must be part of the domain to be able to use AutoPcc through the login script.

Security Agent Installation

`AutoPcc.exe` does not automatically install the Security Agent to endpoints. Users need to connect to the server computer, go to `\\<server computer name>\ofcscan`, right-click `AutoPcc.exe`, and select **Run as administrator**.

For remote desktop installation using `AutoPcc.exe`:

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

Program and Component Updates

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

Windows Server Scripts

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

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

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

Where:

- `<Server_name>` is the endpoint name or IP address of the Apex One server computer.
- "`ofcscan`" is the Apex One shared folder name on the server.
- "`autopcc`" is the link to the autopcc executable file that installs the Security Agent.

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

- `Windows Server 2012: \\Windows 2012 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2016: \\Windows 2016 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2019 \\Windows 2019 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

9. Click **OK**.

   Login Script Setup returns to its initial screen.

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

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

Installing with Agent Packager

Agent Packager creates an installation package that you can send to users using conventional media such as CD-ROM. Users run the package on the agent endpoint to install or upgrade the Security Agent and update components.

Agent Packager is especially useful when deploying the Security Agent or components to endpoints in low-bandwidth remote offices. Security Agents installed using Agent Packager report to the server where the package was created.

Agent Packager requires the following:

- 800MB free disk space
- Windows Installer 2.0 (to run an MSI package)

Package Deployment Guidelines

Send the package to users and ask them to run the Security Agent package on their endpoints.

Note

Send the package only to users whose Security Agent will report to the server where the package was created.

- For `EXE` packages, right-click the installer file and click **Run as administrator**.
- For `MSI` packages:
  1. Deploy the package by performing the following tasks
     - *Deploying an MSI Package Using Active Directory on page 5-25*
     - *Deploying an MSI Package Using Microsoft SMS on page 5-26*.
  2. Launch the MSI package from a command prompt window to install the Security Agent silently to a remote endpoint.

Scan Method Guidelines for Agent Packages

Select the scan method for the package. See *Scan Method Types on page 7-8* for details.

The components included in the package depend on the scan method you have selected. For details on the components available for each scan method, see *Security Agent Updates on page 6-27*.

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

- If you will use the package to upgrade the agent to this Apex One version, check the domain level scan method on the web console. On the console, go to **Agents** > **Agent Management**, select the agent tree domain to which the agent belongs, and click **Settings** > **Scan Settings** > **Scan Methods**. The domain level scan method should be consistent with the scan method for the package.
- If you will use the package to perform a fresh installation of the Security Agent, check the agent grouping setting. On the web console, go to **Agents** > **Agent Grouping**.
- If the agent grouping is by NetBIOS, Active Directory, or DNS domain, check the domain to which the target endpoint belongs. If the domain exists, check the scan method configured for the domain. If the domain does not exist, check the root level scan method (select the root domain icon () in the agent tree and click **Settings** > **Scan Settings** > **Scan Methods**). The domain or root level scan method should be consistent with the scan method for the package.

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

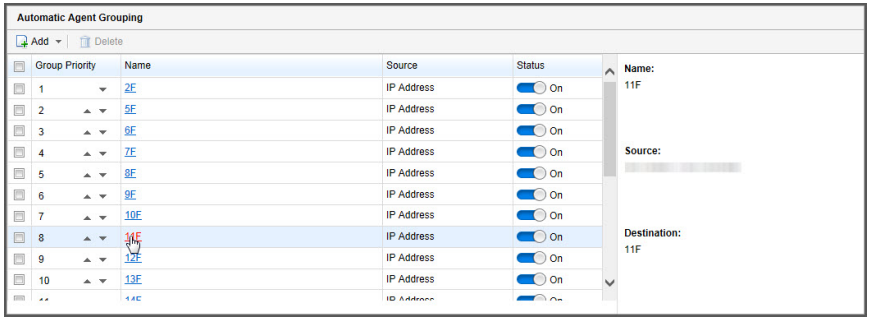


FIGURE 5-1. Automatic Agent Grouping preview pane

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

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

Creating an Installation Package Using Agent Packager

Procedure

1. On the Apex One server computer, browse to <*Server installation folder*>`\PCCSRV\Admin\Utility\ClientPackager`.
2. Double-click `ClnPack.exe` to run the tool.

   The **Agent Packager** console opens.
3. Select the type of package you want to create.

TABLE 5-6. Agent Package Types

PACKAGE TYPE	DESCRIPTION
Setup	Select **Setup** to create the package as an executable file. The package installs the Security Agent program with the components currently available on the server. If the target endpoint has an earlier agent version installed, running the executable file upgrades the agent.
Update	Select **Update** to create a package that contains the components currently available on the server. The package will be created as an executable file. Use this package if there are issues updating components on any agent endpoint.
MSI	Select **MSI** to create a package that conforms to the Microsoft Installer Package format. The package also installs the Security Agent program with the components currently available on the server. If the target endpoint has an earlier agent version installed, running the MSI file upgrades the agent.

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

5. Select the scan method that the agent package deploys.

   For guidelines regarding how to select a scan method, see *Scan Method Guidelines for Agent Packages on page 5-20*.

6. Under **Domain**, select one of the following:

   - **Allow the agent to report its domain automatically**: After installing the Security Agent, the agent queries the Apex One server database and reports its domain settings to the server.
   - Any domain in the list: Agent Packager synchronizes with the Apex One server and lists the domains currently used in the agent tree.

7. Under **Options**, select from the following:

Option	Description
Silent mode	This option creates a package that installs on the agent endpoint in the background, unnoticeable to the agent and without showing an installation status window. Enable this option if you plan to deploy the package remotely to the target endpoint.
Force overwrite with latest version	This option overwrites component versions on the agent with the versions currently available on the server. Enable this option to ensure that components on the server and agent are synchronized.
Disable Prescan (fresh installations only)	If the target endpoint does not have the Security Agent installed, the package first scans the endpoint for security risks before installing the Security Agent. If you are certain that the target endpoint is not infected with security risks, disable prescan. If prescan is enabled, Setup scans for virus/malware in the most vulnerable areas of the endpoint, which include the following: • Boot area and boot directory (for boot viruses) • Windows folder • Program files folder

8. Under **Update Agent Capabilities**, select which features the Update Agent can deploy.

9. Under **Components**, select the components and features to include in the package.

   - For details about components, see *Apex One Components and Programs on page 6-2*.
   - The Data Protection module is only available if you install and activate Data Protection. For details about Data Protection, see *Getting Started with Data Protection on page 3-1*.

10. Next to **Source file**, ensure that the location of the `ofcscan.ini` file is correct. To modify the path, click (...) to browse for the `ofcscan.ini` file.

    By default, this file is in the `<Server installation folder>\PCCSRV` folder of the Apex One server.

11. In **Output file**, click (...), specify where you want to create the Security Agent package, and type the package file name (for example, `AgentSetup.exe`).

12. Click **Create**.

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

13. Deploy the package.

Deploying an MSI Package Using Active Directory

Take advantage of Active Directory features to deploy the MSI package simultaneously to multiple Security Agent endpoints.

For instructions on creating an MSI file, see *Installing with Agent Packager on page 5-19*.

Procedure

1. Perform the following:

   - For Windows Server 2008 R2:

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

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

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

   - For Windows Server 2012 or later:

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

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

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

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

Tip

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

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

4. Locate and select the MSI package.

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

   - **Assigned**: The MSI package is automatically deployed the next time a user logs on to the endpoint (if you selected User Configuration) or when the endpoint restarts (if you selected Computer Configuration). This method does not require any user intervention.
   - **Published**: To run the MSI package, inform users to go to Control Panel, open the Add/Remove Programs screen, and select the option to add/install programs on the network. When the Security Agent MSI package displays, users can proceed to install the Security Agent.

Deploying an MSI Package Using Microsoft SMS

Deploy the MSI package using Microsoft System Management Server (SMS) if you have Microsoft BackOffice SMS installed on the server.

For instructions on creating an MSI file, see *Installing with Agent Packager on page 5-19*.

The SMS server needs to obtain the MSI file from the Apex One server before it can deploy the package to target endpoints.

- Local: The SMS server and the Apex One server are on the same endpoint.
- Remote: The SMS server and the Apex One server are on different endpoints.

Known issues when installing with Microsoft SMS:

- "Unknown" appears in the **Run Time** column of the SMS console.
- If the installation was unsuccessful, the installation status may still show that the installation is complete on the SMS program monitor.

  For instructions on how to check if the installation was successful, see *Post-installation on page 5-59*.

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

Obtaining the Package Locally

Procedure

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

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

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

   The **Open** screen appears.

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

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

7. Click **Next**.

   The **Source Files** screen appears.

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

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

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

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

11. Click **Next**.

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

Obtaining the Package Remotely

Procedure

1. On the Apex One server, use Agent Packager to create a Setup package with an `EXE` extension (you cannot create an `MSI` package). See *Installing with Agent Packager on page 5-19* for details.

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

3. Open the SMS Administrator console.

4. On the **Tree** tab, click **Packages**.

5. On the **Action** menu, click **New** > **Package From Definition**.

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

6. Click **Next**.

   The **Package Definition** screen appears.

7. Click **Browse**.

   The **Open** screen appears.

8. Browse for the MSI package file. The file is on the shared folder you created.

9. Click **Next**.

   The **Source Files** screen appears.

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

    The **Source Directory** screen appears.

11. Click **Network path (UNC name)**.

12. Click **Browse** and select the source directory containing the MSI file (the shared folder you created).

13. Click **Next**.

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

Distributing the Package to Target Endpoints

Procedure

1. On the **Tree** tab, click **Advertisements**.

2. On the **Action** menu, click **All Tasks** > **Distribute Software**.

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

3. Click **Next**.

   The **Package** screen appears.

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

5. Click **Next**.

   The **Distribution Points** screen appears.

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

   The **Advertise a Program** screen appears.

7. Click **Yes** to advertise the Security Agent Setup package, and then click **Next**.

   The **Advertisement Target** screen appears.

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

   The **Browse Collection** screen appears.

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

10. Click **OK**.

    The **Advertisement Target** screen appears again.

11. Click **Next**.

    The **Advertisement Name** screen appears.

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

    The **Advertise to Subcollections** screen appears.

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

14. Click **Next**.

    The **Advertisement Schedule** screen appears.

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

    Note

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

16. Click **Next**.

    The **Assign Program** screen appears.

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

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

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

Installations Using Agent Disk Images

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

Each Security Agent installation needs a Globally Unique Identifier (GUID) so that the server can identify agents individually. Use the Apex One program called `ImgSetup.exe` to create a different GUID for each of the clones.

Creating a Disk Image of the Security Agent

Procedure

1. Install the Security Agent on the endpoint.
2. Copy `ImgSetup.exe` from <*Server installation folder*>`\PCCSRV\Admin\Utility\ImgSetup` to this endpoint.
3. Run `ImgSetup.exe` on this endpoint.

   This creates a `RUN` registry key under `HKEY_LOCAL_MACHINE`.
4. Create a disk image of the Security Agent using the disk imaging software.
5. Restart the clone.

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

WARNING!

To avoid having two computers with the same name in the Apex One database, manually change the endpoint name or domain name of the cloned Security Agent.

Vulnerability Scanner Usage

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

Considerations When Using Vulnerability Scanner

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

Network Administration

TABLE 5-7. Network Administration

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

Network Topology and Architecture

TABLE 5-8. Network Topology and Architecture

SETUP	EFFECTIVENESS OF VULNERABILITY SCANNER
Single location	Very effective. Vulnerability Scanner allows you to scan an entire IP segment and install the Security Agent easily on the LAN.

Setup	Effectiveness of Vulnerability Scanner
Multiple locations with high speed connection	Moderately effective
Multiple locations with low speed connection	Not effective. You need to run Vulnerability Scanner on each location and Security Agent installation must be directed to a local Apex One server.
Remote and isolated computers	Moderately effective

Software/Hardware Specifications

Table 5-9. Software/Hardware Specifications

Setup	Effectiveness of Vulnerability Scanner
Windows NT-based operating systems	Very effective. Vulnerability Scanner can easily install the Security Agent remotely to computers running NT-based operating systems.
Mixed operating systems	Moderately effective. Vulnerability Scanner can only install to computers running Windows NT-based operating systems.
Desktop management software	Not effective. Vulnerability Scanner cannot be used with desktop management software. However, it can help track the progress of the Security Agent installation.

Domain Structure

Table 5-10. Domain Structure

Setup	Effectiveness of Vulnerability Scanner
Microsoft Active Directory	Very effective. Specify the domain administrator account in Vulnerability Scanner to allow remote installation of the Security Agent.
Workgroup	Not effective. Vulnerability Scanner may have difficulty installing to computers using different administrative accounts and passwords.

Setup	Effectiveness of Vulnerability Scanner
Novell™ Directory Service	Not effective. Vulnerability Scanner requires a Windows Domain account to install the Security Agent.
Peer-to-peer	Not effective. Vulnerability Scanner may have difficulty installing to computers using different administrative accounts and passwords.

Network Traffic

Table 5-11. Network Traffic

Setup	Effectiveness of Vulnerability Scanner
LAN connection	Very effective
512 Kbps	Moderately effective
T1 connection and higher	Moderately effective
Dialup	Not effective. It will take a long time to finish installing the Security Agent.

Network Size

Table 5-12. Network Size

Setup	Effectiveness of Vulnerability Scanner
Very large enterprise	Very effective. The bigger the network, the more Vulnerability Scanner is needed for checking Security Agent installations.
Small and medium business	Moderately effective. For small networks, Vulnerability Scanner can be an option to install the Security Agent. Other Security Agent installation methods may prove much easier to implement.

Guidelines When Installing the Security Agent Using Vulnerability Scanner

Vulnerability Scanner will not install the Security Agent if:

- The Apex One server or another security software is installed on the target host machine.
- The remote endpoint runs Windows 7 SP1 Home Basic, Windows 7 SP1 Home Premium, Windows 8.1 (basic versions), or Windows 10 Home.

Note

You can install the Security Agent to the target host machine using the other installation methods discussed in *Deployment Considerations on page 5-9*.

Before using Vulnerability Scanner to install the Security Agent, perform the following steps:

- For Windows 7 SP1 (Professional, Enterprise, Ultimate Edition), Windows 8.1 (Pro, Enterprise), Windows 10 (Pro, Education, Enterprise), or any supported Windows Server (all editions):

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

Vulnerability Scan Methods

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

Method	Details
Manual vulnerability scan	Administrators can run vulnerability scans on demand.
Scheduled vulnerability scan	Vulnerability scans automatically run according to the schedule configured by administrators.

After Vulnerability Scanner runs, it displays the status of the Security Agent on the target host machines. The status can be any of the following:

- **Normal**: The Security Agent is up and running and is working properly
- **Abnormal**: The Security Agent services are not running or the Security Agent does not have real-time protection
- **Not installed**: The TMListen service is missing or the Security Agent has not been installed
- **Unreachable**: Vulnerability Scanner was unable to establish connection with the host machine and determine the status of the Security Agent

Running a Manual Vulnerability Scan

Procedure

1. To run a vulnerability scan on the Apex One server computer, navigate to <Server installation folder>`\PCCSRV\Admin\Utility\TMVS` and double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears. To run vulnerability scan on another endpoint:

   a. On the Apex One server computer, go to `<Server installation folder>\PCCSRV\Admin\Utility`.

   b. Copy the `TMVS` folder to the other endpoint.

c. On the other endpoint, open the `TMVS` folder and then double-click `TMVS.exe`.

The **Trend Micro Vulnerability Scanner** console appears.

Note

You cannot launch the tool from Terminal Server.

2. Go to the **Manual Scan** section.
3. Type the IP address range of the endpoints you want to check.
   a. Type an IPv4 address range.

Note

Vulnerability Scanner can only query an IPv4 address range if it runs on a pure IPv4 or dual-stack host machine. Vulnerability Scanner only supports a class B IP address range, for example, `168.212.1.1` to `168.212.254.254`.

   b. For an IPv6 address range, type the IPv6 prefix and length.

Note

Vulnerability Scanner can only query an IPv6 address range if it runs on a pure IPv6 or dual-stack host machine.

4. Click **Settings**.

   The **Settings** screen appears.
5. Configure the following settings:

Option	Description
Ping settings	Vulnerability Scan can "ping" the IP addresses specified in the previous step to check if they are currently in use. If a target host machine is using an IP address, Vulnerability Scanner can determine the host machine's operating system.

Option	Description
	For details, see *Ping Settings on page 5-49*.
Method for retrieving computer descriptions	For host machines that respond to the "ping" command, Vulnerability Scanner can retrieve additional information about the host machines. For details, see *Method for Retrieving Endpoint Descriptions on page 5-46*.
Product query	Vulnerability Scanner can check for the presence of security software on the target host machines. For details, see *Product Query on page 5-43*.
Apex One server settings	Configure these settings if you want Vulnerability Scanner to automatically install Security Agent to unprotected host machines. These settings identify the parent server and the administrative credentials used by the Security Agent to log on to the host machines. For details, see *Apex One Server Settings on page 5-51*. **Note** Certain conditions may prevent the installation of the Security Agent to the target host machines. For details, see *Guidelines When Installing the Security Agent Using Vulnerability Scanner on page 5-36*.
Notifications	Vulnerability Scanner can send the vulnerability scan results to Apex One administrators. It can also display notifications on unprotected host machines. For details, see *Notifications on page 5-47*.
Save results	In addition to sending the vulnerability scan results to administrators, Vulnerability Scan can also save the results to a `.csv` file. For details, see *Vulnerability Scan Results on page 5-49*.

6. Click **OK**.
7. Click **Start**.

The vulnerability scan results appear in the **Results** table under the **Manual Scan** tab.

8. To save the results to a comma-separated value (CSV) file, click **Export**, locate the folder where you want to save the file, type the file name, and click **Save**.

Configuring a Scheduled Vulnerability Scan

Procedure

1. To run a vulnerability scan on the Apex One server computer, navigate to <Server installation folder>\PCCSRV\Admin\Utility\TMVS and double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears. To run vulnerability scan on another endpoint:

   a. On the Apex One server computer, go to `<Server installation folder>\PCCSRV\Admin\Utility`.

   b. Copy the `TMVS` folder to the other endpoint.

   c. On the other endpoint, open the `TMVS` folder and then double-click `TMVS.exe`.

   The **Trend Micro Vulnerability Scanner** console appears.

   Note

   You cannot launch the tool from Terminal Server.

2. Go to the **Scheduled Scan** section.

3. Click **Add/Edit**.

   The **Scheduled Scan** screen appears.

4. Type a name for the scheduled vulnerability scan.

5. Type the IP address range of the endpoints you want to check.

a. Type an IPv4 address range.

Note

Vulnerability Scanner can only query an IPv4 address range if it runs on a pure IPv4 or dual-stack host machine. Vulnerability Scanner only supports a class B IP address range, for example, `168.212.1.1` to `168.212.254.254`.

b. For an IPv6 address range, type the IPv6 prefix and length.

Note

Vulnerability Scanner can only query an IPv6 address range if it runs on a pure IPv6 or dual-stack host machine.

6. Specify the start time for the **Schedule** using the 24-hour clock format and then select how often the scan will run. Choose from daily, weekly, or monthly.

7. Select which set of vulnerability scan settings to use.

   a. Select **Use current settings** if you have configured and want to use manual vulnerability scan settings.

      For details about manual vulnerability scan settings, see *Running a Manual Vulnerability Scan on page 5-37*.

   b. If you did not specify manual vulnerability scan settings or if you want to use another set of settings, select **Modify settings** and then click **Settings**.

      The **Settings** screen appears.

   c. Configure the following settings:

Ping settings	Vulnerability Scan can "ping" the IP addresses specified in the previous step to check if they are currently in use. If a target host machine is using an IP address, Vulnerability Scanner can determine the host machine's operating system. For details, see *Ping Settings on page 5-49*.

Method for retrieving computer descriptions	For host machines that respond to the "ping" command, Vulnerability Scanner can retrieve additional information about the host machines. For details, see *Method for Retrieving Endpoint Descriptions on page 5-46*.
Product query	Vulnerability Scanner can check for the presence of security software on the target host machines. For details, see *Product Query on page 5-43*.
Apex One server settings	Configure these settings if you want Vulnerability Scanner to automatically install Security Agent to unprotected host machines. These settings identify the parent server and the administrative credentials used by the Security Agent to log on to the host machines. For details, see *Apex One Server Settings on page 5-51*. **Note** Certain conditions may prevent the installation of the Security Agent to the target host machines. For details, see *Guidelines When Installing the Security Agent Using Vulnerability Scanner on page 5-36*.
Notifications	Vulnerability Scanner can send the vulnerability scan results to Apex One administrators. It can also display notifications on unprotected host machines. For details, see *Notifications on page 5-47*.
Save results	In addition to sending the vulnerability scan results to administrators, Vulnerability Scan can also save the results to a `.csv` file. For details, see *Vulnerability Scan Results on page 5-49*.

8. Click **OK**.

   The **Scheduled Scan** screen closes. The scheduled vulnerability scan you created appears under the **Scheduled Scan** section. If you enabled notifications, Vulnerability Scanner sends you the scheduled vulnerability scan results.

9. To execute the scheduled vulnerability scan immediately, click **Run Now**.

   The vulnerability scan results appear in the **Results** table under the **Scheduled Scan** tab.

10. To save the results to a comma-separated value (CSV) file, click **Export**, locate the folder where you want to save the file, type the file name, and click **Save**.

Vulnerability Scan Settings

Vulnerability scan settings are configured from Trend Micro Vulnerability Scanner (`TMVS.exe`) or from the `TMVS.ini` file.

Note

See *Server Debug Logs Using LogServer.exe on page 18-3* for information on how to collect debug logs for Vulnerability Scanner.

Product Query

Vulnerability Scanner can check for the presence of security software on agents. The following table discusses how Vulnerability Scanner checks security products:

TABLE 5-13. Security Products Checked by Vulnerability Scanner

PRODUCT	DESCRIPTION
ServerProtect for Windows	Vulnerability Scanner uses RPC endpoint to check if `SPNTSVC.exe` is running. It returns information including operating system, and Virus Scan Engine, Virus Pattern and product versions. Vulnerability Scanner cannot detect the ServerProtect Information Server or the ServerProtect Management Console.

Product	Description
ServerProtect for Linux	If the target endpoint does not run Windows, Vulnerability Scanner checks if it has ServerProtect for Linux installed by trying to connect to port 14942.
Security Agent	Vulnerability Scanner uses the Security Agent port to check if the Security Agent is installed. It also checks if the `TmListen.exe` process is running. It retrieves the port number automatically if executed from its default location. If you launched Vulnerability Scanner on any endpoint other than the Apex One server, check and then use the other endpoint's communication port.
PortalProtect™	Vulnerability Scanner loads the web page `http://localhost:port/PortalProtect/index.html` to check for product installation.
ScanMail™ for Microsoft Exchange™	Vulnerability Scanner loads the web page `http://ipaddress:port/scanmail.html` to check for ScanMail installation. By default, ScanMail uses port 16372. If ScanMail uses a different port number, specify the port number. Otherwise, Vulnerability Scanner cannot detect ScanMail.
InterScan™ family	Vulnerability Scanner loads each web page for different products to check for product installation. • InterScan Messaging Security Suite 5.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x: `http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security™ (PC-cillin)	Vulnerability Scanner uses port 40116 to check if Trend Micro Internet Security is installed.
McAfee VirusScan ePolicy Orchestrator	Vulnerability Scanner sends a special token to TCP port 8081, the default port of ePolicy Orchestrator for providing connection between the server and agent. The endpoint with this antivirus product replies using a special token type. Vulnerability Scanner cannot detect the standalone McAfee VirusScan.

Product	Description
Norton Antivirus™ Corporate Edition	Vulnerability Scanner sends a special token to UDP port 2967, the default port of Norton Antivirus Corporate Edition RTVScan. The endpoint with this antivirus product replies using a special token type. Since Norton Antivirus Corporate Edition communicates by UDP, the accuracy rate is not guaranteed. Furthermore, network traffic may influence UDP waiting time.

Vulnerability Scanner detects products and computers using the following protocols:

- **RPC**: Detects ServerProtect for NT
- **UDP**: Detects Norton AntiVirus Corporate Edition clients
- **TCP**: Detects McAfee VirusScan ePolicy Orchestrator
- **ICMP**: Detects computers by sending ICMP packets
- **HTTP**: Detects Security Agents
- **DHCP**: If it detects a DHCP request, Vulnerability Scanner checks if antivirus software has already been installed on the requesting endpoint.

Configuring Product Query Settings

Product query settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-37*.

Procedure

1. To specify product query settings from Vulnerability Scanner (`TMVS.exe`):

   a. Launch `TMVS.exe`.

   b. Click **Settings**.

      The **Settings** screen appears.

c. Go to the **Product query** section.

d. Select the products to check.

e. Click **Settings** next to a product name and then specify the port number that Vulnerability Scanner will check.

f. Click **OK**.

The **Settings** screen closes.

2. To set the number of computers that Vulnerability Scanner simultaneously checks for security software:

a. Go to <*Server installation folder*>\PCCSRV\Admin\Utility\TMVS and open TMVS.ini using a text editor such as Notepad.

b. To set the number of computers checked during manual vulnerability scans, change the value for ThreadNumManual. Specify a value between 8 and 64.

For example, type `ThreadNumManual=60` if you want Vulnerability Scanner to check 60 computers at the same time.

c. To set the number of computers checked during scheduled vulnerability scans, change the value for ThreadNumSchedule. Specify a value between 8 and 64.

For example, type `ThreadNumSchedule=50` if you want Vulnerability Scanner to check 50 computers at the same time.

d. Save TMVS.ini.

Method for Retrieving Endpoint Descriptions

When Vulnerability Scanner is able to "ping" host machines, it can retrieve additional information about the host machines. There are two methods for retrieving information:

- **Quick retrieval**: Retrieves only the endpoint name

- **Normal retrieval**: Retrieves both domain and endpoint information

Configuring Retrieval Settings

Retrieval settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-37*.

Procedure

1. Launch `TMVS.exe`.
2. Click **Settings**.

   The **Settings** screen appears.
3. Go to the **Method for retrieving computer descriptions** section.
4. Select **Normal** or **Quick**.
5. If you selected **Normal**, select **Retrieve computer descriptions when available**.
6. Click **OK**.

   The **Settings** screen closes.

Notifications

Vulnerability Scanner can send the vulnerability scan results to Apex One administrators. It can also display notifications on unprotected host machines.

Configuring Notification Settings

Notification settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-37*.

Procedure

1. Launch `TMVS.exe`.

2. Click **Settings**.

   The **Settings** screen appears.

3. Go to the **Notifications** section.

4. To automatically send the Vulnerability Scan results to yourself or to other administrators in your organization:

   a. Select **Email results to the system administrator**.

   b. Click **Configure** to specify email settings.

   c. In **To**, type the email address of the recipient.

   d. In **From**, type the email address of the sender.

   e. In **SMTP server**, type the SMTP server address.

      For example, type `smtp.company.com`. The SMTP server information is required.

   f. In **Subject**, type a new subject for the message or accept the default subject.

   g. Click **OK**.

5. To inform users that their computers do not have security software installed:

   a. Select **Display a notification on unprotected computers**.

   b. Click **Customize** to configure the notification message.

   c. In the **Notification Message** screen, type a new message or accept the default message.

   d. Click **OK**.

6. Click **OK**.

   The **Settings** screen closes.

Vulnerability Scan Results

You can configure Vulnerability Scanner to save the vulnerability scan results to a comma-separated value (CSV) file.

Configuring Scan Results

Vulnerability scan results settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-37*.

Procedure

1. Launch `TMVS.exe`.
2. Click **Settings**.

   The **Settings** screen appears.
3. Go to the **Save results** section.
4. Select **Automatically save the results to a CSV file**.
5. To change the default folder for saving the `CSV` file:

   a. Click **Browse**.

   b. Select a target folder on the endpoint or on the network.

   c. Click **OK**.
6. Click **OK**.

   The **Settings** screen closes.

Ping Settings

Use "ping" settings to validate the existence of a target machine and determine its operating system. If these settings are disabled, Vulnerability Scanner scans all the IP addresses in the specified IP address range – even

those that are not used on any host machine – thereby making the scanning attempt longer than it should be.

Configuring Ping Settings

Ping settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-37*.

Procedure

1. To specify ping settings from Vulnerability Scanner (`TMVS.exe`):
   a. Launch `TMVS.exe`.
   b. Click **Settings**.

      The **Settings** screen appears.
   c. Go to the **Ping** settings section.
   d. Select **Allow Vulnerability Scanner to ping computers on your network to check their status**.
   e. In the **Packet size** and **Timeout** fields, accept or modify the default values.
   f. Select **Detect the type of operating system using ICMP OS fingerprinting**.

      If you select this option, Vulnerability Scanner determines if a host machine runs Windows or another operating system. For host machines running Windows, Vulnerability Scanner can identify the version of Windows.
   g. Click **OK**.

      The **Settings** screen closes.
2. To set the number of computers that Vulnerability Scanner simultaneously pings:
   a. Go to <*Server installation folder*>`\PCCSRV\Admin\Utility\TMVS` and open `TMVS.ini` using a text editor such as Notepad.

b. Change the value for `EchoNum`. Specify a value between 1 and 64.

   For example, type `EchoNum=60` if you want Vulnerability Scanner to ping 60 computers at the same time.

c. Save `TMVS.ini`.

Apex One Server Settings

Apex One server settings are used when:

- Vulnerability Scanner installs the Security Agent to unprotected target machines. Server settings allow Vulnerability Scanner to identify the Security Agent's parent server and the administrative credentials to use when logging on to the target machines.

  Note

  Certain conditions may prevent the installation of the Security Agent to the target host machines.

  For details, see *Guidelines When Installing the Security Agent Using Vulnerability Scanner on page 5-36*.

- Vulnerability Scanner sends agent installation logs to the Apex One server.

Configuring Apex One Server Settings

Apex One server settings are a subset of vulnerability scan settings. For details about vulnerability scan settings, see *Vulnerability Scan Methods on page 5-37*.

Procedure

1. Launch `TMVS.exe`.
2. Click **Settings**.

   The **Settings** screen appears.

3. Go to the **Apex One server settings** section.
4. Type the Apex One server name and port number.
5. Select **Auto-install Security Agent on unprotected computers**.
6. To configure the administrative credentials:
   a. Click **Install to Account**.
   b. In the **Account Information** screen, type a user name and password.
   c. Click **OK**.
7. Select **Send logs to the Apex One server**.
8. Click **OK**.

   The **Settings** screen closes.

Installing with Security Compliance

Install Security Agents on computers within the network domains or install the Security Agent to a target endpoint by using its IP address.

Before installing the Security Agent, take note of the following:

Procedure

1. Record the logon credentials for each endpoint. Apex One will prompt you to specify the logon credentials during installation.
2. The Security Agent will not be installed on the endpoint if:
   - The Apex One server is installed on the endpoint.
   - The endpoint runs Windows 7™ Starter, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8.1 (basic versions), and Windows 10 Home. If you have endpoints running these platforms, choose another installation method. See *Deployment Considerations on page 5-9* for details.

3. If the target endpoint runs Windows 7 (Professional, Enterprise, or Ultimate Edition), Windows 8.1 (Pro, Enterprise), Windows 10 (Pro, Education, Enterprise), Windows Server 2012 (Standard), Windows Server 2016 (all editions), or Windows Server 2019 (all editions) perform the following steps on the endpoint:

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

   b. Disable the Windows firewall.

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

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

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

4. If there are Trend Micro or third-party endpoint security programs installed on the endpoint, check if Apex One can automatically uninstall the software and replace it with the Security Agent. For a list of agent security software that Apex One automatically uninstalls, open the following files in <*Server installation folder*>`\PCCSRV\Admin`. You can open these files using a text editor such as Notepad.

   - `tmuninst.ptn`
   - `tmuninst_as.ptn`

   If the software on the target endpoint is not included in the list, manually uninstall it first. Depending on the uninstallation process of the software, the endpoint may or may not need to restart after uninstallation.

Installing the Security Agent

Procedure

1. Go to **Assessment** > **Unmanaged Endpoints**.
2. Click **Install** on top of the agent tree.
   - If an earlier Security Agent version is already installed on the endpoint and you click **Install**, Apex One skips the installation and does not upgrade the endpoint to this version. To upgrade the endpoint, ensure that you configure the following setting.
     a. Go to **Agents** > **Agent Management**.
     b. Click the **Settings** > **Privileges and Other Settings** > **Other Settings** tab.
     c. Go to the **Update Settings** section.
     d. In the **Security Agents only update the following components** drop-down, select **All components (including hotfixes and the agent program)**.
     e. Click **Apply to All Agents**.
3. Specify the administrator logon account for each endpoint and click **Log on**. Apex One starts installing the agent on the target endpoint.
4. View the installation status.

Migrating to the Security Agent

Replace agent security software installed on a target endpoint with the Security Agent.

Migrating from Other Endpoint Security Software

When you install the Security Agent, the installation program checks for any Trend Micro or third-party endpoint security software installed on the target endpoint. The installation program can automatically uninstall the software and replace it with the Security Agent.

For a list of endpoint security software that Apex One automatically uninstalls, open the following files in <*Server installation folder*>\PCCSRV\Admin. Open these files using a text editor such as Notepad.

- `tmuninst.ptn`
- `tmuninst_as.ptn`

If the software on the target endpoint is not included in the list, manually uninstall it first. Depending on the uninstallation process of the software, the endpoint may or may not need to restart after uninstallation.

Security Agent Migration Issues

- If automatic agent migration is successful but a user encounters problems with the Security Agent right after installation, restart the endpoint.
- If the Apex One installation program proceeded to install the Security Agent but was unable to uninstall the other security software, there will be conflicts between the two software. Uninstall both software, and then install the Security Agent using any of the installation methods discussed in *Deployment Considerations on page 5-9*.

Migrating from ServerProtect Normal Servers

The ServerProtect™ Normal Server Migration Tool is a tool that helps migrate computers running Trend Micro ServerProtect Normal Server to the Security Agent.

The ServerProtect Normal Server Migration Tool shares the same hardware and software specification as the Apex One server. Run the tool on computers running Windows Server platforms.

When uninstallation of the ServerProtect Normal server is successful, the tool installs the Security Agent. It also migrates the scan exclusion list settings (for all scan types) to the Security Agent.

While installing the Security Agent, the migration tool agent installer may sometimes time out and notify you that the installation was unsuccessful. However, the Security Agent may have been installed successfully. Verify the installation on the Security Agent endpoint from the Apex One web console.

Migration is unsuccessful under the following circumstances:

- The remote agent only has an IPv6 address. The migration tool does not support IPv6 addressing.
- The remote agent cannot use the NetBIOS protocol.
- Ports 455, 337, and 339 are blocked.
- The remote agent cannot use the RPC protocol.
- The Remote Registry Service stops.

Note

The ServerProtect Normal Server Migration Tool does not uninstall the Trend Micro Apex Central™ agent for ServerProtect. For instructions on how to uninstall the agent, refer to the ServerProtect and/or Apex Central documentation.

Using the ServerProtect Normal Server Migration Tool

Procedure

1. On the Apex One server computer, open <*Server installation folder*>`\PCCSRV\Admin\Utility\SPNSXfr` and copy the files `SPNSXfr.exe` and `SPNSX.ini` to `<Server installation folder>\PCCSRV\Admin`.

2. Double-click `SPNSXfr.exe` to open the tool.

   The **Server Protect Normal Server Migration Tool** console opens.

3. Select the Apex One server. The path of the Apex One server appears under Apex One server path. If it is incorrect, click **Browse** and select the `PCCSRV` folder in the directory where you installed Apex One. To enable the tool to automatically find the Apex One server again the next time you open the tool, select the **Auto Find Server Path** check box (selected by default).

4. Select the computers running ServerProtect Normal Server on which to perform the migration by clicking one of the following under **Target endpoint**:

   - **Windows Network tree**: Displays a tree of domains on the network. To select computers using this method, click the domains on which to search for agent computers.
   - **Information Server name**: Search by Information Server name. To select computers by this method, type the name of an Information Server on the network in the text box. To search for multiple Information Servers, insert a semicolon ";" between server names.
   - **Certain Normal Server name**: Search by Normal Server name. To select computers by this method, type the name of a Normal Server on the network in the text box. To search for multiple Normal Servers, enter a semicolon ";" between server names.
   - **IP range search**: Search by a range of IP addresses. To select computers by this method, type a range of class B IP addresses under IP range.

   Note

   If a DNS server on the network does not respond when searching for agents, the search stops responding. Wait for the search to time out.

5. Select **Restart after installation** to automatically restart the target computers after migration.

A restart is required for the migration to complete successfully. If you do not select this option, manually restart the computers after migration.

6. Click **Search**.

   The search results appear under **ServerProtect Normal Servers**.

7. Click the computers on which to perform the migration.

   a. To select all computers, click **Select All**.

   b. To clear all computers, click **Unselect All**.

   c. To export the list to a comma-separated value (CSV) file, click **Export to CSV**.

8. If logging on to the target computers requires a user name and password, do the following:

   a. Select the **Use group account/password** check box.

   b. Click **Set Logon Account**.

      The Enter Administration Information window appears.

   c. Type the user name and password.

      Note

      Use the local/domain administrator account to log on to the target endpoint. If you log on with insufficient privileges, such as "Guest" or "Normal user", you will not be able to perform installation.

   d. Click **OK**.

   e. Click **Ask again if logon is unsuccessful** to be able to type the user name and password again during the migration process if you are unable to log on.

9. Click **Migrate**.

10. If you did not select the **Restart after installation** option, restart the target computers to complete the migration.

Post-installation

After completing the installation, verify the following:

- *Programs List on page 5-59*
- *Security Agent Services on page 5-59*
- *Security Agent Installation Logs on page 5-60*

Programs List

Trend Micro Apex One Security Agent is listed on the **Add/Remove Programs** list in the Control Panel of the agent endpoint.

Security Agent Services

The following Security Agent services display on **Microsoft Management Console**:

- Apex One NT Listener (`TmListen.exe`)
- Apex One NT RealTime Scan (`NTRtScan.exe`)
- Apex One NT Firewall (`TmPfw.exe`); if the firewall was enabled during installation
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
- Apex One Common Client Solution Framework (`TmCCSF.exe`)

Security Agent Installation Logs

The Security Agent installation log, `OFCNT.LOG`, exists on the following locations:

- `%windir%` for all installation methods except MSI package installation
- `%temp%` for the MSI package installation method

Recommended Post-installation Tasks

Trend Micro recommends performing the following post-installation tasks.

Component Updates

Update Security Agent components to ensure that agents have the most up-to-date protection from security risks. You can run manual agent updates from the web console or instruct users to run "Update Now" from their endpoints.

Test Scan Using the EICAR Test Script

The European Institute for Computer Antivirus Research (EICAR) developed the EICAR test script as a safe way to confirm proper installation and configuration of antivirus software. Visit the EICAR website for more information:

http://www.eicar.org

The EICAR test script is an inert text file with a `.com` extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software react to it as if it were a virus. Use it to simulate a virus incident and confirm that email notifications and virus logs work properly.

WARNING!

Never use real viruses to test an antivirus product.

Performing a Test Scan

Procedure

1. Enable Real-time Scan on the agent.
2. Copy the following string and paste it into Notepad or any plain text editor: `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. Save the file as `EICAR.com` to a temp directory. Apex One immediately detects the file.
4. To test other computers on the network, attach the EICAR.com file to an email message and send it to one of the computers.

Tip

Trend Micro recommends packaging the EICAR file using compression software (such as WinZip) and then performing another test scan.

Security Agent Uninstallation

There are two ways to uninstall the Security Agent from endpoints:

- *Uninstalling the Security Agent from the Web Console on page 5-61*
- *Running the Security Agent Uninstallation Program on page 5-63*

Uninstalling the Security Agent from the Web Console

Uninstall the Security Agent program from the web console. Perform uninstallation only if you encounter problems with the program and then reinstall it immediately to keep the endpoint protected from security risks.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Tasks** > **Agent Uninstallation**.
4. On the **Agent Uninstallation** screen, click **Initiate Uninstallation**.
5. Check the notification status and check if there are agents that did not receive the notification.
   a. Click **Select Unnotified Endpoints** and then **Initiate Uninstallation** to immediately resend the notification to un-notified agents.
   b. Click **Stop Uninstallation** to prompt Apex One to stop notifying agents currently being notified. Agents already notified and already performing uninstallation ignore this command.

The Security Agent Uninstallation Program

Grant users the privilege to uninstall the Security Agent program and then instruct them to run the agent uninstallation program from their computers.

Depending on your configuration, uninstallation may or may not require a password. If a password is required, ensure that you share the password only to users that will run the uninstallation program and then change the password immediately if it has been divulged to other users.

Granting the Security Agent Uninstallation Privilege

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.

3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Uninstallation** section.
5. To allow uninstallation without a password, select **Allow users to uninstall the Security Agent**. If a password is required, select **Require a password for users to uninstall the Security Agent**, type the password, and then confirm it.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Running the Security Agent Uninstallation Program

Procedure

1. On the Windows **Start** menu, click **Programs** > **Trend Micro Apex One Security Agent** > **Uninstall Security Agent**.

   You can also perform the following steps:

   a. Click **Control Panel** > **Uninstall a program**.

   b. Locate **Trend Micro Apex One Security Agent** and click **Uninstall**.

   c. Follow the on-screen instructions.
2. If prompted, type the uninstallation password. Apex One notifies the user of the uninstallation progress and completion.

Note

If you installed Data Protection on the agent, you must restart the endpoint to complete the uninstallation process.

Chapter 6

Keeping Protection Up-to-Date

This chapter describes Trend Micro Apex One components and update procedures.

Topics include:

Apex One Components and Programs

Apex One makes use of components and programs to keep agent endpoints protected from the latest security risks. Keep these components and programs up-to-date by running manual or scheduled updates.

In addition to the components, Apex One agents also receive updated configuration files from the Apex One server. Security Agents need the configuration files to apply new settings. Each time you modify Apex One settings through the web console, the configuration files change.

Components are grouped as follows:

Antivirus Components

Component	Description
Virus Scan Engine 32/64-bit	At the heart of all Trend Micro products lies the scan engine, which was originally developed in response to early file-based viruses. The scan engine today is exceptionally sophisticated and capable of detecting different types of viruses and malware. The scan engine also detects controlled viruses that are developed and used for research. Rather than scanning every byte of every file, the engine and pattern file work together to identify the following: • Tell-tale characteristics of the virus code • The precise location within a file where the virus resides
Virus Pattern	The Virus Pattern contains information that helps Security Agents identify the latest virus/malware and mixed threat attacks. Trend Micro creates and releases new versions of the Virus Pattern several times a week, and any time after the discovery of a particularly damaging virus/malware.
Virus Scan Driver	The Virus Scan Driver monitors user operations on files. Operations include opening or closing a file, and executing an application. There are two versions for this driver. These are `TmXPFlt.sys` and `TmPreFlt.sys`. `TmXPFlt.sys` is used for real-time configuration of the Virus Scan Engine and `TmPreFlt.sys` for monitoring user operations. **Note** This component does not display on the console. To check its version, go to <*Server installation folder*>`\PCCSRV\Pccnt\Drv`. Right-click the `.sys` file, select **Properties**, and go to the **Version** tab.

Component	Description
Smart Scan Pattern	When in smart scan mode, Security Agents use two lightweight patterns that work together to provide the same protection provided by conventional anti-malware and anti-spyware patterns. The **Smart Scan Pattern** contains majority of the pattern definitions. The **Smart Scan Agent Pattern** contains all the other pattern definitions not found on the Smart Scan Pattern. The Security Agent scans for security threats using the **Smart Scan Agent Pattern**. Security Agents that cannot determine the risk of the file during the scan verify the risk by sending a scan query to the Scan Server, a service hosted on the Apex One server. The Scan Server verifies the risk using the **Smart Scan Pattern**. The Security Agent "caches" the scan query result provided by the Scan Server to improve the scan performance.
Smart Scan Agent Pattern	
IntelliTrap Pattern	The IntelliTrap Pattern detects real-time compression files packed as executable files. For details, see *IntelliTrap on page D-6*.
IntelliTrap Exception Pattern	The IntelliTrap Exception Pattern contains a list of "approved" compression files.

Component	Description
Memory Inspection Pattern	Real-Time Scan uses the Memory Inspection Pattern to evaluate executable compressed files identified by Behavior Monitoring. Real-Time Scan performs the following actions on executable compressed files: 1. Creates a mapping file in memory after verifying the process image path. **Note** The Scan Exclusion list overrides the file scanning. 2. Sends the process ID to the Advanced Protection Service which then: a. Uses the Virus Scan Engine to perform the memory scanning. b. Filters the process through global Approved lists for Windows system files, digitally signed files from reputable sources, and Trend Micro-tested files. After verifying that a file is known to be safe, Apex One does not perform any action on the file. 3. After processing the memory scan, the Advanced Protection Service sends the results to Real-Time Scan. 4. Real-Time Scan then quarantines any detected malware threat and terminates the process.
Contextual Intelligence Engine 32/64-bit	The Contextual Intelligence Engine monitors processes executed by low prevalence files and extracts behavioral features that the Contextual Intelligence Query Handler sends to the Predictive Machine Learning engine for analysis.
Contextual Intelligence Pattern	The Contextual Intelligence Pattern contains a list of "approved" behaviors that are not relevant to any known threats.
Contextual Intelligence Query Handler 32/64-bit	The Contextual Intelligence Query Handler processes the behaviors identified by the Contextual Intelligence Engine and sends the report to the Predictive Machine Learning engine.

Component	Description
Advanced Threat Scan Engine 32/64-bit	The Advanced Threat Scan Engine extracts file features from low prevalence files and sends the the information to the Predictive Machine Learning engine.
Advanced Threat Correlation Pattern	The Advanced Threat Correlation Pattern contains a list of file features that are not relevant to any known threats.

Updating the Scan Engine

By storing the most time-sensitive virus/malware information in the virus patterns, Trend Micro minimizes the number of scan engine updates while keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. Trend Micro releases new engines under the following circumstances:

- Incorporation of new scanning and detection technologies into the software
- Discovery of a new, potentially harmful virus/malware that the scan engine cannot handle
- Enhancement of the scanning performance
- Addition of file formats, scripting languages, encoding, and/or compression formats

Anti-spyware Components

Component	Description
Spyware/Grayware Pattern	The Spyware/Grayware Pattern identifies spyware/grayware in files and programs, modules in memory, Windows registry and URL shortcuts.
Spyware/Grayware Scan Engine 32/64-bit	The Spyware/Grayware Scan Engine scans for and performs the appropriate scan action on spyware/grayware.

Component	Description
Spyware Active-monitoring Pattern	The Spyware Active-monitoring Pattern is used for real-time spyware/grayware scanning. Only conventional scan agents use this pattern. Smart scan agents use the Smart Scan Agent Pattern for real-time spyware/grayware scanning. Agents send scan queries to a smart protection source if the risk of the scan target cannot be determined during scanning.

Damage Cleanup Services Components

Component	Description
Damage Cleanup Engine 32/64-bit	The Damage Cleanup Engine scans for and removes Trojans and Trojan processes.
Damage Cleanup Template	The Damage Cleanup Template is used by the Damage Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.
Early Boot Cleanup Driver 32/64-bit	The Trend Micro Early Boot Cleanup Driver loads before the operating system drivers which enables the detection and blocking of boot-type rootkits. After the Security Agent loads, Trend Micro Early Boot Cleanup Driver calls Damage Cleanup Services to clean the rootkit.

Firewall Components

Component	Description
Common Firewall Driver 32/64-bit	The Common Firewall Driver is used with the Common Firewall Pattern to scan agent endpoints for network viruses. This driver supports 32-bit and 64-bit platforms.
Common Firewall Pattern	Like the Virus Pattern, the Common Firewall Pattern helps agents identify virus signatures, unique patterns of bits and bytes that signal the presence of a network virus.

Behavior Monitoring Components

Component	Description
Behavior Monitoring Detection Pattern 32/64-bit	This pattern contains the rules for detecting suspicious threat behavior.
Behavior Monitoring Core Driver 32/64-bit	This kernel mode driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.
Behavior Monitoring Core Service 32/64-bit	This user mode service has the following functions: • Provides rootkit detection • Regulates access to external devices • Protects files, registry keys, and services
Behavior Monitoring Configuration Pattern	The Behavior Monitoring Driver uses this pattern to identify normal system events and exclude them from policy enforcement.
Digital Signature Pattern	This pattern contains a list of valid digital signatures that are used by the Behavior Monitoring Core Service to determine whether a program responsible for a system event is safe.
Policy Enforcement Pattern	The Behavior Monitoring Core Service checks system events against the policies in this pattern.
Memory Scan Trigger Pattern (32/64-bit)	Behavior Monitoring uses the Memory Scan Trigger Pattern to identify possible threats after detecting the following operations: • File write action • Registry write action • New process creation After identifying one of these operations, Behavior Monitoring calls Real-time Scan's Memory Inspection Pattern to check for security risks. For details about the Real-time Scan operations, see *Memory Inspection Pattern on page 6-5*.
Damage Recovery Pattern	The Damage Recovery Pattern contains policies that are used for monitoring suspicious threat behavior.

Component	Description
Program Inspection Monitoring Pattern	The Program Inspection Monitoring Pattern monitors and stores inspection points that are used for Behavior Monitoring.

Suspicious Connections Components

Component	Description
Global C&C IP List	The Global C&C IP list works in conjunction with the Network Content Inspection Engine (NCIE) to detect network connections with known C&C servers. NCIE detects C&C server contact through any network channel. Apex One logs all connection information to servers in the Global C&C IP list for evaluation.
Relevance Rule Pattern	The Suspicious Connections service uses the Relevance Rule Pattern to detect unique malware family signatures located in the headers of network packets.

Browser Exploit Solution

Component	Description
Browser Exploit Prevention Pattern	This pattern identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser.
Script Analyzer Unified Pattern	This pattern analyzes script in web pages and identifies malicious script.

Programs

Component	Description
Security Agent	The Security Agent program provides the actual protection from security risks.

Component	Description
Hot Fixes, Patches, and Service Packs	After an official product release, Trend Micro often develops the following to address issues, enhance product performance, or add new features: • *Hot Fix on page D-5* • *Patch on page D-9* • *Security Patch on page D-11* • *Service Pack on page D-11* Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix, patch, and service pack releases: http://downloadcenter.trendmicro.com All releases include a readme file that contains installation, deployment, and configuration information. Read the readme file carefully before performing installation.

Hot Fix and Patch History

When the Apex One server deploys hot fix or patch files to Security Agents, the agent program records information about the hot fix or patch in Registry Editor. You can query this information for multiple agents using logistics software such as Microsoft SMS, LANDesk™, or BigFix™.

Note

This feature does not record hot fixes and patches that are deployed only to the server.

Information is stored in the following keys:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- For computers running x64 type platforms:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-
cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>
```

Check for the following keys:

- **Key:** `HotFix_installed`

  Type: `REG_SZ`

  Value: `<Hot fix or patch name>`

- **Key:** `HotfixInstalledNum`

  Type: `DWORD`

  Value: `<Hot fix or patch number>`

Web Reputation Component

Component	Description
URL Filtering Engine	The URL Filtering Engine facilitates communication between Apex One and the Trend Micro URL Filtering Service. The URL Filtering Service is a system that rates URLs and provides rating information to Apex One.

Update Overview

All component updates originate from the Trend Micro ActiveUpdate server. When updates are available, the Apex One server and smart protection sources (Smart Protection Server or Smart Protection Network) download the updated components. There are no component download overlaps between the Apex One server and smart protection sources because each one downloads a specific set of components.

Note

You can configure both the Apex One server and Smart Protection Server to update from a source other than the Trend Micro ActiveUpdate server. To do this, you need to set up a custom update source. If you need assistance setting up this update source, contact your support provider.

Apex One Server and Security Agent Update

The Apex One server downloads most of the components that agents need. The only component it does not download is the Smart Scan Pattern, which is downloaded by smart protection sources.

If the Apex One server manages a large number of agents, updating may utilize a significant amount of server computer resources, affecting the server's stability and performance. To address this issue, Apex One has an Update Agent feature that allows certain agents to share the task of distributing updates to other agents.

The following table describes the different component update options for the Apex One server and agents, and recommendations on when to use them:

TABLE 6-1. Server-Agent Update Options

UPDATE OPTION	DESCRIPTION	RECOMMENDATION
ActiveUpdate server > **Server** > **Agent**	The Apex One server receives updated components from the Trend Micro ActiveUpdate server (or other update source) and initiates component update on agents.	Use this method if there are no low-bandwidth sections between the Apex One server and agents.
ActiveUpdate server > **Server** > **Update Agents** > **Agent**	The Apex One server receives updated components from the ActiveUpdate server (or other update source) and initiates component update on agents. Agents acting as Update Agents then notify agents to update components.	If there are low-bandwidth sections between the Apex One server and agents, use this method to balance the traffic load on the network.

Update Option	Description	Recommendation
ActiveUpdate server > **Update Agents** > **Agent**	Update Agents receive updated components directly from the ActiveUpdate server (or other update source) and notifies agents to update components.	Use this method only if you experience problems updating Update Agents from the Apex One server or from other Update Agents. Under most circumstances, Update Agents receive updates faster from the Apex One server or from other Update Agents than from an external update source.
ActiveUpdate server > **Agent**	Apex One agents receive updated components directly from the ActiveUpdate server (or other update source).	Use this method only if you experience problems updating agents from the Apex One server or from Update Agents. Under most circumstances, agents receive updates faster from the Apex One server or from Update Agents than from an external update source.

Smart Protection Source Update

A smart protection source (Smart Protection Server or Smart Protection Network) downloads the Smart Scan Pattern. Smart scan agents do not download this pattern. Agents verify potential threats against the pattern by sending scan queries to the smart protection source.

Note

See *Smart Protection Sources on page 4-5* for more information about smart protection sources.

The following table describes the update process for smart protection sources.

TABLE 6-2. Smart Protection Source Update Process

UPDATE PROCESS	DESCRIPTION
ActiveUpdate server > **Smart Protection Network**	The Trend Micro Smart Protection Network receives updates from the Trend Micro ActiveUpdate server. Smart scan agents that are not connected to the corporate network send queries to the Trend Micro Smart Protection Network.
ActiveUpdate server > **Smart Protection Server**	A Smart Protection Server (integrated or standalone) receives updates from the Trend Micro ActiveUpdate server. Smart protection agents that are connected to the corporate network send queries to the Smart Protection Server.
Smart Protection Network > **Smart Protection Server**	A Smart Protection Server (integrated or standalone) receives updates from the Trend Micro Smart Protection Network. Smart protection agents that are connected to the corporate network send queries to the Smart Protection Server.

Apex One Server Updates

The Apex One server downloads the following components and deploys them to agents:

TABLE 6-3. Components Downloaded by the Apex One Server

COMPONENT	DISTRIBUTION	
	CONVENTIONAL SCAN AGENTS	SMART SCAN AGENTS
Antivirus		
Smart Scan Agent Pattern	No	Yes
Virus Pattern	Yes	No
IntelliTrap Pattern	Yes	Yes
IntelliTrap Exception Pattern	Yes	Yes
Virus Scan Engine 32/64-bit	Yes	Yes

Component	Distribution	
	Conventional Scan Agents	Smart Scan Agents
Memory Inspection Pattern	Yes	Yes
Early Launch Anti-Malware Pattern 32/64-bit	Yes	Yes
Contextual Intelligence Engine 32/64-bit	Yes	Yes
Contextual Intelligence Pattern	Yes	Yes
Contextual Intelligence Query Handler 32/64-bit	Yes	Yes
Advanced Threat Scan Engine 32/64-bit	Yes	Yes
Advanced Threat Correlation Pattern	Yes	Yes
Anti-spyware		
Spyware/Grayware Pattern	Yes	Yes
Spyware Active-monitoring Pattern	Yes	No
Spyware/Grayware Scan Engine 32/64-bit	Yes	Yes
Damage Cleanup Services		
Damage Cleanup Template	Yes	Yes
Damage Cleanup Engine 32/64-bit	Yes	Yes
Early Boot Cleanup Driver 32/64-bit	Yes	Yes
Firewall		
Common Firewall Pattern	Yes	Yes
Behavior Monitoring Components		
Behavior Monitoring Detection Pattern 32/64-bit	Yes	Yes

Component	Distribution	
	Conventional Scan Agents	Smart Scan Agents
Behavior Monitoring Core Driver 32/64-bit	Yes	Yes
Behavior Monitoring Core Service 32/64-bit	Yes	Yes
Behavior Monitoring Configuration Pattern	Yes	Yes
Policy Enforcement Pattern	Yes	Yes
Digital Signature Pattern	Yes	Yes
Memory Scan Trigger Pattern (32/64-bit)	Yes	Yes
Program Inspection Monitoring Pattern	Yes	Yes
Damage Recovery Pattern	Yes	Yes
Suspicious Connections		
Global C&C IP List	Yes	Yes
Relevance Rule Pattern	Yes	Yes
Browser Exploit Solution		
Browser Exploit Prevention Pattern	Yes	Yes
Script Analyzer Unified Pattern	Yes	Yes

Update reminders and tips:

- To allow the server to deploy the updated components to agents, enable automatic agent update. For details, see *Security Agent Automatic Updates on page 6-38*. If automatic agent update is disabled, the server downloads the updates but does not deploy them to the agents.
- A pure IPv6 Apex One server cannot distribute updates directly to pure IPv4 agents. Similarly, a pure IPv4 Apex One server cannot distribute

updates directly to pure IPv6 agents. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Apex One server to distribute update to the agents.

- Trend Micro releases pattern files regularly to keep agent protection current. Since pattern file updates are available regularly, Apex One uses a mechanism called "component duplication" that allows faster downloads of pattern files. See *Apex One Server Component Duplication on page 6-19* for more information.
- If you use a proxy server to connect to the Internet, use the correct proxy settings to download updates successfully.
- On the web console's Dashboard, add the **Agent Updates** widget to view the current versions of components and determine the number of agents with updated and outdated components.

Apex One Server Update Sources

Configure the Apex One server to download components from the Trend Micro ActiveUpdate server or from another source. You may specify another source if the Apex One server is unable to reach the ActiveUpdate server directly. For a sample scenario, see *Isolated Apex One Server Updates on page 6-23*.

After the server downloads any available updates, it can automatically notify agents to update their components based on the settings you specified in **Updates** > **Agents** > **Automatic Update**. If the component update is critical, let the server notify the agents at once by going to **Updates** > **Agents** > **Manual Update**.

Note

If you do not specify a deployment schedule or event-triggered update settings in **Updates** > **Agents** > **Automatic Update**, the server will download the updates but will not notify agents to update.

IPv6 Support for Apex One Server Updates

A pure IPv6 Apex One server cannot update directly from pure IPv4 update sources, such as:

- Trend Micro ActiveUpdate Server
- Any pure IPv4 custom update source

Similarly, a pure IPv4 Apex One server cannot update directly from pure IPv6 custom update sources.

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

Proxy for Apex One Server Updates

Configure server programs hosted on the server computer to use proxy settings when downloading updates from the Trend Micro ActiveUpdate server. Server programs include the Apex One server and the integrated Smart Protection Server.

Configuring Server Proxy Settings

Procedure

1. Go to **Administration** > **Settings** > **Proxy**.
2. Click the **Server** tab.
3. Select **Use a proxy server when connecting to hosted Trend Micro servers for pattern, engine, and license updates**.
4. Specify the proxy protocol, server name or IPv4/IPv6 address, and port number.
5. If the proxy server requires authentication, type the user name and password.

6. Click **Save**.

Configuring the Server Update Source

Procedure

1. Go to **Updates** > **Server** > **Update Source**.
2. Select the location from where you want to download component updates.

   If you choose ActiveUpdate server, ensure that the server has Internet connection and, if you are using a proxy server, test if Internet connection can be established using the proxy settings. For details, see *Proxy for Apex One Server Updates on page 6-18*.

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

   Note

   The Apex One server uses component duplication when downloading components from the update source. See *Apex One Server Component Duplication on page 6-19* for details.

3. Click **Save**.

Apex One Server Component Duplication

When the latest version of a full pattern file is available for download from the Trend Micro ActiveUpdate server, 14 "incremental patterns" also become available. Incremental patterns are smaller versions of the full pattern file that account for the difference between the latest and previous full pattern

file versions. For example, if the latest version is 175, incremental pattern v_173.175 contains signatures in version 175 not found in version 173 (version 173 is the previous full pattern version since pattern numbers are released in increments of 2. Incremental pattern v_171.175 contains signatures in version 175 not found in version 171.

To reduce network traffic generated when downloading the latest pattern, Apex One performs component duplication, a component update method where the Apex One server or Update Agent downloads only incremental patterns. See *Update Agent Component Duplication on page 6-60* for information on how Update Agents perform component duplication.

Component duplication applies to the following components:

- Virus Pattern
- Smart Scan Agent Pattern
- Damage Cleanup Template
- IntelliTrap Exception Pattern
- Spyware/Grayware Pattern
- Spyware Active-monitoring Pattern

Component Duplication Scenario

To explain component duplication for the server, refer to the following scenario:

TABLE 6-4. Server Component Duplication Scenario

Full patterns on the Apex One server	Current version: 171 Other versions available: 169 167 165 161 159

Latest version on the ActiveUpdate server	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. The Apex One server compares its current full pattern version with the latest version on the ActiveUpdate server. If the difference between the two versions is 14 or less, the server only downloads the incremental pattern that accounts for the difference between the two versions.

   Note

   If the difference is more than 14, the server automatically downloads the full version of the pattern file and 14 incremental patterns.

   To illustrate based on the example:

   - The difference between versions 171 and 175 is 2. In other words, the server does not have versions 173 and 175.
   - The server downloads incremental pattern 171.175. This incremental pattern accounts for the difference between versions 171 and 175.

2. The server merges the incremental pattern with its current full pattern to generate the latest full pattern.

   To illustrate based on the example:

   - On the server, Apex One merges version 171 with incremental pattern 171.175 to generate version 175.
   - The server has 1 incremental pattern (171.175) and the latest full pattern (version 175).

3. The server generates incremental patterns based on the other full patterns available on the server. If the server does not generate these incremental patterns, agents that missed downloading earlier incremental patterns automatically download the full pattern file, which will consequently generate more network traffic.

To illustrate based on the example:

- Because the server has pattern versions 169, 167, 165, 163, 161, 159, it can generate the following incremental patterns:

  169.175, 167.175, 165.175, 163.175, 161.175, 159.175

- The server does not need to use version 171 because it already has the incremental pattern 171.175.

- The server now has 7 incremental patterns:

  171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

- The server keeps the last 7 full pattern versions (versions 175, 171, 169, 167, 165, 163, 161). It removes any older version (version 159).

4. The server compares its current incremental patterns with the incremental patterns available on the ActiveUpdate server. The server downloads the incremental patterns it does not have.

   To illustrate based on the example:

   - The ActiveUpdate server has 14 incremental patterns:

     173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - The Apex One server has 7 incremental patterns:

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - The Apex One server downloads an additional 7 incremental patterns:

     173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - The server now has all the incremental patterns available on the ActiveUpdate server.

5. The latest full pattern and the 14 incremental patterns are made available to agents.

Isolated Apex One Server Updates

If the Apex One server belongs to a network that is isolated completely from all outside sources, you can keep the server's components up-to-date by letting it update from an internal source that contains the latest components.

This topic explains the tasks that you need to perform to update an isolated Apex One server.

Updating an Isolated Apex One Server

This procedure is provided for your reference. If you are able to fulfill all the tasks in this procedure, please ask your support provider for the detailed steps for each task.

Procedure

1. Identify the update source, such as Trend Micro Apex Central or a random host machine. The update source must have:
   - A reliable Internet connection so that it can download the latest components from the Trend Micro ActiveUpdate server. Without Internet connection, the only way for the update source to have the latest components is if you obtain the components yourself from Trend Micro and then copy them into the update source.
   - A functional connection with the Apex One server. Configure proxy settings if there is a proxy server between the Apex One server and the update source. For details, see *Proxy for Apex One Server Updates on page 6-18*.
   - Enough disk space for downloaded components
2. Point the Apex One server to the new update source. For details, see *Apex One Server Update Sources on page 6-17*.
3. Identify the components that the server deploys to agents. For a list of deployable components, see *Security Agent Updates on page 6-27*.

Tip

One of the ways to determine if a component is being deployed to agents is by going to the **Update Summary** screen on the web console (**Updates** > **Summary**). In this screen, the update rate for a component that is being deployed will always be larger than 0%.

4. Determine how often to download the components. Pattern files are updated frequently (some on a daily basis) so it is a good practice to update them regularly. For engines and drivers, you can ask your support provider to notify you of critical updates.

5. On the update source:

   a. Connect to the ActiveUpdate server. The server's URL depends on your Apex One version.

   b. Download the following items:

      - The `server.ini` file. This file contains information about the latest components.
      - The components you identified in step 3.

   c. Save the downloaded items to a directory in the update source.

6. Run a manual update of the Apex One server. For details, see *Manually Updating the Apex One Server on page 6-25*.

7. Repeat step 5 to step 6 each time you need to update components.

Apex One Server Update Methods

Update Apex One server components manually or by configuring an update schedule.

To allow the server to deploy the updated components to agents, enable automatic agent update. For details, see *Security Agent Automatic Updates on page 6-38*. If automatic agent update is disabled, the server downloads the updates but does not deploy them to the agents.

Update methods include:

- **Manual server update**: When an update is critical, perform manual update so the server can obtain the updates immediately. See *Manually Updating the Apex One Server on page 6-25* for details.
- **Scheduled server update**: The Apex One server connects to the update source during the scheduled day and time to obtain the latest components. See *Scheduling Updates for the Apex One Server on page 6-25* for details.

Manually Updating the Apex One Server

Manually update the components on the Apex One server after installing or upgrading the server and whenever there is an outbreak.

Procedure

1. Go to **Updates** > **Server** > **Manual Update**.
2. Select the components to update.
3. Click **Update**.

   The server downloads the updated components.

Scheduling Updates for the Apex One Server

Configure the Apex One server to regularly check its update source and automatically download any available updates. Because agents normally get updates from the server, using scheduled update is an easy and effective way of ensuring that protection against security risks is always current.

Procedure

1. Go to **Updates** > **Server** > **Scheduled Update**.
2. Select **Enable scheduled update of the Apex One server**.

3. Select the components to update.
4. Specify the update schedule.

   For daily, weekly, and monthly updates, the period of time is the number of hours during which Apex One will perform the update. Apex One updates at any given time during this time period.
5. Click **Save**.

Apex One Server Update Logs

Check the server update logs to determine if there are problems updating certain components. Logs include component updates for the Apex One server.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing the Update Logs

Procedure

1. Go to **Logs** > **Server Update**.
2. Check the **Result** column to see if there are components that were not updated.
3. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Integrated Smart Protection Server Updates

The integrated Smart Protection Server downloads two components, namely the Smart Scan Pattern and Web Blocking List. For details on these

components and how to update them, see *Integrated Smart Protection Server Management on page 4-19*.

Security Agent Updates

To ensure that agents stay protected from the latest security risks, update agent components regularly.

Before updating agents, check if their update source (Apex One server or a custom update source) has the latest components. For information on how to update the Apex One server, see *Apex One Server Updates on page 6-14*.

The following table lists all components that update sources deploy to agents and the components in use when using a particular scan method.

TABLE 6-5. Apex One Components Deployed to Agents

COMPONENT	DISTRIBUTION	
	CONVENTIONAL SCAN AGENTS	SMART SCAN AGENTS
Antivirus		
Smart Scan Agent Pattern	No	Yes
Virus Pattern	Yes	No
IntelliTrap Pattern	Yes	Yes
IntelliTrap Exception Pattern	Yes	Yes
Virus Scan Engine 32/64-bit	Yes	Yes
Memory Inspection Pattern	Yes	Yes
Early Launch Anti-Malware Pattern 32/64-bit	Yes	Yes
Contextual Intelligence Engine 32/64-bit	Yes	Yes
Contextual Intelligence Pattern	Yes	Yes

Component	Distribution	
	Conventional Scan Agents	Smart Scan Agents
Contextual Intelligence Query Handler 32/64-bit	Yes	Yes
Advanced Threat Scan Engine 32/64-bit	Yes	Yes
Advanced Threat Correlation Pattern	Yes	Yes
Anti-spyware		
Spyware/Grayware Pattern	Yes	Yes
Spyware Active-monitoring Pattern	Yes	No
Spyware/Grayware Scan Engine 32/64-bit	Yes	Yes
Damage Cleanup Services		
Damage Cleanup Template	Yes	Yes
Damage Cleanup Engine 32/64-bit	Yes	Yes
Early Boot Cleanup Driver 32/64-bit	Yes	Yes
Web Reputation Services		
URL Filtering Engine	Yes	Yes
Firewall		
Common Firewall Pattern	Yes	Yes
Common Firewall Driver 32/64-bit	Yes	Yes
Behavior Monitoring Components		
Behavior Monitoring Detection Pattern 32/64-bit	Yes	Yes
Behavior Monitoring Core Driver 32/64-bit	Yes	Yes

Component	Distribution	
	Conventional Scan Agents	Smart Scan Agents
Behavior Monitoring Core Service 32/64-bit	Yes	Yes
Behavior Monitoring Configuration Pattern	Yes	Yes
Policy Enforcement Pattern	Yes	Yes
Digital Signature Pattern	Yes	Yes
Memory Scan Trigger Pattern (32/64-bit)	Yes	Yes
Program Inspection Monitoring Pattern	Yes	Yes
Damage Recovery Pattern	Yes	Yes
Suspicious Connections		
Global C&C IP List	Yes	Yes
Relevance Rule Pattern	Yes	Yes
Browser Exploit Solution		
Browser Exploit Prevention Pattern	Yes	Yes
Script Analyzer Unified Pattern	Yes	Yes

Security Agent Update Sources

Agents can obtain updates from the standard update source (Apex One server) or specific components from custom update sources such as the Trend Micro ActiveUpdate server. For details, see *Standard Update Source for Security Agents on page 6-30* and *Customized Update Sources for Security Agents on page 6-32*.

IPv6 Support for Security Agent Updates

A pure IPv6 agent cannot update directly from pure IPv4 update sources, such as:

- A pure IPv4 Apex One server
- A pure IPv4 Update Agent
- Any pure IPv4 custom update source
- Trend Micro ActiveUpdate Server

Similarly, a pure IPv4 agent cannot update directly from pure IPv6 update sources, such as a pure IPv6 Apex One server or Update Agent.

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

Standard Update Source for Security Agents

The Apex One server is the standard update source for agents.

If the Apex One server is unreachable, agents will not have a backup source and will therefore remain outdated. To update agents that cannot reach the Apex One server, Trend Micro recommends using Agent Packager. Use this tool to create a package with the latest components available on the server and then run the package on agents.

Note

The agent's IP address (IPv4 or IPv6) determines if connection to the Apex One server can be established. For details about IPv6 support for agent updates, see *IPv6 Support for Security Agent Updates on page 6-30*.

Configuring the Standard Update Source for Security Agents

Procedure

1. Go to **Updates** > **Agents** > **Update Source**.
2. Select **Standard update source (update from Apex One server)**.
3. Click **Notify All Agents**.

Security Agent Update Process

Note

This topic discusses the update process for Security Agents. The update process for Update Agents is discussed in *Standard Update Source for Security Agents on page 6-30*.

If you configure Security Agents to update directly from the Apex One server, the update process proceeds as follows:

1. The Security Agent obtains updates from the Apex One server.
2. If unable to update from the Apex One server, the Security Agent tries connecting directly to the Trend Micro ActiveUpdate server if the option **Security Agents download updates from the Trend Micro ActiveUpdate Server** is enabled in **Agents** > **Agent Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings (tab)** > **Update Settings**.

Note

Only components can be updated from the ActiveUpdate server. Domain settings, programs and hot fixes can only be downloaded from the Apex One server or Update Agents. You can speed up the update process by configuring Security Agents to only download pattern files from the ActiveUpdate server. For more information, see *ActiveUpdate Server as the Security Agent Update Source on page 6-36*.

Customized Update Sources for Security Agents

Aside from the Apex One server, Security Agents can update from custom update sources. Custom update sources help reduce Security Agent update traffic directed to the Apex One server and allow Security Agents that cannot connect to the Apex One server to get timely updates. Specify the custom update sources on the Customized Update Source List, which can accommodate up to 1024 update sources.

Tip

Trend Micro recommends assigning some Security Agents as Update Agents and then adding them to the list.

Configuring Customized Update Sources for Security Agents

Important

OfficeScan XG Service Pack 1 (or later) supports the use of HTTPS as the communication protocol between Update Agents and the Security Agents configured to receive updates from Update Agents. You must upgrade Update Agents and all Security Agents that report to the Update Agents to OfficeScan XG Service Pack 1 (or later) before changing the communication protocol to HTTPS.

Procedure

1. Go to **Updates** > **Agents** > **Update Source**.
2. Select **Customized Update Source**.
3. Select how Update Agents and Security Agents receive updates.
   - **Update Agents update components, domain settings, and agent programs and hot fixes, only from the Apex One server**
   - Security Agents update the following items from the Apex One server if all customized sources are unavailable or not found:

- **Components**
- **Domain settings**
- **Security Agent programs and hot fixes**

For more information, see *Security Agent Update Process on page 6-31*.

4. If you specified at least one Update Agent as an update source, click **Update Agent Analytical Report** to generate a report that highlights the update status of endpoints.

   For details about the report, see *Update Agent Analytical Report on page 6-61*.

5. Add or edit **Customized Update Source List**.

   - Click **Add** to specify a new update source.
   - Click a value in the **IP Range** column to edit an existing update source.

   Note

   Edit an existing update source to change the communication protocol of an existing OfficeScan XG SP1 (or later) Update Agent to HTTPS.

   The **Add/Edit IP Range and Update Source** screen appears.

6. Configure the IP addresses of endpoints that receive updates from the update source.

   - **IPv4**: Specify the IPv4 address range of the endpoints that use the update source
   - **IPv6**: Specify the IPv6 prefix and length of the endpoints that use the update source

Note

Ensure that the Security Agents can connect to the update source using their IP addresses. For example, if you specified an IPv4 address range, the update source must have an IPv4 address. If you specified an IPv6 prefix and length, the update source must have an IPv6 address.

For details about IPv6 support for endpoint updates, see *Security Agent Update Sources on page 6-29*.

7. Specify the update source. You can select an Update Agent if one has been assigned or type the URL of a specific source.

   - **URL**: Specify the URL of the update source

     Note

     To change a preexisting Update Agent protocol from HTTP to HTTPS, modify the **URL** value.

   - **Update Agent**: Select a preconfigured Update Agent from the drop-down and choose how Security Agents connect to the Update Agent
     - **Use the Update Agent IP address to connect**
     - **Use the Update Agent hostname to connect**

     Note

     Apex One automatically configures the **External Source** URL to use HTTPS protocol if the Update Agent has been updated to OfficeScan XG SP1 or later.

8. Click **Save**.

9. Manage the **Customized Update Source List**.

   a. Remove an update source from the list by selecting the check box and clicking **Delete**.

   b. To move an update source, click the up or down arrow. You can only move one source at a time.

10. Click **Notify All Agents**.

Security Agent Update Process

Note

This topic discusses the update process for Security Agents. The update process for Update Agents is discussed in *Customized Update Sources for Update Agents on page 6-57*.

After you have set up and saved the customized update source list, the update process proceeds as follows:

1. The Security Agent updates from the first source on the list.
2. If unable to update from the first source, the Security Agent updates from the second source, and so on.
3. If unable to update from all sources, the Security Agent checks the following settings on the **Update Source** screen:

TABLE 6-6. Additional Settings for Custom Update Sources

SETTING	DESCRIPTION
Update Agents update components, domain settings, and agent programs and hot fixes, only from the Apex One server	If this setting is enabled, Update Agents update directly from the Apex One server and disregard the Customized Update Source List. If disabled, Update Agents apply the customized update source settings configured for normal agents.
Security Agents update the following items from the Apex One server if all customized sources are unavailable or not found:	

Setting	Description
Components	If this setting is enabled, the agent updates components from the Apex One server. If disabled, the agent then tries connecting directly to the Trend Micro ActiveUpdate server if any of the following is true: • In **Agents** > **Agent Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings (tab)** > **Update Settings**, the option **Security Agents download updates from the Trend Micro ActiveUpdate Server** is enabled. • The ActiveUpdate server is not included in the Customized Update Source List. **Note** Only components can be updated from the ActiveUpdate server. Domain settings, programs and hot fixes can only be downloaded from the Apex One server or Update Agents. You can speed up the update process by configuring agents to only download pattern files from the ActiveUpdate server. For more information, see *ActiveUpdate Server as the Security Agent Update Source on page 6-36*.
Domain settings	If this setting is enabled, the agent updates domain-level settings from the Apex One server.
Security Agent programs and hot fixes	If this setting enabled, the agent updates programs and hot fixes from the Apex One server.

4. If unable to update from all possible sources, the agent quits the update process.

ActiveUpdate Server as the Security Agent Update Source

When Security Agents download updates directly from the Trend Micro ActiveUpdate server, you can limit the download to only the pattern files to

reduce the bandwidth consumed during updates and speed up the update process.

Scan engines and other components are not updated as frequently as pattern files, which is another reason to limit the download to only the pattern files.

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

Limiting Downloads from the ActiveUpdate Server

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **System** tab.
3. Go to the **Updates** section.
4. Select **Download only the pattern files from the ActiveUpdate server when performing updates**.

Security Agent Update Methods

Security Agents that update components from the Apex One server or a customized update source can use the following update methods:

- **Automatic updates**: Agent update runs automatically when certain events occur or based on a schedule. For details, see *Security Agent Automatic Updates on page 6-38*.
- **Manual updates**: When an update is critical, use manual update to immediately notify agents to perform component update. For details, see *Security Agent Manual Updates on page 6-44*.
- **Privilege-based updates**: Users with update privileges have greater control over how the Security Agent on their computers gets updated.

For details, see *Configuring Update Privileges and Other Settings on page 6-45*.

Security Agent Automatic Updates

Automatic update relieves you of the burden of notifying all agents to update and eliminates the risk of agent computers not having up-to-date components.

In addition to components, Security Agents also receive updated configuration files during automatic update. Agents need the configuration files to apply new settings. Each time you modify Apex One settings through the web console, the configuration files change. To specify how often configuration files are applied to agents, see step 3 *Configuring Security Agent Automatic Updates on page 6-40*.

Note

You can configure agents to use proxy settings during automatic update. See *Proxy for Security Agent Component Updates on page 6-48* for details.

There are two types of automatic updates:

- *Event-triggered Updates on page 6-38*
- *Schedule-based Updates on page 6-40*

Event-triggered Updates

The server can notify online agents to update components after it downloads the latest components, and offline agents when they restart and then connect to the server. Optionally initiate Scan Now (manual scan) on Security Agent endpoints after the update.

TABLE 6-7. Event-triggered Update Options

OPTION	DESCRIPTION
Initiate component update on agents immediately after the Apex One server downloads a new component	The server notifies agents to update as soon as it completes an update. Frequently updated agents only need to download incremental patterns, thus reducing the time it takes to complete the update (see *Apex One Server Component Duplication on page 6-19* for details about incremental patterns). However, updating frequently may adversely affect the server's performance, especially if you have a large number of agents updating at the same time. If you have agents in Independent mode and you want these agents to update as well, select **Include Independent and offline agent(s)**. See *Security Agent Independent Mode Privilege on page 15-20* for details about Independent mode.
Let agents initiate component update after restarting and connecting to the Apex One server (Independent agents excluded)	Any agent that missed an update immediately downloads components when it establishes connection with the server. The agent may miss an update if it is offline or if the endpoint where it is installed is not up and running.
Perform Scan Now after update (Independent agents excluded)	The server notifies agents to scan after an event-triggered update. Consider enabling this option if a particular update is a response to a security risk that has already spread within the network.

Note

If the Apex One server is unable to successfully send an update notification to agents after it downloads components, it automatically resends the notification after 15 minutes. The server continues to send update notifications up to a maximum of five times until the agent responds. If the fifth attempt is unsuccessful, the server stops sending notifications. If you select the option to update components when agents restart and then connect to the server, component update will still proceed.

Schedule-based Updates

Running scheduled updates is a privilege. You need to first select Security Agents that will have the privilege and these Security Agents will then run updates based on the schedule.

Note

To use schedule-based update with Network Address Translation, see *Configuring Scheduled Security Agent Updates with NAT on page 6-42*.

Configuring Security Agent Automatic Updates

Procedure

1. Go to **Updates** > **Agents** > **Automatic Update**.
2. Select the events for an **Event-triggered Update**:
   - **Initiate component update on agents immediately after the Apex One server downloads a new component**
     - **Include Independent and offline agent(s)**
   - **Let agents initiate component update after restarting and connecting to the Apex One server (Independent agents excluded)**
   - **Perform Scan Now after update (Independent agents excluded)**

   For details about the available options, see *Event-triggered Updates on page 6-38*.
3. Configure the schedule for a **Schedule-based Update**.
   - **Hour(s)**

     The option to **Update agent configurations only once per day** is available when scheduling an hourly update frequency. The configuration file contains all Security Agent settings configured using the web console.

Tip

Trend Micro updates components often; however, Apex One configuration settings probably change less frequently. Updating the configuration files with the components requires more bandwidth and increases the time Apex One needs to complete the update. For this reason, Trend Micro recommends updating Security Agent configurations only once per day.

- **Daily** or **Weekly**

  Specify the time of the update and the time period the Apex One server notifies agents to update components.

Tip

This setting prevents all online agents from simultaneously connecting to the server at the specified start time, significantly reducing the amount of traffic directed to the server. For example, if the start time is 12pm and the time period is 2 hours, Apex One randomly notifies all online agents to update components from 12pm until 2pm.

Note

After configuring the update schedule, enable the schedule on selected agents.

For details on enabling scheduled-based updates, see step 4 of *Configuring Update Privileges and Other Settings on page 6-45*.

4. Click **Save**.

   Apex One cannot notify offline agents immediately. Select **Let agents initiate component update after restarting and connecting to the Apex One server (Independent agents excluded)** to update offline agents that become online after the time period expires. Offline agents without this setting enabled update components on the next schedule or during a manual update.

Configuring Scheduled Security Agent Updates with NAT

The following issues may arise if the local network uses NAT:

- Security Agents appear offline on the web console.
- The Apex One server is not able to successfully notify agents of updates and configuration changes.

Work around these issues by deploying updated components and configuration files from the server to the Security Agent with a scheduled update as described below.

Procedure

- Before installing the Security Agent on agent computers:
  a. Configure the agent update schedule in the **Schedule-based Update** section of **Updates** > **Agents** > **Automatic Update**.
  b. Grant agents the privilege to enable scheduled update in **Agents** > **Agent Management**, click **Settings** > **Privileges and Other Settings** > **Privileges (tab)** > **Component Updates**.
- If Security Agents already exist on agent computers:
  a. Grant agents the privilege to perform "Update Now" in **Agents** > **Agent Management**, click **Settings** > **Privileges and Other Settings** > **Privileges (tab)** > **Component Updates**.
  b. Instruct users to manually update components on the agent endpoint (by right-clicking the Security Agent icon in the system tray and clicking "Update Now") to obtain the updated configuration settings.

When Security Agents update, they will receive both the updated components and the configuration files.

Using the Domains Schedule Update Tool

The update schedule configured in automatic agent updates only applies to agents with scheduled update privileges. For other agents, you can set a

separate update schedule. To do this, you will need to configure a schedule by agent tree domains. All agents belonging to the domain will apply the schedule.

Note

It is not possible to set an update schedule for a specific agent or a specific subdomain. All subdomains apply the schedule configured for their parent domain.

Procedure

1. Record the agent tree domain names and update schedules.
2. Go to <*Server installation folder*>\PCCSRV\Admin\Utility\DomainScheduledUpdate.
3. Copy the following files to <Server installation folder>\PCCSRV:
   - DomainSetting.ini
   - dsu_convert.exe
4. Open DomainSetting.ini using a text editor such as Notepad.
5. Specify the agent tree domain and then configure the update schedule for the domain. Repeat this step to add more domains.

   Note

   Detailed configuration instructions are provided in the .ini file.
6. Save DomainSetting.ini.
7. Open a command prompt and change to the directory of the PCCSRV folder.
8. Type the following command and press Enter.

   ```
   dsuconvert.exe DomainSetting.ini
   ```

9. On the web console, go to **Agents** > **Global Agent Settings**.
10. Click **Save**.

Security Agent Manual Updates

Update Security Agent components manually when Security Agent components are severely out-of-date and whenever there is an outbreak. Security Agent components become severely out-of-date when the Security Agent is unable to update components from the update source for an extended period of time.

In addition to components, Security Agents also receive updated configuration files automatically during manual update. Security Agents need the configuration files to apply new settings. Each time you modify Apex One settings through the web console, the configuration files change.

Note

In addition to initiating manual updates, you can grant users the privilege to run manual updates (also called **Update Now** on Security Agent endpoints). For details, see *Configuring Update Privileges and Other Settings on page 6-45*.

Updating Security Agents Manually

Procedure

1. Go to **Updates** > **Agents** > **Manual Update**.
2. The components currently available on the Apex One server and the date these components were last updated display on top of the screen. Ensure the components are up-to-date before notifying agents to update.

   Note

   Manually update any outdated components on the server.

   See *Security Agent Manual Updates on page 6-44* for details.

3. To update only agents with outdated components:

   a. Click **Select agents with outdated components**.

   b. (Optional) Select **Include Independent and offline agent(s)**:

      - To update Independent agents with a functional connection to the server.
      - To update offline agents when they become online.

   c. Click **Initiate Update**.

   Note

   The server searches for agents whose component versions are earlier than the versions on the server and then notifies these agents to update. To check the notification status, go to the **Updates** > **Summary** screen.

4. To update the agents of your choice:

   a. Select **Manually select agents**.

   b. Click **Select**.

   c. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.

   d. Click **Initiate Update**.

   Note

   The server starts notifying each agent to download updated components. To check the notification status, go to the **Updates** > **Summary** screen.

Configuring Update Privileges and Other Settings

Configure update settings and grant agent users certain privileges, such as performing "Update Now" and enabling scheduled update.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and configure the following options in the **Update Settings** section:

Option	Description
Security Agents download updates from the Trend Micro ActiveUpdate Server	When initiating updates, Security Agents first get updates from the update source specified on the **Updates** > **Agents** > **Update Source** screen. If the update is unsuccessful, the agents attempt to update from the Apex One server. Selecting this option enables agents to attempt to update from the Trend Micro ActiveUpdate server if the update from the Apex One server is unsuccessful. **Note** A pure IPv6 agent cannot update directly from the Trend Micro ActiveUpdate Server. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the agents to connect to the ActiveUpdate server.
Enable schedule-based updates on Apex One agents	Selecting this option configures all Security Agents to enable schedule-based updates by default. Users with the **Enable/Disable schedule-based updates** privilege may override this setting. For details on configuring the update schedule, see *Configuring Security Agent Automatic Updates on page 6-40*.
Security Agents only update the following components	This option controls how component updates proceed. Select from the following options: • **All components (including hotfixes and the agent program)**: Security Agents update all components • **Pattern files, engines, drivers**: Security Agents do not upgrade the Security Agent program or deploy hotfixes

Option	Description
	• **Pattern files**: Security Agents do not upgrade the Security Agent program, deploy hotfixes, or update engines and drivers **Note** Selecting **All components (including hotfixes and the agent program)** may significantly affect server performance as all agents simultaneously connect to the server to upgrade or install a hotfix.

5. Click the **Privileges** tab and configure the following options in the **Component Updates** section:

Option	Description
Perform "Update Now"	Users with this privilege can update components on demand by right-clicking the Security Agent icon on the system tray and selecting **Update Now**. **Note** Security Agent users can use proxy settings during "Update Now". For more information, see *Granting Proxy Configuration Privileges on page 15-55*.
Enable/ Disable schedule-based updates	Selecting this option allows Security Agent users to enable and disable scheduled updates using the Security Agent right-click menu, which can override the **Enable Schedule-based Updates** setting. **Note** Administrators must first select the **Enable schedule-based updates on Security Agents** setting on the **Other Settings** tab before the menu item appears on the Security Agent menu.

6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Configuring Reserved Disk Space for Security Agents Updates

Apex One can allocate a certain amount of agent disk space for hot fixes, pattern files, scan engines, and program updates. Apex One reserves 60MB of disk space by default.

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **System** tab.
3. Go to the **Updates** section.
4. Select **Reserve __ MB of disk space for updates**.
5. Select the amount of disk space.
6. Click **Save**.

Proxy for Security Agent Component Updates

Security Agents can use proxy settings during automatic update or if they have the privilege to perform "Update Now".

TABLE 6-8. Proxy Settings Used During Security Agent Component Updates

UPDATE METHOD	PROXY SETTINGS USED	USAGE
Automatic update	• Internal proxy settings. For more information, see *Configuring Internal Agent Proxy Settings on page 15-52*.	1. Agents apply internal proxy settings first. 2. If you do not configure internal proxy settings, agents dol not use any proxy settings.
Update Now	• Internal proxy settings. For more information, see *Configuring Internal Agent Proxy Settings on page 15-52*. • User-configured proxy settings. You can grant agent users the privilege to configure proxy settings. For more information, see *Granting Proxy Configuration Privileges on page 15-55*.	1. Agents apply internal proxy settings first. 2. If no proxy settings are enabled and agent users do not have the required privilege, agents do not use any proxy when updating components.

Configuring Security Agent Update Notifications

Apex One notifies agent users when update-related events occur.

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **Agent Control** tab.
3. Go to the **Alert Settings** section.
4. Select the following options:

- **Show the alert icon on the Windows taskbar if the virus pattern file is not updated after __ day(s)**: An alert icon displays on the Windows task bar to remind users to update a Virus Pattern that has not been updated within the specified number of days. To update the pattern, use any of the update methods discussed in *Security Agent Update Methods on page 6-37*.

  All agents managed by the server will apply this setting.

- **Display a notification message if the endpoint needs to restart to load a kernel mode driver**: After installing a hot fix or an upgrade package that contains a new version of a kernel mode driver, the driver's previous version may still exist on the endpoint. The only way to unload the previous version and load the new one is to restart the endpoint. After restarting the endpoint, the new version automatically installs and no further restart is necessary.

  The notification message displays immediately after the agent endpoint installs the hot fix or upgrade package.

5. Click **Save**.

Viewing Security Agent Update Logs

Check the agent update logs to determine if there are problems updating the Virus Pattern on agents.

Note

In this product version, only logs for Virus Pattern updates can be queried from the web console.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Procedure

1. Go to **Logs** > **Agents** > **Agent Component Update**.
2. To view the number of agent updates, click **View** under the **Progress** column. In the **Component Update Progress** screen that displays, view the number of agents updated for every 15-minute interval and the total number of agents updated.
3. To view agents that have updated the Virus Pattern, click **View** under the **Details** column.
4. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Enforcement of Security Agent Updates

Use Security Compliance to ensure that agents have the latest components. Security Compliance determines component inconsistencies between the Apex One server and agents. Inconsistencies typically occur when agents cannot connect to the server to update components. If the agent obtains an update from another source (such as the ActiveUpdate server), it is possible for a component in the agent to be newer than the one in the server.

For more information, see *Security Compliance for Managed Agents on page 15-58*.

Rolling Back Components for Security Agents

Rollback refers to reverting to the previous version of the Virus Pattern, Smart Scan Agent Pattern, and Virus Scan Engine. If these components do not function properly, roll them back to their previous versions. Apex One retains the current and the previous versions of the Virus Scan Engine, and the last five versions of the Virus Pattern and Smart Scan Agent Pattern.

Note

Only the above-mentioned components can be rolled back.

Apex One uses different scan engines for agents running 32-bit and 64-bit platforms. You need to roll back these scan engines separately. The rollback procedure for all types of scan engines is the same.

Procedure

1. Go to **Updates** > **Rollback**
2. Click **Synchronize with Server** under the appropriate section.
   a. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
   b. Click **Rollback**.
   c. Click **View Update Logs** to check the result or **Back** to return to the Rollback screen.
3. If an older version pattern file exists on the server, click **Roll Back Server and Agent Versions** to roll back the pattern file for both the agent and the server.

Running the Touch Tool for Security Agent Hot Fixes

The Touch Tool synchronizes the time stamp of one file with the time stamp of another file or with the system time of the endpoint. If you unsuccessfully attempt to deploy a hot fix on the Apex One server, use the Touch Tool to change the time stamp of the hot fix. This causes Apex One to interpret the hot fix file as new, which makes the server attempt to automatically deploy the hot fix again.

Procedure

1. On the Apex One server, go to <*Server installation folder*>`\PCCSRV\Admin\Utility\Touch`.
2. Copy `TMTouch.exe` to the folder that contains the file you want to change. If synchronizing the file time stamp with the time stamp of another file, put both files in the same location with the Touch tool.

3. Open a command prompt and go to the location of the Touch Tool.
4. Type the following:

   `TmTouch.exe <destination file name> <source file name>`

   Where:

   - `<destination file name>` is the name of the hot fix file whose time stamp you want to change
   - `<source file name>` is the name of the file whose time stamp you want to replicate

   Note

   If you do not specify a source file name, the tool sets the destination file time stamp to the system time of the endpoint. Use the wild card character (*) for the destination file, but not for the source file name.

5. To check if the time stamp changed, type `dir` in the command prompt, or check the file's properties from Windows Explorer.

Update Agents

To distribute the task of deploying components, domain settings, or agent programs and hotfixes to Security Agents, assign some Security Agents to act as Update Agents, or update sources for other Security Agents. This helps ensure that Security Agents receive updates in a timely manner without directing a significant amount of network traffic to the Apex One server.

If the network is segmented by location and the network link between segments experiences a heavy traffic load, assign at least one Update Agent on each location.

Note

Security Agents assigned to update components from an Update Agent only receive updated components and settings from the Update Agent. All Security Agents still report their status back to the Apex One server.

Update Agent System Requirements

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

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

Update Agent Configuration

Update Agent configuration is a 2-step process:

1. Assign the Security Agent as an Update Agent for specific components.
2. Specify the agents that will update from this Update Agent.

Note

The number of concurrent agent connections that a single Update Agent can handle depends on the hardware specifications of the endpoint.

Assigning Security Agents as Update Agents

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, select the agents that will be designated as Update Agents.

Note

It is not possible to select the root domain icon as this will designate all agents as Update Agents. A pure IPv6 Update Agent cannot distribute updates directly to pure IPv4 agents. Similarly, a pure IPv4 Update Agent cannot distribute updates directly to pure IPv6 agents. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Update Agent to distribute updates to the agents.

3. Click **Settings** > **Update Agent Settings**.
4. Select the items that Update Agents can share.
   - Component updates
   - Domain settings
   - Security Agent programs and hot fixes
5. Click **Save**.

Specifying the Security Agents that Update from an Update Agent

Procedure

1. Go to **Updates** > **Agents** > **Update Source**.
2. Under **Customized Update Source List**, click **Add**.
3. In the screen that displays, specify the agents' IP addresses. You can type an IPv4 range and/or an IPv6 prefix and length.
4. In the **Update Agent** field, select the Update Agent you wish to assign to the agents.

Note

Ensure that the agents can connect to the Update Agent using their IP addresses. For example, if you specified an IPv4 address range, the Update Agent must have an IPv4 address. If you specified an IPv6 prefix and length, the Update Agent must have an IPv6 address.

5. Click **Save**.

Update Sources for Update Agents

Update Agents can obtain updates from various sources, such as the Apex One server or a customized update source. Configure the update source from the web console's Update Source screen.

IPv6 Support for Update Agents

A pure IPv6 Update Agent cannot update directly from pure IPv4 update sources, such as:

- A pure IPv4 Apex One server
- Any pure IPv4 custom update source
- Trend Micro ActiveUpdate server

Similarly, a pure IPv4 Update Agent cannot update directly from pure IPv6 update sources, such as a pure IPv6 Apex One server.

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

Standard Update Source for Update Agents

The Apex One server is the standard update source for Update Agents. If you configure agents to update directly from the Apex One server, the update process proceeds as follows:

1. The Update Agent obtains updates from the Apex One server.
2. If unable to update from the Apex One server, the agent tries connecting directly to the Trend Micro ActiveUpdate server if any of the following are true:
   - In **Agents** > **Agent Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings** > **Update Settings**, the option **Security Agents download updates from the Trend Micro ActiveUpdate Server** is enabled.
   - The ActiveUpdate server is the first entry in the Customized Update Source List.

   Tip

   Place the ActiveUpdate server at the top of the list only if you experience problems updating from the Apex One server. When Update Agents update directly from the ActiveUpdate server, significant bandwidth is consumed between the network and the Internet.
3. If unable to update from all possible sources, the Update Agent quits the update process.

Customized Update Sources for Update Agents

Aside from the Apex One server, Update Agents can update from custom update sources. Custom update sources help reduce agent update traffic directed to the Apex One server. Specify the custom update sources on the Customized Update Source List, which can accommodate up to 1024 update sources. See *Customized Update Sources for Security Agents on page 6-32* for steps to configure the list.

Note

Ensure that the **Update Agents update components, domain settings, and agent programs and hot fixes, only from the Apex One server** option is disabled on the **Update Source for Agents** screen (**Updates** > **Agents** > **Update Source**) in order for Update Agents to connect to the customized update sources.

After you have set up and saved the list, the update process proceeds as follows:

1. The Update Agent updates from the first entry on the list.
2. If unable to update from the first entry, the agent updates from the second entry, and so on.
3. If unable to update from all entries, the agent checks the following options under the **Security Agents update the following items from the Apex One server if all customized sources are unavailable or not found** heading:

    - **Components**: If enabled, the agent updates from the Apex One server.

      If the option is disabled, the agent then tries connecting directly to the Trend Micro ActiveUpdate server if any of the following are true:

      Note

      You can only update components from the Active Update server. Domain settings, programs and hot fixes can only be downloaded from the server or Update Agents.

        - In **Agents** > **Agent Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings** > **Update Settings**, the option **Agents download updates from the Trend Micro ActiveUpdate Server** is enabled.
        - The ActiveUpdate server is not included in the Customized Update Source List.

    - **Domain settings**: If enabled, the agent updates from the Apex One server.
    - **Security Agent programs and hot fixes**: If enabled, the agent updates from the Apex One server.
4. If unable to update from all possible sources, the Update Agent quits the update process.

The update process is different if the option **Standard update source (update from Apex One server)** is enabled and the Apex One server notifies the agent to update components. The process is as follows:

1. The agent updates directly from the Apex One server and disregards the update source list.
2. If unable to update from the server, the agent tries connecting directly to the Trend Micro ActiveUpdate server if any of the following are true:
   - In **Agents** > **Agent Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings** > **Update Settings**, the option **Security Agents download updates from the Trend Micro ActiveUpdate Server** is enabled.
   - The ActiveUpdate server is the first entry in the Customized Update Source List.

   Tip

   Place the ActiveUpdate server at the top of the list only if you experience problems updating from the Apex One server. When Security Agents update directly from the ActiveUpdate server, significant bandwidth is consumed between the network and the Internet.
3. If unable to update from all possible sources, the Update Agent quits the update process.

Configuring the Update Source for the Update Agent

Procedure

1. Go to **Updates** > **Agents** > **Update Source**.
2. Select whether to update from the standard update source for Update Agents (Apex One server) or customized update source for update agents.
3. Click **Notify All Agents**.

Update Agent Component Duplication

Like the Apex One server, Update Agents also use component duplication when downloading components. See *Apex One Server Component Duplication on page 6-19* for details on how the server performs component duplication.

The component duplication process for Update Agents is as follows:

1. The Update Agent compares its current full pattern version with the latest version on the update source. If the difference between the two versions is 14 or less, the Update Agent downloads the incremental pattern that accounts for the difference between the two versions.

   Note

   If the difference is more than 14, the Update Agent automatically downloads the full version of the pattern file.

2. The Update Agent merges the incremental pattern it downloaded with its current full pattern to generate the latest full pattern.
3. The Update Agent downloads all the remaining incremental patterns on the update source.
4. The latest full pattern and all the incremental patterns are made available to agents.

Update Methods for Update Agents

Update Agents use the same update methods available to regular agents. For details, see *Security Agent Update Methods on page 6-37*.

You can also use the Scheduled Update Configuration tool to enable and configure scheduled updates on an Update Agent that was installed using Agent Packager.

Note

This tool is not available if the Update Agent was installed using other installation methods. See *Deployment Considerations on page 5-9* for more information.

Using the Scheduled Update Configuration Tool

Procedure

1. On the Update Agent endpoint, navigate to <*Agent installation folder*>.
2. Double-click `SUCTool.exe` to run the tool. The Schedule Update Configuration Tool console opens.
3. Select **Enable Scheduled Update**.
4. Specify the update frequency and time.
5. Click **Apply**.

Update Agent Analytical Report

Generate the Update Agent Analytical Report to analyze the update infrastructure and determine which agents download partial updates from Update Agents and other update sources.

Note

This report includes all Security Agents configured to receive partial updates from Update Agents. If you have delegated the task of managing one or several domains to other administrators, they will also see all Security Agents configured to receive partial updates from Update Agents belonging to the domains that they are not managing.

Apex One exports the Update Agent Analytical Report to a comma-separated value (`.csv`) file.

This report contains the following information:

- Security Agent endpoint
- IP address
- Agent tree path
- Update source
- If agents download the following from Update Agents:
  - Components
  - Domain settings
  - Security Agent programs and hot fixes

Important

The Update Agent Analytical Report only lists Security Agents configured to receive partial updates from an Update Agent. Security Agents configured to perform complete updates from an Update Agent (including components, domain settings, and Security Agent programs and hot fixes) do not appear in the report.

For details on generating the report, see *Customized Update Sources for Security Agents on page 6-32*.

Component Update Summary

The web console provides an **Update Summary** screen (go to **Updates** > **Summary**) that informs you of the overall component update status and lets you update outdated components. If you enable server scheduled update, the screen will also show the next update schedule.

Refresh the screen periodically to view the latest component update status.

Note

To view component updates on the integrated Smart Protection Server, go to **Administration** > **Smart Protection** > **Integrated Server**.

Update Status for Security Agents

If you initiated component update to agents, view the following information in this section:

- Number of agents notified to update components.
- Number of agents not yet notified but already in the notification queue. To cancel the notification to these agents, click **Cancel Notification**.

Components

In the **Update Status** table, view the update status for each component that the Apex One server downloads and distributes.

For each component, view its current version and the last update date. Click the number link to view agents with out-of-date components. Manually update agents with out-of-date components.

Chapter 7

Scanning for Security Risks

This chapter describes how to protect endpoints from security risks using file-based scanning.

Topics include:

About Security Risks

Security risk is the collective term for viruses/malware and spyware/grayware. Apex One protects endpoints from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak. Apex One can help contain outbreaks by enforcing outbreak prevention policies and isolating infected endpoints until they are completely risk-free. Notifications and logs help you keep track of security risks and alert you if you need to take immediate action.

Viruses and Malware

Tens of thousands of virus/malware exist, with more being created each day. Although once most common in DOS or Windows, endpoint viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and websites.

TABLE 7-1. Virus/Malware Types

VIRUS / MALWARE TYPE	DESCRIPTION
Joke program	Joke programs are virus-like programs that often manipulate the appearance of things on the endpoint's monitor.
Others	"Others" include viruses/malware not categorized under any of the other virus/malware types.
Packer	Packers are compressed and/or encrypted Windows or Linux™ executable programs, often a Trojan horse program. Compressing executables makes packers more difficult for antivirus products to detect.
Ransomware	Ransomware is a type of threat that encrypts, modifies, or locks files and then attempts to extort the user into paying some sort of ransom demand to retrieve the data. Some ransomware threats automatically delete the data if the ransom is not paid in time.

Virus / Malware Type	Description
Rootkit	Rootkits are programs (or collections of programs) that install and execute code on a system without end user consent or knowledge. They use stealth to maintain a persistent and undetectable presence on the machine. Rootkits do not infect machines, but rather, seek to provide an undetectable environment for malicious code to execute. Rootkits are installed on systems via social engineering, upon execution of malware, or simply by browsing a malicious website. Once installed, an attacker can perform virtually any function on the system to include remote access, eavesdropping, as well as hide processes, files, registry keys and communication channels.
Test virus	Test viruses are inert files that act like a real virus and are detectable by virus-scanning software. Use test viruses, such as the EICAR test script, to verify that your antivirus installation scans properly.
Trojan horse	Trojan horse programs often use ports to gain access to computers or executable programs. Trojan horse programs do not replicate but instead reside on systems to perform malicious acts, such as opening ports for hackers to enter. Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those already running on the system.

Virus / Malware Type	Description
Virus	Viruses are programs that replicate. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes, including: • **ActiveX malicious code**: Code that resides on web pages that execute ActiveX™ controls. • **Boot sector virus**: A virus that infects the boot sector of a partition or a disk. • **COM and EXE file infector**: An executable program with `.com` or `.exe` extension. • **Java malicious code**: Operating system-independent virus code written or embedded in Java™. • **Macro virus**: A virus encoded as an application macro and often included in a document. • **VBScript**, **JavaScript** or **HTML virus**: A virus that resides on web pages and downloaded through a browser. • **Worm**: A self-contained program or set of programs able to spread functional copies of itself or its segments to other endpoint systems, often through email.
Network Virus	A virus spreading over a network is not, strictly speaking, a network virus. Only some virus/malware types, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of agent endpoints, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.

Virus / Malware Type	Description
Probable virus/ malware	Probable viruses/malware are suspicious files that have some of the characteristics of viruses/malware. For details, see the Trend Micro Threat Encyclopedia: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware **Note** Clean cannot be performed on probable virus/malware, but the scan action is configurable.

Spyware and Grayware

Endpoints are at risk from potential threats other than viruses/malware. Spyware/Grayware refers to applications or files not classified as viruses or Trojans, but can still negatively affect the performance of the endpoints on your network and introduce significant security, confidentiality, and legal risks to your organization. Often spyware/grayware performs a variety of undesired and threatening actions such as irritating users with pop-up windows, logging user keystrokes, and exposing endpoint vulnerabilities to attack.

If you find an application or file that Trend Micro Apex One cannot detect as grayware but you think is a type of grayware, send it to Trend Micro for analysis:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Type	Description
Spyware	Gathers data, such as account user names and passwords, and transmits them to third parties.
Adware	Displays advertisements and gathers data, such as user web surfing preferences, used for targeting advertisements at the user through a web browser.

Type	Description
Dialer	Changes endpoint Internet settings and can force the endpoint to dial pre-configured phone numbers through a modem. These are often pay-per-call or international numbers that can result in a significant expense for your organization.
Joke program	Causes abnormal endpoint behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes.
Hacking tool	Helps hackers enter endpoints.
Remote access tool	Helps hackers remotely access and control endpoints.
Password cracking application	Helps hackers decipher account user names and passwords.
Others	Other types of potentially malicious programs.

How Spyware/Grayware Gets into the Network

Spyware/Grayware often gets into a corporate network when users download legitimate software that have grayware applications included in the installation package. Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the application and its intended use to collect personal data; however, users often overlook this information or do not understand the legal jargon.

Potential Risks and Threats

The existence of spyware and other types of grayware on the network has the potential to introduce the following:

TABLE 7-2. Potential Risks and Threats

RISK OR THREAT	DESCRIPTION
Reduced Endpoint Performance	To perform their tasks, spyware/grayware applications often require significant CPU and system memory resources.
Increased Web Browser-related Crashes	Certain types of grayware, such as adware, often display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require the endpoint to restart.
Reduced User Efficiency	By needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users become unnecessarily distracted from their main tasks.
Degradation of Network Bandwidth	Spyware/Grayware applications often regularly transmit the data they collect to other applications running on or outside the network.
Loss of Personal and Corporate Information	Not all data spyware/grayware applications collect is as innocuous as a list of websites users visit. Spyware/Grayware can also collect user credentials, such as those used to access online banking accounts and corporate networks.
Higher Risk of Legal Liability	If endpoint resources on the network are hijacked, hackers may be able to utilize agent computers to launch attacks or install spyware/grayware on computers outside the network. The participation of network resources in these types of activities could leave an organization legally liable to damages incurred by other parties.

Guarding Against Spyware/Grayware and Other Threats

There are many steps you can take to prevent the installation of spyware/grayware onto your endpoint. Trend Micro suggests the following:

- Configure all types of scans (Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now) to scan for and remove spyware/grayware files and applications. See *Scan Types on page 7-14* for more information.
- Educate your agent users to do the following:

  - Read the End User License Agreement (EULA) and included documentation of applications they download and install on their computers.
  - Click **No** to any message asking for authorization to download and install software unless agent users are certain both the creator of the software and the website they view are trustworthy.
  - Disregard unsolicited commercial email (spam), especially if the spam asks users to click a button or hyperlink.
- Configure web browser settings that ensure a strict level of security. Trend Micro recommends requiring web browsers to prompt users before installing ActiveX controls.
- If using Microsoft Outlook, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages.
- Do not allow the use of peer-to-peer file-sharing services. Spyware and other grayware applications may be masked as other types of files your users may want to download, such as MP3 music files.
- Periodically examine the installed software on your agent computers and look for applications that may be spyware or other grayware.
- Keep your Windows operating systems updated with the latest patches from Microsoft. See the Microsoft website for details.

Scan Method Types

Security Agents can use one of two scan methods when scanning for security risks. The scan methods are smart scan and conventional scan.

- **Smart Scan**

  Security Agents that use smart scan are referred to as **smart scan agents** in this document. Smart scan agents benefit from local scans and in-the-cloud queries provided by File Reputation Services.

- **Conventional Scan**

  Agents that do not use smart scan are called **conventional scan agents**. A conventional scan agent stores all Security Agent components on the endpoint and scans all files locally.

Default Scan Method

In this Apex One version, the default scan method for fresh installations is smart scan. This means that if you perform a fresh Apex One server installation and do not change the scan method on the web console, all agents that the server manages use smart scan.

If you upgrade the Apex One server from an earlier version and automatic agent upgrade is enabled, all agents managed by the server still use the scan method configured before the upgrade. For example, if you upgrade from a previous version of Apex One that supports smart scan and conventional scan, all upgraded agents that use smart scan continue to use smart scan and all agents using conventional scan continue to use conventional scan.

Scan Methods Compared

The following table provides a comparison between the two scan methods:

TABLE 7-3. Conventional Scan and Smart Scan Compared

BASIS OF COMPARISON	CONVENTIONAL SCAN	SMART SCAN
Scanning behavior	The conventional scan Security Agent performs scanning on the local endpoint.	• The smart scan Security Agent performs scanning on the local endpoint. • If the Security Agent cannot determine the risk of the file during the scan, the Security Agent verifies the risk by sending a scan query to a smart protection source. • The Security Agent "caches" the scan query result to improve the scan performance.
Components in use and updated	All components available on the update source, except the Smart Scan Agent Pattern	All components available on the update source, except the Virus Pattern and Spyware Active-monitoring Pattern
Typical update source	Apex One server	Apex One server

Changing the Scan Method

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Scan Settings** > **Scan Methods**.
4. Select **Conventional scan** or **Smart scan**.
5. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Switching from Smart Scan to Conventional Scan

The following table outlines some considerations you should be aware of before switching the scan method that Security Agents use.

1. Number of Security Agents to switch

   Switching a relatively small number of Security Agents at a time allows efficient use of the Apex One server and Smart Protection Server resources. These servers can perform other critical tasks while Security Agents change scan methods.

2. Timing

   When switching scan methods, Security Agents need to download full versions of the required pattern files for the new scan method.

   Consider switching during off-peak hours to minimize the impact to network bandwidth and interruption to end user daily operations. Trend Micro recommends disabling "Update Now" on Security Agents during the conversion process.

3. Agent tree settings

   Scan method is a granular setting that you can apply on the root, domain, or individual Security Agent level. When switching the scan method, you can:

   - Create a new agent tree domain and assign conventional scan as its scan method. Any agent you move to this domain will use conventional scan. When you move the agent, enable the setting **Apply settings of new domain to selected agents**.

- Select a domain and configure it to use conventional scan. Smart scan agents belonging to the domain will switch to conventional scan.
- Select one or several smart scan agents from a domain and then switch them to conventional scan.

Note

Any changes to the domain's scan method overrides the scan method you have configured for individual agents.

Switching from Conventional Scan to Smart Scan

If you are switching agents from conventional scan to smart scan, ensure that you have set up Smart Protection Services.

For details, see *Setting Up Smart Protection Services on page 4-13*.

The following table provides other considerations when switching to smart scan.

TABLE 7-4. Considerations When Switching to Smart Scan

CONSIDERATION	DETAILS
Product license	To use smart scan, ensure that you have activated the licenses for the following services and that the licenses are not expired: • Antivirus • Web Reputation and Anti-spyware

Consideration	Details
Apex One server	Ensure that agents can connect to the Apex One server. Only online agents will be notified to switch to smart scan. Offline agents get notified when they become online. Independent agents are notified when they become online or, if the agent has scheduled update privileges, when scheduled update runs. Also verify that the Apex One server has the latest components because smart scan agents need to download the Smart Scan Agent Pattern from the server. To update components, see *Apex One Server Updates on page 6-14*.
Number of agents to switch	Switching a relatively small number of agents at a time allows efficient use of Apex One server resources. The Apex One server can perform other critical tasks while agents change their scan methods.
Timing	When switching to smart scan for the first time, agents need to download the full version of the Smart Scan Agent Pattern from the Apex One server. The Smart Scan Pattern is only used by smart scan agents. Consider switching during off-peak hours to ensure the download process finishes within a short amount of time. Also consider switching when no agent is scheduled to update from the server. Also temporarily disable "Update Now" on agents and re-enable it after the agents have switched to smart scan.

Consideration	Details
Agent tree settings	Scan method is a granular setting that can be set on the root, domain, or individual agent level. When switching to smart scan, you can: • Create a new agent tree domain and assign smart scan as its scan method. Any agent you move to this domain will use smart scan. When you move the agent, enable the setting **Apply settings of new domain to selected agents**. • Select a domain and configure it to use smart scan. Conventional scan agents belonging to the domain will switch to smart scan. • Select one or several conventional scan agents from a domain and then switch them to smart scan. **Note** Any changes to the domain's scan method overrides the scan method you have configured for individual agents.
IPv6 support	Smart scan agents send scan queries to smart protection sources. A pure IPv6 smart scan agent cannot send queries directly to pure IPv4 sources, such as: • Trend Micro Smart Protection Network Similarly, a pure IPv4 smart scan agent cannot send queries to pure IPv6 Smart Protection Servers. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow smart scan agents to connect to the sources.

Scan Types

Apex One provides the following scan types to protect Security Agent computers from security risks:

TABLE 7-5. Scan Types

SCAN TYPE	DESCRIPTION
Real-time Scan	Automatically scans a file on the endpoint as it is received, opened, downloaded, copied, or modified See *Real-time Scan on page 7-15* for details.
Manual Scan	A user-initiated scan that scans a file or a set of files requested by the user See *Manual Scan on page 7-18* for details.
Scheduled Scan	Automatically scans files on the endpoint based on the schedule configured by the administrator or end user See *Scheduled Scan on page 7-20* for details.
Scan Now	An administrator-initiated scan that scans files on one or several target computers See *Scan Now on page 7-22* for details.

Real-time Scan

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If the Security Agent does not detect a security risk, users can proceed to access the file. If the Security Agent detects a security risk or a probable virus/malware, a notification message displays indicating the name of the infected file and the specific security risk.

Real-time Scan maintains a persistent scan cache which reloads each time the Security Agent starts. The Security Agent tracks any changes to files or folders that occurred since the Security Agent unloaded and removes these files from the cache.

Note

To modify the notification message, open the web console and go to **Administration** > **Notifications** > **Agent**.

Configure and apply Real-time Scan settings to one or several Security Agents and domains, or to all Security Agents that the server manages.

Configuring Real-time Scan Settings

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Scan Settings** > **Real-time Scan Settings**.
4. Select the following options:
   - **Enable virus/malware scan**
   - **Enable spyware/grayware scan**

   Note

   If you disable virus/malware scanning, spyware/grayware scanning also becomes disabled. During a virus outbreak, Real-time Scan cannot be disabled (or will automatically be enabled if initially disabled) to prevent the virus from modifying or deleting files and folders on agent computers.
5. On the **Target** tab, configure the following:
   - *User Activity on Files on page 7-26*
   - *Files to Scan on page 7-27*
   - *Scan Settings on page 7-27*
6. Click the **Action** tab and then configure the following:

TABLE 7-6. Scan Actions

ACTION	REFERENCE
Virus/Malware action	Primary action (select one): • *Use ActiveAction on page 7-38* • *Use the Same Action for all Virus/Malware Types on page 7-40* • *Use a Specific Action for Each Virus/Malware Type on page 7-40* **Note** For details about the different actions, see *Virus/Malware Scan Actions on page 7-37*. Additional virus/malware actions: • *Quarantine Directory on page 7-40* • *Back Up Files Before Cleaning on page 7-42* • *Damage Cleanup Services on page 7-42* • *Display a Notification Message When Virus/Malware is Detected on page 7-44* • *Display a Notification Message When Probable Virus/Malware is Detected on page 7-44*
Spyware/Grayware action	Primary action: • *Spyware/Grayware Scan Actions on page 7-49* Additional spyware/grayware action: • *Display a Notification Message When Spyware/Grayware is Detected on page 7-50*

7. On the **Scan Exclusion** tab, configure the directories, files, and extensions to exclude from scanning.

   For details, see *Scan Exclusions on page 7-31*.

8. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Manual Scan

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the Security Agent console. The time it takes to complete scanning depends on the number of files to scan and the Security Agent endpoint's hardware resources.

Configure and apply Manual Scan settings to one or several agents and domains, or to all agents that the server manages.

Configuring Manual Scan Settings

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Scan Settings** > **Manual Scan Settings**.
4. On the **Target** tab, configure the following:
   - *Files to Scan on page 7-27*
   - *Scan Settings on page 7-27*

- *CPU Usage on page 7-30*

5. Click the **Action** tab and then configure the following:

TABLE 7-7. Scan Actions

ACTION	REFERENCE
Virus/Malware action	Primary action (select one): • *Use ActiveAction on page 7-38* • *Use the Same Action for all Virus/Malware Types on page 7-40* • *Use a Specific Action for Each Virus/Malware Type on page 7-40* **Note** For details about the different actions, see *Virus/Malware Scan Actions on page 7-37*. Additional virus/malware actions: • *Quarantine Directory on page 7-40* • *Back Up Files Before Cleaning on page 7-42* • *Damage Cleanup Services on page 7-42*
Spyware/Grayware action	Primary action: • *Spyware/Grayware Scan Actions on page 7-49*

6. On the **Scan Exclusion** tab, configure the directories, files, and extensions to exclude from scanning.

   For details, see *Scan Exclusions on page 7-31*.

7. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Scheduled Scan

Scheduled Scan runs automatically on the appointed date and time. Use Scheduled Scan to automate routine scans on the agent and improve scan management efficiency.

Configure and apply Scheduled Scan settings to one or several agents and domains, or to all agents that the server manages.

Configuring Scheduled Scan Settings

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Scan Settings** > **Scheduled Scan Settings**.
4. Select the following options:
   - **Enable virus/malware scan**
   - **Enable spyware/grayware scan**

   Note

   You must enable virus/malware scanning before you can enable spyware/grayware scanning.
5. On the **Target** tab, configure the following:
   - *Schedule on page 7-30*

- *Files to Scan on page 7-27*
- *Scan Settings on page 7-27*
- *CPU Usage on page 7-30*

6. Click the **Action** tab and then configure the following:

TABLE 7-8. Scan Actions

ACTION	REFERENCE
Virus/Malware action	Primary action (select one): • *Use ActiveAction on page 7-38* • *Use the Same Action for all Virus/Malware Types on page 7-40* • *Use a Specific Action for Each Virus/Malware Type on page 7-40* **Note** For details about the different actions, see *Virus/Malware Scan Actions on page 7-37*. Additional virus/malware actions: • *Quarantine Directory on page 7-40* • *Back Up Files Before Cleaning on page 7-42* • *Damage Cleanup Services on page 7-42* • *Display a Notification Message When Virus/Malware is Detected on page 7-44* • *Display a Notification Message When Probable Virus/Malware is Detected on page 7-44*

Action	Reference
Spyware/Grayware action	Primary action: • *Spyware/Grayware Scan Actions on page 7-49* Additional spyware/grayware action: • *Display a Notification Message When Spyware/Grayware is Detected on page 7-50*

7. On the **Scan Exclusion** tab, configure the directories, files, and extensions to exclude from scanning.

   For details, see *Scan Exclusions on page 7-31*.

8. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Scan Now

Scan Now is initiated remotely by administrators through the web console and can be targeted to one or several Security Agent endpoints.

Configure and apply Scan Now settings to one or several Security Agents and domains, or to all Security Agents that the server manages.

Configuring Scan Now Settings

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Scan Settings** > **Scan Now Settings**.
4. Select the following options:
   - **Enable virus/malware scan**
   - **Enable spyware/grayware scan**

   Note

   You must enable virus/malware scanning before you can enable spyware/grayware scanning.
5. On the **Target** tab, configure the following:
   - *Files to Scan on page 7-27*
   - *Scan Settings on page 7-27*
   - *CPU Usage on page 7-30*
6. Click the **Action** tab and then configure the following:

TABLE 7-9. Scan Actions

ACTION	REFERENCE
Virus/Malware action	Primary action (select one): • *Use ActiveAction on page 7-38* • *Use the Same Action for all Virus/Malware Types on page 7-40* • *Use a Specific Action for Each Virus/Malware Type on page 7-40* **Note** For details about the different actions, see *Virus/Malware Scan Actions on page 7-37*. Additional virus/malware actions: • *Quarantine Directory on page 7-40* • *Back Up Files Before Cleaning on page 7-42* • *Damage Cleanup Services on page 7-42*
Spyware/Grayware action	Primary action: • *Spyware/Grayware Scan Actions on page 7-49*

7. On the **Scan Exclusion** tab, configure the directories, files, and extensions to exclude from scanning.

   For details, see *Scan Exclusions on page 7-31*.

8. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Initiating Scan Now

Initiate Scan Now on computers that you suspect to be infected.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Tasks** > **Scan Now**.
4. To change the pre-configured **Scan Now** settings before initiating the scan, click **Settings**.

   The **Scan Now Settings** screen opens. See *Scan Now on page 7-22* for details.
5. In the agent tree, select the agents that will perform scanning and then click **Initiate Scan Now**.

   The server sends a notification to the agents.
6. Check the notification status and see if there are agents that did not receive the notification.
7. Click **Select Unnotified Endpoints** and then **Initiate Scan Now** to immediately resend the notification to un-notified agents.

   Example: Total number of agents: 50

TABLE 7-10. Un-notified Agent Scenarios

AGENT TREE SELECTION	NOTIFIED AGENTS (AFTER CLICKING "INITIATE SCAN NOW")	UN-NOTIFIED AGENTS
None (all 50 agents automatically selected)	35 out of 50 agents	15 agents
Manual selection (45 out of 50 agents selected)	40 out of 45 agents	5 agents + another 5 agents not included in the manual selection

8. Click **Stop Notification** to prompt Apex One to stop notifying agents currently being notified. Agents already notified and in the process of scanning will ignore this command.
9. For agents already in the process of scanning, click **Stop Scan Now** to notify them to stop scanning.

Settings Common to All Scan Types

For each scan type, configure three sets of settings: scan criteria, scan exclusions, and scan actions. Deploy these settings to one or several agents and domains, or to all agents that the server manages.

Scan Criteria

Specify which files a particular scan type should scan using file attributes such as file type and extension. Also specify conditions that will trigger scanning. For example, configure Real-time Scan to scan each file after it is downloaded to the endpoint.

User Activity on Files

Choose activities on files that will trigger Real-time Scan. Select from the following options:

- **Scan files being created/modified**: Scans new files introduced into the endpoint (for example, after downloading a file) or files being modified
- **Scan files being retrieved**: Scans files as they are opened
- **Scan files being created/modified and retrieved**

For example, if the third option is selected, a new file downloaded to the endpoint will be scanned and stays in its current location if no security risk is detected. The same file will be scanned when a user opens the file and, if the user modified the file, before the modifications are saved.

Files to Scan

Select from the following options:

- **All scannable files**: Scan all files
- **File types scanned by IntelliScan**: Only scan files known to potentially harbor malicious code, including files disguised by a harmless extension name.

  See *IntelliScan on page D-6* for details.
- **Files with the following extensions**: Only scan files whose extensions are included in the file extension list. Add new extensions or remove any of the existing extensions.

Scan Settings

Select one or more of the following options:

- **Scan floppy disk during system shutdown**: Real-time Scan scans any floppy disk for boot viruses before shutting down the endpoint. This prevents any virus/malware from executing when a user reboots the endpoint from the disk.
- **Scan hidden folders**: Allows Apex One to detect and then scan hidden folders on the endpoint during Manual Scan

- **Scan network drive**: Scans network drives or folders mapped to the Security Agent endpoint during Manual Scan or Real-time Scan.
- **Scan the boot sector of the USB storage device after plugging in**: Automatically scans only the boot sector of a USB storage device every time the user plugs it in (Real-time Scan).
- **Scan all files in removable storage devices after plugging in**: Automatically scans all files on a USB storage device every time the user plugs it in (Real-time Scan).
- **Quarantine malware variants detected in memory**: Behavior Monitoring scans the system memory for suspicious processes and Real-time Scan maps the process and scans it for malware threats. If a malware threat exists, Real-Time scan quarantines the process and/or file.

Note

- This feature requires that administrators enable the Unauthorized Change Prevention Service and the Advanced Protection Service.
- Memory scanning works in conjunction with Anti-exploit Protection in Behavior Monitoring to provide enhanced protection against Fileless Attacks.

- **Scan compressed files**: Allows Apex One to scan up to a specified number of compression layers and skip scanning any excess layers. Apex One also cleans or deletes infected files within compressed files. For example, if the maximum is two layers and a compressed file to be scanned has six layers, Apex One scans two layers and skips the remaining four. If a compressed file contains security threats, Apex One cleans or deletes the file.

Note

Apex One treats Microsoft Office 2007 files in Office Open XML format as compressed files. Office Open XML, the file format for Office 2007 applications, uses ZIP compression technologies. If you want files created using these applications to be scanned for viruses/malware, you need to enable scanning of compressed files.

- **Scan OLE objects**: When a file contains multiple Object Linking and Embedding (OLE) layers, Apex One scans the specified number of layers and ignores the remaining layers.

  All agents managed by the server check this setting during Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now. Each layer is scanned for virus/malware and spyware/grayware.

  For example:

  The number of layers you specify is 2. Embedded within a file is a Microsoft Word document (first layer), within the Word document is a Microsoft Excel spreadsheet (second layer), and within the spreadsheet is an `.exe` file (third layer). Apex One will scan the Word document and Excel spreadsheet, and skip the `.exe` file.

  - **Detect exploit code in OLE files**: OLE Exploit Detection heuristically identifies malware by checking Microsoft Office files for exploit code.

    Note

    The specified number of layers is applicable to both **Scan OLE objects** and **Detect exploit code** options.

- **Enable IntelliTrap**: Detects and removes virus/malware on compressed executable files. This option is available only for Real-time Scan.

  See *IntelliTrap on page D-6* for details.

- **Enable CVE exploit scanning for files downloaded through web and email channels**: Blocks processes that attempt to exploit known vulnerabilities in commercially available products based on the Common Vulnerabilities and Exposures (CVE) system. This option is available only for Real-time Scan.

- **Scan boot area**: Scans the boot sector of the hard disk for virus/malware during Manual Scan, Scheduled Scan and Scan Now

CPU Usage

Apex One can pause after scanning one file and before scanning the next file. This setting is used during Manual Scan, Scheduled Scan, and Scan Now.

Select from the following options:

- **High**: No pausing between scans
- **Medium**: Pause between file scans if CPU consumption is higher than 50%, and do not pause if 50% or lower
- **Low**: Pause between file scans if CPU consumption is higher than 20%, and do not pause if 20% or lower

If you choose Medium or Low, when scanning is launched and CPU consumption is within the threshold (50% or 20%), Apex One will not pause between scans, resulting in faster scanning time. Apex One uses more CPU resource in the process but because CPU consumption is optimal, endpoint performance is not drastically affected. When CPU consumption begins to exceed the threshold, Apex One pauses to reduce CPU usage, and stops pausing when consumption is within the threshold again.

If you choose High, Apex One does not check the actual CPU consumption and scans files without pausing.

Schedule

Configure how often (daily, weekly, or monthly) and what time Scheduled Scan will run.

For monthly Scheduled Scans, you can choose either a particular day of a month or a day of a week and the order of its occurrence.

- **A particular day of a month**: Select between the 1st and 31st day. If you selected the 29th, 30th, or 31st day and a month does not have this day, Apex One runs Scheduled Scan on the last day of the month. Therefore:
  - If you selected 29, Scheduled Scan runs on February 28 (except on a leap year) and on the 29th day of all the other months.

- If you selected 30, Scheduled Scan runs on February 28 or 29, and on the 30th day of all the other months.
- If you selected 31, Scheduled Scan runs on February 28 or 29, April 30, June 30, September 30, November 30, and on the 31st day of all the other months.

- **A day of a week and the order of its occurrence**: A day of a week occurs four or five times a month. For example, there are typically four Mondays in a month. Specify a day of a week and the order in which it occurs during a month. For example, choose to run Scheduled Scan on the second Monday of each month. If you choose the fifth occurrence of a day and it does not exist during a particular month, the scan runs on the fourth occurrence.

Scan Exclusions

Configure scan exclusions to increase the scanning performance and skip scanning files causing false alarms. When a particular scan type runs, Apex One checks the scan exclusion list to determine which files on the endpoint will be excluded from both virus/malware and spyware/grayware scanning.

When you enable scan exclusion, Apex One will not scan a file under the following conditions:

- The file is found under a specific directory (or any of its sub-directories).
- The file name matches any of the names in the exclusion list.
- The file extension matches any of the extensions in the exclusion list.

Tip

For a list of products that Trend Micro recommends excluding from Real-Time scans, go to:

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

Wildcard Exceptions

Scan exclusion lists for files and directories support the use of wildcard characters. Use the "?" character to replace one character and "*" to replace several characters.

Use wildcard characters cautiously. Using the wrong character might exclude incorrect files or directories. For example, adding `C:\*` to the Scan Exclusion List (Files) would exclude the entire `C:\` drive.

TABLE 7-11. Scan Exclusions Using Wildcard Characters

VALUE	EXCLUDED	NOT EXCLUDED

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	All `.txt` files in the `C:\` directory	All other file types in the `C:\` directory
`[]`	Not supported	Not supported

Scan Exclusion List (Directories)

Apex One will not scan all files found under a specific directory on the computer. You can specify a maximum of 256 directories.

Note

By excluding a directory from scans, Apex One automatically excludes all of the directory's sub-directories from scans.

You can also choose **Exclude directories where Trend Micro products are installed**. If you select this option, Apex One automatically excludes the directories of the following Trend Micro products from scanning:

- <*Server installation folder*>

  Note

  During a Manual Scan, Apex One still scans the server installation folder.

- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ for Microsoft Exchange

If you have a Trend Micro product NOT included in the list, add the product directories to the scan exclusion list.

Also configure Apex One to exclude Microsoft Exchange 2000/2003 directories by going to the **Scan Settings** section of **Agents** > **Global Agent Settings** on the **Security Settings** tab. If you use Microsoft Exchange 2007 or

later, manually add the directory to the scan exclusion list. Refer to the following site for scan exclusion details:

http://technet.microsoft.com/en-us/library/bb332342.aspx

When you configure the file list, choose from the following options:

- **Retains current list** (default): Apex One provides this option to prevent the accidental overwriting of the agent's existing exclusion list. In order to save and deploy changes made to the exclusion list, select any of the other options.
- **Overwrites**: This option removes and replaces the entire exclusion list on the agent with the current list. After clicking **Apply to All Agents**, Apex One displays a confirmation warning message.
- **Adds paths to**: This option adds the items in the current list to the agent's existing exclusion list. If an item already exists in the agent's exclusion list, the agent ignores the item.
- **Removes paths from**: This option removes the items in the current list from the agent's existing exclusion list, if found.

Supported System Variables for Scan Exclusion List (Directories)

You can configure the Scan Exclusion List of directories using common Windows system variables. The following table displays the variables supported by Apex One.

System Variable	Description
%ALLUSERSPROFILE%	Refers to the `%PROFILESFOLDER%\Public` or `%PROFILESFOLDER%\all users` folders For example: • The default location of %ALLUSERSPROFILE% in Windows 7: `C:\ProgramData`

System Variable	Description
%COMMONPROGRAMFILES(X86)%	Refers to the `C:\Program Files (x86)\Common Files` folder on 64-bit systems
%PROGRAMFILES%	The Program Files folder A typical path is `C:\Program Files`
%PROGRAMFILES(X86)%	Refers to the `C:\Program Files (x86)` folder on 64-bit systems
%SYSTEMROOT%	Refers to the root of the system drive A typical path is `C:\Windows`
%WINDIR%	Refers to the Windows folder located on the system drive A typical path is `C:\Windows`

Scan Exclusion List (Files)

Apex One will not scan a file if its file name matches any of the names included in this exclusion list. If you want to exclude a file found under a specific location on the endpoint, include the file path, such as `C:\Temp\sample.jpg`.

You can specify a maximum of 256 files.

When you configure the file list, choose from the following options:

- **Retains current list** (default): Apex One provides this option to prevent the accidental overwriting of the agent's existing exclusion list. In order to save and deploy changes made to the exclusion list, select any of the other options.
- **Overwrites**: This option removes and replaces the entire exclusion list on the agent with the current list. After clicking **Apply to All Agents**, Apex One displays a confirmation warning message.
- **Adds paths to**: This option adds the items in the current list to the agent's existing exclusion list. If an item already exists in the agent's exclusion list, the agent ignores the item.

- **Removes paths from**: This option removes the items in the current list from the agent's existing exclusion list, if found.

Scan Exclusion List (File Extensions)

Apex One will not scan a file if its file extension matches any of the extensions included in this exclusion list. You can specify a maximum of 256 file extensions. A period (.) is not required before the extension.

For Manual Scan, Scheduled Scan, and Scan Now, use a question mark (?) to replace a single character or an asterisk (*) to replace multiple characters as wildcard characters. For example, if you do not want to scan all files with extensions starting with D, such as `DOC`, `DOT`, or `DAT`, type `D*` or `D??`.

Note

Real-time Scan does not support the use of wildcard characters when specifying extensions.

Apply Scan Exclusion Settings to All Scan Types

Apex One allows you to configure scan exclusion settings for a particular scan type and then apply the same settings to all the other scan types. For example:

On January 1, Apex One administrator Chris found out that there are a large number of `JPG` files on agent computers and realized that these files do not pose any security threat. Chris added `JPG` in the file exclusion list for Manual Scan and then applied this setting to all scan types. Real-time Scan, Scan Now, and Scheduled Scan are now set to skip scanning `.jpg` files.

A week later, Chris removed `JPG` from the exclusion list for Real-time Scan but did not apply scan exclusion settings to all scan types. `JPG` files will now be scanned but only during Real-time Scan.

Scan Actions

Specify the action Apex One performs when a particular scan type detects a security risk. Apex One has a different set of scan actions for virus/malware and spyware/grayware.

Virus/Malware Scan Actions

The scan action Apex One performs depends on the virus/malware type and the scan type that detected the virus/malware. For example, when Apex One detects a Trojan horse program (virus/malware type) during Manual Scan (scan type), it cleans (action) the infected file.

For information on the different virus/malware types, see *Viruses and Malware on page 7-2*.

The following are the actions Apex One can perform against viruses/malware.

TABLE 7-12. Virus/Malware Scan Actions

ACTION	DESCRIPTION
Delete	Apex One deletes the infected file.
Quarantine	Apex One renames,encrypts, and moves the infected file to a temporary quarantine directory on the agent endpoint located in <*Agent installation folder*>\Suspect. The Security Agent then sends quarantined files to the designated quarantine directory. See *Quarantine Directory on page 7-40* for details. The default quarantine directory is on the Apex One server, under <*Server installation folder*>\PCCSRV\Virus. If you need to restore any of the quarantined files, use Central Quarantine Restore. For details, see *Restoring Quarantined Files on page 7-44*.

Action	Description
Clean	Apex One cleans the infected file before allowing full access to the file. If the file is uncleanable, Apex One performs a second action, which can be one of the following actions: Quarantine, Delete, Rename, and Pass. To configure the second action, go to **Agents** > **Agent Management**. Click **Settings** > **Scan Settings** > **{Scan Type}** > **Action** tab. This action can be performed on all types of malware except probable virus/malware.
Rename	Apex One changes the infected file's extension to "`vir`". Users cannot open the renamed file initially, but can do so if they associate the file with a certain application. The virus/malware may execute when opening the renamed infected file.
Pass	Apex One can only use this scan action when it detects any type of virus during Manual Scan, Scheduled Scan, and Scan Now. Apex One cannot use this scan action during Real-time Scan because performing no action when an attempt to open or execute an infected file is detected will allow virus/malware to execute. All the other scan actions can be used during Real-time Scan.
Deny Access	This scan action can only be performed during Real-time Scan. When Apex One detects an attempt to open or execute an infected file, it immediately blocks the operation. Users can manually delete the infected file.

Use ActiveAction

Different types of virus/malware require different scan actions. Customizing scan actions requires knowledge about virus/malware and can be a tedious task. Apex One uses ActiveAction to counter these issues.

ActiveAction is a set of pre-configured scan actions for viruses/malware. If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus/malware, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:

- ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- Virus writers constantly change the way virus/malware attack computers. ActiveAction settings are updated to protect against the latest threats and the latest methods of virus/malware attacks.

Note

ActiveAction is not available for spyware/grayware scan.

The following table illustrates how ActiveAction handles each type of virus/malware:

TABLE 7-13. Trend Micro Recommended Scan Actions Against Viruses and Malware

VIRUS/MALWARE TYPE	REAL-TIME SCAN		MANUAL SCAN/SCHEDULED SCAN/SCAN NOW	
	FIRST ACTION	SECOND ACTION	FIRST ACTION	SECOND ACTION
CVE exploit	Deny Access	N/A	N/A	N/A
Joke	Quarantine	N/A	Quarantine	N/A
Trojans	Quarantine	N/A	Quarantine	N/A
Virus	Clean	Quarantine	Clean	Quarantine
Test virus	Deny Access	N/A	Pass	N/A
Packer	Quarantine	N/A	Quarantine	N/A
Probable malware	Deny Access or user-configured action	N/A	Pass or user-configured action	N/A
Other malware	Clean	Quarantine	Clean	Quarantine

For probable malware, the default action is "Deny Access" during Real-time Scan and "Pass" during Manual Scan, Scheduled Scan, and Scan Now. If these

are not your preferred actions, you can change them to Quarantine, Delete, or Rename.

Use the Same Action for all Virus/Malware Types

Select this option if you want the same action performed on all types of virus/malware, except probable virus/malware. If you choose "Clean" as the first action, select a second action that Apex One performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable.

If you choose "Clean" as the first action, Apex One performs the second action when it detects probable virus/malware.

Use a Specific Action for Each Virus/Malware Type

Manually select a scan action for each virus/malware type.

For all virus/malware types except probable virus/malware, all scan actions are available. If you choose "Clean" as the first action, select a second action that Apex One performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable.

For probable virus/malware, all scan actions, except "Clean", are available.

Quarantine Directory

If the action for an infected file is "Quarantine", the Security Agent encrypts the file and moves it to a temporary quarantine folder located in <*Agent installation folder*>\SUSPECT and then sends the file to the designated quarantine directory.

Note

You can restore encrypted quarantined files in case you need to access them in the future.

For details, see *Restoring Encrypted Files on page 7-46*.

Accept the default quarantine directory, which is located on the Apex One server computer. The directory is in URL format and contains the server's host name or IP address.

- If the server is managing both IPv4 and IPv6 agents, use the host name so that all Security Agents can send quarantined files to the server.
- If the server only has or is identified by its IPv4 address, only pure IPv4 and dual-stack Security Agents can send quarantined files to the server.
- If the server only has or is identified by its IPv6 address, only pure IPv6 and dual-stack Security Agents can send quarantined files to the server.

You can also specify an alternative quarantine directory by typing the location in URL, UNC path, or absolute file path format. Security Agents should be able to connect to this alternative directory. For example, the alternative directory should have an IPv6 address if it will receive quarantined files from dual-stack and pure IPv6 Security Agents. Trend Micro recommends designating a dual-stack alternative directory, identifying the directory by its host name, and using UNC path when typing the directory.

Refer to the following table for guidance on when to use URL, UNC path, or absolute file path:

TABLE 7-14. Quarantine Directory

QUARANTINE DIRECTORY	ACCEPTED FORMAT	EXAMPLE	NOTES
A directory on the managing server computer	URL	`http://<osceserver>`	This is the default directory. Configure settings for this directory, such as the size of the quarantine folder. For details, see *Quarantine Manager on page 14-58*.
	UNC path	`\\<osceserver>\ofcscan\Virus`	

Quarantine Directory	Accepted Format	Example	Notes
A directory on another Apex One server computer (if you have other Apex One servers on the network)	URL	`http://<osceserver2>`	Ensure that Security Agents can connect to this directory. If you specify an incorrect directory, the Security Agent keeps the quarantined files on the SUSPECT folder until a correct quarantine directory is specified. In the server's virus/malware logs, the scan result is "Unable to send the quarantined file to the designated quarantine folder". If you use UNC path, ensure that the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this group.
	UNC path	`\\<osceserver2>\ofcscan\Virus`	
Another endpoint on the network	UNC path	`\\<computer_name>\temp`	
A different directory on the Security Agent	Absolute path	`C:\temp`	

Back Up Files Before Cleaning

If Apex One is set to clean an infected file, it can first back up the file. This allows you to restore the file in case you need it in the future. Apex One encrypts the backup file to prevent it from being opened, and then stores the file on the <*Agent installation folder*>`\Backup` folder.

To restore encrypted backup files, see *Restoring Encrypted Files on page 7-46*.

Damage Cleanup Services

Damage Cleanup Services cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, and viral files).

The agent triggers Damage Cleanup Services before or after virus/malware scanning, depending on the scan type.

- When Manual Scan, Scheduled Scan, or Scan Now runs, the Security Agent triggers Damage Cleanup Services first and then proceeds with

virus/malware scanning. During virus/malware scanning, the agent may trigger Damage Cleanup Services again if cleanup is required.

- During Real-time Scan, the Security Agent first performs virus/malware scanning and then triggers Damage Cleanup Services if cleanup is required.

You can select the type of cleanup that Damage Cleanup Services runs:

- **Standard cleanup**: The Security Agent performs any of the following actions during standard cleanup:
  - Detects and removes live Trojans
  - Kills processes that Trojans create
  - Repairs system files that Trojans modify
  - Deletes files and applications that Trojans drop
- **Advanced cleanup**: In addition to the standard cleanup actions, the Security Agent stops activities by rogue security software (also known as FakeAV) and certain rootkit variants. The Security Agent also uses advanced cleanup rules to proactively detect and stop applications that exhibit FakeAV and rootkit behavior.

Note

While providing proactive protection, advanced cleanup also results in a high number of false-positives.

Damage Cleanup Services does not run cleanup on probable virus/malware unless you select the option **Run cleanup when probable virus/malware is detected**. You can only select this option if the action on probable virus/malware is not **Pass** or **Deny Access**. For example, if the Security Agent detects probable virus/malware during Real-time Scan and the action is quarantine, the Security Agent first quarantines the infected file and then runs cleanup if necessary. The cleanup type (standard or advanced) depends on your selection.

Display a Notification Message When Virus/Malware is Detected

When Apex One detects virus/malware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection.

To modify the notification message, select **Virus/Malware** from the **Type** drop-down in **Administration** > **Notifications** > **Agent**.

Display a Notification Message When Probable Virus/Malware is Detected

When Apex One detects probable virus/malware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection.

To modify the notification message, select **Virus/Malware** from the **Type** drop-down in **Administration** > **Notifications** > **Agent**.

Restoring Quarantined Files

You can restore files that Apex One quarantined if you believe that the detection was inaccurate. The Central Quarantine Restore feature allows you to search for files in the quarantine directory and perform SHA1 verification checking to ensure that the files you want to restore have not been modified in any way.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, select a domain or select any agent.
3. Click **Tasks** > **Central Quarantine Restore**.

   The **Central Quarantine Restore Criteria** screen appears.
4. Type the name of the data you want to restore in the **Infected file/object** field.

5. Optionally specify the time period, security threat name, and file path of the data.
6. Click **Search**.

   The **Central Quarantine Restore** screen appears displaying the results of the search.
7. Select **Add restored file to the domain-level exclusion list** to ensure that all Security Agents in the domain(s) where the files are restored add the file to the scan exclusion list.

   This ensures that Apex One does not detect the file as a threat during future scans.

   Important

   Security Agents managed using Apex Central policies only apply the restored file exclusion until the next time that the Apex Central server updates the Security Agent policy and overwrites the exclusion list. To prevent the Security Agent from rescanning restored files, add the file exclusion to the Apex Central Security Agent policy.
8. Optionally type the SHA-1 value of the file for verification purposes.
9. Select the files to restore from the list and click **Restore**.

   Tip

   To view the individual Security Agents that restore the file, click the link in the **Endpoints** column.
10. Click **Close** in the confirmation dialog.

    To verify that Apex One successfully restored the quarantined file, see *Viewing Central Quarantine Restore Logs on page 7-96*.

Restoring Encrypted Files

To prevent infected from being opened, Apex One encrypts the file during the following instances:

- Before quarantining a file
- When backing up a file before cleaning it

Apex One provides a tool that decrypts and then restores the file in case you need to retrieve information from it. Apex One can decrypt and restore the following files:

TABLE 7-15. Files that Apex One can Decrypt and Restore

FILE	DESCRIPTION
Quarantined files on the agent endpoint	These files are found in the <*Agent installation folder*>\SUSPECT\Backup folder and are automatically purged after 7 days. These files are also uploaded to the designated quarantine directory on the Apex One server.
Quarantined files on the designated quarantine directory	By default, this directory is located on the Apex One server computer. For details, see *Quarantine Directory on page 7-40*.
Backed up encrypted files	These are the backup of infected files that Apex One was able to clean. These files are found in the `<Agent installation folder>\Backup` folder. To restore these files, users need to move them to the `<Agent installation folder>\SUSPECT\Backup` folder. Apex One only backs up and encrypts files before cleaning if you select **Backup files before cleaning** by going to **Agents** > **Agent Management** and clicking the **Settings** > **Scan Settings** > **{Scan Type}** > **Action** tab.

WARNING!

Restoring an infected file may spread the virus/malware to other files and computers. Before restoring the file, isolate the infected endpoint and move important files on this endpoint to a backup location.

Decrypting and Restoring Files

Procedure

- If the file is on the Security Agent endpoint:

  a. Open a command prompt and go to <*Agent installation folder*>.

  b. Run `VSEncode.exe` by double-clicking the file or by typing the following at a command prompt:

     ```
     VSEncode.exe /u
     ```

     This parameter opens a screen with a list of files found under `<Agent installation folder>\SUSPECT\Backup`.

  c. Select a file to restore and click **Restore**. The tool can only restore one file at a time.

  d. In the screen that opens, specify the folder where to restore the file.

  e. Click **Ok**. The file is restored to the specified folder.

     Note

     It might be possible for Apex One to scan the file again and treat it as infected as soon as the file is restored. To prevent the file from being scanned, add it to the scan exclusion list. See *Scan Exclusions on page 7-31* for details.

  f. Click **Close** when you have finished restoring files.

- If the file is on the Apex One server or a custom quarantine directory:

  a. If the file is on the Apex One server computer, open a command prompt and go to <*Server installation folder*>`\PCCSRV\Admin\Utility\VSEncrypt`.

     If the file is on a custom quarantine directory, navigate to `<Server installation folder>\PCCSRV\Admin\Utility` and copy the `VSEncrypt` folder to the endpoint where the custom quarantine directory is located.

b. Create a text file and then type the full path of the files you want to encrypt or decrypt.

   For example, to restore files in `C:\My Documents\Reports`, type `C:\My Documents\Reports\*.*` in the text file.

   Quarantined files on the Apex One server computer are found under `<Server installation folder>\PCCSRV\Virus`.

c. Save the text file with an `INI` or `TXT` extension. For example, save it as `ForEncryption.ini` on the `C:` drive.

d. Open a command prompt and go to the directory where the `VSEncrypt` folder is located.

e. Run `VSEncode.exe` by typing the following:

   ```
   VSEncode.exe /d /i <location of the INI or TXT file>
   ```

   Where:

   `<location of the INI or TXT file>` is the path of the `INI` or `TXT` file you created (for example, `C:\ForEncryption.ini`).

f. Use the other parameters to issue various commands.

TABLE 7-16. Restore Parameters

PARAMETER	DESCRIPTION
None (no parameter)	Encrypt files
/d	Decrypt files
/debug	Create a debug log and save it to the endpoint. On the Security Agent endpoint, the debug log `VSEncrypt.log` is created in the `<Agent installation folder>`.
/o	Overwrite an encrypted or decrypted file if it already exists
/f <filename>	Encrypt or decrypt a single file

Parameter	Description
/nr	Do not restore the original file name
/v	Display information about the tool
/u	Launch the tool's user interface
/r <Destination folder>	The folder where a file will be restored
/s <Original file name>	The file name of the original encrypted file

For example, type `VSEncode [/d] [/debug]` to decrypt files in the `Suspect` folder and create a debug log. When you decrypt or encrypt a file, Apex One creates the decrypted or encrypted file in the same folder. Before decrypting or encrypting a file, ensure that it is not locked.

Spyware/Grayware Scan Actions

The scan action Apex One performs depends on the scan type that detected the spyware/grayware. While specific actions can be configured for each virus/malware type, only one action can be configured for all types of spyware/grayware. For example, when Apex One detects any type of spyware/grayware during Manual Scan (scan type), it cleans (action) the affected system resources.

For information on the different types of spyware/grayware, see *Spyware and Grayware on page 7-5*.

Note

The spyware/grayware scan actions are configurable through the web console only. The Security Agent console does not provide access to these settings.

The following table lists the actions Apex One can perform against spyware/grayware.

TABLE 7-17. Spyware/Grayware Scan Actions

ACTION	DESCRIPTION
Clean	Apex One terminates processes or delete registries, files, cookies, and shortcuts. After cleaning spyware/grayware, Security Agents back up spyware/grayware data, which you can restore if you consider the spyware/grayware safe to access. See *Restoring Spyware/Grayware on page 7-52* for details.
Pass	Apex One performs no action on detected spyware/grayware components but records the spyware/grayware detection in the logs. This action can only be performed during Manual Scan, Scheduled Scan, and Scan Now. During Real-time Scan, the action is "Deny Access". Apex One will not perform any action if the detected spyware/grayware is included in the approved list. See *Spyware/Grayware Approved List on page 7-50* for details.
Deny Access	Apex One denies access (copy, open) to the detected spyware/grayware components. This action can only be performed during Real-time Scan. During Manual Scan, Scheduled Scan, and Scan Now, the action is "Pass".

Display a Notification Message When Spyware/Grayware is Detected

When Apex One detects spyware/grayware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection.

To modify the notification message, select **Spyware/Grayware** from the **Type** drop-down in **Administration** > **Notifications** > **Agent**.

Spyware/Grayware Approved List

The Security Agent provides a list of "approved" spyware/grayware, which contains files or applications that you do not want treated as spyware or grayware. When a particular spyware/grayware is detected during scanning,

the Security Agent checks the approved list and performs no action if it finds a match in the approved list.

Apply the approved list to one or several Security Agents and domains, or to all Security Agents that the server manages. The approved list applies to all scan types, which means that the same approved list will be used during Manual Scan, Real-time Scan, Scheduled Scan, and Scan Now.

Adding Already Detected Spyware/Grayware to the Approved List

Procedure

1. Go to one of the following:
   - **Agents** > **Agent Management**
   - **Logs** > **Agents** > **Security Risks**
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Logs** > **Spyware/Grayware Logs** or **View Logs** > **Spyware/Grayware Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. Select logs and click **Add to Approved List**.
6. Apply the approved spyware/grayware only to the selected agent computers or to certain domain(s).
7. Click **Save**. The selected agents apply the setting and the Apex One server adds the spyware/grayware to the approved list found in **Agents** > **Agent Management > Settings** > **Spyware/Grayware Approved List**.

Note

Apex One can accommodate a maximum of 1024 spyware/grayware in the approved list.

Managing the Spyware/Grayware Approved List

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Spyware/Grayware Approved List**.
4. On the **Spyware/Grayware names** table, select a spyware/grayware name. To select multiple names, hold the CTRL key while selecting.
   - You can also type a keyword in the **Search** field and click **Search**. The table refreshes with names that match the keyword.
5. Click **Add**.

   The names move to the **Approved List** table.
6. To remove names from the approved list, select the names and click **Remove**. To select multiple names, hold the CTRL key while selecting.
7. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Restoring Spyware/Grayware

After cleaning spyware/grayware, Security Agents back up spyware/grayware data. Notify an online agent to restore backed up data if you consider the

data harmless. Choose the spyware/grayware data to restore based on the backup time.

Note

Security Agent users cannot initiate spyware/grayware restore and are not notified about which backup data the agent was able to restore.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, open a domain and then select any agent.

   Note

   Only one agent at a time can perform spyware/grayware restore.

3. Click **Tasks** > **Spyware/Grayware Restore**.
4. To view the items to restore for each data segment, click **View**.

   A new screen displays. Click **Back** to return to the previous screen.
5. Select the data segments that you want to restore.
6. Click **Restore**.

   Apex One notifies you of the restoration status. Check the spyware/grayware restore logs for a full report. See *Viewing Spyware/Grayware Restore Logs on page 7-100* for details.

Trusted Program List

You can configure Security Agents to skip scanning of trusted processes during Application Control, Behavior Monitoring, Data Loss Prevention, Device Control, Endpoint Sensor, and Real-time Scans. After adding a program to the Trusted Programs List, the Security Agent does not subject the program or any processes initiated by the program to Real-time Scan.

Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints.

Note

You can add files to the Trusted Programs List if the following requirements are met:

- The file is not located in the Windows system directory.
- The file has a valid digital signature.

After adding a program to the Trusted Programs List, the Security Agent automatically excludes the program from the following scans:

- Application Control (configurable only on the Apex Central console)
- Behavior Monitoring
- Data Loss Prevention
- Device Control
- Endpoint Sensor (configurable only on the Apex Central console)
- Real-time Scan: file checking and process scanning

Configuring the Trusted Programs List

The Trusted Programs List excludes programs and all child processes called by the program from Application Control, Behavior Monitoring, Data Loss Prevention, Device Control, Endpoint Sensor, and Real-time Scan.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Trusted Program List**.

4. Type the full program path of the program to exclude from the list.
5. Click **Add to Trusted Program List**.
6. To remove a program from the list, click the **Delete** icon.
7. To export the Trusted Programs List, click **Export** and select a location for the file.

   Note

   Apex One saves the list in DAT format.

8. To import a Trusted Programs List, click **Import**. and select the location of the file.
   a. Click **Browse...** and select the location of the DAT file.
   b. Click **Import**.
9. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Scan Privileges and Other Settings

Users with scan privileges have greater control over how files on their computers get scanned. Scan privileges allow users or the Security Agent to perform the following tasks:

- Users can configure Manual Scan, Scheduled Scan, and Real-time Scan settings. For details, see *Scan Type Privileges on page 7-56*.

- Users can postpone, stop, or skip Scheduled Scan. For details, see *Scheduled Scan Privileges and Other Settings on page 7-57*.
- Users enable scanning of POP3 email messages for virus/malware. For details, see *Mail Scan Privileges and Other Settings on page 7-61*.
- The Security Agent can use cache settings to improve its scan performance. For details, see *Cache Settings for Scans on page 7-62*.
- Users can customize an individual Trusted Program List. For details, see *Trusted Program List Privilege on page 7-66*.

Scan Type Privileges

Allow users to configure their own Manual Scan, Real-time Scan and Scheduled Scan settings.

Granting Scan Type Privileges

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Scans** section.
5. Select the scan types that users are allowed to configure.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Configuring Scan Settings for the Security Agent

Procedure

1. Right-click the Security Agent icon on the system tray and select **Open Security Agent Console**.
2. Click **Settings** > **{Scan Type}**.
3. Configure the following settings:
   - Real-time Scan settings: User Activity on Files, Files to Scan, Scan Settings, Scan Exclusions, Scan Actions
   - Manual Scan settings: Files to Scan, Scan Settings, CPU Usage, Scan Exclusions, Scan Actions
   - Scheduled Scan settings: Schedule, Files to Scan, Scan Settings, CPU Usage, Scan Exclusions, Scan Actions
4. Click **OK**.

Scheduled Scan Privileges and Other Settings

If Scheduled Scan is set to run on the agent, users can postpone and skip/stop Scheduled Scan.

Postpone Scheduled Scan

Users with the "Postpone Scheduled Scan" privilege can perform the following actions:

- Postpone Scheduled Scan before it runs and then specify the postpone duration. Scheduled Scan can only be postponed once.

- If Scheduled Scan is in progress, users can stop scanning and restart it later. Users then specify the amount of time that should elapse before scanning restarts. When scanning restarts, all previously scanned files are scanned again. Scheduled Scan can be stopped and then restarted only once.

Note

The minimum postpone duration/elapsed time users can specify is 15 minutes. The maximum is 12 hours and 45 minutes.

You can modify the postpone time by going to **Agents** > **Global Agent Settings** on the **Security Settings** tab. In the **Scheduled Scan Settings** section, modify the **Postpone Scheduled Scan for up to __ hour(s) and __ minute(s)** setting.

Skip and Stop Scheduled Scan

This privilege allows users to perform the following actions:

- Skip Scheduled Scan before it runs
- Stop Scheduled Scan when it is in progress

Note

Users cannot skip or stop a Scheduled Scan more than one time. Even after a system restart, Scheduled Scan resumes scanning based on the next scheduled time.

Scheduled Scan Privilege Notification

To allow users to take advantage of Scheduled Scan privileges, remind them about the privileges you have granted them by configuring Apex One to display a notification message before Scheduled Scan runs.

Granting Scheduled Scan Privileges and Displaying the Privilege Notification

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Scheduled Scans** section.
5. Select the following options:
   - **Postpone Scheduled Scan**
   - **Skip and stop Scheduled Scan**
6. Click the **Other Settings** tab and go to the **Scheduled Scan Settings** section.
7. Select **Display a notification before a scheduled scan occurs**.

   When you enable this option, a notification message displays on the agent endpoint minutes before Scheduled Scan runs. Users are notified of the scan schedule (date and time) and their Scheduled Scan privileges, such as postponing, skipping, or stopping Scheduled Scan.

   Note

   The number of minutes is configurable. To configure the number of minutes, go to **Agents** > **Global Agent Settings** on the **Security Settings** tab. In the **Scheduled Scan Settings** section, modify the **Remind users of the Scheduled Scan __ minutes before it runs** setting.

8. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Postponing/Skipping and Stopping Scheduled Scan on the Agent

Procedure

- If Scheduled Scan has not started:
  a. Right-click the Security Agent icon on the system tray and select **Advanced Schedule Scan Setting**.

  Note

  Users do not need to perform this step if the notification message is enabled and is set to display minutes before Scheduled Scan runs. For details about the notification message, see *Scheduled Scan Privilege Notification on page 7-58*.

  b. On the notification window that displays, select from the following options:
     - **Postpone scanning for __ hours and __ minutes.**
     - **Skip this Scheduled Scan. The next Scheduled Scan runs on <date> at <time>.**
- If Scheduled Scan is in progress:
  a. Right-click the Security Agent icon on the system tray and select **Scheduled Scan Advanced Settings**.
  b. On the notification window that displays, select from the following options:

- **Stop scanning. Restart the scan after __ hours and __ minutes.**
- **Stop scanning. The next Scheduled Scan runs on <date> at <time>.**

Mail Scan Privileges and Other Settings

When Security Agents have the mail scan privileges, the **Mail Scan** option displays on the Security Agent console. The **Mail Scan** option shows the POP3 mail scan.

The following table describes the POP3 mail scan program.

TABLE 7-18. Mail Scan Programs

DETAILS	DESCRIPTION
Purpose	Scans POP3 email messages for viruses/malware
Prerequisites	• Must be enabled by administrators from the web console before users can use it **Note** To enable POP3 Mail Scan, see *Granting Mail Scan Privileges and Enabling POP3 Mail Scan on page 7-62*. • Action against viruses/malware configurable from the Security Agent console but not from the web console
Scan types supported	Real-time Scan Scanning is done as email messages are retrieved from the POP3 mail server.
Scan results	• Information about detected security risks available after scanning is complete • Scan results not logged on the Security Agent console's **Logs** screen • Scan results not sent to the server

Details	Description
Other details	Shares the Web Reputation feature

Granting Mail Scan Privileges and Enabling POP3 Mail Scan

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Mail Scan** section.
5. Select **Display the Mail Scan settings on the Security Agent console**.
6. Click the **Other Settings** tab and go to the **POP3 Email Scan Settings** section.
7. Select **Scan POP3 email**.
8. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Cache Settings for Scans

The Security Agent can build the digital signature and on-demand scan cache files to improve its scan performance. When an on-demand scan runs, the

Security Agent first checks the digital signature cache file and then the on-demand scan cache file for files to exclude from the scan. Scanning time is reduced if a large number of files are excluded from the scan.

Digital Signature Cache

The digital signature cache file is used during Manual Scan, Scheduled Scan, and Scan Now. Agents do not scan files whose signatures have been added to the digital signature cache file.

The Security Agent uses the same Digital Signature Pattern used for Behavior Monitoring to build the digital signature cache file. The Digital Signature Pattern contains a list of files that Trend Micro considers trustworthy and therefore can be excluded from scans.

Note

Behavior Monitoring is automatically disabled on Windows server platforms. If the digital signature cache is enabled, Security Agents on these platforms download the Digital Signature Pattern for use in the cache and do not download the other Behavior Monitoring components.

Agents build the digital signature cache file according to a schedule, which is configurable from the web console. Agents do this to:

- Add the signatures of new files that were introduced to the system since the last cache file was built
- Remove the signatures of files that have been modified or deleted from the system

During the cache building process, agents check the following folders for trustworthy files and then adds the signatures of these files to the digital signature cache file:

- `%PROGRAMFILES%`
- `%WINDIR%`

The cache building process does not affect the endpoint's performance because agents use minimal system resources during the process. Agents are

also able to resume a cache building task that was interrupted for some reason (for example, when the host machine is powered off or when a wireless endpoint's AC adapter is unplugged).

On-demand Scan Cache

The on-demand scan cache file is used during Manual Scan, Scheduled Scan, and Scan Now. Security Agents do not scan files whose caches have been added to the on-demand scan cache file.

Each time scanning runs, the Security Agent checks the properties of threat-free files. If a threat-free file has not been modified for a certain period of time (the time period is configurable), the Security Agent adds the cache of the file to the on-demand scan cache file. When the next scan occurs, the file will not be scanned if its cache has not expired.

The cache for a threat-free file expires within a certain number of days (the time period is also configurable). When scanning occurs on or after the cache expiration, the Security Agent removes the expired cache and scans the file for threats. If the file is threat-free and remains unmodified, the cache of the file is added back to the on-demand scan cache file. If the file is threat-free but was recently modified, the cache is not added and the file will be scanned again on the next scan.

The cache for a threat-free file expires to prevent the exclusion of infected files from scans, as illustrated in the following examples:

- It is possible that a severely outdated pattern file may have treated an infected, unmodified file as threat-free. If the cache does not expire, the infected file remains in the system until it is modified and detected by Real-time Scan.
- If a cached file was modified and Real-time Scan is not functional during the file modification, the cache needs to expire so that the modified file can be scanned for threats.

The number of caches added to the on-demand scan cache file depends on the scan type and its scan target. For example, the number of caches may be less if the Security Agent only scanned 200 of the 1,000 files in the endpoint during Manual Scan.

If on-demand scans are run frequently, the on-demand scan cache file reduces the scanning time significantly. In a scan task where all caches are not expired, scanning that usually takes 12 minutes can be reduced to 1 minute. Reducing the number of days a file must remain unmodified and extending the cache expiration usually improve the performance. Since files must remain unmodified for a relatively short period of time, more caches can be added to the cache file. The caches also expire longer, which means that more files are skipped from scans.

If on-demand scans are seldom run, you can disable the on-demand scan cache since caches would have expired when the next scan runs.

Configuring Cache Settings for Scans

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Cache Settings for Scans** section.
5. Configure settings for the digital signature cache.
   a. Select **Enable the digital signature cache**.
   b. In **Build the cache every __ days**, specify how often the agent builds the cache.
6. Configure settings for the on-demand scan cache.
   a. Select **Enable the on-demand scan cache**.
   b. In **Add the cache for safe files that are unchanged for __ days**, specify the number of days a file must remain unchanged before it is cached.

c. In **The cache for each safe file expires within __ days**, specify the maximum number of days a cache remains in the cache file.

Note

To prevent all caches added during a scan from expiring on the same day, caches expire randomly within the maximum number of days you specified. For example, if 500 caches were added to the cache today and the maximum number of days you specified is 10, a fraction of the caches will expire the next day and the majority will expire on the succeeding days. On the 10th day, all caches that remain will expire.

7. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Trusted Program List Privilege

You can grant end users the privilege to configure Apex One to skip scanning of trusted processes from Application Control, Behavior Monitoring, Data Loss Prevention, Device Control, Endpoint Sensor, and Real-time Scan. After adding a program to the Trusted Programs List, Apex One does not subject the program or any processes initiated by the program to Real-time Scan. Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints.

Granting the Trusted Program List Settings

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Trusted Program List** section.
5. Select **Display the Trusted Program List on the Security Agent console**.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Global Scan Settings

There are a number of ways global scan settings get applied to agents.

- A particular scan setting can apply to all agents that the server manages or only to agents with certain scan privileges. For example, if you configure the postpone Scheduled Scan duration, only agents with the privilege to postpone Scheduled Scan will use the setting.
- A particular scan setting can apply to all or only to a particular scan type. For example, on endpoints with both the Apex One server and Security Agent installed, you can exclude the Apex One server database

from scanning. However, this setting applies only during Real-time Scan.

- A particular scan setting can apply when scanning for either virus/malware or spyware/grayware, or both. For example, assessment mode only applies during spyware/grayware scanning.

Configuring Global Scan Settings

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **Security Settings** tab and configure the Global Scan Settings in each of the available sections.
   - *Scan Settings Section on page 7-70*
   - *Scheduled Scan Settings Section on page 7-75*
3. Click the **System** tab.
4. In the **Certified Safe Software Service Settings** section, configure the **Enable the Certified Safe Software Service for Behavior Monitoring, Firewall, and antivirus scans** setting.

   The Certified Safe Software Service queries Trend Micro datacenters to verify the safety of a program detected by Malware Behavior Blocking, Event Monitoring, Firewall, or antivirus scans. Enable Certified Safe Software Service to reduce the likelihood of false positive detections.

Note

Ensure that Security Agents have the correct proxy settings (for details, see *Security Agent Proxy Settings on page 15-50*) before enabling Certified Safe Software Service. Incorrect proxy settings, along with an intermittent Internet connection, can result in delays or failure to receive a response from Trend Micro datacenters, causing monitored programs to appear unresponsive.

In addition, pure IPv6 Security Agents cannot query directly from Trend Micro datacenters. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Security Agents to connect to the Trend Micro datacenters.

5. Click the **Network** tab.

6. In the **Virus/Malware Log Bandwidth Settings** section, configure the **Enable the Security Agent to create a single virus/malware log entry for recurring detections of the same virus/malware within an hour** setting.

   Apex One consolidates virus log entries when detecting multiple infections from the same virus/malware over a short period of time. Apex One may detect a single virus/malware multiple times, quickly filling the virus/malware log and consuming network bandwidth when the Security Agent sends log information to the server. Enabling this feature helps reduce both the number of virus/malware log entries made and the amount of network bandwidth Security Agents consume when they report virus log information to the server.

7. Click the **Agent Control** tab.

8. In the **General Settings** section, configure the **Add Manual Scan to the Windows shortcut menu on endpoints** setting.

   When this setting is enabled, all Security Agents managed by the server add a **Scan with Apex One** option to the right-click menu in Windows Explorer. When users right-click a file or folder on the Windows desktop or in Windows Explorer and select the option, Manual Scan scans the file or folder for virus/malware and spyware/grayware.

9. Click **Save**.

Scan Settings Section

The **Scan Settings** section on the **Security Settings** tab of the **Global Agent Settings** screen allows administrators to configure the following:

- *Exclude the Apex One Server Database Folder from Real-time Scan on page 7-70*
- *Exclude Microsoft Exchange Server Folders and Files from Scans on page 7-70*
- *Enable Deferred Scanning on File Operations on page 7-71*
- *Enable Early Launch Anti-Malware Protection on Endpoints on page 7-71*
- *Clean/Delete Infected Files Within Compressed Files on page 7-72*
- *Enable Assessment Mode on page 7-74*
- *Scan for Cookies on page 7-75*

Exclude the Apex One Server Database Folder from Real-time Scan

If the Security Agent and Apex One server exist on the same endpoint, the Security Agent will not scan the server database for virus/malware and spyware/grayware during Real-time Scan.

Tip

Enable this setting to prevent database corruption that may occur during scanning.

Exclude Microsoft Exchange Server Folders and Files from Scans

If the Security Agent and a Microsoft Exchange 2000/2003 server exist on the same endpoint, Apex One will not scan the following Microsoft Exchange folders and files for virus/malware and spyware/grayware during Manual Scan, Real-time Scan, Scheduled Scan and Scan Now:

- The following folders in `\Exchsrvr\Mailroot\vsi 1`: `Queue`, `PickUp`, and `BadMail`
- `.\Exchsrvr\mdbdata`, including these files: `priv1.stm`, `priv1.edb`, `pub1.stm`, and `pub1.edb`
- `.\Exchsrvr\Storage Group`

For Microsoft Exchange 2007 or later folders, you need to manually add the folders to the scan exclusion list. For scan exclusion details, see the following website:

http://technet.microsoft.com/en-us/library/bb332342.aspx

See *Scan Exclusions on page 7-31* for steps in configuring the scan exclusion list.

Enable Deferred Scanning on File Operations

Administrators can configure Apex One to defer the scanning of files. Apex One allows the user to copy files and then scans the files after the copy process completes. This deferred scanning improves the performance of the copy and scan processes.

Note

Deferred scanning requires that the Virus Scan Engine (VSAPI) be version 9.713 or later. For details on upgrading the server, see *Manually Updating the Apex One Server on page 6-25*.

Enable Early Launch Anti-Malware Protection on Endpoints

Apex One supports the Early Launch Anti-Malware (ELAM) feature as part of the Secure Boot standard to provide boot time protection on endpoints. Administrators can enable this feature to start Apex One agents before other third-party software drivers when endpoints start up. This feature enables Apex One agents to detect malware during the operating system boot process.

After scanning all third-party software drivers, the Apex One agent reports the driver classification information to the system kernel. Administrators

can define actions based on the driver classifications in Group Policy in Windows and view scan results using Event Viewer on endpoints.

Note

ELAM is supported only on Windows 8.1 (or later) and Windows Server 2012 (or later) platforms.

Clean/Delete Infected Files Within Compressed Files

When all agents managed by the server detect virus/malware within compressed files during Manual Scan, Real-time Scan, Scheduled Scan and Scan Now, and the following conditions are met, agents clean or delete the infected files.

- "Clean" or "Delete" is the action Apex One is set to perform. Check the action Apex One performs on infected files by going to **Agents** > **Agent Management > Settings** > **Scan Settings** > **{Scan Type}** > **Action** tab.
- You enable this setting. Enabling this setting may increase endpoint resource usage during scanning and scanning may take longer to complete. This is because Apex One needs to decompress the compressed file, clean/delete infected files within the compressed file, and then re-compress the file.
- The compressed file format is supported. Apex One only supports certain compressed file formats, including ZIP and Office Open XML, which uses ZIP compression technologies. Office Open XML is the default format for Microsoft Office 2007 applications such as Excel, PowerPoint, and Word.

  Note

  Contact your support provider for a complete list of supported compressed file formats.

For example, Real-time Scan is set to delete files infected with a virus. After Real-time Scan decompresses a compressed file named `abc.zip` and detects an infected file `123.doc` within the compressed file, Apex One deletes `123.doc` and then re-compresses `abc.zip`, which is now safe to access.

The following table describes what happens if any of the conditions is not met.

TABLE 7-19. Compressed File Scenarios and Results

STATUS OF "CLEAN/ DELETE INFECTED FILES WITHIN COMPRESSED FILES"	ACTION APEX ONE IS SET TO PERFORM	COMPRESSED FILE FORMAT	RESULT
Enabled	Clean or Delete	Not supported Example: `def.rar` contains an infected file `123.doc`.	Apex One encrypts `def.rar` but does not clean, delete, or perform any other action on `123.doc`.
Disabled	Clean or Delete	Supported/Not supported Example: `abc.zip` contains an infected file `123.doc`.	Apex One does not clean, delete, or perform any other action on both `abc.zip` and `123.doc`.

Status of "Clean/ Delete infected files within compressed files"	Action Apex One is set to perform	Compressed file format	Result
Enabled/ Disabled	Not Clean or Delete (in other words, any of the following: Rename, Quarantine, Deny Access or Pass)	Supported/Not supported Example: `abc.zip` contains an infected file `123.doc`.	Apex One performs the configured action (Rename, Quarantine, Deny Access or Pass) on `abc.zip`, not `123.doc`. If the action is: **Rename**: Apex One renames `abc.zip` to `abc.vir`, but does not rename `123.doc`. **Quarantine**: Apex One quarantines `abc.zip` (`123.doc` and all non-infected files are quarantined). **Pass**: Apex One performs no action on both `abc.zip` and `123.doc` but logs the virus detection. **Deny Access**: Apex One denies access to `abc.zip` when it is opened (`123.doc` and all non-infected files cannot be opened).

Enable Assessment Mode

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

Trend Micro provides assessment mode to allow you to evaluate items that Trend Micro detects as spyware/grayware and then take appropriate action based on your evaluation. For example, detected spyware/grayware that you

do not consider a security risk can be added to the spyware/grayware approved list.

When in assessment mode, Apex One performs the following scan actions:

- **Pass**: During Manual Scan, Scheduled Scan and Scan Now
- **Deny Access**: During Real-time Scan

Note

Assessment mode overrides any user-configured scan action. For example, even if you choose "Clean" as the scan action during Manual Scan, "Pass" remains as the scan action when the agent is on assessment mode.

Scan for Cookies

Select this option if you consider cookies as potential security risks. When selected, all agents managed by the server will scan cookies for spyware/grayware during Manual Scan, Scheduled Scan, Real-time Scan, and Scan Now.

Scheduled Scan Settings Section

Only agents set to run Scheduled Scan will use the following settings. Scheduled Scan can scan for virus/malware and spyware/grayware.

The Scheduled Scan Settings section of the Global Scan Settings allows administrators to configure the following:

- *Remind Users of the Scheduled Scan __ Minutes Before it Runs on page 7-76*
- *Postpone Scheduled Scan for up to __ Hours and __ Minutes on page 7-76*
- *Automatically Stop Scheduled Scan When Scanning Lasts More Than __ Hours and __ Minutes on page 7-76*
- *Skip Scheduled Scan When a Wireless Endpoint's Battery Life is Less Than __ % and its AC Adapter is Unplugged on page 7-77*

- *Resume a Missed Scheduled Scan on page 7-77*

Remind Users of the Scheduled Scan __ Minutes Before it Runs

Apex One displays a notification message minutes before scanning runs to remind users of the scan schedule (date and time) and any Scheduled Scan privilege you grant them.

The notification message can be enabled/disabled from **Agents** > **Agent Management > Settings** > **Privileges and Other Settings** > **Other Settings (tab)** > **Scheduled Scan Settings**. If disabled, no reminder displays.

Postpone Scheduled Scan for up to __ Hours and __ Minutes

Only users with the "Postpone Scheduled Scan" privilege can perform the following actions:

- Postpone Scheduled Scan before it runs and then specify the postpone duration.
- If Scheduled Scan is in progress, users can stop scanning and restart it later. Users then specify the amount of time that should elapse before scanning restarts. When scanning restarts, all previously scanned files are scanned again.

  The maximum postpone duration/elapsed time users can specify is 12 hours and 45 minutes, which you can reduce by specifying the number of hour(s) and/or minute(s) in the fields provided.

Automatically Stop Scheduled Scan When Scanning Lasts More Than __ Hours and __ Minutes

Apex One stops scanning when the specified amount of time is exceeded and scanning is not yet complete. Apex One immediately notifies users of any security risk detected during scanning.

Skip Scheduled Scan When a Wireless Endpoint's Battery Life is Less Than __ % and its AC Adapter is Unplugged

Apex One immediately skips scanning when Scheduled Scan launches if it detects that a wireless endpoint's battery life is running low and its AC adapter is not connected to any power source. If battery life is low but the AC adapter is connected to a power source, scanning proceeds.

Resume a Missed Scheduled Scan

When Scheduled Scan did not launch because Apex One is not running on the day and time of Scheduled Scan or if the user interrupts Scheduled Scan (for example, turns off the endpoint after the scan begins), you can specify when Apex One resumes scanning.

Specify which Scheduled Scan to resume:

- **Resume an interrupted Scheduled Scan**: Resumes Scheduled Scans that the user interrupted by turning off the endpoint
- **Resume a missed Scheduled Scan**: Resumes Scheduled Scans missed because the endpoint was not running

Specify when to resume scanning:

- **Same time next day**: If Apex One is running at the exact same time the next day, scanning is resumed.
- **__ minutes after the endpoint starts**: Apex One resumes scanning a number of minutes after the user turns on the endpoint. The number of minutes is between 10 and 120.

Note

Users can postpone or skip a resumed Scheduled Scan if the administrator enabled this privilege. For details, see *Scheduled Scan Privileges and Other Settings on page 7-57*.

Security Risk Notifications

Apex One comes with a set of default notification messages that inform you, other Apex One administrators, and Security Agent users of detected security risks.

For details on notifications sent to administrators, see *Security Risk Notifications for Administrators on page 7-78*.

For details on notifications sent to Security Agent users, see *Security Risk Notifications for Security Agent Users on page 7-85*.

Security Risk Notifications for Administrators

Configure Apex One to send you and other Apex One administrators a notification when it detects a security risk, or only when the action on the security risk is unsuccessful and therefore requires your intervention.

Apex One comes with a set of default notification messages that inform you and other Apex One administrators of security risk detections. You can modify the notifications and configure additional notification settings to suit your requirements.

TABLE 7-20. Types of Security Risk Notifications

TYPE	REFERENCE
Virus/Malware	*Configuring Security Risk Notifications for Administrators on page 7-79*
Spyware/Grayware	*Configuring Security Risk Notifications for Administrators on page 7-79*
Digital Asset Transmissions	*Configuring Data Loss Prevention Notification for Administrators on page 11-53*
C&C Callbacks	*Configuring C&C Callback Notifications for Administrators on page 12-13*

Note

Apex One can send notifications through email, SNMP trap, and Windows NT Event logs. Configure settings when Apex One sends notifications through these channels. For details, see *Administrator Notification Settings on page 14-38*.

Configuring Security Risk Notifications for Administrators

Procedure

1. Go to **Administration** > **Notifications** > **Administrator**.

   The **Administrator Notifications** screen appears.

2. In the **Criteria** tab:

   a. Go to the **Virus/Malware** and **Spyware/Grayware** sections.

   b. Specify whether to send notifications when Apex One detects virus/malware and spyware/grayware, or only when the action on these security risks is unsuccessful.

3. In the **Email** tab:

   a. Go to the **Virus/Malware Detections** and **Spyware/Grayware Detections** sections.

   b. Select **Enable notification via email**.

   c. Select **Send notifications to users with agent tree domain permissions**.

      You can use Role-based Administration to grant agent tree domain permissions to users. If a detection occurs on any Security Agent belonging to a specific domain, the email will be sent to the email addresses of the users with domain permissions. See the following table for examples:

TABLE 7-21. Agent Tree Domains and Permissions

AGENT TREE DOMAIN	ROLES WITH DOMAIN PERMISSIONS	USER ACCOUNT WITH THE ROLE	EMAIL ADDRESS FOR THE USER ACCOUNT
Domain A	Administrator (built-in)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domain B	Administrator (built-in)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

If any Security Agent belonging to Domain A detects a virus, the email will be sent to mary@xyz.com, john@xyz.com, and chris@xyz.com.

If any Security Agent belonging to Domain B detects spyware, the email will be sent to mary@xyz.com and jane@xyz.com.

Note

If you enable this option, all users with domain permissions must have a corresponding email address. The email notification will not be sent to users without an email address. Users and email addresses are configured from **Administration** > **Account Management** > **User Accounts**.

d. Select **Send notifications to the following email address(es)** and then type the email addresses.

e. Specify the **Subject** used in the email notification.

f. Specify the **Message** contents.

Apex One supports use of tokens in the **Subject** and **Message** fields.

TABLE 7-22. Token Variables for Security Risk Notifications

VARIABLE TOKEN	DESCRIPTION
Virus/Malware detections	
%v	Security threat name
%s	Endpoint with the detection
%i	IP address of the endpoint
%c	MAC address of the endpoint
%m	Domain of the endpoint
%p	Location of virus/malware
%y	Date and time of detection
%e	Virus Scan Engine version
%r	Virus Pattern version
%a	Action performed on the security risk
%n	Name of the user logged on to the endpoint
%g	GUID of the Security Agent
%b	Scan type
Spyware/Grayware detections	
%s	Endpoint with the detection
%i	IP address of the endpoint
%m	Domain of the endpoint
%y	Date and time of detection
%n	Name of the user logged on to the endpoint
%T	Spyware/Grayware and scan result

Variable Token	Description
%d	Detailed information regarding spyware/grayware detection
%g	GUID of the Security Agent
%b	Scan type

4. In the **SNMP Trap** tab:

   a. Go to the **Virus/Malware Detections** and **Spyware/Grayware Detections** sections.

   b. Select **Enable notification via SNMP trap**.

   c. Accept or modify the default message. You can use token variables in the following table to represent data in the **Message** field.

Table 7-23. Token Variables for Security Risk Notifications

Variable	Description
Virus/Malware detections	
%v	Security threat name
%s	Endpoint with the detection
%i	IP address of the endpoint
%c	MAC address of the endpoint
%m	Domain of the endpoint
%p	Location of virus/malware
%y	Date and time of detection
%e	Virus Scan Engine version
%r	Virus Pattern version
%a	Action performed on the security risk

VARIABLE	DESCRIPTION
%n	Name of the user logged on to the endpoint
%g	GUID of the Security Agent
%b	Scan type
Spyware/Grayware detections	
%s	Endpoint with the detection
%i	IP address of the endpoint
%m	Domain of the endpoint
%y	Date and time of detection
%n	Name of the user logged on to the endpoint
%T	Spyware/Grayware and scan result
%v	Security threat name
%a	Action performed on the security risk
%d	Detailed information regarding spyware/grayware detection
%g	GUID of the Security Agent

5. In the **NT Event Log** tab:

   a. Go to the **Virus/Malware Detections** and **Spyware/Grayware Detections** sections.

   b. Select **Enable notification via NT Event Log**.

   c. Accept or modify the default message. You can use token variables in the following table to represent data in the **Message** field.

TABLE 7-24. Token Variables for Security Risk Notifications

VARIABLE	DESCRIPTION
Virus/Malware detections	

VARIABLE	DESCRIPTION
%v	Security threat name
%s	Endpoint with the detection
%i	IP address of the endpoint
%c	MAC address of the endpoint
%m	Domain of the endpoint
%p	Location of virus/malware
%y	Date and time of detection
%e	Virus Scan Engine version
%r	Virus Pattern version
%a	Action performed on the security risk
%n	Name of the user logged on to the endpoint
%g	GUID of the Security Agent
%b	Scan type
Spyware/Grayware detections	
%s	Endpoint with the detection
%i	IP address of the endpoint
%m	Domain of the endpoint
%y	Date and time of detection
%n	Name of the user logged on to the endpoint
%T	Spyware/Grayware and scan result
%v	Security threat name
%a	Action performed on the security risk
%d	Detailed information regarding spyware/grayware detection

Variable	Description
%g	GUID of the Security Agent

6. Click **Save**.

Security Risk Notifications for Security Agent Users

Apex One can display notification messages on Security Agent endpoints:

- Immediately after Real-time Scan and Scheduled Scan detect virus/malware and spyware/grayware. Enable the notification message and optionally modify its content.
- If restarting the endpoint is necessary to finish cleaning infected files. For Real-time Scan, the message displays after a particular security risk has been scanned. For Manual Scan, Scheduled Scan, and Scan Now, the message displays once and only after Apex One finishes scanning all the scan targets.

Table 7-25. Types of Security Risk Agent Notifications

Type	Reference
Virus/Malware	*Configuring Virus/Malware Notifications for Security Agents on page 7-87*
Spyware/Grayware	*Configuring Spyware/Grayware Notifications on page 7-87*
Firewall violations	*Modifying the Content of the Firewall Notification Message on page 13-27*
Web reputation violations	*Modifying the Web Threat Notifications on page 12-13*
Device control violations	*Modifying Device Control Notifications on page 10-18*
Behavior monitoring policy violations	*Modifying the Content of the Notification Message on page 9-22*

Type	Reference
Digital asset transmissions	*Configuring Data Loss Prevention Notification for Agents on page 11-56*
C&C callbacks	*Modifying the Web Threat Notifications on page 12-13*

Notifying Users of Virus/Malware and Spyware/Grayware Detections

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Scan Settings** > **Real-time Scan Settings** or **Settings** > **Scan Settings** > **Scheduled Scan Settings**.
4. Click the **Action** tab.
5. Select the following options:
   - **Display a notification message on the agent endpoint when virus/malware is detected**
   - **Display a notification message on the agent endpoint when probable virus/malware is detected**
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Configuring Virus/Malware Notifications for Security Agents

You can configure the Security Agent to notify end users of the result of attempting to clean or quarantine a virus/malware threat.

Procedure

1. Go to **Administration** > **Notifications** > **Agent**.
2. From the **Type** drop-down, select **Virus/Malware**.
3. Configure detection settings.
   a. Choose to display one notification for all virus/malware related events, or separate notifications depending on the following severity levels:
      - **High**: The Security Agent was unable to handle critical malware
      - **Medium**: The Security Agent was unable to handle malware
      - **Low**: The Security Agent was able to resolve all threats
   b. Accept or modify the default messages.
4. Click **Save**.

Configuring Spyware/Grayware Notifications

Procedure

1. Go to **Administration** > **Notifications** > **Agent**.
2. From the **Type** drop-down, select **Spyware/Grayware**.

3. Accept or modify the default message.
4. Click **Save**.

Notifying Agents of a Restart to Finish Cleaning Infected Files

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Restart Notification** section.
5. Select **Display a notification message if the endpoint needs to restart to finish cleaning infected files**.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Security Risk Logs

Apex One generates logs when it detects virus/malware or spyware/grayware, and when it restores spyware/grayware.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing Virus/Malware Logs

The Security Agent generates logs when it detects viruses and malware and sends the logs to the server.

Procedure

1. Go to one of the following:
   - **Logs** > **Agents** > **Security Risks**
   - **Agents** > **Agent Management**
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Go to the **Virus/Malware Log Criteria** screen:
   - From the **Security Risk Logs** screen, click **View Logs** > **Virus/Malware Logs**.
   - From the **Agent Management** screen, click **Logs** > **Virus/Malware Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

Item	Description
Date/Time	The time the detection occurred
Endpoint	The endpoint on which the detection occurred
Security Threat	The name of the security threat
Infection Channel	The channel the threat originated from

Item	Description
Infected File/Object	The location of the file/object on the endpoint
Scan Type	The scan that detected the threat
Result	The result of the action taken **Note** For more information on scan results, see *Virus/ Malware Scan Results on page 7-90*.
IP Address	The IP address and port number of the source endpoint
MAC Address	The MAC address of the infected endpoint
Details	A link that displays the detailed analysis for the specific detection

6. To save logs to a comma-separated value (CSV) file, click **Export All to CSV**. Open the file or save it to a specific location.

   The CSV file contains the following information:

   - All information in the logs
   - User name logged on to the endpoint at the time of detection

Virus/Malware Scan Results

The following scan results display in the virus/malware logs:

Table 7-26. Scan Results

Result	Description
Deleted	• First action is “Delete” and the infected file was deleted. • First action is “Clean” but cleaning was unsuccessful. Second action is “Delete” and the infected file was deleted.

Result	Description
Quarantined	• First action is “Quarantine” and the infected file was quarantined. • First action is “Clean” but cleaning was unsuccessful. Second action is “Quarantine” and the infected file was quarantined.
Cleaned	An infected file was cleaned.
Renamed	• First action is “Rename” and the infected file was renamed. • First action is “Clean” but cleaning was unsuccessful. Second action is “Rename” and the infected file was renamed.
Access denied	• First action is “Deny Access” and access to the infected file was denied when the user attempted to open the file. • First action is “Clean” but cleaning was unsuccessful. Second action is “Deny Access” and access to the infected file was denied when the user attempted to open the file. • Probable Virus/Malware was detected during Real-time Scan. • Real-time Scan may deny access to files infected with a boot virus even if the scan action is “Clean” (first action) and “Quarantine” (second action). This is because attempting to clean a boot virus may damage the Master Boot Record (MBR) of the infected endpoint. Run Manual Scan so Apex One can clean or quarantine the file.
Passed	• First action is “Pass”. Apex One did not perform any action on the infected file. • First action is “Clean” but cleaning was unsuccessful. Second action is “Pass” so Apex One did not perform any action on the infected file.
Passed a potential security risk	This scan result only displays when Apex One detects "probable virus/malware" during Manual Scan, Scheduled Scan, and Scan Now. Refer to the following page on the Trend Micro online Virus Encyclopedia for information about probable virus/malware and how to submit suspicious files to Trend Micro for analysis. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/possible_virus

Result	Description
Unable to clean or quarantine the file	"Clean" is the first action. "Quarantine" is the second action, and both actions were unsuccessful. Solution: See *Unable to quarantine the file/Unable to rename the file on page 7-92*.
Unable to clean or delete the file	"Clean" is the first action. "Delete" is the second action, and both actions were unsuccessful. Solution: See *Unable to delete the file on page 7-92*.
Unable to clean or rename the file	"Clean" is the first action. "Rename" is the second action, and both actions were unsuccessful. Solution: See *Unable to quarantine the file/Unable to rename the file on page 7-92*.
Unable to quarantine the file/ Unable to rename the file	Explanation 1 The infected file may be locked by another application, is executing, or is on a CD. Apex One will quarantine/rename the file after the application releases the file or after it has been executed. Solution For infected files on a CD, consider not using the CD as the virus may infect other endpoints on the network.
	Explanation 2 The infected file is in the Temporary Internet Files folder of the agent endpoint. Since the endpoint downloads files while you are browsing, the web browser may have locked the infected file. When the web browser releases the file, Apex One will quarantine/rename the file. Solution: None
Unable to delete the file	Explanation 1 The infected file may be contained in a compressed file and the **Clean/ Delete infected files within compressed files** setting in **Agents** > **Global Agent Settings** on the **Security Settings** tab is disabled. Solution Enable the **Clean/Delete infected files within compressed files** option. When enabled, Apex One decompresses a compressed file,

Result	Description
	cleans/deletes infected files within the compressed file, and then re-compresses the file. **Note** Enabling this setting may increase endpoint resource usage during scanning and scanning may take longer to complete.
	Explanation 2 The infected file may be locked by another application, is executing, or is on a CD. Apex One will delete the file after the application releases the file or after it has been executed. Solution For infected files on a CD, consider not using the CD as the virus may infect other endpoints on the network.
	Explanation 3 The infected file is in the Temporary Internet Files folder of the Security Agent endpoint. Since the endpoint downloads files while you are browsing, the web browser may have locked the infected file. When the web browser releases the file, Apex One will delete the file. Solution: None
Unable to send the quarantined file to the designated quarantine folder	Although Apex One successfully quarantined a file in the `\Suspect` folder of the Security Agent endpoint, it cannot send the file to the designated quarantine directory. Solution Determine which scan type (Manual Scan, Real-time Scan, Scheduled Scan, or Scan Now) detected the virus/malware and then check the quarantine directory specified in **Agents** > **Agent Management > Settings** > **{Scan Type}** > **Action** tab. If the quarantine directory is on the Apex One server computer or is on another Apex One server computer: 1. Check if the agent can connect to the server. 2. If you use URL as the quarantine directory format:

Result	Description
	a. Ensure that the endpoint name you specify after `http://` is correct. b. Check the size of the infected file. If it exceeds the maximum file size specified in **Administration** > **Settings** > **Quarantine Manager**, adjust the setting to accommodate the file. You may also perform other actions such as deleting the file. c. Check the size of the quarantine directory folder and determine whether it has exceeded the folder capacity specified in **Administration** > **Settings** > **Quarantine Manager**. Adjust the folder capacity or manually delete files in the quarantine directory. 3. If you use UNC path, ensure that the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this group. Also check if the quarantine directory folder exists and if the UNC path is correct. If the quarantine directory is on another endpoint on the network (You can only use UNC path for this scenario): 1. Check if the Security Agent can connect to the endpoint. 2. Ensure that the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this group. 3. Check if the quarantine directory folder exists. 4. Check if the UNC path is correct. If the quarantine directory is on a different directory on the Security Agent endpoint (you can only use absolute path for this scenario), check if the quarantine directory folder exists.
Unable to clean the file	Explanation 1 The infected file may be contained in a compressed file and the "Clean/Delete" infected files within compressed files setting in **Agents** > **Global Agent Settings** on the **Security Settings** tab is disabled. Solution Enable the **Clean/Delete infected files within compressed files** option. When enabled, Apex One decompresses a compressed file,

Result	Description
	cleans/deletes infected files within the compressed file, and then re-compresses the file. **Note** Enabling this setting may increase endpoint resource usage during scanning and scanning may take longer to complete.
	Explanation 2 The infected file is in the `Temporary Internet Files` folder of the Security Agent endpoint. Since the endpoint downloads files while you are browsing, the web browser may have locked the infected file. When the web browser releases the file, Apex One will clean the file. Solution: None
	Explanation 3 The file may be uncleanable. For details and solutions, see *Uncleanable Files on page D-16*.
Action required	Apex One is unable to complete the configured action on the infected file without user intervention. Hover over the **Action required** column to see the following details. • "Action required - Contact Support for details on how to remove this threat with the Anti-Threat Tool Kit "Clean Boot" tool found in the Apex One ToolBox" • "Action required - Contact Support for details on how to remove this threat with the Anti-Threat Tool Kit "Rescue Disk" tool found in the Apex One ToolBox" • "Action required - Contact Support for details on how to remove this threat with the Anti-Threat Tool Kit "Rootkit Buster" tool found in the Apex One ToolBox" • "Action Required - Apex One detected a threat on an infected agent. Restart the endpoint to finish cleaning the security threat" • "Action required – A full system scan is required to finish removing a detected rootkit threat from the endpoint"

Viewing Central Quarantine Restore Logs

After cleaning malware, Security Agents back up malware data. Notify an online agent to restore backed up data if you consider the data harmless. Information about which malware backup data was restored, the affected endpoint, and the restore result available in the logs.

Procedure

1. Go to **Logs** > **Agents** > **Central Quarantine Restore**.
2. Check the **Successful**, **Unsuccessful**, and **Pending** columns to see if Apex One successfully restored the quarantined data.
3. Click the count links in each column to view detailed information about each affected endpoint.

   Note

   For **Unsuccessful** restorations, you can attempt to restore the file again on the **Central Quarantine Restore Details** screen by clicking **Restore All**.

4. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Viewing Spyware/Grayware Logs

The Security Agent generates logs after detecting spyware and grayware and then sends the logs to the server.

Procedure

1. Go to one of the following:
   - **Logs** > **Agents** > **Security Risks**
   - **Agents** > **Agent Management**

2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Go to the **Spyware/Grayware Log Criteria** screen:
   - From the **Security Risk Logs** screen, click **View Logs** > **Spyware/Grayware Logs**.
   - From the **Agent Management** screen, click **Logs** > **Spyware/Grayware Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

Item	Description
Date/Time	The time the detection occurred
Endpoint	The endpoint on which the detection occurred
Spyware/Grayware	The name of the security threat
Scan Type	The scan that detected the threat
Result	The result of the action taken **Note** For more information on scan results, see *Spyware/Grayware Scan Results on page 7-98*.
IP Address	The IP address and port number of the source endpoint
MAC Address	The MAC address of the infected endpoint
Details	A link that displays the detailed analysis for the specific detection

6. (Optional) Select any spyware/grayware detection you consider harmless and click **Add to Approved List** to exclude the program from further scanning.
7. To save logs to a comma-separated value (CSV) file, click **Export All to CSV**. Open the file or save it to a specific location.

The CSV file contains the following information:

- All information in the logs
- User name logged on to the endpoint at the time of detection

Spyware/Grayware Scan Results

The following scan results display in the spyware/grayware logs:

TABLE 7-27. First Level Spyware/Grayware Scan Results

RESULT	DESCRIPTION
Successful, No Action Required	This is the first level result if the scan action was successful. The second level result can be any of the following: • *Cleaned* • *Access denied*
Further Action Required	This is the first level result if the scan action was unsuccessful. The second level results will have at least one of the following messages: • *Passed* • *Unable to delete spyware/grayware in protected system files* • *Spyware/Grayware scan stopped manually. Please perform a complete scan* • *Spyware/Grayware cleaned, restart required. Please restart the computer* • *Spyware/Grayware cannot be cleaned* • *Spyware/Grayware scan result unidentified. Please contact Trend Micro technical support*

TABLE 7-28. Second Level Spyware/Grayware Scan Results

RESULT	DESCRIPTION	SOLUTION
Cleaned	Apex One terminated processes or deleted registries, files, cookies and shortcuts.	N/A

Result	Description	Solution
Access denied	Apex One denied access (copy, open) to the detected spyware/grayware components.	N/A
Passed	Apex One did not perform any action but logged the spyware/grayware detection for assessment.	Add spyware/grayware that you consider safe to the spyware/grayware approved list.
Unable to delete spyware/grayware in protected system files	This message displays if the Spyware Scan Engine attempts to delete any single folder and the following criteria are met: • Items to clean exceed 250MB. • The operating system uses the files in the folder. The folder may also be necessary for normal system operation. • The folder is a root directory (such as `C:` or `F:`)	Contact your support provider for assistance.
Spyware/Grayware scan stopped manually. Please perform a complete scan	A user stopped scanning before it was completed.	Run a Manual Scan and wait for the scan to finish.
Spyware/Grayware cleaned, restart required. Please restart the computer	Apex One deleted spyware/grayware components but the endpoint needs to restart to complete the task.	Restart the endpoint immediately.
Spyware/Grayware cannot be cleaned	Spyware/Grayware was detected on a CD-ROM or network drive. Apex One cannot delete spyware/grayware detected on these locations.	Manually remove the infected file.
Spyware/Grayware scan result unidentified. Please contact Trend Micro technical support	A new version of the Spyware Scan Engine provides a new scan result that Apex One has not been configured to handle.	Contact your support provider for help in determining the new scan result.

Viewing Spyware/Grayware Restore Logs

After cleaning spyware/grayware, Security Agents back up spyware/grayware data. Notify an online agent to restore backed up data if you consider the data harmless. Information about which spyware/grayware backup data was restored, the affected endpoint, and the restore result available in the logs.

Procedure

1. Go to **Logs** > **Agents** > **Spyware/Grayware Restore**.
2. Check the **Result** column to see if Apex One successfully restored the spyware/grayware data.
3. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Viewing Suspicious File Logs

The Security Agent generates logs when it detects files in the Suspicious File list and sends the logs to the server.

Procedure

1. Go to one of the following:
   - **Logs** > **Agents** > **Security Risks**
   - **Agents** > **Agent Management**
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Logs** > **Suspicious File Logs** or **View Logs** > **Suspicious File Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

- Date and time of suspicious file detection
- Endpoint
- Domain
- Infection source SHA-1 hash value of the file
- Path of the file
- Scan type that detected the suspicious file
- Scan results

Note

For more information on scan results, see *Virus/Malware Scan Results on page 7-90*.

- IP address

Viewing Scan Operation Logs

When Manual Scan, Scheduled Scan, or Scan Now runs, the Security Agent creates a scan log that contains information about the scan. You can view the scan log by accessing the Apex One server or Security Agent consoles.

To view the Scan Operation logs on the Apex One server, go to one of the following locations:

- **Logs** > **Agents** > **Security Risks** and click **View Logs** > **Scan Operation Logs**
- **Agents** > **Agent Management** and click **Logs** > **Scan Operation Logs**

Scan Operation logs show the following information:

- Date and time Apex One started scanning
- Date and time Apex One stopped scanning

- Scan status
  - **Completed**: The scan completed normally.
  - **Interrupted**: The user stopped the scan before it completed.
  - **Stopped unexpectedly**: The scan was interrupted by the user, system, or an unexpected event. For example, the Apex One Real-time Scan service might have terminated unexpectedly or the user performed a forced restart of the endpoint.
- Scan type
- Number of scanned objects
- Number of virus/malware infected detections
- Number of spyware/grayware detections
- Smart Scan Agent Pattern version
- Virus Pattern version
- Spyware/Grayware Pattern version

Security Risk Outbreaks

A security risk outbreak occurs when detections of virus/malware, spyware/grayware, and shared folder sessions over a certain period of time exceed a certain threshold. There are several ways to respond to and contain outbreaks in the network, including:

- Enabling Apex One to monitor the network for suspicious activity
- Blocking critical agent endpoint ports and folders
- Sending outbreak alert messages to agents
- Cleaning up infected endpoints

Security Risk Outbreak Criteria and Notifications

Configure Apex One to send you and other Apex One administrators a notification whenever an outbreak occurs.

TABLE 7-29. Types of Security Risk Outbreak Notifications

TYPE	REFERENCE
• Virus/Malware outbreak • Spyware/Grayware outbreak • Shared folder session outbreak	*Configuring the Security Risk Outbreak Criteria and Notifications on page 7-104*
Firewall Violations outbreak	*Configuring the Firewall Violation Outbreak Criteria and Notifications on page 13-30*
C&C callbacks outbreak	*Configuring the C&C Callback Outbreak Criteria and Notifications on page 12-18*

Define an outbreak by the number of detections and the detection period. Apex One triggers an outbreak alert when the number of detections exceeds the configured value during the detection period.

Apex One comes with a set of default notification messages that inform you and other Apex One administrators of an outbreak. You can modify the notifications and configure additional notification settings as required.

Note

Apex One can send security risk outbreak notifications through email, SNMP trap, and Windows NT Event logs. For shared folder session outbreaks, Apex One sends notifications through email. Configure settings when Apex One sends notifications through these channels.

For details, see *Administrator Notification Settings on page 14-38*.

Configuring the Security Risk Outbreak Criteria and Notifications

Procedure

1. Go to **Administration** > **Notifications** > **Outbreak**.
2. In the **Criteria** tab:
   a. Go to the **Virus/Malware** and **Spyware/Grayware** sections:
   b. Specify the number of unique sources of detections.
   c. Specify the number of detections and the detection period for each security risk.

   Tip
   Trend Micro recommends accepting the default values in this screen.

   Apex One sends the notification after receiving 101 virus/malware detections within a 24-hour period.
3. In the **Criteria** tab:
   a. Go to the **Shared Folder Sessions** section.
   b. Select **Monitor shared folder sessions on your network**.
   c. In **Shared folder sessions recorded**, click the number link to view the endpoints with shared folders and the endpoints accessing the shared folders.
   d. Specify the number of shared folder sessions and the detection period.

   Apex One sends a notification message when the number of shared folder sessions is exceeded.
4. In the **Email** tab:
   a. Go to the **Virus/Malware Outbreaks**, **Spyware/Grayware Outbreaks**, and **Shared Folder Session Outbreaks** sections.

b. Select **Enable notification via email**.

c. Specify the email recipients.

d. Accept or modify the default email subject and message. You can use token variables to represent data in the **Subject** and **Message** fields.

TABLE 7-30. Token Variables for Security Risk Outbreak Notifications

VARIABLE	DESCRIPTION
Virus/Malware outbreaks	
%CV	Total number of viruses/malware detected
%CC	Total number of endpoints with virus/malware
Spyware/Grayware outbreaks	
%CV	Total number of spyware/grayware detected
%CC	Total number of endpoints with spyware/grayware
Shared folder session outbreaks	
%S	Number of shared folder sessions
%T	Time period when shared folder sessions accumulated
%M	Time period, in minutes

e. Select additional virus/malware and spyware/grayware information to include in the email. You can include the agent/domain name, security risk name, date and time of detection, path and infected file, and scan result.

f. Accept or modify the default notification messages.

5. In the **SNMP Trap** tab:

a. Go to the **Virus/Malware Outbreaks** and **Spyware/Grayware Outbreaks** sections.

b. Select **Enable notification via SNMP trap**.

c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 7-30: Token Variables for Security Risk Outbreak Notifications on page 7-105* for details.

6. In the **NT Event Log** tab:

   a. Go to the **Virus/Malware Outbreaks** and **Spyware/Grayware Outbreaks** sections.

   b. Select **Enable notification via NT Event Log**.

   c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 7-30: Token Variables for Security Risk Outbreak Notifications on page 7-105* for details.

7. Click **Save**.

Configuring Security Risk Outbreak Prevention

When an outbreak occurs, enforce outbreak prevention measures to respond to and contain the outbreak. Configure prevention settings carefully because incorrect configuration may cause unforeseen network issues.

Procedure

1. Go to **Agents** > **Outbreak Prevention**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click any of the following outbreak prevention policies and then configure the settings for the policy:
   - *Limiting/Denying Access to Shared Folders on page 7-108*
   - *Blocking Vulnerable Ports on page 7-109*
   - *Denying Write Access to Files and Folders on page 7-110*

- *Denying Access to Executable Compressed Files on page 7-113*
- *Creating Mutual Exclusion Handling on Malware Processes/Files on page 7-112*

5. Select the policies you want to enforce.
6. Select the number of hours outbreak prevention will stay in effect. The default is 48 hours. You can manually restore network settings before the outbreak prevention period expires.

WARNING!

Do not allow outbreak prevention to remain in effect indefinitely. To block or deny access to certain files, folders, or ports indefinitely, modify endpoint and network settings directly instead of using Apex One.

7. Accept or modify the default agent notification message.

Note

To configure Apex One to notify you during an outbreak, go to **Administration** > **Notifications** > **Outbreak**.

8. Click **Start Outbreak Prevention**.

   The outbreak prevention measures you selected display in a new window.

9. Back in the Outbreak Prevention agent tree, check the **Outbreak Prevention** column.

   A check mark appears on endpoints applying outbreak prevention measures.

Apex One records the following events in the system event logs:

- Server events (initiating outbreak prevention and notifying agents to enable outbreak prevention)
- Security Agent event (enabling outbreak prevention)

Outbreak Prevention Policies

When outbreaks occur, enforce any of the following policies:

- *Limiting/Denying Access to Shared Folders on page 7-108*
- *Blocking Vulnerable Ports on page 7-109*
- *Denying Write Access to Files and Folders on page 7-110*
- *Denying Access to Executable Compressed Files on page 7-113*
- *Creating Mutual Exclusion Handling on Malware Processes/Files on page 7-112*

Limiting/Denying Access to Shared Folders

During outbreaks, limit or deny access to shared folders on the network to prevent security risks from spreading through the shared folders.

When this policy takes effect, users can still share folders but the policy will not apply to the newly shared folders. Therefore, inform users not to share folders during an outbreak or deploy the policy again to apply the policy to the newly shared folders.

Procedure

1. Go to **Agents** > **Outbreak Prevention**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Limit/Deny access to shared folders**.
5. Select from the following options:
   - **Allow read-only access**: Limits access to shared folders
   - **Deny access**

Note

The read access only setting does not apply to shared folders already configured to deny full access.

6. Click **Save**.

   The **Outbreak Prevention Settings** screen displays again.

7. Click **Start Outbreak Prevention**.

   The outbreak prevention measures you selected display in a new window.

Blocking Vulnerable Ports

During outbreaks, block vulnerable ports that viruses/malware might use to gain access to Security Agent endpoints.

WARNING!

Configure Outbreak Prevention settings carefully. Blocking ports that are in use makes network services that depend on them unavailable. For example, if you block the trusted port, Apex One cannot communicate with the agent for the duration of the outbreak.

Procedure

1. Go to **Agents** > **Outbreak Prevention**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Block Ports**.
5. Select whether to **Block trusted port**.
6. Select the ports to block under the **Blocked Ports** column.

a. If there are no ports in the table, click **Add**. In the screen that opens, select the ports to block and click **Save**.

- **All ports (including ICMP)**: Blocks all ports except the trusted port. If you also want to block the trusted port, select the Block trusted port check box in the previous screen.
- **Specified ports**
  - **Commonly used ports**: Select at least one port number for Apex One to save the port blocking settings.
  - **Ports commonly used by Trojan programs**: Blocks ports commonly used by Trojan horse programs.
  - **Any port between 1 and 65535, or a port range**: Optionally specify the direction of the traffic to block and some comments, such as the reason for blocking the ports you specified.
  - **Ping protocol (Reject ICMP)**: Click if you only want to block ICMP packets, such as ping requests.

b. To edit settings for the blocked port(s), click the port number.

c. In the screen that opens, modify the settings and click **Save**.

d. To remove a port from the list, select the check box next to the port number and click **Delete**.

7. Click **Save**.

   The **Outbreak Prevention Settings** screen displays again.

8. Click **Start Outbreak Prevention**.

   The outbreak prevention measures you selected display in a new window.

Denying Write Access to Files and Folders

Viruses/Malware can modify or delete files and folders on the host endpoints. During an outbreak, configure Apex One to prevent viruses/

malware from modifying or deleting files and folders on Security Agent endpoints.

WARNING!

Apex One does not support denying write access to mapped network drives.

Procedure

1. Go to **Agents** > **Outbreak Prevention**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Deny write access to files and folders**.
5. Type the directory path. When you finish typing the directory path you want to protect, click **Add**.

   Note

   Type the absolute path, not the virtual path, for the directory.

6. Specify the files to protect in the protected directories. Select all files or files based on specific file extensions. For file extensions, to specify an extension that is not in the list, type it in the text box, and then click **Add**.
7. To protect specific files, under **Files to Protect**, type the full file name and click **Add**.
8. Click **Save**.

   The **Outbreak Prevention Settings** screen displays again.
9. Click **Start Outbreak Prevention**.

The outbreak prevention measures you selected display in a new window.

Creating Mutual Exclusion Handling on Malware Processes/Files

You can configure Outbreak Prevention to protect against security threats that utilize mutex processes by overriding the resources that the threat requires to infect and spread throughout the system. Outbreak Prevention creates mutual exclusions on files and processes related to known malware, preventing the malware from accessing these resources.

Tip

Trend Micro recommends maintaining these exclusions until a solution to the malware threat can be implemented. Contact Support to obtain the correct mutex names to protect against during an outbreak.

Note

Mutual exclusion handling requires the Unauthorized Change Prevention Service and only supports 32-bit platforms.

Procedure

1. Go to **Agents** > **Outbreak Prevention**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Create mutual exclusion (mutex) handling on malware processes/files**.
5. Type the mutex name to protect against in the text field provided.

   Add or remove mutex names from the list using the **+** and **-** buttons.

Note

Outbreak Prevention supports mutual exclusion handling on a maximum of six mutex threats.

6. Click **Save**.

   The **Outbreak Prevention Settings** screen displays again.

7. Click **Start Outbreak Prevention**.

   The outbreak prevention measures you selected display in a new window.

Denying Access to Executable Compressed Files

During outbreaks, denying access to executable compressed files can prevent the possible security risks that these files may contain from spreading across the network. You can choose to allow access to trusted files created by the supported executable packer programs.

Procedure

1. Go to **Agents** > **Outbreak Prevention**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Deny access to executable compressed files**.
5. Select from the list of supported executable packer programs and click **Add** to allow access to executable packed files created by these packer programs.

Note

You can only approve the use of packed files created by the packer programs in the Executable Packers list. Outbreak Prevention denies access to all other executable packed file formats.

6. Click **Save**.

   The **Outbreak Prevention Settings** screen displays again.

7. Click **Start Outbreak Prevention**.

   The outbreak prevention measures you selected display in a new window.

Disabling Outbreak Prevention

When you are confident that an outbreak has been contained and that Apex One already cleaned or quarantined all infected files, restore network settings to normal by disabling Outbreak Prevention.

Procedure

1. Go to **Agents** > **Outbreak Prevention**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Restore Settings**.
4. To inform users that the outbreak is over, select **Notify users after restoring the original settings**.
5. Accept or modify the default agent notification message.
6. Click **Restore Settings**.

Note

If you do not restore network settings manually, Apex One automatically restores these settings after the number of hours specified in **Automatically restore network settings to normal after __ hours** on the **Outbreak Prevention Settings** screen. The default setting is 48 hours.

Apex One records the following events in the system event logs:

- Server events (initiating outbreak prevention and notifying Security Agents to enable outbreak prevention)
- Security Agent event (enabling outbreak prevention)

7. After disabling outbreak prevention, scan networked endpoints for security risks to ensure that the outbreak has been contained.

Chapter 8

Protecting Against Unknown Threats

This chapter describes how to protect endpoints from unknown threats attempting to infiltrate your network.

Topics include:

Predictive Machine Learning

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

Predictive Machine Learning is a powerful tool that helps protect your environment from unidentified threats and zero-day attacks.

Detection Type	Description
File	After detecting an unknown or low-prevalence file, the Security Agent scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network. Through use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains. If a functional Internet connection is unavailable, Predictive Machine Learning automatically switches to the local model to provide constant unknown threat protection against portable executable file threats. Depending on how you configure Predictive Machine Learning, the Security Agent can attempt to “Quarantine” the affected file to prevent the threat from continuing to spread across your network.

Detection Type	Description
Process	After detecting an unknown or low-prevalence process, the Security Agent monitors the process using the Contextual Intelligence Engine, and sends the behavioral report to the Predictive Machine Learning engine. Through use of behavioral malware modeling, Predictive Machine Learning compares the process behavior to the model, assigns a probability score, and determines the probable malware type the process is executing. Process detection also monitors script execution. If the Contextual Intelligence Engine detects the execution of a suspicious script, Predictive Machine Learning takes the configured action. Predictive Machine Learning performs script blocking on the following types of scripts: • cscript • jar • powershell • vbs • wscript Depending on how you configure Predictive Machine Learning, the Security Agent can "Terminate" the affected process or script and attempt to clean the file that executed the process or script.

Configuring Predictive Machine Learning Settings

Note

Predictive Machine Learning requires that you enable the following services:

- Unauthorized Change Prevention
- Advanced Protection Service

For more information, see *Configuring Additional Security Agent Services on page 15-9*.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Predictive Machine Learning Settings**.

   The **Predictive Machine Learning Settings** screen appears.
4. Select **Enable Predictive Machine Learning**.
5. Under **Detection Settings**, select the type of detections and related action that Predictive Machine Learning takes.

Detection Type	Actions
File	• **Quarantine**: Select to automatically quarantine files that exhibit malware-related features based on the Predictive Machine Learning analysis • **Log only**: Select to scan unknown files and log the Predictive Machine Learning analysis for further in-house investigation of the threat
Process	• **Terminate**: Select to automatically terminate processes or scripts that exhibit malware-related behaviors based on the Predictive Machine Learning analysis **Important** Predictive Machine Learning attempts to clean the files that executed the malicious processes or scripts. If the clean action is unsuccessful, Predictive Machine Learning quarantines the affected files. • **Log only**: Select to scan unknown processes or scripts and log the Predictive Machine Learning analysis for further in-house investigation of the threat

6. Under **Exceptions**, configure the global Predictive Machine Learning file exceptions to prevent all agents from detecting a file as malicious.

a. Click **Add File Hash**.

   The **Add File to Exception List** screen appears.

b. Specify the file SHA-1 hash value to exclude from scanning.

c. Optionally provide a note regarding the reason for the exception or to describe the file name(s) associated with the hash value.

d. Click **Add**.

   Predictive Machine Learning adds the file hash to the Exceptions list.

7. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Suspicious Connection Service

The Suspicious Connection Service manages the User-defined and Global IP C&C lists, and monitors the behavior of connections that endpoints make to potential C&C servers.

- The User-defined Approved and Blocked IP lists allow further control over whether endpoints can access specific IP addresses. Configure these lists when you want to allow access to an address blocked by the Global C&C IP list or block access to an address that may pose a security risk.

  For details, see *Configuring Global User-defined IP List Settings on page 8-6*.

- The Global C&C IP list works in conjunction with the Network Content Inspection Engine (NCIE) to detect network connections with Trend Micro confirmed C&C servers. NCIE detects C&C server contact through any network channel. The Suspicious Connection Service logs all connection information to servers in the Global C&C IP list for evaluation.

  For details on enabling the Global C&C IP list, see *Configuring Suspicious Connection Settings on page 8-7*.

- After detecting malware on endpoints through Relevance Rule Pattern matching on network packets, the Suspicious Connection Service can further investigate the connection behavior to determine if a C&C callback occurred. After detecting a C&C callback, the Suspicious Connection Service can attempt to block and clean the source of the connection using GeneriClean technology.

  For details on configuring the Suspicious Connection Service, see *Configuring Suspicious Connection Settings on page 8-7*.

  For details about GeneriClean, see *GeneriClean on page D-4*.

Enable the Suspicious Connection Service on the **Additional Service Settings** screen to protect agents against C&C server callbacks. For details, see *Configuring Additional Security Agent Services on page 15-9*.

Configuring Global User-defined IP List Settings

Administrators can configure Apex One to allow, block, or log all connections between agents and user-defined C&C IP addresses.

Note

The User-defined IP Lists only support IPv4 addresses.

Procedure

1. Go to **Agents** > **Global Agent Settings**.

2. Click the **Security Settings** tab.
3. Go to the **Suspicious Connections Settings** section.
4. Click **Edit User-defined IP List**.
5. On the **Approved List** or **Blocked List** tab, add the IP addresses that you want to monitor.

   Tip

   You can configure Apex One to only log connections made to addresses in the User-defined Blocked IP list. To only log connections made to the addresses in the User-defined Blocked IP list, see *Configuring Suspicious Connection Settings on page 8-7*.

   a. Click **Add**.

   b. On the new screen that appears, type the IP address, IP address range, or IPv4 address and subnet mask for Apex One to monitor.

   c. Click **Save**.

6. To remove IP addresses from the list, select the check box next to the address and click **Delete**.
7. After configuring the lists, click **Close** to return to the **Global Agent Settings** screen.
8. Click **Save** to deploy the updated list to agents.

Configuring Suspicious Connection Settings

Security Agents can log and block all connections made between endpoints and addresses in the Global C&C IP list. You can also log, but still allow access to, IP addresses configured in the User-defined Blocked IP List.

Security Agents can also monitor connections that may be the result of a botnet or other malware threat. After detecting a malware threat, Security Agents can attempt to clean the infection.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Suspicious Connection Settings**.

   The **Suspicious Connection Settings** screen appears.
4. Enable the **Detect network connections made to addresses in the Global C&C IP list** setting to monitor connections made to Trend Micro confirmed C&C servers and select to **Log only** or **Block** connections.

   - To allow agents to connect to addresses in the User-defined Blocked IP list, enable the **Log and allow access to User-defined Blocked IP list addresses** setting.

   Note

   You must enable network connection logging before Security Agents can allow access to addresses in the User-defined Blocked IP list.

   For details about the Global C&C IP list, see *Suspicious Connection Service on page 8-5*.
5. Enable the **Detect connections using malware network fingerprinting** setting and select to **Log only** or **Block** connections.

   Malware network fingerprinting performs pattern matching on packet headers. Security Agents log all connections made by packets with headers that match known malware threats using the Relevance Rule pattern.

   - To allow Security Agents to attempt to clean connections made to C&C servers, enable the **Clean suspicious connections when a C&C callback is detected** setting. Security Agents use GeneriClean to clean the malware threat and terminate the connection to the C&C server.

Note

You must enable **Log connections using malware network fingerprinting** before Security Agents can attempt to clean the connections made to C&C servers detected by packet structure matching.

6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Sample Submission

You can configure Security Agents to submit file objects that may contain previously unidentified threats to a Virtual Analyzer for further analysis. After assessing the objects, Virtual Analyzer adds any objects found to contain unknown threats to the Virtual Analyzer Suspicious Objects lists and distributes the lists to other Security Agents throughout the network.

For more information, see *Suspicious Object List Settings on page 14-34*.

Sample Submission requires the following:

- You must register the Apex One server with a Control Manager server (7.0 or later) or the Trend Micro Apex Central server (2019 or later)
- The Control Manager or Trend Micro Apex Central server must have an active connection to a Trend Micro Deep Discovery Analyzer server (5.1 or later)

Suspicious files include any of the following:

- Programs not known to Trend Micro (downloaded through supported web browsers or email channels)

- Heuristic detections of processes (downloaded through supported web browsers or email channels)
- Low prevalence autorun programs on removable storage

Important

The size of the sample files that the Security Agents can submit changes based on the type of Virtual Analyzer you use. For the Deep Discovery Analyzer server, sample files can be up to 50 MB in size. For Deep Discovery Analyzer as a Service Add-on, sample files can be up to 60 MB in size.

Configuring Sample Submission

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Sample Submission Settings**.

   The **Sample Submission Settings** screen appears.
4. Select **Enable suspicious file submission to Virtual Analyzer**.
5. Click **Save**.

Unknown Threat Logs

Security Agents log unknown threat activity and send the logs to the server. Any Security Agent that runs continuously aggregates the logs and sends them at specified intervals, which is every 60 minutes by default.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing Predictive Machine Learning Logs

Procedure

1. Go to one of the following:
   - **Logs** > **Agents** > **Security Risks**
   - **Agents** > **Agent Management**
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Go to the **Predictive Machine Learning Log Criteria** screen:
   - From the **Security Risk Logs** screen, click **View Logs** > **Predictive Machine Learning Logs**.
   - From the **Agent Management** screen, click **Logs** > **Predictive Machine Learning Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

Item	Description
Date/Time	The time the detection occurred
Endpoint	The endpoint on which the detection occurred
IP Address	The IP address and port number of the source endpoint
Security Threat	The name of the security threat determined by the Predictive Machine Learning engine
Result	The result of the action taken

Item	Description
Infected File/Object	The name of the file object or the program that executed the process
Type	The type of object that triggered the detection (“File” or “Process”)
File Path	The path of the file object or the path of the program that executed the process
Infection Channel	The channel the threat originated from
Details	A link that displays the detailed analysis for the specific detection For more information, see *Predictive Machine Learning Log Details on page 8-12*.

6. To save logs to a comma-separated value (CSV) file, click **Export All to CSV**. Open the file or save it to a specific location.

Predictive Machine Learning Log Details

You can view a comprehensive report for each Predictive Machine Learning log detection by clicking the **View** link under the **Details** column.

The **Log Details** screen consists of two sections:

- Top banner: Specific details related to this particular log detection
- Bottom tab controls: Details related to the Predictive Machine Learning threat, including threat probability scores, file information, and other endpoints across your network that have the same detection

The following table discusses the information provided in the top banner.

TABLE 8-1. Log Details - Top Banner

SECTION	DESCRIPTION
Detection time / Action	Indicates when this specific log detection occurred and the action that the agent took on the threat
File name	Indicates the name of the file that triggered the detection on the specified endpoint **Tip** Click **Add to Exception List** to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the **Predictive Machine Learning Settings** screen. For more information, see *Configuring Predictive Machine Learning Settings on page 8-3*. **Important** The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the **Affected Endpoints** tab to verify the file name on other endpoints.
Endpoint information	Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint
Channel information	Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to

The following table discusses the information provided on the bottom tabs.

TABLE 8-2. Log Details - Tab Information

TAB	DESCRIPTION
Threat Indicators	Provides the results of the Predictive Machine Learning analysis • **Threat Probability**: Indicates how closely the file/process matched the malware model • **Probable Threat Type**: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats • **Threat Identifiers**: Provides a list a API functions used by the file/process that may be indicative of the detected threat type **Important** API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. • **Similar Known Threats**: Provides a list of known threat types that exhibit similar file/process features to the detection
File Details	Provides general details related the file properties and certificate information for this specific detection log
Affected Endpoints	Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents

Viewing Suspicious Connection Logs

Procedure

1. Go to one of the following:
   - **Logs** > **Agents** > **Security Risks**
   - **Agents** > **Agent Management**

2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Go to the **Suspicious Connection Log Criteria** screen:
   - From the **Security Risk Logs** screen, click **View Logs** > **Suspicious Connection Logs**.
   - From the **Agent Management** screen, click **Logs** > **Suspicious Connection Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

Item	Description
Date/Time	The time the detection occurred
Endpoint	The endpoint on which the detection occurred
Domain	The domain of the endpoint on which the detection occurred
Process	The process through which the contact was attempted (path\application_name)
Local IP and Port	The IP address and port number of the source endpoint
Remote IP and Port	The IP address and port number of the destination endpoint
Result	The result of the action taken
List Source	The C&C list source that identified the C&C server
Traffic Direction	The direction of the transmission

6. To save logs to a comma-separated value (CSV) file, click **Export to All to CSV**. Open the file or save it to a specific location.

Viewing Sample Submission Logs

Apex One stores sample submission data in the system events logs. For a more comprehensive summary of the sample submission data, Trend Micro recommends viewing the logs using the Apex Central console. Apex Central provides a detailed analysis of the suspicious object file handling process, providing better visibility regarding how suspicious objects may affect your network.

Procedure

1. Go to **Logs** > **System Events**.
2. Under **Event**, check for the following log types:
   - "Sample submitted to Virtual Analyzer [file[<file_name], SHA1[<file_SHA1_value>]"
   - "Virtual Analyzer sample analysis complete [<date_time_analysis_completed>, file[<file_name], SHA1[<file_SHA1_value>], virus[<detection_type], rule[<virtual_analyzer_rule_type]]"

Chapter 9

Using Behavior Monitoring

This chapter describes how to protect computers from security risks using the Behavior Monitoring feature.

Topics include:

Behavior Monitoring

Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through **Malware Behavior Blocking** and **Event Monitoring**. Complementing these two features are a user-configured **exception list** and the **Certified Safe Software Service**.

Important

By default, Behavior Monitoring is disabled on all versions of Windows Server platforms.

Malware Behavior Blocking

Malware Behavior Blocking provides a necessary layer of additional threat protection from programs that exhibit malicious behavior. It observes system events over a period of time. As programs execute different combinations or sequences of actions, Malware Behavior Blocking detects known malicious behavior and blocks the associated programs. Use this feature to ensure a higher level of protection against new, unknown, and emerging threats.

Behavior Monitoring can detect malicious scripts executed by legitimate Windows programs and the true payload path of script files executed by legitimate DLLs to protect endpoints against malware hidden in fileless attack vectors.

Malware Behavior Monitoring provides the following threat-level scanning options:

- **Known threats**: Blocks behaviors associated with known malware threats
- **Known and potential threats**: Blocks behavior associated with known threats and takes action on behavior that is potentially malicious

After blocking a program with notifications enabled, the Security Agent displays a notification on the endpoint.

For details about notifications, see *Behavior Monitoring Notifications for Security Agent Users on page 9-21*.

Ransomware Protection

Ransomware Protection prevents the unauthorized modification or encryption of files on agents by "ransomware" threats. Ransomware is a type of malware which restricts access to files and demands payment to restore the affected files.

Apex One provides the following methods to protect your environment from ransomware threats.

Note

To reduce the chance of the Security Agent detecting a safe process as malicious, ensure that the agent has Internet access to perform additional verification processes using Trend Micro servers.

Option	Description
Protect documents against unauthorized encryption or modification	You can configure Behavior Monitoring to detect a specific sequence of events that may indicate a ransomware attack. After Behavior Monitoring matches all of the following criteria, the Security Agent terminates and attempts to quarantine malicious programs: 1. A process not recognized as safe attempts to modify, delete, or rename three files within a certain time interval. 2. The process attempted to modify a protected file extension type Additionally enable **Automatically back up files changed by suspicious programs** to create copies of files being encrypted on endpoints. After the encryption process completes and Apex One detects a ransomware threat, Apex One prompts end users to restore the affected files without suffering any loss of data. **Note** Automatic file backup requires at least 100 MB of disk space on the agent endpoint and only backs up files that are less than 10 MB in size. The backup folder location on agent endpoints is: <Agent installation folder>`\CCSF\module\DRE\data`. **WARNING!** If **Automatically back up files changed by suspicious programs** is not enabled, Apex One cannot recover the first files affected by a ransomware threat.
Block processes commonly associated with ransomware	Ransomware commonly distributes executable files in specific locations on endpoints before attempting to hijack files. Blocking the processes started from these locations can help prevent the ransomware from being able to hijack files.

Option	Description
Enable program inspection to detect and block compromised executable files	Program inspection monitors processes and performs API hooking to determine if a program is behaving in an unexpected manner. Although this procedure increases the overall detection ratio of compromised executable files, it may result in decreased system performance. **Tip** Program inspection provides increased security if you select **Known and potential threats** in the **Threats to block** drop-down.

Anti-Exploit Protection

Anti-exploit protection works in conjunction with program inspection to monitor the behavior of programs and detect abnormal behavior that may indicate that an attacker has exploited a program vulnerability. Once detected, Behavior Monitoring terminates the program processes.

Important

Anti-exploit Protection requires that you select **Enable program inspection to detect and block compromised executable files**.

Newly Encountered Program Protection

Behavior Monitoring works in conjunction with Web Reputation Services and Real-time Scan to verify the prevalence of files downloaded through web channels, email applications, or Microsoft Office macro scripts. After detecting a "newly encountered" file, administrators can choose to prompt users before executing the file. Trend Micro classifies a program as newly encountered based on the number of file detections or historical age of the file as determined by the Smart Protection Network.

Behavior Monitoring scans the following file types for each channel:

- Web (HTTP/HTTPS): Scans `.exe` files.
- Email applications: Scans `.exe`, and compressed `.exe` files in unencrypted `.zip` and `.rar` files.

Note

- Administrators must enable Web Reputation Services on the agent to allow the Security Agent to scan HTTP or HTTPS traffic before this prompt can display.
- The Security Agent matches the file names downloaded through email applications during the execution process. If the file name has been changed, the user does not receive a prompt.

Event Monitoring

Event Monitoring provides a more generic approach to protecting against unauthorized software and malware attacks. It monitors system areas for certain events, allowing administrators to regulate programs that trigger such events. Use Event Monitoring if you have specific system protection requirements that are above and beyond what is provided by Malware Behavior Blocking.

The following table provides a list of monitored system events.

TABLE 9-1. Monitored System Events

EVENTS	DESCRIPTION
Duplicated System File	Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.
Hosts File Modification	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the web browser is redirected to infected, non-existent, or fake websites.

Events	Description
Suspicious Behavior	Suspicious behavior can be a specific action or a series of actions that is rarely carried out by legitimate programs. Programs exhibiting suspicious behavior should be used with caution.
New Internet Explorer Plugin	Spyware/grayware programs often install unwanted Internet Explorer plugins, including toolbars and Browser Helper Objects.
Internet Explorer Setting Modification	Malware programs may change Internet Explorer settings, including the home page, trusted websites, proxy server settings, and menu extensions.
Security Policy Modification	Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.
Program Library Injection	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.
Shell Modification	Many malicious programs modify Windows shell settings to associate themselves to certain file types. This routine allows malicious programs to launch automatically if users open the associated files in Windows Explorer. Changes to Windows shell settings can also allow malicious programs to track the programs used and start alongside legitimate applications.
New Service	Windows services are processes that have special functions and typically run continuously in the background with full administrative access. Malicious programs sometimes install themselves as services to stay hidden.
System File Modification	Certain Windows system files determine system behavior, including startup programs and screen saver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.
Firewall Policy Modification	The Windows Firewall policy determines the applications that have access to the network, the ports that are open for communication, and the IP addresses that can communicate with the computer. Many malicious programs modify the policy to allow themselves to access to the network and the Internet.

Events	Description
System Process Modification	Many malicious programs perform various actions on built-in Windows processes. These actions can include terminating or modifying running processes.
New Startup Program	Malicious applications usually add or modify autostart entries in the Windows registry to automatically launch every time the computer starts.

When Event Monitoring detects a monitored system event, it performs the action configured for the event.

The following table lists possible actions that administrators can take on monitored system events.

Table 9-2. Actions on Monitored System Events

Action	Description
Assess	The Security Agent always allows programs associated with an event to run and logs the event for assessment. This is the default action for all monitored system events. **Note** This option is not supported for the Program Library Injection (DLL injection) event on 64-bit systems.
Allow	The Security Agent always allows programs associated with an event to run.

Action	Description
Ask when necessary	The Security Agent prompts users to allow or deny programs associated with an event from running and adds the programs to the exception list If the user does not respond within a certain time period, the Security Agent automatically allows the program to run. The default time period is 30 seconds. To modify the time period, see *Configuring Global Behavior Monitoring Settings on page 9-18*. **Note** This option is not supported for the Program Library Injection (DLL injection) event on 64-bit systems.
Deny	The Security Agent always blocks programs associated with an event from running and logs the event. After blocking a program with notifications enabled, the Security Agent displays a notification on the endpoint. For details about notifications, see *Behavior Monitoring Notifications for Security Agent Users on page 9-21*.

Behavior Monitoring Exception List

The Behavior Monitoring exception list contains programs that the Security Agent does not monitor using Behavior Monitoring.

- **Approved Programs**: The Security Agent allows all programs in the Approved Programs list to pass Behavior Monitoring scanning.

Note

Although Behavior Monitoring does not take action on programs added to the Approved Programs list, other scan features (such as file-based scanning) continue to scan the program before allowing the program to run.

- **Blocked Programs**: The Security Agent blocks all programs in the Blocked Programs list. To configure the Blocked Programs list, enable Event Monitoring.

Configure the exception list from the web console. You can also grant users the privilege to configure their own exception list from the Security Agent console.

For details, see *Behavior Monitoring Privileges on page 9-20*.

Exception List Wildcard Support

The Behavior Monitoring Approved List supports the use of wildcard characters when defining file path, file name, and file extension exception types. Use the following tables to properly format your exception lists to ensure that Apex One excludes the correct files and folders from scanning.

Supported wildcard characters:

- Asterisk (*): Represents any character or string of characters
- Question mark (?): Represents a single character

Important

The Behavior Monitoring Approved List does not support the use of wildcard characters to replace system drive designations or UNC addresses.

Exception Type	Wildcard Usage	Matched	Not Matched
Directories	`C:\*` Excludes all files and folders on the specified drive	• `C:\sample.exe` • `C:\folder\test.doc`	• `D:\sample.exe` • `E:\folder\test.doc`

Exception Type	Wildcard Usage	Matched	Not Matched
Specific files under a specific folder layer	`C:\*\Sample.exe` Excludes the `Sample.exe` file only if the file is located in any subfolder of the `C:\` directory	• `C:\files\Sample.exe` • `C:\temp\files\Sample.exe`	• `C:\sample.exe`
UNC paths	`\\<UNC path>\*\Sample.exe` Excludes the `Sample.exe` file only if the file is located in any subfolder of the specified UNC path	• `\\<UNC path>\files\Sample.exe` • `\\<UNC path>\temp\files\Sample.exe`	• `R:\files\Sample.exe` Reason: Mapped drives are not supported. • `\\<UNC path>\Sample.exe` Reason: The file does not exist within a subfolder of the UNC path.
File names and extensions	`C:\*.*` Excludes all files with extensions in all folders and subfolders of the `C:\` directory	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\test.doc`	• `D:\sample.exe` • `C:\Sample` **Note** `C:\Sample` does not have a file extension and is therefore not excluded from scanning.

Exception Type	Wildcard Usage	Matched	Not Matched
File names	`C:\*.exe` Excludes all files with the `.exe` extension in all folders and subfolders of the `C:\` directory	• `C:\Sample.exe` • `C:\temp\test.exe`	• `C:\Sample.doc` • `C:\temp\test.bat` • `C:\Sample` **Note** `C:\Sample` does not have a file extension and is therefore not excluded from scanning.
File extensions	`C:\Sample.*` Excludes all files with the name `Sample` and any extension in the `C:\` directory	• `C:\Sample.exe`	• `C:\Sample1.doc` • `C:\temp\Sample.bat` • `C:\Sample` **Note** `C:\Sample` does not have a file extension and is therefore not excluded from scanning.

Exception Type	Wildcard Usage	Matched	Not Matched
Files in specific directory structures	`C:\*\*\Sample.exe` Excludes all files located within the second subfolder layer or any subsequent subfolders of the `C:\` directory with the file name and extension `Sample.exe`	• `C:\files\temp\Sample.exe` • `C:\files\temp\test\Sample.exe`	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\files\temp\Sample.doc`

Exception Type	Wildcard Usage	Matched	Not Matched
Complex paths or file names	`C:\Sam*e??.exe` Excludes all files with names that satisfy the following conditions: • Begin with the characters "Sam" • The third last character of the file name must be "e" • At least 1 character exists between the opening "Sam" string and closing "e??" string of the file name • Exactly 2 characters exist before the file extension and after the "e" in the file name • The file extension is `.exe` If a file meets all the required conditions and is located the `C:\` directory, Behavior Monitoring excludes the file from scans.	• `C:\Sample12.exe` • `C:\SamSamSample12.exe`	• `C:\SaSmple12.exe` Reason: Does not start with "Sam" • `C:\SamSamSam12.exe` Reason: Does not contain "e" as the third last character • `C:\Same12.exe` Reason: Does not include characters between the starting "Sam" string and third last "e" character • `C:\Sample1.exe` Reason: Does not include 2 characters before the extension and after the "e" • `C:\Sample12.doc` Reason: Incorrect extension

Exception List Environment Variable Support

The following table lists the environment variables you can use when adding a file or folder path to the list.

Environment Variable	Example	Equivalent Path
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{current_user_account}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

Configuring Malware Behavior Blocking, Event Monitoring, and the Exception List

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Behavior Monitoring Settings**.
4. Click the **Rules** tab.

5. In the **Malware Behavior Blocking** section:

   a. Select **Enable Malware Behavior Blocking** and specify the types of threats to block:

      - **Known threats**: Blocks behaviors associated with known malware threats
      - **Known and potential threats**: Blocks behaviors associated with known threats and takes action on behavior that is potentially malicious

   b. Select which Ransomware Protection features you want to enable to protect against ransomware threats.

      - **Protect documents against unauthorized encryption or modification**: Stops potential ransomware threats from encrypting or modifying the contents of documents
        - **Automatically back up and restore files changed by suspicious programs**: Creates backup copies of files being encrypted on endpoints to prevent any loss of data after detecting a ransomware threat

        Note

        Automatic file backup requires at least 100 MB of disk space on the agent endpoint and only backs up files that are less than 10 MB in size.

      - **Block processes commonly associated with ransomware**: Blocks processes associated with known ransomware threats before any encryption or modification of documents can occur
      - **Enable program inspection to detect and block compromised executable files**: Program inspection monitors processes and performs API hooking to determine if a program is behaving in an unexpected manner. Although this procedure increases the overall detection ratio of compromised executable files, it may result in decreased system performance.

Tip

Program inspection provides increased security if you select **Known and potential threats** in the **Threats to block** drop-down.

For details, see *Ransomware Protection on page 9-3*.

c. Under **Anti-exploit Protection**, enable **Terminate programs that exhibit abnormal behavior associated with exploit attacks** to protect against potentially exploited programs.

Note

Anti-exploit Protection requires that you select **Enable program inspection to detect and block compromised executable files**.

For details, see *Anti-Exploit Protection on page 9-5*.

6. In the **Newly Encountered Programs** section, enable **Monitor newly encountered programs downloaded through web or email application channels** and select whether to **Prompt user** before executing the downloaded program or to have Apex One log the detections only.

7. In the **Event Monitoring** section:

   a. Select **Enable Event Monitoring**.

   b. Choose the system events to monitor and select an action for each of the selected events.

      For information about monitored system events and actions, see *Event Monitoring on page 9-6*.

8. Click the **Exceptions** tab to configure the exception lists.

   a. Under **Type the full program path**, type the full path of the program to approve or block.

   b. Click **Add to Approved List** or **Add to Blocked List**.

   c. To remove a blocked or approved program from the list, click the trash bin icon ( ) next to the program.

Note

Apex One accepts a maximum combined total of 1024 approved programs and blocked programs.

9. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Configuring Global Behavior Monitoring Settings

Apex One applies global agent settings to all agents or only to agents with certain privileges.

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **Security Settings** tab.
3. Go to the **Behavior Monitoring Settings** section.
4. Configure the **Automatically take action if the user does not respond within __ second(s)** setting as required.

   This setting only works if Event Monitoring is enabled and the action for a monitored system event is "Ask when necessary". This action prompts a user to allow or deny programs associated with the event. If the user does not respond within a certain time period, Apex One automatically allows the program to run.

   For details, see *Event Monitoring on page 9-6*.

5. Click the **System** tab.

6. Go to the **Certified Safe Software Service Settings** section and enable the Certified Safe Software Service as required.

   The Certified Safe Software Service queries Trend Micro datacenters to verify the safety of a program detected by Malware Behavior Blocking, Event Monitoring, Firewall, or antivirus scans. Enable Certified Safe Software Service to reduce the likelihood of false positive detections.

   Note

   Ensure that Security Agents have the correct proxy settings (for details, see *Security Agent Proxy Settings on page 15-50*) before enabling Certified Safe Software Service. Incorrect proxy settings, along with an intermittent Internet connection, can result in delays or failure to receive a response from Trend Micro datacenters, causing monitored programs to appear unresponsive.

   In addition, pure IPv6 Security Agents cannot query directly from Trend Micro datacenters. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Security Agents to connect to the Trend Micro datacenters.

7. Click **Save**.

Behavior Monitoring Privileges

If agents have the Behavior Monitoring privileges, the Behavior Monitoring option displays on the **Settings** screen on the Security Agent console. Users can then manage their own exception list.

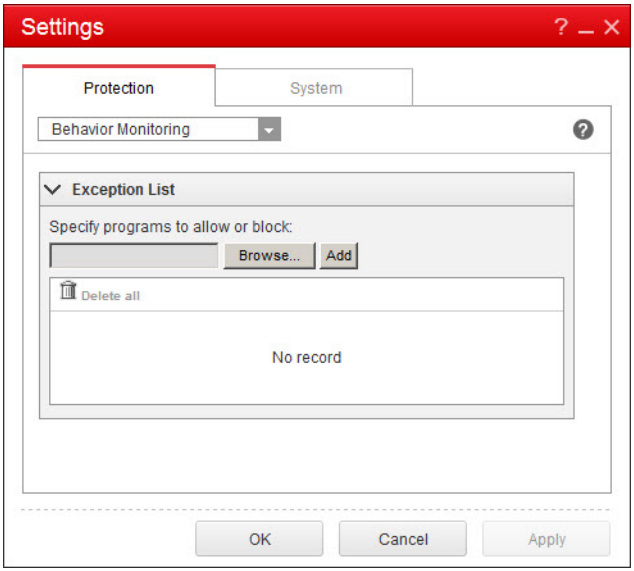


FIGURE 9-1. Behavior Monitoring option on the Security Agent console

Granting Behavior Monitoring Privileges

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.

4. On the **Privileges** tab, go to the **Behavior Monitoring Privileges** section.
5. Select **Display the Behavior Monitoring settings on the Security Agent console**.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Behavior Monitoring Notifications for Security Agent Users

Apex One can display a notification message on the Security Agent computer immediately after Behavior Monitoring blocks a program. Enable the sending of notification messages and optionally modify the content of the message.

Enabling the Sending of Notification Messages

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Behavior Monitoring Settings** section.

5. Select **Display a notification when a program is blocked**.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Modifying the Content of the Notification Message

Procedure

1. Go to **Administration** > **Notifications** > **Agent**.
2. From the **Type** drop-down, select **Behavior Monitoring Policy Violations**.
3. Modify the default messages in the text boxed provided.
   - Behavior Monitoring policy violations: Specify the message that end users receive when Malware Behavior Blocking detects a policy violation.
   - Newly encountered programs: Specify the message that end users receive when Behavior Blocking detects an unrecognized program downloaded through web or email application channels.
4. Click **Save**.

Behavior Monitoring Logs

Security Agents log unauthorized program access instances and send the logs to the server. Any Security Agent that runs continuously aggregates the

logs and sends them at specified intervals, which is every 60 minutes by default.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing Behavior Monitoring Logs

Procedure

1. Go to **Logs** > **Agents** > **Security Risks** or **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Logs** > **Behavior Monitoring Logs** or **View Logs** > **Behavior Monitoring Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date/Time unauthorized process was detected
   - Endpoint where unauthorized process was detected
   - Endpoint domain
   - Violation, which is the event monitoring rule violated by the process
   - Action performed when violation was detected
   - Event, which is the type of object accessed by the program
   - Risk level of the unauthorized program
   - Program, which is the unauthorized program
   - Operation, which is the action performed by the unauthorized program

- Target, which is the process that was accessed
- Infection channel from where the threat originated

6. To save logs to a comma-separated value (`CSV`) file, click **Export to CSV**. Open the file or save it to a specific location.

Configuring the Behavior Monitoring Log Sending Schedule

Procedure

1. Access <*Server installation folder*>`\PCCSRV`.
2. Open the `ofcscan.ini` file using a text editor such as Notepad.
3. Search for the string "`SendBMLogPeriod`" and then check the value next to it.

   The default value is 3600 seconds and the string appears as `SendBMLogPeriod=3600`.
4. Specify the value in seconds.

   For example, to change the log period to 2 hours, change the value to 7200.
5. Save the file.
6. Go to **Agents** > **Global Agent Settings**.
7. Click **Save** without changing any settings.
8. Restart the agent.

Chapter 10

Using Device Control

This chapter describes how to protect computers from security risks using the Device Control feature.

Topics include:

Device Control

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

You can configure Device Control policies for internal and external agents. Administrators typically configure a stricter policy for external agents.

Policies are granular settings in the Apex One agent tree. You can enforce specific policies to agent groups or individual agents. You can also enforce a single policy to all agents.

After you deploy the policies, agents use the location criteria you have set in the **Endpoint Location** screen (see *Endpoint Location on page 15-2*) to determine their location and the policy to apply. Agents switch policies each time the location changes.

Important

- By default, Device Control is disabled on all versions of Windows Server. Before enabling Device Control on these server platforms, read the guidelines and best practices outlined in *Security Agent Services on page 15-6*.
- For a list of supported device models, see the *Data Protection Lists* document at:

  http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

The types of devices that Apex One can monitor depends on whether the Data Protection license is activated. Data Protection is a separately licensed module and must be activated before you can use it. For details about the Data Protection license, see *Data Protection License on page 3-4*.

TABLE 10-1. Devices Monitored by the Unauthorized Change Prevention Service

DEVICE TYPE	DEVICE DESCRIPTION
Storage Devices	CD/DVD **Important** Device Control can only limit access to CD/DVD recording devices that use the Live File System format. Some third-party applications that use Master Format can still perform read/write operations even with Device Control enabled. Use Data Loss Prevention to limit access to CD/DVD recording devices that use any format type. For details, see *Blocking Access to Data Recorders (CD/DVD) on page 11-33*.
	Floppy disks
	Network drives
	USB storage devices

TABLE 10-2. Devices Monitored by Data Loss Prevention

DEVICE TYPE	DEVICE DESCRIPTION
Mobile Devices	Mobile devices
Storage Devices	CD/DVD
	Floppy disks
	Network drives
	USB storage devices

Device Type	Device Description
Non-storage Devices	Bluetooth adapters
	COM and LPT ports
	IEEE 1394 interface
	Imaging devices
	Infrared devices
	Modems
	PCMCIA cards
	Print screen key
	Wireless NICs

Permissions for Storage Devices

Device Control permissions for storage devices are used when you:

- Allow access to USB storage devices, CD/DVD, floppy disks, and network drives. You can grant full access to these devices or limit the level of access.
- Configure the list of approved USB storage devices. Device Control allows you to block access to all USB storage devices, except those that have been added to the list of approved devices. You can grant full access to the approved devices or limit the level of access.

The following table lists the permissions for storage devices.

TABLE 10-3. Device Control Permissions for Storage Devices

PERMISSIONS	FILES ON THE DEVICE	INCOMING FILES
Full access	Permitted operations: Copy, Move, Open, Save, Delete, Execute	Permitted operations: Save, Move, Copy This means that a file can be saved, moved, and copied to the device.
Modify	Permitted operations: Copy, Move, Open, Save, Delete Prohibited operations: Execute	Permitted operations: Save, Move, Copy
Read and execute	Permitted operations: Copy, Open, Execute Prohibited operations: Save, Move, Delete	Prohibited operations: Save, Move, Copy
Read	Permitted operations: Copy, Open Prohibited operations: Save, Move, Delete, Execute	Prohibited operations: Save, Move, Copy
List device content only	Prohibited operations: All operations The device and the files it contains are visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy
Block (available after installing Data Protection)	Prohibited operations: All operations The device and the files it contains are not visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy

File-based scanning complements, and may override, the device permissions. For example, if the permission allows a file to be opened but the Security Agent detects that the file is infected with malware, a specific scan action is performed on the file to eliminate the malware. If the scan action is Clean, the file opens after it is cleaned. However, if the scan action is Delete, the file is deleted.

Tip

Device Control for Data Protection supports all 64-bit platforms. For Unauthorized Change Prevention monitoring on systems that the Security Agent does not support, set the device permission to **Block** to limit access to these devices.

Advanced Permissions for Storage Devices

Advanced permissions apply when you grant limited permissions to most storage devices. The permission can be any of the following:

- **Modify**
- **Read and execute**
- **Read**
- **List device content only**

You can keep the permissions limited but grant advanced permissions to certain programs on the storage devices and on the local endpoint.

To define programs, configure the following program lists.

TABLE 10-4. Program Lists

PROGRAM LIST	DESCRIPTION	VALID INPUTS
Programs with read and write access to devices	This list contains local programs and programs on storage devices that have read and write access to the devices. An example of a local program is Microsoft Word (`winword.exe`), which is usually found in `C:\Program Files\Microsoft Office \Office`. If the permission for USB storage devices is "List device content only" but "`C:\Program Files\Microsoft Office \Office\winword.exe`" is included in this list: • A user will have read and write access to any file on the USB storage device that is accessed from Microsoft Word. • A user can save, move, or copy a Microsoft Word file to the USB storage device.	Program path and name For details, see *Wildcard Support for the Device Control Allowed Programs List on page 10-9*.
Programs on devices that are allowed to execute	This list contains programs on storage devices that users or the system can execute. For example, if you want to allow users to install software from a CD, add the installation program path and name, such as "`E:\Installer\Setup.exe`", to this list.	Program path and name or Digital Signature Provider For details, see *Wildcard Support for the Device Control Allowed Programs List on page 10-9* or *Specifying a Digital Signature Provider on page 10-8*.

There are instances when you need to add a program to both lists. Consider the data lock feature in a USB storage device, which, if enabled, prompts users for a valid user name and password before the device can be unlocked. The data lock feature uses a program on the device called "`Password.exe`", which must be allowed to execute so that users can unlock the device successfully. "`Password.exe`" must also have read and write access to the device so that users can change the user name or password.

Each program list on the user interface can contain up to 100 programs.

If you want to add more programs to a program list, you will need to add them to the `ofcscan.ini` file, which can accommodate up to 1,000 programs. For instructions on adding programs to the `ofcscan.ini` file, see *Adding Programs to the Device Control Lists Using ofcscan.ini on page 10-16*.

WARNING!

Programs added to the `ofcscan.ini` file will be deployed to the root domain and will overwrite programs on individual domains and agents.

Specifying a Digital Signature Provider

Specify a Digital Signature Provider if you trust programs issued by the provider. For example, type Microsoft Corporation or Trend Micro, Inc. You can obtain the Digital Signature Provider by checking the properties of a

program (for example, by right-clicking the program and selecting **Properties**).

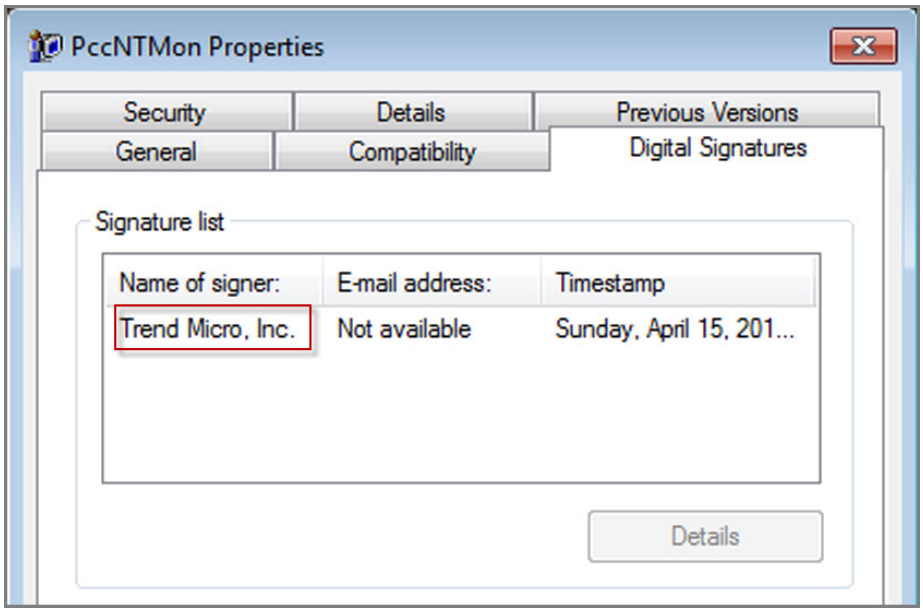


FIGURE 10-1. Digital Signature Provider for the Security Agent program (PccNTMon.exe)

Wildcard Support for the Device Control Allowed Programs List

A program path and name should have a maximum of 259 characters and must only contain alphanumeric characters (A-Z, a-z, 0-9). It is not possible to specify only the program name.

You can use wildcards in place of drive letters and program names. Use a question mark (?) to represent single-character data, such as a drive letter. Use an asterisk (*) to represent multi-character data, such as a program name.

Note

Wildcards cannot be used to represent folder names. The exact name of a folder must be specified.

Wildcards are used correctly in the following examples:

TABLE 10-5. Correct Usage of Wildcards

EXAMPLE	MATCHED DATA
?:\Password.exe	The "Password.exe" file located directly under any drive
C:\Program Files\Microsoft*.exe	Any file in C:\Program Files that has a file extension
C:\Program Files*.*	Any file in C:\Program Files that has a file extension
C:\Program Files\a?c.exe	Any .exe file in C:\Program Files that has 3 characters starting with the letter "a" and ending with the letter "c"
C:*	Any file located directly under the C:\ drive, with or without file extensions

Wildcards are used incorrectly in the following examples:

TABLE 10-6. Incorrect Usage of Wildcards

EXAMPLE	REASON
??:\Buffalo\Password.exe	?? represents two characters and drive letters only have a single alphabetic character.
*:\Buffalo\Password.exe	* represents multi-character data and drive letters only have a single alphabetic character.
C:*\Password.exe	Wildcards cannot be used to represent folder names. The exact name of a folder must be specified.
C:\?\Password.exe	

Permissions for Non-storage Devices

You can allow or block access to non-storage devices. There are no granular or advanced permissions for these devices.

Managing Access to External Devices (Data Protection Activated)

Procedure

1. Navigate to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Device Control Settings**.
4. Click the **External Agents** tab to configure settings for external agents or the **Internal Agents** tab to configure settings for internal agents.
5. Select **Enable Device Control**.
6. Apply settings as follows:
   - If you are on the **External Agents** tab, you can apply settings to internal agents by selecting **Apply all settings to internal agents**.
   - If you are on the **Internal Agents** tab, you can apply settings to external agents by selecting **Apply all settings to external agents**.

   A confirmation message appears. Allow some time for the deployment command to propagate to all agents.
7. Choose to allow or block the AutoRun function (`autorun.inf`) on USB storage devices.
8. Configure settings for storage devices.

a. Select a permission for each storage device.

   For details about permissions, see *Permissions for Storage Devices on page 10-4*.

b. If the permission for USB storage devices is **Block**, configure a list of approved devices. Users can access these devices and you can control the level of access using permissions.

   See *Configuring an Approved List of USB Devices on page 10-13*.

9. For each non-storage device, select **Allow** or **Block**.

10. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

    - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
    - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Configuring Advanced Permissions

Although you can configure advanced permissions and notifications for a specific storage device on the user interface, the permissions and notifications are actually applied to all storage devices. This means that when you click **Advanced permissions and notifications** for CD/DVD, you are actually defining permissions and notifications for all storage devices.

Note

For details about advanced permissions and how to correctly define programs with advanced permissions, see *Advanced Permissions for Storage Devices on page 10-6*.

Procedure

1. Click **Advanced permissions and notifications**.

   A new screen opens.

2. Below **Programs with read and write access to storage devices**, type a program path and file name and then click **Add**.

   Digital Signature Provider is not accepted.

3. Below **Programs on storage devices that are allowed to execute**, type the program path and name or the Digital Signature Provider and then click **Add**.

4. Select **Display a notification message on the endpoint when Apex One detects unauthorized device access**.

   - Unauthorized device access refers to prohibited device operations. For example, if the device permission is "Read", users will not be able to save, move, delete, or execute a file on the device.
   - You can modify the notification message. For details, see *Modifying Device Control Notifications on page 10-18*.

5. Click **Back**.

Configuring an Approved List of USB Devices

The approved list for USB devices supports the use of the asterisk (*) wildcard. Replace any field with the asterisk (*) to include all devices that satisfy the other fields. For example, [vendor]-[model]-* places all USB devices from the specified vendor and the specified model type, regardless of serial ID, to the approved list.

Procedure

1. Click **Approved devices**.

2. Type the device vendor.
3. Type the device model and serial ID.

Tip

Use the Device List Tool to query devices connected to endpoints. The tool provides the device vendor, model, and serial ID for each device.

4. Select the permission for the device.

   For details about permissions, see *Permissions for Storage Devices on page 10-4*.

5. To add more devices, click the plus (+) icon.
6. Click **< Back**.

Device List Tool

Run the Device List Tool locally on each endpoint to query external devices connected to the endpoint. The tool scans an endpoint for external devices and then displays device information in a browser window. You can then use the information when configuring device settings for Data Loss Prevention and Device Control.

Running the Device List Tool

Procedure

1. Locate the Device List Tool.
   - On the Apex One server computer, go to <*Server installation folder*>`\PCCSRV\Admin\Utility\ListDeviceInfo`.
   - On the target endpoint that has the Security Agent installed, go to `C:\Windows\System32\dgagent\listDeviceInfo.exe`.

- Obtain `listDeviceInfo.zip` from the Support portal and extract the package on the target endpoint.

  https://success.trendmicro.com/solution/1120385

2. Copy `listDeviceInfo.exe` to the target endpoint.
3. On the endpoint, run `listDeviceInfo.exe`.
4. View device information in the browser window that displays. Data Loss Prevention and Device Control use the following information:
   - Vendor (required)
   - Model (optional)
   - Serial ID (optional)

Managing Access to External Devices (Data Protection Not Activated)

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Device Control Settings**.
4. Click the **External Agents** tab to configure settings for external agents or the **Internal Agents** tab to configure settings for internal agents.
5. Select **Enable Device Control**.
6. Apply settings as follows:
   - If you are on the **External Agents** tab, you can apply settings to internal agents by selecting **Apply all settings to internal agents**.

- If you are on the **Internal Agents** tab, you can apply settings to external agents by selecting **Apply all settings to external agents**.

A confirmation message appears. Allow some time for the deployment command to propagate to all agents.

7. Choose to allow or block the AutoRun function (`autorun.inf`) on USB storage devices.
8. Select a permission for each storage device.
9. Configure advanced permissions and notifications if the permission for a storage device is any of the following: **Modify**, **Read and execute**, **Read**, or **List device content only**.

   See *Configuring Advanced Permissions on page 10-12*.
10. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
    - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
    - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Adding Programs to the Device Control Lists Using ofcscan.ini

Note

For details about program lists and how to correctly define programs that can be added to the lists, see *Advanced Permissions for Storage Devices on page 10-6*.

Procedure

1. On the Apex One server computer, go to <*Server installation folder*>`\PCCSRV`.

2. Open `ofcscan.ini` using a text editor.
3. To add programs with read and write access to storage devices:
   a. Locate the following lines:

      ```
      [DAC_APPROVED_LIST]

      Count=x
      ```

   b. Replace "x" with the number of programs in the program list.
   c. Below "Count=x", add programs by typing the following:

      ```
      Item<number>=<program path and name or Digital Signature
      Provider>
      ```

      For example:

      ```
      [DAC_APPROVED_LIST]

      Count=3

      Item0=C:\Program Files\program.exe

      Item1=?:\password.exe

      Item2=Microsoft Corporation
      ```

4. To add programs on storage devices that are allowed to execute:
   a. Locate the following lines:

      ```
      [DAC_EXECUTABLE_LIST]

      Count=x
      ```

   b. Replace "x" with the number of programs in the program list.
   c. Below "Count=x", add programs by typing the following:

      ```
      Item<number>=<program path and name or Digital Signature
      Provider>
      ```

      For example:

```
[DAC_EXECUTABLE_LIST]

Count=3

Item0=?:\Installer\Setup.exe

Item1=E:\*.exe

Item2=Trend Micro, Inc.
```

5. Save and close the `ofcscan.ini` file.
6. Open the Apex One web console and go to **Agents** > **Global Agent Settings**.
7. Click **Save** to deploy the program lists to all agents.

Modifying Device Control Notifications

Notification messages display on endpoints when Device Control violations occur. Administrators can modify the default notification message, if needed.

Procedure

1. Go to **Administration** > **Notifications** > **Agent**.
2. From the **Type** drop-down, select **Device Control Violation**.
3. Modify the default messages in the text box provided.
4. Click **Save**.

Device Control Logs

Security Agents log unauthorized device access instances and send the logs to the server. Any agent that runs continuously aggregates the logs and sends

them after a 1-hour time period. Any agent that got restarted checks the last time the logs were sent to the server. If the elapsed time exceeds 1 hour, the agent sends the logs immediately.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing Device Control Logs

Note

Only attempts to access **Storage Devices** generate log data. Security Agents block or allow access to **Non-storage Devices** as configured but do not log the action.

Procedure

1. Go to **Logs** > **Agents** > **Security Risks** or **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Logs** > **Device Control Logs** or **View Logs** > **Device Control Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date/Time unauthorized access was detected
   - Endpoint where external device is connected or where network resource is mapped
   - Endpoint domain where external device is connected or where network resource is mapped
   - Device type or network resource accessed
   - Target, which is the item on the device or network resource that was accessed

- Accessed by, which specifies where access was initiated
- Permissions set for the target

6. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Chapter 11

Using Data Loss Prevention

This chapter discusses how to use the Data Loss Prevention feature.

Topics include:

Data Loss Prevention (DLP)

Traditional security solutions are focused on preventing external security threats from reaching the network. In today's security environment, this is only half the story. Data breaches are now commonplace, exposing an organization's confidential and sensitive data – referred to as digital assets – to outside unauthorized parties. A data breach may occur as a result of internal employee mistakes or carelessness, data outsourcing, stolen or misplaced computing devices, or malicious attacks.

Data breaches can:

- Damage brand reputation
- Erode customer trust in the organization
- Result in unnecessary costs to cover for remediation and to pay fines for violating compliance regulations
- Lead to lost business opportunities and revenue when intellectual property is stolen

With the prevalence and damaging effects of data breaches, organizations now see digital asset protection as a critical component of their security infrastructure.

Data Loss Prevention safeguards an organization's sensitive data against accidental or deliberate leakage. Data Loss Prevention allows you to:

- Identify the sensitive information that requires protection using data identifiers
- Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email and external devices
- Enforce compliance to established privacy standards

Before you can monitor sensitive information for potential loss, you must be able to answer the following questions:

- What data needs protection from unauthorized users?
- Where does the sensitive data reside?
- How is the sensitive data transmitted?
- What users are authorized to access or transmit the sensitive data?
- What action should be taken if a security violation occurs?

This important audit typically involves multiple departments and personnel familiar with the sensitive information in your organization.

If you already defined your sensitive information and security policies, you can begin to define data identifiers and company policies.

Data Loss Prevention Policies

Apex One evaluates a file or data against a set of rules defined in DLP policies. Policies determine files or data that requires protection from unauthorized transmission and the action that Apex One performs after detecting a transmission.

Note

Apex One does not monitor data transmissions between the server and Security Agents.

Apex One allows administrators to configure policies for internal and external Security Agents. Administrators typically configure a stricter policy for external agents.

Administrators can enforce specific policies to agent groups or individual agents.

After deploying policies, agents use the location criteria set in the **Endpoint Location** screen (see *Endpoint Location on page 15-2*) to determine the correct location settings and the policy to apply. Agents switch policies each time the location changes.

Policy Configuration

Define DLP policies by configuring the following settings and deploying the settings to selected agents:

TABLE 11-1. Settings that Define a DLP Policy

SETTINGS	DESCRIPTION
Rules	A DLP rule can consist of multiple templates, channels, and actions. Each rule is a subset of the encompassing DLP policy. **Note** Data Loss Prevention processes rules and templates by priority. If a rule is set to "Pass", Data Loss Prevention processes the next rule in the list. If a rule is set to "Block" or "User Justification", Data Loss Prevention blocks or accepts the user action and does not process that rule/template further.
Templates	A DLP template combines data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement are subject to a DLP rule. Data Loss Prevention comes with a set of predefined templates and allows administrators to create customized templates. A DLP rule can contain one or several templates. Data Loss Prevention uses the first-match rule when checking templates. This means that if a file or data matches the data identifiers in a template, Data Loss Prevention no longer checks the other templates.
Channels	Channels are entities that transmit sensitive information. Data Loss Prevention supports popular transmission channels, such as email, removable storage devices, and instant messaging applications.
Actions	Data Loss Prevention performs one or several actions when it detects an attempt to transmit sensitive information through any of the channels.
Exceptions	Exceptions act as overrides to the configured DLP rules. Configure exceptions to manage non-monitored targets, monitored targets, and compressed file scanning.

Settings	Description
Data Identifiers	Data Loss Prevention uses data identifiers to identify sensitive information. Data identifiers include expressions, file attributes, and keywords which act as the building blocks for DLP templates.

Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. Administrators can define digital assets using the following data identifiers:

- **Expressions**: Data that has a certain structure.

  For details, see *Expressions on page 11-5*.

- **File attributes**: File properties such as file type and file size.

  For details, see *File Attributes on page 11-10*.

- **Keyword lists**: A list of special words or phrases.

  For details, see *Keywords on page 11-13*.

Note

Administrators cannot delete a data identifier that a DLP template is using. Delete the template before deleting the data identifier.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

Administrators can use predefined and customized expressions.

For details, see *Predefined Expressions on page 11-6* and *Customized Expressions on page 11-7*.

Predefined Expressions

Data Loss Prevention comes with a set of predefined expressions. These expressions cannot be modified or deleted.

Data Loss Prevention verifies these expressions using pattern matching and mathematical equations. After Data Loss Prevention matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Viewing Settings for Predefined Expressions

Note

Predefined expressions cannot be modified or deleted.

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Expression** tab.
3. Click the expression name.
4. View settings in the screen that opens.

Customized Expressions

Create customized expressions if none of the predefined expressions meet the company's requirements.

Expressions are a powerful string-matching tool. Become comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, when creating an expression that includes a date, refer to the expressions prefixed with "Date".
- Note that Data Loss Prevention follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:

  http://www.pcre.org/
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

Administrators can choose from several criteria when creating expressions. An expression must satisfy the chosen criteria before Data Loss Prevention subjects it to a DLP policy. For details about the different criteria options, see *Criteria for Customized Expressions on page 11-7*.

Criteria for Customized Expressions

TABLE 11-2. Criteria Options for Customized Expressions

CRITERIA	RULE	EXAMPLE
None	None	All - Names from US Census Bureau • Expression: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]

CRITERIA	RULE	EXAMPLE
Specific characters	An expression must include the characters you have specified. In addition, the number of characters in the expression must be within the minimum and maximum limits.	US - ABA Routing Number • Expression: [^\d]([0123678]\d{8})[^\d] • Characters: 0123456789 • Minimum characters: 9 • Maximum characters: 9
Suffix	Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters. In addition, the number of characters in the expression must be within the minimum and maximum limits.	All - Home Address • Expression: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • Suffix characters: 0123456789- • Number of characters: 5 • Minimum characters in the expression: 25 • Maximum characters in the expression: 80
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address • Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Separator: @ • Minimum characters to the left: 3 • Maximum characters to the left: 15 • Maximum characters to the right: 30

Creating a Customized Expression

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Add**.

   A new screen displays.
4. Type a name for the expression. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /
5. Type a description that does not exceed 256 bytes in length.
6. Type the displayed data.

   For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.
7. Choose one of the following criteria and configure additional settings for the chosen criteria (see *Criteria for Customized Expressions on page 11-7*):

   - None
   - Specific characters
   - Suffix
   - Single-character separator
8. Test the expression against an actual data.

   For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.
9. Click **Save** if you are satisfied with the result.

Note

Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

10. A message appears, reminding you to deploy the settings to agents. Click **Close**.
11. Back in the **DLP Data Identifiers** screen, click **Apply to All Agents**.

Importing Customized Expressions

Use this option if you have a properly-formatted `.dat` file containing the expressions. You can generate the file by exporting the expressions from either the server you are currently accessing or from another server.

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Import** and then locate the `.dat` file containing the expressions.
4. Click **Open**.

   A message appears, informing you if the import was successful. If an expression to be imported already exists, it will be skipped.
5. Click **Apply to All Agents**.

File Attributes

File attributes are specific properties of a file. You can use two file attributes when defining data identifiers, namely, file type and file size. For example, a software development company may want to limit the sharing of the company's software installer to the R&D department, whose members are

responsible for the development and testing of the software. In this case, the Apex One administrator can create a policy that blocks the transmission of executable files that are 10 to 40 MB in size to all departments except R&D.

By themselves, file attributes are poor identifiers of sensitive files. Continuing the example in this topic, third-party software installers shared by other departments will most likely be blocked. Trend Micro therefore recommends combining file attributes with other DLP data identifiers for a more targeted detection of sensitive files.

For a complete list of supported file types, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Predefined File Attributes List

Data Loss Prevention comes with a predefined file attributes list. This list cannot be modified or deleted. The list has its own built-in conditions that determine if the template should trigger a policy violation.

Use the predefined file attributes list to limit access to data recorders (CD/DVD).

For details, see *Blocking Access to Data Recorders (CD/DVD) on page 11-33*.

Creating a File Attribute List

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **File Attribute** tab.
3. Click **Add**.

   A new screen displays.

4. Type a name for the file attribute list. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /

5. Type a description that does not exceed 256 bytes in length.

6. Select your preferred true file types.

7. If a file type you want to include is not listed, select **File extensions** and then type the file type's extension. Data Loss Prevention checks files with the specified extension but does not check their true file types. Guidelines when specifying file extensions:

   - Each extension must start with an asterisk (*), followed by a period (.), and then the extension. The asterisk is a wildcard, which represents a file's actual name. For example, `*.pol` matches `12345.pol` and `test.pol`.

   - You can include wildcards in extensions. Use a question mark (?) to represent a single character and an asterisk (*) to represent two or more characters. See the following examples:

     - `*.*m` matches the following files: `ABC.dem`, `ABC.prm`, `ABC.sdcm`

     - `*.m*r` matches the following files: `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

     - `*.fm?` matches the following files: `ABC.fme`, `ABC.fml`, `ABC.fmp`

   - Be careful when adding an asterisk at the end of an extension as this might match parts of a file name and an unrelated extension. For example: `*.do*` matches `abc.doctor_john.jpg` and `abc.donor12.pdf`.

   - Use semicolons (;) to separate file extensions. There is no need to add a space after a semicolon.

8. Type the minimum and maximum file sizes in bytes. Both file sizes must be whole numbers larger than zero.

9. Click **Save**.

10. A message appears, reminding you to deploy the settings to agents. Click **Close**.

11. Back in the **DLP Data Identifiers** screen, click **Apply to All Agents**.

Importing a File Attribute List

Use this option if you have a properly-formatted `.dat` file containing the file attribute lists. You can generate the file by exporting the file attribute lists from either the server you are currently accessing or from another server.

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.

2. Click the **File Attribute** tab.

3. Click **Import** and then locate the `.dat` file containing the file attribute lists.

4. Click **Open**.

   A message appears, informing you if the import was successful. If a file attribute list to be imported already exists, it will be skipped.

5. Click **Apply to All Agents**.

Keywords

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure Data Loss Prevention to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see *Predefined Keyword Lists on page 11-14* and *Customized Keyword Lists on page 11-15*.

Predefined Keyword Lists

Data Loss Prevention comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

For details about the predefined keyword lists in Data Loss Prevention, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

How Keyword Lists Work

Number of Keywords Condition

Each keyword list contains a condition that requires a certain number of keywords be present in a document before the list triggers a violation.

The number of keywords condition contains the following values:

- **All**: All of the keywords in the list must be present in the document.
- **Any**: Any one of the keywords in the list must be present in the document.
- **Specific number**: There must be at least the specified number of keywords in the document. If there are more keywords in the document than the number specified, Data Loss Prevention triggers a violation.

Distance Condition

Some of the lists contain a "distance" condition to determine if a violation is present. "Distance" refers to the amount of characters between the first character of one keyword and the first character of another keyword. Consider the following entry:

F**irst Name:_John_ L**ast Name:_Smith_

The **Forms - First Name, Last Name** list has a "distance" condition of fifty (50) and the commonly used form fields of "First Name" and "Last Name". In the example above, Data Loss Prevention triggers a violation as the number of characters between the "F" in First Name and the "L" in Last Name is equal to eighteen (18).

For an example of an entry that does not trigger a violation, consider the following:

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

In this example, the number of characters between the "f" in "first name" and the "l" in "last name" is sixty-one (61). This exceeds the distance threshold and does not trigger a violation.

Customized Keyword Lists

Create customized keyword lists if none of the predefined keyword lists meets your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before Data Loss Prevention subjects it to a policy. Choose one of the following criteria for each keyword list:

- **Any keyword**
- **All keywords**
- **All keywords within <x> characters**

- **Combined score for keywords exceeds threshold**

For details regarding the criteria rules, see *Customized Keyword List Criteria on page 11-16*.

Customized Keyword List Criteria

TABLE 11-3. Criteria for a Keyword List

CRITERIA	RULE
Any keyword	A file must contain at least one keyword in the keyword list.
All keywords	A file must contain all the keywords in the keyword list.
All keywords within <x> characters	A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within <x> characters of each other. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If Data Loss Prevention detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "W" (in WEB) and from the "W" to the "U" (in USB) must be 20 characters or less. The following data matches the criteria: DISK####WEB############USB The following data does not match the criteria: DISK******************WEB****USB(23 characters between "D" and "W") When deciding on the number of characters, remember that a small number, such as 10, usually results in a faster scanning time but only covers a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.

Criteria	Rule
Combined score for keywords exceeds threshold	A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.

Creating a Keyword List

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Add**.

   A new screen displays.
4. Type a name for the keyword list. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /
5. Type a description that does not exceed 256 bytes in length.
6. Choose one of the following criteria and configure additional settings for the chosen criteria:

   - **Any keyword**
   - **All keywords**

- **All keywords within <x> characters**
- **Combined score for keywords exceeds threshold**

7. To manually add keywords to the list:
   a. Type a keyword that is 3 to 40 bytes in length and specify whether it is case-sensitive.
   b. Click **Add**.
8. To add keywords by using the "import" option:

   Note

   Use this option if you have a properly-formatted `.csv` file containing the keywords. You can generate the file by exporting the keywords from either the server you are currently accessing or from another server.

   a. Click **Import** and then locate the `.csv` file containing the keywords.
   b. Click **Open**.

      A message appears, informing you if the import was successful. If a keyword to be imported already exists in the list, it will be skipped.
9. To delete keywords, select the keywords and click **Delete**.
10. To export keywords:

    Note

    Use the "export" feature to back up the keywords or to import them to another server. All keywords in the keyword list will be exported. It is not possible to export individual keywords.

    a. Click **Export**.
    b. Save the resulting `.csv` file to your preferred location.
11. Click **Save**.

12. A message appears, reminding you to deploy the settings to agents. Click **Close**.
13. Back in the **DLP Data Identifiers** screen, click **Apply to All Agents**.

Importing a Keyword List

Use this option if you have a properly-formatted `.dat` file containing the keyword lists. You can generate the file by exporting the keyword lists from either the server you are currently accessing or from another server.

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Import** and then locate the `.dat` file containing the keyword lists.
4. Click **Open**.

   A message appears, informing you if the import was successful. If a keyword list to be imported already exists, it will be skipped.
5. Click **Apply to All Agents**.

Data Loss Prevention Templates

A DLP template combines DLP data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a DLP policy.

For example, a file must be a Microsoft Word file (file attribute) AND must contain certain legal terms (keywords) AND must contain ID numbers (expressions) for it to be subject to the "Employment Contracts" policy. This policy allows Human Resources personnel to transmit the file through printing so that the printed copy can be signed by an employee. Transmission through all other possible channels, such as email, is blocked.

You can create your own templates if you have configured DLP data identifiers. You can also use predefined templates. For details, see *Customized DLP Templates on page 11-20* and *Predefined DLP Templates on page 11-20*.

Note

It is not possible to delete a template that is being used in a DLP policy. Remove the template from the policy before deleting it.

Predefined DLP Templates

Data Loss Prevention comes with the following set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

- **GLBA**: Gramm-Leach-Billey Act
- **HIPAA**: Health Insurance Portability and Accountability Act
- **PCI-DSS**: Payment Card Industry Data Security Standard
- **SB-1386**: US Senate Bill 1386
- **US PII**: United States Personally Identifiable Information

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Customized DLP Templates

Create your own templates if you have configured data identifiers. A template combines data identifiers and logical operators (And, Or, Except) to form condition statements.

For more information and examples on how condition statements and logical operators work, see *Condition Statements and Logical Operators on page 11-21*.

Condition Statements and Logical Operators

Data Loss Prevention evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

See the examples in the following table.

TABLE 11-4. Sample Condition Statements

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
[Data Identifier1] **And** [Data Identifier 2] **Except** [Data Identifier 3]	A file must satisfy [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 3]. For example: A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].
[Data Identifier 1] **Or** [Data Identifier 2]	A file must satisfy [Data Identifier 1] or [Data Identifier 2]. For example: A file must be [an Adobe PDF document] or [a Microsoft Word document].
Except [Data Identifier 1]	A file must not satisfy [Data Identifier 1]. For example: A file must not be [a multimedia file].

As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not satisfy all of the data identifiers in the statement. In most cases, however, the first data identifier does not have an operator.

Creating a Template

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **DLP Templates**.
2. Click **Add**.

   A new screen displays.
3. Type a name for the template. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /
4. Type a description that does not exceed 256 bytes in length.
5. Select data identifiers and then click the "add" icon.

   When selecting definitions:

   - Select multiple entries by pressing and holding the CTRL key and then selecting the data identifiers.
   - Use the search feature if you have a specific definition in mind. You can type the full or partial name of the data identifier.
   - Each template can contain a maximum of 30 data identifiers.
6. To create a new expression, click **Expressions** and then click **Add new expression**. In the screen that appears, configure settings for the expression.
7. To create a new file attribute list, click **File attributes** and then click **Add new file attribute**. In the screen that appears, configure settings for the file attribute list.
8. To create a new keyword list, click **Keywords** and then click **Add new keyword**. In the screen that appears, configure settings for the keyword list.

9. If you selected an expression, type the number of occurrences, which is the number of times an expression must occur before Data Loss Prevention subjects it to a policy.

10. Choose a logical operator for each definition.

Note

Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see *Condition Statements and Logical Operators on page 11-21*.

11. To remove a data identifier from the list of selected identifiers, click the trash bin icon.

12. Below **Preview**, check the condition statement and make changes if this is not your intended statement.

13. Click **Save**.

14. A message appears, reminding you to deploy the settings to agents. Click **Close**.

15. Back in the **DLP Templates** screen, click **Apply to All Agents**.

Importing Templates

Use this option if you have a properly-formatted `.dat` file containing the templates. You can generate the file by exporting the templates from either the server you are currently accessing or from another server.

Procedure

1. Go to **Agents** > **Data Loss Prevention** > **DLP Templates**.

2. Click **Import** and then locate the `.dat` file containing the templates.

3. Click **Open**.

A message appears, informing you if the import was successful. If a template to be imported already exists, it will be skipped.

4. Click **Apply to All Agents**.

DLP Channels

Users can transmit sensitive information through various channels. Apex One can monitor the following channels:

- **Network channels**: Sensitive information is transmitted using network protocols, such as HTTP and FTP.
- **System and application channels**: Sensitive information is transmitted using the local applications and peripherals on the endpoint.

Network Channels

Data Loss Prevention can monitor data transmission through the following network channels:

- Email clients
- FTP
- HTTP and HTTPS
- IM applications
- SMB protocol
- Webmail

To determine data transmissions to monitor, Data Loss Prevention checks the transmission scope, which you need to configure. Depending on the scope that you selected, Data Loss Prevention will monitor all data transmissions or only transmissions outside the Local Area Network (LAN).

For details about transmission scope, see *Transmission Scope and Targets for Network Channels on page 11-29*.

Email Clients

Data Loss Prevention monitors email transmitted through various email clients. Data Loss Prevention checks the email subject, body, and attachments for data identifiers. For a list of supported email clients, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Monitoring occurs when a user attempts to send the email. If the email contains data identifiers, Data Loss Prevention will either allow or block the email.

You can define non-monitored internal email domains and monitored subdomains.

- **Non-monitored email domains**: Data Loss Prevention immediately allows the transmission of emails sent to non-monitored domains.

  Note

  Data transmissions to non-monitored email domains and to monitored email subdomains where "Monitor" is the action are similar in that the transmission is allowed. The only difference is that for non-monitored email domains, Data Loss Prevention does not log the transmission, whereas for monitored email subdomains, the transmission is always logged.

- **Monitored email subdomains**: When Data Loss Prevention detects email transmitted to a monitored subdomain, it checks the action for the policy. Depending on the action, the transmission is allowed or blocked.

  Note

  If you select email clients as a monitored channel, an email must match a policy for it to be monitored. In contrast, an email sent to monitored email subdomains is automatically monitored, even if it does not match a policy.

Specify domains using any of the following formats, separating multiple domains with commas:

- X400 format, such as /O=Trend/OU=USA, /O=Trend/OU=China
- Email domains, such as `example.com`

For email messages sent through the SMTP protocol, Data Loss Prevention checks if the target SMTP server is on the following lists:

1. Monitored targets
2. Non-monitored targets

> **Note**
>
> For details about monitored and non-monitored targets, see *Defining Non-monitored and Monitored Targets on page 11-41*.

3. Non-monitored email domains
4. Monitored email subdomains

This means that if an email is sent to an SMTP server on the monitored targets list, the email is monitored. If the SMTP server is not on the monitored targets list, Data Loss Prevention checks the other lists.

For emails sent through other protocols, Data Loss Prevention only checks the following lists:

1. Non-monitored email domains
2. Monitored email subdomains

FTP

When Apex One detects that an FTP client is attempting to upload files to an FTP server, it checks for the presence of data identifiers in the files. No file has been uploaded at this point. Depending on the DLP policy, Apex One will allow or block the upload.

When you configure a policy that blocks file uploads, remember the following:

- When Apex One blocks an upload, some FTP clients will try to re-upload the files. In this case, Apex One terminates the FTP client to prevent the re-upload. Users do not receive a notification after the FTP client terminates. Inform them of this situation when you roll out your DLP policies.
- If a file to be uploaded will overwrite a file on the FTP server, the file on the FTP server may be deleted.

For a list of supported FTP clients, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

HTTP and HTTPS

Apex One monitors data to be transmitted through HTTP and HTTPS. For HTTPS, Apex One checks the data before it is encrypted and transmitted.

For a list of supported web browsers and applications, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

IM Applications

Apex One monitors messages and files that users send through instant messaging (IM) applications. Messages and files that users receive are not monitored.

For a list of supported IM applications, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

When Apex One blocks a message or file sent through AOL Instant Messenger, MSN, Windows Messenger, or Windows Live Messenger, it also terminates the application. If Apex One does not do this, the application will become unresponsive and users will be forced to terminate the application anyway. Users do not receive a notification after the application terminates. Inform them of this situation when you roll out your DLP policies.

SMB Protocol

Apex One monitors data transmissions through the Server Message Block (SMB) protocol, which facilitates shared file access. When another user attempts to copy or read a user's shared file, Apex One checks if the file is or contains a data identifier and then allows or blocks the operation.

Note

The Device Control action has a higher priority than the DLP action. For example, if Device Control does not allow files on mapped network drives to be moved, transmission of sensitive data does not proceed even if DLP allows it.

For details on Device Control actions, see *Permissions for Storage Devices on page 10-4*.

For a list of applications that Apex One monitors for shared file access, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Webmail

Web-based email services transmit data through HTTP. If Apex One detects outgoing data from supported services, it checks the data for the presence of data identifiers.

For a list of supported web-based email services, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Transmission Scope and Targets for Network Channels

Transmission scope and targets define data transmissions on network channels that Data Loss Prevention must monitor. For transmissions that should be monitored, Data Loss Prevention checks for the presence of data identifiers before allowing or blocking the transmission. For transmissions that should not be monitored, Data Loss Prevention does not check for the presence of data identifiers and immediately allows the transmission.

Transmission Scope: All Transmissions

Data Loss Prevention monitors data transmitted outside the host computer.

Note

Trend Micro recommends choosing this scope for external agents.

If you do not want to monitor data transmissions to certain targets outside the host computer, define the following:

- **Non-monitored targets**: Data Loss Prevention does not monitor data transmitted to these targets.

  Note

  Data transmissions to non-monitored targets and to monitored targets where "Monitor" is the action are similar in that the transmission is allowed. The only difference is that for non-monitored targets, Data Loss Prevention does not log the transmission, whereas for monitored targets, the transmission is always logged.

- **Monitored targets**: These are specific targets within the non-monitored targets that should be monitored. Monitored targets are:
  - Optional if you defined non-monitored targets.

- Not configurable if you did not define non-monitored targets.

For example:

The following IP addresses are assigned to your company's Legal Department:

- `10.201.168.1` to `10.201.168.25`

You are creating a policy that monitors the transmission of Employment Certificates to all employees except the Legal Department's full time staff. To do this, you would select **All transmissions** as the transmission scope and then:

OPTION	STEPS
Option 1	1. Add `10.201.168.1-10.201.168.25` to the non-monitored targets. 2. Add the IP addresses of the Legal Department's part-time staff to the monitored targets. Assume that there are 3 IP addresses, `10.201.168.21-10.201.168.23`.
Option 2	Add the IP addresses of the Legal Department's full time staff to the non-monitored targets: • `10.201.168.1-10.201.168.20` • `10.201.168.24-10.201.168.25`

For guidelines on defining monitored and non-monitored targets, see *Defining Non-monitored and Monitored Targets on page 11-41*.

Transmission Scope: Only Transmissions Outside the Local Area Network

Data Loss Prevention monitors data transmitted to any target outside the Local Area Network (LAN).

Note

Trend Micro recommends choosing this scope for internal agents.

"Network" refers to the company or local network. This includes the current network (IP address of the endpoint and netmask) and the following standard private IP addresses:

- Class A: `10.0.0.0` to `10.255.255.255`
- Class B: `172.16.0.0` to `172.31.255.255`
- Class C: `192.168.0.0` to `192.168.255.255`

If you select this transmission scope, you can define the following:

- **Non-monitored targets**: Define targets outside the LAN that you consider safe and therefore should not be monitored.

  Note

  Data transmissions to non-monitored targets and to monitored targets where "Monitor" is the action are similar in that the transmission is allowed. The only difference is that for non-monitored targets, Data Loss Prevention does not log the transmission, whereas for monitored targets, the transmission is always logged.

- **Monitored targets**: Define targets within the LAN that you want to monitor.

For guidelines on defining monitored and non-monitored targets, see *Defining Non-monitored and Monitored Targets on page 11-41*.

Resolving Conflicts

If settings for transmission scope, monitored targets, and non-monitored targets conflict, Apex One recognizes the following priorities, in order of highest priority to lowest:

- Monitored targets
- Non-monitored targets
- Transmission scope

System and Application Channels

Data Loss Prevention can monitor the following system and application channels:

- Cloud storage services
- Data recorders (CD/DVD)
- Peer-to-peer applications
- PGP Encryption
- Printer
- Removable storage
- Synchronization software (ActiveSync)
- Windows clipboard

Cloud Storage Service

Apex One monitors files that users access using cloud storage services. For a list of supported cloud storage services, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Note

Data Loss Prevention supports encryption on cloud storage services when Endpoint Encryption is installed on the agent endpoint.

Data Recorders (CD/DVD)

Apex One monitors data recorded to a CD or DVD. For a list of supported data recording devices and software, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

When Apex One detects a "burn" command initiated on any of the supported devices or software and the action is Pass, data recording proceeds. If the action is Block, Apex One checks if any of the files to be recorded is or contains a data identifier. If Apex One detects at least one data identifier, all files—including those that are not, or do not contain, data identifiers—will not be recorded. Apex One may also prevent the CD or DVD from ejecting. If this issue occurs, instruct users to restart the software process or reset the device.

Apex One implements additional CD/DVD recording rules:

- To reduce false positives, Apex One does not monitor the following files:

.bud	.dll	.gif	.gpd	.htm	.ico	.ini
.jpg	.lnk	.sys	.ttf	.url	.xml	

- Two file types used by Roxio data recorders (`*.png` and `*.skn`) are not monitored to increase performance.
- Apex One does not monitor files in the following directories:

*:\autoexec.bat	*:\Windows
..\Application Data	..\Cookies
..\Local Settings	..\ProgramData
..\Program Files	..\Users*\AppData
..\WINNT	

- ISO images created by the devices and software are not monitored.

Blocking Access to Data Recorders (CD/DVD)

Device Control can only limit access to CD/DVD recording devices that use the Live File System format. Some third-party applications that use Master Format can still perform read/write operations even with Device Control

enabled. Use Data Loss Prevention to limit access to CD/DVD recording devices that use any format type.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **DLP Settings**.
4. Click the **External Agents** tab to configure a policy for external agents or the **Internal Agents** tab to configure a policy for internal agents.

   Note

   Configure agent location settings if you have not done so. Agents use these location settings to determine the correct Data Loss Prevention policy to apply. For details, see *Endpoint Location on page 15-2*.

5. Choose one of the following:
   - If you are on the **External Agents** tab, you can apply all Data Loss Prevention settings to internal agents by selecting **Apply all settings to internal agents**.
   - If you are on the **Internal Agents** tab, you can apply all Data Loss Prevention settings to external agents by selecting **Apply all settings to external agents**.
6. On the **Rules** tab, click **Add**.
7. Select **Enable this rule**.
8. Specify a name for the rule.
9. Click the **Template** tab.
10. Select the **All File Extension** template from the list and click **Add**.
11. Click the **Channel** tab.

12. In the **System and Applications Channels** section, select **Data recorders (CD/DVD)**.
13. Click the **Action** tab.
14. Select the **Block** action.
15. Click **Save**.
16. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
    - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
    - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Peer-to-Peer Applications

Apex One monitors files that users share through peer-to-peer applications.

For a list of supported peer-to-peer applications, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

PGP Encryption

Apex One monitors data to be encrypted by PGP encryption software. Apex One checks the data before encryption proceeds.

For a list of supported PGP encryption software, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Printer

Apex One monitors printer operations initiated from various applications.

Apex One does not block printer operations on new files that have not been saved because printing information has only been stored in the memory at this point.

For a list of supported applications that can initiate printer operations, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Removable Storage

Apex One monitors data transmissions to or within removable storage devices. Activities related to data transmission include:

- Creation of a file within the device
- Copying of a file from the host machine to the device
- Closing of a modified file within the device
- Modifying of file information (such as the file's extension) within the device

When a file to be transmitted contains a data identifier, Apex One either blocks or allows the transmission.

Note

- The Device Control action has a higher priority than the DLP action. For example, If Device Control does not allow copying of files to a removable storage device, transmission of sensitive information does not proceed even if DLP allows it.
- Data Loss Prevention supports encryption on removable storage devices when Endpoint Encryption is installed on the agent endpoint.

For a list of supported removable storage devices and applications that facilitate data transmission activities, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

The handling of file transmission to a removable storage device is a straightforward process. For example, a user who creates a file from Microsoft Word may want to save the file to an SD card (it does not matter which file type the user saves the file as). If the file contains a data identifier that should not be transmitted, Apex One prevents the file from being saved.

For file transmission within the device, Apex One first backs up the file (if its size is 75MB or less) to `%WINDIR%\system32\dgagent\temp` before processing it. Apex One removes the backup file if it allowed the file transmission. If Apex One blocked the transmission, it is possible that the file may have been deleted in the process. In this case, Apex One will copy the backup file to the folder containing the original file.

Apex One allows you to define exceptions. Apex One always allows data transmissions to or within these devices. Identify devices by their vendors and optionally provide the device models and serial IDs.

Tip

Use the Device List Tool to query devices connected to endpoints. The tool provides the device vendor, model, and serial ID for each device. For details, see *Device List Tool on page 10-14*.

Synchronization Software (ActiveSync)

Apex One monitors data transmitted to a mobile device through synchronization software.

For a list of supported synchronization software, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

If the data has a source IP address of 127.0.0.1 and is sent through either port 990 or 5678 (the ports used for synchronization), Apex One checks if the data is a data identifier before allowing or blocking its transmission.

When Apex One blocks a file transmitted on port 990, a file of the same name containing malformed characters may still be created at the destination folder on the mobile device. This is because parts of the file have been copied to the device before Apex One blocked the transmission.

Windows Clipboard

Apex One monitors data to be transmitted to Windows clipboard before allowing or blocking the transmission.

Apex One can also monitor clipboard activities between the host machine and VMWare or Remote Desktop. Monitoring occurs on the entity with the Security Agent. For example, the Security Agent on a VMware virtual machine can prevent clipboard data on the virtual machine from being transmitted to the host machine. Similarly, a host machine with the Security Agent may not copy clipboard data to an endpoint accessed through Remote Desktop.

Data Loss Prevention Actions

When Data Loss Prevention detects the transmission of data identifiers, it checks the DLP policy for the detected data identifiers and performs the action configured for the policy.

The following table lists the Data Loss Prevention actions.

TABLE 11-5. Data Loss Prevention Actions

ACTION	DESCRIPTION
Actions	
Pass	Data Loss Prevention allows and logs the transmission.
Block	Data Loss Prevention blocks and logs the transmission.
Additional Actions	
Notify the agent user	Data Loss Prevention displays a notification message to inform the user of the data transmission and whether it was passed or blocked.
Record data	Regardless of the primary action, Data Loss Prevention records the sensitive information to `<Security Agent installation folder>\DLPLite\Forensic`. Select this action to evaluate sensitive information that is being flagged by Data Loss Prevention. Recorded sensitive information may consume too much hard disk space. Therefore, Trend Micro highly recommends that you choose this option only for highly sensitive information.
Encrypt supported channels using the specified key/ password (only available if Endpoint Encryption is installed) **Note** This option is only available for Removable storage and Cloud storage service channels and when selecting the **Pass** action.	If Trend Micro Endpoint Encryption is installed alongside theSecurity Agents, Data Loss Prevention can automatically encrypt files before allowing a user to pass them to another location. If Endpoint Encryption is not installed, Data Loss Prevention performs the Block action on files. Choose one of the following encryption keys or a fixed password: • **User key**: Also known as a **Local Key**, this key is unique to each user and limits access to the encrypted file to the user that created the file. • **Shared key**: This key refers to the **Group Key** or **Enterprise Key** and the Endpoint Encryption administrator configures the type using PolicyServer MMC. • **Fixed password**: Users manually provide a fixed password using an on-screen prompt. Endpoint

Action	Description
	Encryption creates a self-extracting package that users can access on any endpoint after providing the decryption password. **Important** • The target endpoint must have Endpoint Encryption installed and the user must log in to Endpoint Encryption in order to encrypt data. • Encrypted files located on USB devices are subject to Data Loss Prevention scanning when users attempt to decrypt the files. Decrypting files containing sensitive data on a USB device triggers the USB encryption protocol resulting in the system requiring that the sensitive data be encrypted (again). To prevent Data Loss Prevention from attempting to "re-encrypt" the data, move the encrypted files to a local drive before attempting to access the data. • Data Loss Prevention blocks attempts to upload files to cloud storage when using a web client. Encrypt the files manually before uploading using a web client.
User justification **Note** This option is only available after selecting the **Block** action.	Data Loss Prevention prompts the user before performing the “Block” action. User can select to override the “Block” action by providing an explanation as to why the sensitive data is safe to pass. The available justification reasons are: • **This is part of an established business process.** • **My manager approved the data transfer.** • **The data in this file is not confidential.** • **Other**: Users provide an alternate explanation in the text field provided.

Data Loss Prevention Exceptions

DLP exceptions apply to the entire policy, including all rules defined within the policy. Data Loss Prevention applies the exception settings to all transmissions before scanning for digital assets. If a transmission matches one of the exception rules, Data Loss Prevention immediately allows or scans the transmission depending on the exception type.

Defining Non-monitored and Monitored Targets

Define the non-monitored and monitored targets based on the transmission scope configured on the **Channel** tab. For details on how to define non-monitored and monitored targets for **All transmissions**, see *Transmission Scope: All Transmissions on page 11-29*. For details on how to define non-monitored and monitored targets for **Only transmissions outside the Local Area Network**, see *Transmission Scope: Only Transmissions Outside the Local Area Network on page 11-30*.

Follow these guidelines when defining monitored and non-monitored targets:

1. Define each target by:
   - IP address
   - Host name
   - FQDN
   - Network address and subnet mask, such as 10.1.1.1/32

   Note

   For the subnet mask, Data Loss Prevention only supports a classless inter-domain routing (CIDR) type port. That means that you can only type a number like 32 instead of 255.255.255.0.

2. To target specific channels, include the default or company-defined port numbers for those channels. For example, port 21 is typically for FTP

traffic, port 80 for HTTP, and port 443 for HTTPS. Use a colon to separate the target from the port numbers.

3. You can also include port ranges. To include all ports, ignore the port range.

   Examples of targets with port numbers and port ranges:

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20

4. Separate targets with commas.

Decompression Rules

Files contained in compressed files can be scanned for digital assets. To determine the files to scan, Data Loss Prevention subjects a compressed file to the following rules:

- **Size of a decompressed file exceeds: __ MB (1-10240 MB)**
- **Compression layers exceed: __ (1-20)**
- **Number of files to scan exceeds: __ (1-2000)**

Rule 1: Maximum Size of a Decompressed File

A compressed file – upon decompression – must meet the specified limit.

Example: You set the limit to 20MB.

Scenario 1: If the size of `archive.zip` upon decompression is 30MB, none of the files contained in `archive.zip` will be scanned. The other two rules are no longer checked.

Scenario 2: If the size of `my_archive.zip` upon decompression is 10MB:

- If `my_archive.zip` does not contain compressed files, Apex One skips Rule 2 and proceeds to Rule 3.
- If `my_archive.zip` contains compressed files, the size of all decompressed files must be within the limit. For example, if `my_archive.zip` contains `AAA.rar`, `BBB.zip` and `EEE.zip`, and `EEE.zip` contains `222.zip`:

```
my_archive.zip                          = 10MB upon decompression

              \AAA.rar                  = 25MB upon decompression

              \BBB.zip                  = 3MB upon decompression

              \EEE.zip                  = 1MB upon decompression

                        \222.zip        = 2MB upon decompression
```

`my_archive.zip`, `BBB.zip`, `EEE.zip`, and `222.zip` will be checked against Rule 2 because the combined size of these files is within the 20MB limit. `AAA.rar` is skipped.

Rule 2: Maximum Compression Layers

Files within the specified number of layers will be flagged for scanning.

For example:

```
my_archive.zip

              \BBB.zip          \CCC.xls

              \DDD.txt

              \EEE.zip          \111.pdf

                                \222.zip          \333.txt
```

If you set the limit to two layers:

- Apex One will ignore `333.txt` because it is located on the third layer.

- Apex One will flag the following files for scanning and then check Rule 3:
  - `DDD.txt` (located on the first layer)
  - `CCC.xls` (located on the second layer)
  - `111.pdf` (located on the second layer)

Rule 3: Maximum Number of Files to Scan

Apex One scans files up to the specified limit. Apex One scans files and folders in numeric and then alphabetic order.

Continuing from the example in Rule 2, Apex One has flagged the highlighted files for scanning:

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

In addition, `my_archive.zip` contains a folder named `7Folder`, which was not checked against Rule 2. This folder contains `FFF.doc` and `GGG.ppt`. This brings the total number of files to be scanned to 5, as highlighted below:

```
my_archive.zip
                    \7Folder            \FFF.doc
                    \7Folder            \GGG.ppt
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
```

```
                                    \222.zip          \333.txt
```

If you set the limit to 4 files, the following files are scanned:

- `FFF.doc`
- `GGG.ppt`
- `CCC.xls`
- `DDD.txt`

Note

For files that contain embedded files, Apex One extracts the content of the embedded files.

If the extracted content is text, the host file (such as `123.doc`) and embedded files (such as `abc.txt` and `xyz.xls`) are counted as one.

If the extracted content is not text, the host file (such as `123.doc`) and embedded files (such as `abc.exe`) are counted separately.

Events that Trigger Decompression Rules

The following events trigger decompression rules:

TABLE 11-6. Events that Trigger Decompression Rules

A compressed file to be transmitted matches a policy and the action on the compressed file is Pass (transmit the file).	For example, to monitor .ZIP files that users are transmitting, you defined a file attribute (.ZIP), added it to a template, used the template in a policy, and then set the action to **Pass**. **Note** If the action is Block, the entire compressed file is not transmitted and therefore, there is no need to scan the files it contains.
A compressed file to be transmitted does not match a policy.	In this case, Apex One will still subject the compressed file to the decompression rules to determine which of the files it contains should be scanned for digital assets and whether to transmit the entire compressed file.

Both events have the same result. When Apex One encounters a compressed file:

- If Rule 1 is not satisfied, Apex One allows the transmission of the entire compressed file.
- If Rule 1 is satisfied, the other two rules are checked. Apex One allows the transmission of the entire compressed file if:
  - All scanned files do not match a policy.
  - All scanned files match a policy and the action is **Pass**.

    The transmission of the entire compressed file is blocked if at least one scanned file matches a policy and the action is **Block**.

Data Loss Prevention Policy Configuration

You can start to create Data Loss Prevention policies after you have configured data identifiers and organized them in templates.

In addition to data identifiers and templates, you need to configure channels and actions when creating a policy. For details about policies, see *Data Loss Prevention Policies on page 11-3*.

Creating a Data Loss Prevention Policy

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **DLP Settings**.
4. Click the **External Agents** tab to configure a policy for external agents or the **Internal Agents** tab to configure a policy for internal agents.

   Note

   Configure agent location settings if you have not done so. Agents use these location settings to determine the correct Data Loss Prevention policy to apply. For details, see *Endpoint Location on page 15-2*.

5. Select **Enable Data Loss Prevention**.
6. Choose one of the following:
   - If you are on the **External Agents** tab, you can apply all Data Loss Prevention settings to internal agents by selecting **Apply all settings to internal agents**.
   - If you are on the **Internal Agents** tab, you can apply all Data Loss Prevention settings to external agents by selecting **Apply all settings to external agents**.

7. On the **Rules** tab, click **Add**.

   A policy can contain a maximum of 40 rules.

8. Configure the rule settings.

   For details creating DLP rules, see *Creating Data Loss Prevention Rules on page 11-48*.

9. Click the **Exceptions** tab and configure any necessary exception settings.

   For details on the available exception settings, see *Data Loss Prevention Exceptions on page 11-41*.

10. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

    - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
    - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Creating Data Loss Prevention Rules

Note

Data Loss Prevention processes rules and templates by priority. If a rule is set to "Pass", Data Loss Prevention processes the next rule in the list. If a rule is set to "Block" or "User Justification", Data Loss Prevention blocks or accepts the user action and does not process that rule/template further.

Procedure

1. Select **Enable this rule**.
2. Specify a name for the rule.

Configure the template settings:

3. Click the **Template** tab.
4. Select templates from the **Available templates** list and then click **Add**.

   When selecting templates:

   - Select multiple entries by clicking the template names which highlights the name.
   - Use the search feature if you have a specific template in mind. You can type the full or partial name of the template.

   Note

   Each rule can contain a maximum of 200 templates.

5. If your preferred template is not found in the **Available templates** list:

   a. Click **Add new template**.

      The **Data Loss Prevention Templates** screen displays.

      For instructions on adding templates in the **Data Prevention Templates screen**, see *Data Loss Prevention Templates on page 11-19*.

   b. After creating the template, select it and then click **Add**.

   Note

   Apex One uses the first-match rule when checking templates. This means that if a file or data matches the definition on a template, Apex One will no longer check the other templates. Priority is based on the order of the templates in the list.

Configure the channel settings:

6. Click the **Channel** tab.
7. Select the channels for the rule.

   For details about channels, see *Network Channels on page 11-24* and *System and Application Channels on page 11-32*.

8. If you selected any of the network channels, select the transmission scope:

   - **All transmissions**
   - **Only transmissions outside the Local Area Network**

   See *Transmission Scope and Targets for Network Channels on page 11-29* for details on transmission scope, how targets work depending on the transmission scope, and how to define targets correctly.

9. If you selected **Email clients**:

   a. Click **Exceptions**.

   b. Specify monitored and non-monitored internal email domains.

      For details on monitored and non-monitored email domains, see *Email Clients on page 11-25*.

10. If you selected **Removable storage**:

    a. Click **Exceptions**.

    b. Add non-monitored removable storage devices, identifying them by their vendors. The device model and serial ID are optional.

       The approved list for USB devices supports the use of the asterisk (*) wildcard. Replace any field with the asterisk (*) to include all devices that satisfy the other fields.

       For example, [vendor]-[model]-* places all USB devices from the specified vendor and the specified model type, regardless of serial ID, to the approved list.

    c. To add more devices, click the plus (**+**) icon.

Tip

Use the Device List Tool to query devices connected to endpoints. The tool provides the device vendor, model, and serial ID for each device. For details, see *Device List Tool on page 10-14*.

Configure the action settings:

11. Click the **Action** tab.

12. Select a primary action and any additional actions.

    For details about actions, see *Data Loss Prevention Actions on page 11-38*.

> **Note**
>
> Data Loss Prevention only supports the encryption of sensitive data on removable devices and cloud storage services. Data Loss Prevention performs the "Pass" action without encryption on all channels where encryption is not supported. The target endpoint must have Endpoint Encryption installed and the user must log in to Endpoint Encryption in order to encrypt data.

13. After configuring the **Template**, **Channel**, and **Action** settings, click **Save**.

Importing, Exporting, and Copying DLP Rules

Administrators can import previously defined rules (contained in a properly formatted `.dat` file) or export the list of configured DLP rules. Copying a DLP rule allows an administrator to modify the contents of a previously defined rule to save time.

The following table describes how each function works.

TABLE 11-7. Import, Export, and Copy Functions for DLP Rules

FUNCTION	DESCRIPTION
Import	Importing a rule list appends non-existing rules to the existing DLP rule list. Data Loss Prevention skips rules that already exist in the target list. Data Loss Prevention maintains all pre-configured settings for each rule, including the enabled or disabled status.

Function	Description
Export	Exporting a rule list exports the entire list to a `.dat` file that administrators can then import and deploy to other domains or agents. Data Loss Prevention saves all rule settings based on the current configuration. **Note** • Administrators must save or apply any new or modified rules before exporting the list. • Data Loss Prevention does not export any exceptions configured for the policy, only the settings configured for each rule.
Copy	Copying a rule creates an exact replica of the current configuration settings for the rule. Administrators must type a new name for the rule and can make any configuration modifications necessary for the new rule.

Data Loss Prevention Notifications

Apex One comes with a set of default notification messages that inform Apex One administrators and agent users of digital asset transmissions.

For details on notifications sent to administrators, see *Data Loss Prevention Notifications for Administrators on page 11-52*.

For details on notifications sent to agent users, see *Data Loss Prevention Notifications for Agent Users on page 11-56*.

Data Loss Prevention Notifications for Administrators

Configure Apex One to send administrators a notification when it detects the transmission of digital assets, or only when the transmission is blocked.

Apex One comes with a set of default notification messages that inform administrators of digital asset transmissions. Modify the notifications and configure additional notification settings to suit company requirements.

Note

Apex One can send notifications through email, SNMP trap, and Windows NT Event logs. Configure settings when Apex One sends notifications through these channels. For details, see *Administrator Notification Settings on page 14-38*.

Configuring Data Loss Prevention Notification for Administrators

Procedure

1. Go to **Administration** > **Notifications** > **Administrator**.
2. On the **Criteria** tab:
   a. Go to the **Digital Asset Transmissions** section.
   b. Specify whether to send notifications when transmission of digital assets is detected (the action can be blocked or passed) or only when the transmission is blocked.
3. On the **Email** tab:
   a. Go to the **Digital Asset Transmissions** section.
   b. Select **Enable notification via email**.
   c. Select **Send notifications to users with agent tree domain permissions**.

      Use Role-based Administration to grant agent tree domain permissions to users. If transmission occurs on any agent belonging to a specific domain, the email are sent to the email addresses of the users with domain permissions. See the following table for examples:

TABLE 11-8. Agent Tree Domains and Permissions

AGENT TREE DOMAIN	ROLES WITH DOMAIN PERMISSIONS	USER ACCOUNT WITH THE ROLE	EMAIL ADDRESS FOR THE USER ACCOUNT
Domain A	Administrator (built-in)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domain B	Administrator (built-in)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

If any Security Agent belonging to Domain A detects a digital asset transmission, the email will be sent to mary@xyz.com, john@xyz.com, and chris@xyz.com.

If any Security Agent belonging to Domain B detects the transmission, the email is sent to mary@xyz.com and jane@xyz.com.

Note

When enabling this option, all users with domain permissions must have a corresponding email address. The email notification will not be sent to users without an email address. Users and email addresses are configured from **Administration** > **Account Management** > **User Accounts**.

d. Select **Send notifications to the following email address(es)** and then type the email addresses.

e. Accept or modify the default subject and message. Use token variables to represent data in the **Subject** and **Message** fields.

TABLE 11-9. Token Variables for Data Loss Prevention Notifications

VARIABLE	DESCRIPTION
%USER%	The user logged on to the endpoint when transmission was detected
%COMPUTER%	Endpoint where transmission was detected
%DOMAIN%	Domain of the endpoint
%DATETIME%	Date and time transmission was detected
%CHANNEL%	The channel through which transmission was detected
%TEMPLATE%	The digital asset template that triggered the detection
%RULE%	The rule name that triggered the detection **Note** To display the rule name in the message, add this variable in the **Message** field.

4. On the **SNMP Trap** tab:

   a. Go to the **Digital Asset Transmissions** section.

   b. Select **Enable notification via SNMP trap**.

   c. Accept or modify the default message. Use token variables to represent data in the **Message** field. See *Table 11-9: Token Variables for Data Loss Prevention Notifications on page 11-55* for details.

5. On the **NT Event Log** tab:

   a. Go to the **Digital Asset Transmissions** section.

   b. Select **Enable notification via NT Event Log**.

   c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 11-9: Token Variables for Data Loss Prevention Notifications on page 11-55* for details.

6. Click **Save**.

Data Loss Prevention Notifications for Agent Users

Apex One can display notification messages on agent computers immediately after it allows or blocks the transmission of digital assets.

To notify users that digital asset transmission was blocked or allowed, select the option **Notify the agent user** when creating a Data Loss Prevention policy. For instructions on creating a policy, see *Data Loss Prevention Policy Configuration on page 11-47*.

Configuring Data Loss Prevention Notification for Agents

Procedure

1. Go to **Administration** > **Notifications** > **Agent**.
2. In the **Type** drop-down, select **Digital Asset Transmissions**.
3. Accept or modify the default message.
4. Click **Save**.

Data Loss Prevention Logs

Agents log digital asset transmissions (blocked and allowed transmissions) and send the logs to the server immediately. If the agent is unable to send logs, it retries after 5 minutes.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing Data Loss Prevention Logs

Procedure

1. Go to **Agents** > **Agent Management** or **Logs** > **Agents** > **Security Risks**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Logs** > **Data Loss Prevention Logs** or **View Logs** > **DLP Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs.

   Logs contain the following information:

TABLE 11-10. Data Loss Prevention Log Information

COLUMN	DESCRIPTION
Date/Time	The date and time that Data Loss Prevention logged the incident
User Name	The user name logged on to the endpoint
Endpoint	The name of endpoint where Data Loss Prevention detected the transmission
Domain	The domain of the endpoint
IP Address	The IP address of the endpoint
Rule Name	The rule name(s) that triggered the incident **Note** Policies created in a previous version of OfficeScan display the default name of LEGACY_DLP_Policy.
Channel	The channel through which the transmission occurred

Column	Description
Process	The process that facilitated the transmission of a digital asset (the process depends on the channel) For details, see *Processes by Channel on page 11-58*.
Source	The source of the file containing the digital asset, or channel (if no source is available)
Destination	The intended destination of the file containing the digital asset, or channel (if no source is available)
Action	The action taken on the transmission
File/Data Size	The size of the detected object
Details	A link which includes additional details about the transmission For details, see *Data Loss Prevention Log Details on page 11-61*.

6. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Processes by Channel

The following table lists the processes that display under the **Process** column in the Data Loss Prevention logs.

Table 11-11. Processes by Channel

Channel	Process
Synchronization software (ActiveSync)	Full path and process name of the synchronization software Example: `C:\Windows\system32\WUDFHost.exe`
Data recorder (CD/DVD)	Full path and process name of the data recorder Example: `C:\Windows\Explorer.exe`

Channel	Process
Windows clipboard	Not applicable
Email client - Lotus Notes	Full path and process name of Lotus Notes Example: `C:\Program Files\IBM\Lotus\Notes\nlnotes.exe`
Email client - Microsoft Outlook	Full path and process name of Microsoft Outlook Example: `C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE`
Email client - All clients that use the SMTP protocol	Full path and process name of the email client Example: `C:\Program Files\Mozilla Thunderbird\thunderbird.exe`
Removable storage	Process name of the application that transmitted data to or within the storage device Example: `explorer.exe`
FTP	Full path and process name of the FTP client Example: `D:\Program Files\FileZilla FTP Client\filezilla.exe`
HTTP	"HTTP application"
HTTPS	Full path and process name of the browser or application Example: `C:\Program Files\Internet Explorer\iexplore.exe`
IM application	Full path and process name of the IM application Example: `C:\Program Files\Skype\Phone\Skype.exe`

Channel	Process
IM application - MSN	• Full path and process name of MSN Example: `C:\Program Files\Windows Live\Messenger\msnmsgr.exe` • "HTTP application" if data is transmitted from a chat window
Peer-to-peer application	Full path and process name of the peer-to-peer application Example: `D:\Program Files\BitTorrent\bittorrent.exe`
PGP encryption	Full path and process name of the PGP encryption software Example: `C:\Program Files\PGP Corporation\PGP Desktop\PGPmnApp.exe`
Printer	Full path and process name of the application that initiated a printer operation Example: `C:\Program Files\Microsoft Office\Office12\ WINWORD.EXE`
SMB protocol	Full path and process name of the application from which shared file access (copying or creating a new file) was performed Example: `C:\Windows\Explorer.exe`
Webmail (HTTP mode)	"HTTP application"
Webmail (HTTPS mode)	Full path and process name of the browser or application Example: `C:\Program Files\Mozilla Firefox\firefox.exe`

Data Loss Prevention Log Details

The **Data Loss Prevention Log Details** screen shows additional details about the digital asset transmission. The details of a transmission vary based on the channel and process through which Apex One detected the incident.

The following table lists the details that display.

TABLE 11-12. Data Loss Prevention Log Details

DETAIL	DESCRIPTION
Date/Time	The date and time that Data Loss Prevention logged the incident
Violation ID	The unique ID of the incident
User	The user name logged on to the endpoint
Endpoint	The name of endpoint where Data Loss Prevention detected the transmission
Domain	The domain of the endpoint
IP	The IP address of the endpoint
Channel	The channel through which the transmission occurred
Process	The process that facilitated the transmission of a digital asset (the process depends on the channel) For details, see *Processes by Channel on page 11-58*.
Source	The source of the file containing the digital asset, or channel (if no source is available)
Email sender	The email address where the transmission originated
Email subject	The subject line of the email message containing the digital asset
Email recipient	The destination email address(es) of the email message
URL	The URL of a website or web page
FTP user	The user name used to log on to the FTP server

Detail	Description
File class	The type of file in which Data Loss Prevention detected the digital asset
Rule/Template	A list of the exact rule name(s) and template(s) that triggered the detection
Action	The action taken on the transmission
User justification reason	The reason the user provided for continuing to transfer the sensitive data

Enabling Debug Logging for the Data Protection Module

Procedure

1. Obtain the `logger.cfg` file from your support provider.
2. Add the following data in `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite` (for 32-bit systems) or `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\DlpLite` (for 64-bit systems):
   - **Type**: `String`
   - **Name**: `debugcfg`
   - **Value**: `C:\Log\logger.cfg`
3. Create a folder named "Log" in the `C:\ directory`.
4. Copy `logger.cfg` to the "Log" folder.
5. Deploy Data Loss Prevention and Device Control settings from the web console to start collecting logs.

Note

Disable debug logging for the Data Protection module by deleting `debugcfg` in the registry key and restarting the endpoint.

Chapter 12

Using Web Reputation

This chapter describes web-based threats and using Apex One to protect your network and computers from web-based threats.

Topics include:

About Web Threats

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, web threat creators constantly change the version or variant used. Because the web threat is in a fixed location of a website rather than on an infected endpoint, the web threat creator constantly modifies its code to avoid detection.

In recent years, individuals once characterized as hackers, virus writers, spammers, and spyware makers are now known as cyber criminals. web threats help these individuals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is leakage of confidential information in the form of identity loss. The infected endpoint may also become a vector to deliver phish attacks or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in web commerce, corrupting the trust needed for Internet transactions. The second goal is to hijack a user's CPU power to use it as an instrument to conduct profitable activities. Activities include sending spam or conducting extortion in the form of distributed denial-of-service attacks or pay-per-click activities.

Command & Control Contact Alert Services

Trend Micro Command & Control (C&C) Contact Alert Services provides enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks. C&C Contact Alert Services are integrated with Web Reputation Services which determines the action taken on detected callback addresses based on the web reputation security level.

The C&C IP list further enhances C&C callback detections using the Network Content Inspection Engine to identify C&C contacts through any network channel.

For details on configuring the Web Reputation Services security level, see *Configuring a Web Reputation Policy on page 12-5*.

TABLE 12-1. C&C Contact Alert Services Features

FEATURE	DESCRIPTION
Global Intelligence list	Trend Micro Smart Protection Network compiles the Global Intelligence list from sources all over the world and tests and evaluates the risk level of each C&C callback address. Web Reputation Services uses the Global Intelligence list in conjunction with the reputation scores for malicious websites to provide enhanced security against advanced threats. The web reputation security level determines the action taken on malicious websites or C&C servers based on assigned risk levels.
Virtual Analyzer list	Smart Protection Servers can integrate with Virtual Analyzer to obtain the Virtual Analyzer C&C server list. Virtual Analyzer evaluates potential risks in a secure environment and, through use of advanced heuristics and behavioral testing methods, assigns a risk level to the analyzed threats. The Virtual Analyzer populates the Virtual Analyzer list with any threat that attempts to connect to a possible C&C server. The Virtual Analyzer list is highly company-specific and provides a more customized defense against targeted attacks. Apex One retrieves the list from Virtual Analyzer and can evaluate all possible C&C threats against both the Global Intelligence and the local Virtual Analyzer list. For details on connecting the Virtual Analyzer Suspicious Objects lists, see *Configuring Suspicious Object List Settings on page 14-35*.
Suspicious Connection Service	The Suspicious Connection Service manages the User-defined and Global IP C&C lists, and monitors the behavior of connections that endpoints make to potential C&C servers. For details, see *Suspicious Connection Service on page 8-5*.
Administrator notifications	Administrators can choose to receive detailed and customizable notifications after detecting a C&C callback. For details, see *Configuring C&C Callback Notifications for Administrators on page 12-13*.

Feature	Description
Agent notifications	Administrators can choose to send detailed and customizable notifications to end users after detecting a C&C callback on an endpoint. For details, see *C&C Contact Alert Notifications for Agent Users on page 12-16*.
Outbreak notifications	Administrators can customize outbreak notifications specific to C&C callback events and specify whether the outbreak occurs on a single endpoint or across the entire network. For details, see *C&C Callback Outbreaks on page 12-17*.
C&C callback logs	Logs provide detailed information regarding all C&C callback events. For details, see *Viewing C&C Callback Logs on page 12-21*.

Web Reputation

Web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. Trend Micro continually analyzes websites and updates web reputation scores to prevent users from accessing potentially malicious content.

When a user attempts to access a website, the Security Agent queries a smart protection source to ascertain the risk level of the content. The configured Web Reputation policy for the Security Agent determines whether to allow access to the website.

Note

For details about smart protection sources, see *Smart Protection Source List on page 4-23*.

Web Reputation allows you to add websites that you consider safe or dangerous to Approved or Blocked lists. The Security Agent does not query

web reputation scores for websites added to the lists but instead, automatically allows or blocks access.

Web Reputation Policies

Web reputation policies dictate whether Apex One will block or allow access to a website.

You can configure policies for internal and external agents. Apex One administrators typically configure a stricter policy for external agents.

Policies are granular settings in the Apex One agent tree. You can enforce specific policies to agent groups or individual agents. You can also enforce a single policy to all agents.

After you deploy the policies, agents use the location criteria you have set in the **Endpoint Location** screen (see *Endpoint Location on page 15-2*) to determine their location and the policy to apply. Agents switch policies each time the location changes.

Configuring a Web Reputation Policy

Specify proxy server authentication credentials if you have set up a proxy server to handle HTTP communication in your organization and authentication is required before web access is allowed.

For more information, see *Configuring External Agent Proxy Settings on page 15-53*.

Procedure

1. Go to **Agents** > **Agent Management**.
2. Select the targets in the agent tree.
3. Click **Settings** > **Web Reputation Settings**.

4. Click the **External Agents** tab to configure a policy for external agents or the **Internal Agents** tab to configure a policy for internal agents.

> **Tip**
>
> Configure agent location settings if you have not done so. Agents will use these settings to determine their location and apply the correct web reputation policy. For details, see *Endpoint Location on page 15-2*.

5. Under **Enable Web Reputation on the following operating systems**, select the types of Windows platforms to protect (**Windows desktop platforms** and **Windows Server platforms**).

> **Tip**
>
> Trend Micro recommends disabling Web Reputation for internal agents if you already use a Trend Micro product with the web reputation capability, such as InterScan Web Security Virtual Appliance.

When a web reputation policy is enabled:

- You can only configure internal on-premises Security Agents to send web reputation queries to local Smart Protection Servers.
- Internal agents send web reputation queries to:
  - Smart Protection Servers if the **Send queries to Smart Protection Servers** option is enabled.
  - Smart Protection Network if the **Send queries to Smart Protection Servers** option is disabled.

6. Select **Enable assessment mode**.

Note

When in assessment mode, Security Agents allow access to all websites. For any accessed website that violates the configured **Security Level** setting, the Security Agent logs the event. Assessment mode allows you to monitor website access and evaluate the safety of websites before actively blocking users access. Based on your evaluation of the access logs, you can add trusted websites to the Approved URL List before disabling assessment mode.

7. Select **Check HTTPS URLs**.

Important

HTTPS URL scanning also supports the HTTP/2 protocol. Before Web Reputation can check HTTPS or HTTP/2 URLs, you must configure some prerequisite settings for different browsers.

For more information, see *HTTPS URL Scan Support on page 12-11*.

8. For internal Security Agents, select **Send queries to Smart Protection Servers** if you want Security Agents to send web reputation queries to Smart Protection Servers.

   - If you enable this option:
     - Agents refer to the smart protection source list to determine the Smart Protection Servers to which they send queries.

       For details about the smart protection source list, see *Smart Protection Source List on page 4-23*.

     - Be sure that Smart Protection Servers are available. If all Smart Protection Servers are unavailable, agents do not send queries to Smart Protection Network. The only remaining sources of web reputation data for agents are the approved and blocked URL lists.

     - If you want agents to connect to Smart Protection Servers through a proxy server, specify proxy settings in the **Internal Proxy** section on the **Administration** > **Settings** > **Proxy** > **Agent** tab.

- Be sure to update Smart Protection Servers regularly so that protection remains current.
- Agents do not block untested websites. Smart Protection Servers do not store web reputation data for these websites.

- If you disable this option:
  - Agents send web reputation queries to the Smart Protection Network. Endpoints must have an Internet connection to send queries successfully.
  - If connection to Smart Protection Network requires proxy server authentication, specify authentication credentials in **Administration** > **Settings** > **Proxy > Agent (tab)** > **External Proxy**.
  - Agents can block untested websites if you select the **Block pages that have not been tested by Trend Micro** option.

9. Select from the available web reputation security levels: **High**, **Medium**, or **Low**

Note

The security levels determine whether Web Reputation allows or blocks access to a URL. For example, if you set the security level to Low, Web Reputation only blocks URLs that are known to be web threats. As you set the security level higher, the web threat detection rate improves but the possibility of false positives also increases.

10. If you disabled the **Send queries to Smart Protection Servers** option, you can select **Block pages that have not been tested by Trend Micro**.

Note

While Trend Micro actively tests web pages for safety, users may encounter untested pages when visiting new or less popular websites. Blocking access to untested pages can improve safety but can also prevent access to safe pages.

11. Select **Block pages containing malicious script** to identify web browser exploits and malicious scripts, and prevent the use of these threats from compromising the web browser.

    Web Reputation utilizes both the Browser Exploit Prevention pattern and the Script Analyzer pattern to identify and block web pages before exposing the system.

    Important

    - The Browser Exploit Prevention feature provides support for Internet Explorer, Microsoft Edge Legacy, and Chrome browsers.
    - The Browser Exploit Prevention feature requires that you enable the Advanced Protection Service.

    Important

    The Browser Exploit Prevention feature requires that you enable the Advanced Protection Service.

    To enable the Advanced Protection Service, go to **Agents** > **Agent Management**, click **Settings** > **Additional Service Settings**.

    After enabling the Browser Exploit Prevention feature for the first time on Security Agents, users must enable the required add-on in the browser before Browser Exploit Prevention is operational. For Security Agents running Internet Explorer 9, 10, or 11, users must enable the `Trend Micro IE Protection` add-on in the browser pop-up window.

12. Configure the approved and blocked lists.

    Note

    The approved list takes precedence over the blocked list. When a URL matches an entry in the approved list, agents always allow access to the URL, even if it is in the blocked list.

    a. Select **Enable approved/blocked list**.

    b. Type a URL.

You can add a wildcard character (*) anywhere on the URL.

For example:

- Typing `www.trendmicro.com/*` means that Web Reputation approves all pages in the Trend Micro website.
- Typing `*.trendmicro.com/*` means that Web Reputation approves all pages on any sub-domain of `trendmicro.com`.

You can type URLs containing IP addresses. If a URL contains an IPv6 address, enclose the address in parentheses.

c. Click **Add to Approved List** or **Add to Blocked List**.

d. To export the list to a `.dat` file, click **Export** and then click **Save**.

e. If you have exported a list from another server and want to import it to this screen, click **Import** and locate the `.dat` file. The list loads on the screen.

Important

Web Reputation does not perform any scanning on addresses located in the Approved and Blocked lists.

13. To submit Web Reputation feedback, click the URL provided under **Reassess URL**. The Trend Micro Web Reputation Query system opens in a browser window.

14. Select whether to allow the Security Agent to send web reputation logs to the server. Allow agents to send logs if you want to analyze URLs blocked by Web Reputation and take the appropriate action on URLs you think are safe to access.

15. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

    - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

HTTPS URL Scan Support

HTTPS communication uses certificates to identify web servers. It encrypts data to prevent theft and eavesdropping. Although more secure, accessing websites using HTTPS still has risks. Compromised sites, even those with valid certificates, can host malware and steal personal information. In addition, certificates are relatively easy to obtain, making it easy to set up malicious web servers that use HTTPS.

Important

HTTPS scanning for Internet Explorer only supports Windows 8.1 (or later) and Windows Server 2012 (or later) platforms operating in desktop mode.

Enable checking of HTTPS URLs to reduce exposure to compromised and malicious sites that use HTTPS. Web Reputation can monitor HTTPS traffic on the following browsers:

TABLE 12-2. Supported Browsers for HTTPS Traffic

BROWSER	VERSION	PREREQUISITES
Microsoft Internet Explorer	8.x	Latest version
	9.x	Users must enable the `Trend Micro Osprey Plugin Class` add-on in the browser pop-up window.
	10.x	
	11.x	
Mozilla Firefox	3.5 or later	None
Chrome	Latest version	
Microsoft Edge	Legacy	

For more information on configuring Internet Explorer settings for Web Reputation, see the following Knowledge Base articles:

- http://esupport.trendmicro.com/solution/en-us/1060643.aspx
- http://esupport.trendmicro.com/solution/en-us/1095350.aspx

Web Threat Notifications for Agent Users

Apex One can display a notification message on the Security Agent endpoint immediately after it blocks a URL that violates a web reputation policy. You need to enable the notification message and optionally modify the content of the notification message.

Enabling the Web Threat Notification Message

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab.
5. In the **Web Reputation Settings** section, select **Display a notification when a web site is blocked**.
6. In the **C&C Callback Settings** section, select **Display a notification when a C&C callback is detected**.
7. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.

- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Modifying the Web Threat Notifications

Procedure

1. Go to **Administration** > **Notifications** > **Agent**.
2. From the **Type** drop-down, select the type of web threat notification to modify:
   - **Web Reputation Violations**
   - **C&C Callbacks**
3. Modify the default message in the text box provided.
4. Click **Save**.

C&C Callback Notifications for Administrators

Apex One comes with a set of default notification messages that inform you and other Apex One administrators of C&C callback detections. You can modify the notifications and configure additional notification settings to suit your requirements.

Configuring C&C Callback Notifications for Administrators

Procedure

1. Go to **Administration** > **Notifications** > **Administrator**.
2. On the **Criteria** tab:

a. Go to the **C&C Callbacks** section.

b. Specify whether to send notifications when Apex One detects a C&C callback (the action can be blocked or logged) or only when the risk level of the callback address is High.

3. On the **Email** tab:

a. Go to the **C&C Callbacks** section.

b. Select **Enable notification via email**.

c. Select **Send notifications to users with agent tree domain permissions**.

Use Role-based Administration to grant agent tree domain permissions to users. If transmission occurs on any agent belonging to a specific domain, the email are sent to the email addresses of the users with domain permissions. See the following table for examples:

TABLE 12-3. Agent Tree Domains and Permissions

AGENT TREE DOMAIN	ROLES WITH DOMAIN PERMISSIONS	USER ACCOUNT WITH THE ROLE	EMAIL ADDRESS FOR THE USER ACCOUNT
Domain A	Administrator (built-in)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domain B	Administrator (built-in)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

If any Security Agent belonging to Domain A detects a C&C callback, the email will be sent to mary@xyz.com, john@xyz.com, and chris@xyz.com.

If any Security Agent belonging to Domain B detects the C&C callback, the email is sent to mary@xyz.com and jane@xyz.com.

Note

When enabling this option, all users with domain permissions must have a corresponding email address. The email notification will not be sent to users without an email address. Users and email addresses are configured from **Administration** > **Account Management** > **User Accounts**.

d. Select **Send notifications to the following email address(es)** and then type the email addresses.

e. Accept or modify the default subject and message. Use token variables to represent data in the **Subject** and **Message** fields.

TABLE 12-4. Token Variables for C&C Callback Notifications

VARIABLE	DESCRIPTION
%CLIENTCOMPUTER%	Target endpoint that sent the callback
%IP%	IP address of the targeted endpoint
%DOMAIN%	Domain of the endpoint
%DATETIME%	Date and time the transmission was detected
%CALLBACKADDRESS%	Callback address of the C&C server
%CNCRISKLEVEL%	Risk level of the C&C server
%CNCLISTSOURCE%	Indicates the C&C source list
%ACTION%	Action taken

4. On the **SNMP Trap** tab:

a. Go to the **C&C Callbacks** section.

b. Select **Enable notification via SNMP trap**.

c. Accept or modify the default message. Use token variables to represent data in the **Message** field. See *Table 12-4: Token Variables for C&C Callback Notifications on page 12-15* for details.

5. On the **NT Event Log** tab:
   a. Go to the **C&C Callbacks** section.
   b. Select **Enable notification via NT Event Log**.
   c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 12-4: Token Variables for C&C Callback Notifications on page 12-15* for details.
6. Click **Save**.

C&C Contact Alert Notifications for Agent Users

Apex One can display a notification message on Security Agent computers immediately after blocking a C&C server URL. You need to enable the notification message and optionally modify the content of the notification message

Enabling the C&C Callback Notification Message

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab.
5. In the **C&C Callback Settings** section, select **Display a notification when a C&C callback is detected**.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

- **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
- **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Modifying the C&C Callback Notifications

Procedure

1. Go to **Administration** > **Notifications** > **Agent**.
2. From the **Type** drop-down, select **C&C Callbacks**.
3. Modify the default message in the text box provided.
4. Click **Save**.

C&C Callback Outbreaks

Define a C&C callback outbreak by the number, source, and risk level of the callbacks.

Apex One comes with a default notification message that inform you and other Apex One administrators of an outbreak. You can modify the notification message to suit your requirements.

Note

Apex One can send C&C callback outbreak notifications through email. Configure email settings to allow Apex One to send emails successfully. For details, see *Administrator Notification Settings on page 14-38*.

Configuring the C&C Callback Outbreak Criteria and Notifications

Procedure

1. Go to **Administration** > **Notifications** > **Outbreak**.

   The **Outbreak Notifications** screen appears.

2. On the **Criteria** tab in the **C&C Callbacks** section, configure the following:

Option	Description
Same compromised host	Select to define an outbreak based on the callback detections per endpoint
C&C risk level	Specify whether to trigger an outbreak on all C&C callbacks or only high risk sources
Action	Specify which actions Apex One counts to determine an outbreak scenario
Detections	Specify the number of detections that Apex One must exceed to trigger an outbreak scenario
Time period	Specify the monitoring period

3. On the **Email** tab:

   a. In the **C&C Callbacks** section, select **Enable notification via email**.

   b. Specify the email recipients beside the **To** field.

   c. Specify the **Subject** used in the email notification.

   d. Specify the **Message** contents.

      Apex One supports use of tokens in the **Subject** and **Message** fields.

TABLE 12-5. Token Variables for C&C Callback Outbreak Notifications

VARIABLE TOKEN	DESCRIPTION
%C	Number of C&C callback logs
%T	Time period when the C&C callback logs accumulated

e. Specify any additional log data you want to include in the notification (in tabular format).

LOG COLUMN	DESCRIPTION
Date/Time	Date and time of detection
Compromised Host	Endpoint with the detection
IP Address	IP address of the compromised host
Domain	The domain of the endpoint on which the detection occurred
Callback Address	The URL that triggered the detection
C&C Risk Level	The risk level of the callback address
C&C List Source	The C&C list source that identified the C&C server
Action	Action performed on the security risk

4. In the **SNMP Trap** tab:

   a. Go to the **C&C Callbacks** section.

   b. Select **Enable notification via SNMP trap**.

   c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 12-5: Token Variables for C&C Callback Outbreak Notifications on page 12-19* for details.

5. In the **NT Event Log** tab:

a. Go to the **C&C Callbacks** section.

b. Select **Enable notification via NT Event Log**.

c. Accept or modify the default message. You can use token variables to represent data in the **Message** field. See *Table 12-5: Token Variables for C&C Callback Outbreak Notifications on page 12-19* for details.

6. Click **Save**.

Web Threat Logs

Configure both internal and external agents to send web reputation logs to the server. Do this if you want to analyze URLs that Apex One blocks and take appropriate action on URLs you think are safe to access.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing Web Reputation Logs

Procedure

1. Go to one of the following:
   - **Logs** > **Agents** > **Security Risks**
   - **Agents** > **Agent Management**
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Go to the **Web Reputation Log Criteria** screen:
   - From the **Security Risk Logs** screen, click **View Logs** > **Web Reputation Logs**.

- From the **Agent Management** screen, click **Logs** > **Web Reputation Logs**.

4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

Item	Description
Date/Time	The time the detection occurred
Endpoint	The endpoint on which the detection occurred
Domain	The domain of the endpoint on which the detection occurred
URL	The URL blocked by Web Reputation Services
Risk Level	The risk level of the URL
Description	A description of the security threat
Process	The process through which the contact was attempted (path\application_name)
Action	The action taken on the detection

6. Click **Add to Approved List** to add URLs that you do not want blocked to the Approved URL list.
7. To save logs to a comma-separated value (CSV) file, click **Export All to CSV**. Open the file or save it to a specific location.

Viewing C&C Callback Logs

Procedure

1. Go to one of the following:
   - **Logs** > **Agents** > **Security Risks**

- **Agents** > **Agent Management**

2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Go to the **C&C Callback Log Criteria** screen:
   - From the **Security Risk Logs** screen, click **View Logs** > **C&C Callback Logs**.
   - From the **Agent Management** screen, click **Logs** > **C&C Callback Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

Item	Description
Date/Time	The time the detection occurred
User	The user logged on at the time of the detection
Compromised Host	The endpoint from which the callback originated
IP Address	The IP address of the compromised host
Domain	The domain of the endpoint on which the detection occurred
Callback Address	The address to which the endpoint sent the callback
C&C List Source	The C&C list source that identified the C&C server
C&C Risk Level	The risk level of the C&C server
Protocol	The Internet Protocol used for the transmission
Process	The process that initiated the transmission (path \application_name)
Action	The action taken on the detection

6. If Web Reputation blocked a URL that you do not want blocked, click the **Add to Web Reputation Approved List** button to add the address to the Web Reputation Approved List.

Note

Apex One can only add URLs to the Web Reputation Approved List. For detections made by the Global C&C IP List or the Virtual Analyzer (IP) C&C List, manually add these IP addresses to the User-defined Approved C&C IP List.

For details, see *Configuring Global User-defined IP List Settings on page 8-6*.

7. To save logs to a comma-separated value (CSV) file, click **Export All to CSV**. Open the file or save it to a specific location.

Chapter 13

Using the Apex One Firewall

This chapter describes the Apex One Firewall features and configurations.

Topics include:

About the Apex One Firewall

The Apex One Firewall protects Security Agents and servers on the network using stateful inspection and high performance network virus scanning. Through the central management console, you can create rules to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.

The Apex One firewall includes the following key features and benefits:

Traffic Filtering

The Apex One Firewall filters all incoming and outgoing traffic, providing the ability to block certain types of traffic based on the following criteria:

- Direction (inbound/outbound)
- Protocol (TCP/UDP/ICMP/ICMPv6)
- Destination ports
- Source and destination endpoints

Application Filtering

The Apex One Firewall filters incoming and outgoing traffic for applications specified in the Firewall Exception List, allowing these applications access to the network. The availability of network connections depends on the policies set by the administrator.

Certified Safe Software List

The local Certified Safe Software List contains a list of applications that can bypass firewall policy security levels. The Apex One Firewall automatically allows applications in the Certified Safe Software List to run and access the network.

You can also allow Security Agents to query the dynamically-updated global Certified Safe Software List hosted on Trend Micro servers.

Important

Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.

Scanning for Network Viruses

The Apex One firewall also examines each packet for network viruses. For details, see *Viruses and Malware on page 7-2*.

Customizable Profiles and Policies

The Apex One firewall gives you the ability to configure policies to block or allow specified types of network traffic. Assign a policy to one or more profiles, which you can then deploy to specified Security Agents. This provides a highly customized method of organizing and configuring firewall settings for agents.

Stateful Inspection

The Apex One Firewall uses stateful inspection to monitors and remember all connections and connection states to the Security Agent. The Apex One Firewall can identify specific conditions in any connection, predict what actions should follow, and detect disruptions in normal connections. Therefore, effective use of the firewall not only involves creating profiles and policies, but also analyzing connections and filtering packets that pass through the firewall.

Intrusion Detection System

The Intrusion Detection System (IDS) helps identify patterns in network packets that may indicate an attack on the endpoint.

The Intrusion Detection System (IDS) can help prevent the following well-known intrusions:

Intrusion	Description
Too Big Fragment	A Denial of Service attack where a hacker directs an oversized TCP/UDP packet at a target endpoint. This can cause a buffer overflow, which can freeze or restart the endpoint.
Ping of Death	A Denial of Service attack where a hacker directs an oversized ICMP/ICMPv6 packet at a target endpoint. This can cause a buffer overflow, which can freeze or reboot the endpoint.
Conflicted ARP	A type of attack where a hacker sends an Address Resolution Protocol (ARP) request with the same source and destination IP address to a targeted endpoint. The target endpoint continually sends an ARP response (its MAC address) to itself, causing the endpoint to freeze or crash.
SYN Flood	A Denial of Service attack where a program sends multiple TCP synchronization (SYN) packets to the endpoint, causing the endpoint to continually send synchronization acknowledgment (SYN/ACK) responses. This can exhaust endpoint memory and eventually crash the endpoint.

Intrusion	Description
Overlapping Fragment	Similar to a Teardrop attack, this Denial of Service attack sends overlapping TCP fragments to the endpoint. This overwrites the header information in the first TCP fragment and may pass through a firewall. The firewall may then allow subsequent fragments with malicious code to pass through to the target endpoint.
Teardrop	Similar to an overlapping fragment attack, this Denial of Service attack deals with IP fragments. A confusing offset value in the second or later IP fragment can cause the operating system on the receiving endpoint to crash when attempting to reassemble the fragments.
Tiny Fragment Attack	A type of attack where a small TCP fragment size forces the first TCP packet header information into the next fragment. This can cause routers that filter traffic to ignore the subsequent fragments, which may contain malicious data.
Fragmented IGMP	A Denial of Service attack that sends fragmented IGMP packets to a target endpoint, which cannot properly process the IGMP packets. This can freeze or slow down the endpoint.
LAND Attack	A type of attack that sends IP synchronization (SYN) packets with the same source and destination address to the endpoint, causing the endpoint to send the synchronization acknowledgment (SYN/ACK) response to itself. This can freeze or slow down the endpoint.

Firewall Violation Outbreak Monitor

The Apex One firewall sends a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack.

Security Agent Firewall Privileges

Grant Security Agent users the privilege to view their firewall settings on the Security Agent console. Also grant users the privilege to enable or disable the firewall, the Intrusion Detection System, and the firewall violation notification message.

Enabling or Disabling the Apex One Firewall

During the Apex One server installation, you are prompted to enable or disable the Apex One firewall.

If you enabled the firewall during installation and noticed an impact on performance, especially on Windows Server platforms, consider disabling the firewall.

If you disabled the firewall during installation but now want to enable it to protect the agent from intrusions, first read the guidelines and instructions in *Security Agent Services on page 15-6*.

You can enable or disable the firewall on all or select Security Agent endpoints.

Use one of the following methods to enable or disable the firewall on the web console.

Method	Procedure
Enable/Disable the Apex One Firewall on all Security Agents	Configure the Apex One Firewall service on all Security Agents using **Global Agent Settings**. For more information, see *Configuring Global Firewall Settings on page 13-25*. **Note** Disabling the Apex One Firewall automatically disables all firewall policies on all Security Agents.
Enable/Disable the firewall service from the web console	Configure the Apex One Firewall service on selected Security Agents using **Additional Service Settings**. For more information, see *Security Agent Services on page 15-6*. **Note** Disabling the firewall service automatically disables all firewall policies on the selected agents.

Method	Procedure
Create a new policy and apply it to Security Agents	1. Create a new policy that enables/disables the firewall. For steps in creating a new policy, see *Adding a Firewall Policy on page 13-9*. 2. Apply the policy to the Security Agents.

Firewall Policies and Profiles

The Apex One firewall uses policies and profiles to organize and customize methods for protecting networked endpoints.

With Active Directory integration and role-based administration, each user role, depending on the permission, can create, configure, or delete policies and profiles for specific domains.

Tip

Multiple firewall installations on the same endpoint may produce unexpected results. Consider uninstalling other software-based firewall applications on Security Agents before deploying and enabling the Apex One firewall.

The following steps are necessary to successfully use the Apex One firewall:

1. Create a policy. The policy allows you to select a security level that blocks or allows traffic on networked endpoints and enables firewall features.
2. Add exceptions to the policy. Exceptions allow Security Agents to deviate from a policy. With exceptions, you can specify agents, and allow or block certain types of traffic, despite the security level setting in the policy. For example, block all traffic for a set of agents in a policy, but create an exception that allows HTTP traffic so agents can access a web server.
3. Create and assign profiles to Security Agents. A firewall profile includes a set of agent attributes and is associated with a policy. When any agent

matches the attributes specified in the profile, the associated policy is triggered.

Firewall Policies

Apex One Firewall policies allow you to block or allow certain types of network traffic not specified in a policy exception. A policy also defines which Apex One Firewall features are enabled or disabled. Assign a policy to one or multiple Firewall profiles.

With Active Directory integration and role-based administration, each user role, depending on the permission, can create, configure, or delete policies for specific domains.

The following table outlines the settings available when configuring a firewall policy.

Settings	Description
Security level	A general setting that blocks or allows all inbound and/or all outbound traffic on the Security Agent endpoint
Firewall Features	Specify whether to enable or disable the Apex One firewall, the Intrusion Detection System (IDS), and the firewall violation notification message. For details, see *Intrusion Detection System on page 13-4*.
Certified Safe Software List	Specify whether to allow certified safe applications to connect to the network. For details, see *Certified Safe Software List on page 13-3*.
Policy exception list	A list of configurable exceptions that block or allow various types of network traffic

Note

You can grant end-users the privilege to modify the security level and policy exception list when creating Firewall Profiles.

For details, see *Adding a Firewall Profile on page 13-20*.

Default Firewall Policies

Apex One comes with a set of default policies, which you can modify or delete.

Policy Name	Security Level	Agent Settings	Exceptions	Recommended Use
All access policy	Low	Enable firewall	None	Use to allow agents unrestricted access to the network
Communication Ports for Trend Micro Apex Central	Low	Enable firewall	Allow all incoming and outgoing TCP/UDP traffic through ports 80 and 10319	Use when agents have an MCP agent installation
ScanMail for Microsoft Exchange console	Low	Enable firewall	Allow all incoming and outgoing TCP traffic through port 16372	Use when agents need to access the ScanMail console
InterScan Messaging Security Suite (IMSS) console	Low	Enable firewall	Allow all incoming and outgoing TCP traffic through port 80	Use when agents need to access the IMSS console

Adding a Firewall Policy

Procedure

1. Go to **Agents** > **Firewall** > **Policies**.

2. To add a new policy, click **Add**.

   If a new policy you want to create has similar settings with an existing policy, select the existing policy and click **Copy**.

3. Type a name for the policy.

4. Select a security level.

   The selected security level will not apply to traffic that meet the firewall policy exception criteria.

5. Select the firewall features to use for the policy.

   - The firewall violation notification message displays when the firewall blocks an outgoing packet. To modify the message, see *Modifying the Content of the Firewall Notification Message on page 13-27*.
   - If the administrator enables all the firewall features and grants Security Agent users the privilege to configure firewall settings, users can enable/disable the features and modify firewall settings in the Security Agent console.

     WARNING!

     You cannot use the Apex One web console to override Security Agent console settings that the user configures.

   - If you do not enable the features, the firewall settings you configure from the Apex One web console display under **Network card list** on the Security Agent console.
   - The information under **Settings** on the Security Agent console's **Firewall** tab always reflects the settings configured from the Security Agent console, not from the server web console.

6. Enable the local or global Certified Safe Software List.

Note

Ensure that the Unauthorized Change Prevention Service and Certified Safe Software Services have been enabled before enabling this service.

7. Under Exception, select the firewall policy exceptions. The policy exceptions included here are based on the firewall exception template. See *Editing the Firewall Exception Template on page 13-12* for details.

   - Modify an existing policy exception by clicking the policy exception name and changing the settings in the page that opens.

     Note

     The modified policy exception will only apply to the policy to be created. If you want the policy exception modification to be permanent, you will need to make the same modification to the policy exception in the firewall exception template.

   - Click **Add** to create a new policy exception. Specify the settings in the page that opens.

     Note

     The policy exception will also apply only to the policy to be created. To apply this policy exception to other policies, you need to add it first to the list of policy exceptions in the firewall exception template.

8. Click **Save**.

Modifying an Existing Firewall Policy

Procedure

1. Go to **Agents** > **Firewall** > **Policies**.
2. Click a policy.
3. Modify the following:

- Policy name
- Security level
- Firewall features to use for the policy
- Certified Safe Software Service List status
- Firewall policy exceptions to include in the policy
  - Edit an existing policy exception (click the policy exception name and change settings in the page that opens)
  - Click **Add** to create a new policy exception. Specify the settings in the page that opens.

4. Click **Save** to apply the modifications to the existing policy.

Editing the Firewall Exception Template

The firewall exception template contains policy exceptions that you can configure to allow or block different kinds of network traffic based on the Security Agent endpoint's port number(s) and IP address(es). After creating a policy exception, edit the policies to which the policy exception applies.

Decide which type of policy exception you want to use. There are two types:

- **Restrictive**

  Blocks only specified types of network traffic and applies to policies that allow all network traffic. An example use of a restrictive policy exception is to block Security Agent ports vulnerable to attack, such as ports that Trojans often use.

- **Permissive**

  Allows only specified types of network traffic and applies to policies that block all network traffic. For example, you may want to permit Security Agents to access only the Apex One server and a web server. To do this, allow traffic from the trusted port (the port used to communicate with the Apex One server) and the port the Security Agent uses for HTTP communication.

Security Agent listening port: **Agents** > **Agent Management > Status**. The port number is under **Basic Information**.

Server listening port: **Administration** > **Settings** > **Agent Connection**. The port number is under **Agent Connection Settings**.

Apex One comes with a set of default firewall policy exceptions, which you can modify or delete.

TABLE 13-1. Default Firewall Policy Exceptions

EXCEPTION NAME	ACTION	PROTOCOL	PORT	DIRECTION
DNS	Allow	TCP/UDP	53	Incoming and outgoing
NetBIOS	Allow	TCP/UDP	137, 138, 139, 445	Incoming and outgoing
HTTPS	Allow	TCP	443	Incoming and outgoing
HTTP	Allow	TCP	80	Incoming and outgoing
Telnet	Allow	TCP	23	Incoming and outgoing
SMTP	Allow	TCP	25	Incoming and outgoing
FTP	Allow	TCP	21	Incoming and outgoing
POP3	Allow	TCP	110	Incoming and outgoing
LDAP	Allow	TCP/UDP	389	Incoming and outgoing

Note

Default exceptions apply to all agents. If you want a default exception to apply only to certain agents, edit the exception and specify the IP addresses of the agents.

The LDAP exception is not available if you upgrade from a previous Apex One version. Manually add this exception if you do not see it on the exception list.

Adding a Firewall Policy Exception

When adding new exceptions, ensure that you do not block the ports used for communication between the Apex One server and Security Agents.

You can locate the listening ports used by the Apex One server and Security Agents as follows:

- Server listening port: Go to **Administration** > **Settings** > **Agent Connection**. The port number is under **Agent Connection Settings**.
- Security Agent listening port: Go to **Agents** > **Agent Management** > **Status**. The port number is under **Basic Information**.

Procedure

1. Go to **Agents** > **Firewall** > **Policies**.
2. Click **Edit Exception Template**.
3. Click **Add**.
4. Type a name for the policy exception.
5. Select the type of application. You can select all applications, or specify application path or registry keys.

   Note

   Verify the name and full paths entered. Application exception does not support wildcards.

6. Select the action Apex One performs on network traffic (block or allow traffic that meets the exception criteria) and the traffic direction (inbound or outbound network traffic on the Security Agent endpoint).
7. Select the type of network protocol: TCP, UDP, ICMP, or ICMPv6.
8. Specify ports on the Security Agent endpoint on which to perform the action.
9. Select Security Agent endpoint IP addresses to include in the exception.

For example, if you chose to deny all network traffic (inbound and outbound) and type the IP address for a single endpoint on the network, then any Security Agent that has this exception in its policy cannot send or receive data to or from that IP address.

- **All IP addresses**: Includes all IP addresses
- **Single IP address**: Type an IPv4 or IPv6 address, or a host name.
- **Range (for IPv4 or IPv6)**: Type an IPv4 or IPv6 address range.
- **Range (for IPv6)**: Type an IPv6 address prefix and length.
- **Subnet mask**: Type an IPv4 address and its subnet mask.

10. Click **Save**.

    The **Edit Exception Template** screen appears with the new exception added.

11. Click one of the following buttons to apply the new exception to the list:

    - **Save Temple Changes**: Saves the current exception template list settings but does not apply the settings to existing policies
    - **Save and Apply to Existing Policies**: Saves the current exception template list settings and immediately applies the settings to all existing policies

Modifying a Firewall Policy Exception

Procedure

1. Go to **Agents** > **Firewall** > **Policies**.
2. Click **Edit Exception Template**.
3. Click a policy exception.
4. Modify the following:

- Policy exception name
- Application type, name, or path
- Action Apex One will perform on network traffic and the traffic direction
- Type of network protocol
- Port numbers for the policy exception
- Security Agent endpoint IP addresses

5. Click **Save**.

Saving the Policy Exception List Settings

Procedure

1. Go to **Agents** > **Firewall** > **Policies**.
2. Click **Edit Exception Template**.
3. Click one of the following save options:
   - **Save Template Changes**: Saves the exception template with the current policy exceptions and settings. This option only applies the template to policies created in the future, not existing policies.
   - **Save and Apply to Existing Policies**: Saves the exception template with the current policy exceptions and settings. This option applies the template to existing and future policies.

Firewall Profiles

Firewall profiles provide flexibility by allowing you to choose the attributes that a single agent or group of agents must have before applying a policy. Create user roles that can create, configure, or delete profiles for specific domains.

Users using the built-in administrator account or users with full management permissions can also enable the **Overwrite agent security level/exception list** option to replace the Security Agent profile settings with the server settings.

Profiles include the following:

- **Associated policy**: Each profile uses a single policy
- **Agent attributes**: Security Agents with one or more of the following attributes apply the associated policy:
  - **IP address**: Any Security Agent that has a specific IP address, an IP address that falls within a range of IP addresses, or an IP address belonging to a specified subnet
  - **Domain**: Any Security Agent that belongs to a certain Apex One domain
  - **Endpoint**: The Security Agent with a specific endpoint name
  - **Platform**: Any Security Agent running a specific platform type
  - **Logon name**: Security Agent endpoints to which specified users have logged on
  - **NIC description**: Any Security Agent endpoint with a matching NIC description
  - **Agent location**: If the Security Agent is online or offline

Note

The Security Agent is online if it can connect to the Apex One server or any of the reference servers, and offline if it cannot connect to any server.

Apex One comes with a default profile named "All agents profile", which uses the "All access" policy. You can modify or delete this default profile. You can also create new profiles. All default and user-created firewall profiles, including the policy associated to each profile and the current profile status, display on the firewall profile list on the web console. Manage the profile list

and deploy all profiles to Security Agents. Security Agents store all the firewall profiles on the agent endpoint.

Configuring the Firewall Profile List

Procedure

1. Go to **Agents** > **Firewall** > **Profiles**.
2. For users using the built-in administrator account or users with full management permissions, optionally enable the **Overwrite agent security level/exception list** option to replace the Security Agent profile settings with the server settings.
3. To add a new profile, click **Add**. To edit an existing profile, select the profile name.

   A profile configuration screen appears. See *Adding and Editing a Firewall Profile on page 13-20* for more information.
4. To delete an existing profile, select the check box next to the policy and click **Delete**.
5. To change the order of profiles in the list, select the check box next to the profile to move, and then click **Move Up** or **Move Down**.

   Apex One applies firewall profiles to Security Agents in the order in which the profiles appear in the profile list. For example, if the agent matches the first profile, Apex One applies the actions configured for that profile to the agent. Apex One ignores the other profiles configured for that agent.

   Tip

   The more exclusive a policy, the better it is at the top of the list. For example, move a policy you create for a single agent to the top, followed by those for a range of agents, a network domain, and all agents.
6. To manage reference servers, click **Edit Reference Server List**. Reference servers are endpoints that act as substitutes for the Apex One

server when it applies firewall profiles. A reference server can be any endpoint on the network (see *Reference Servers on page 14-36* for more information). Apex One makes the following assumptions when you enable reference servers:

- Security Agents connected to reference servers are online, even if the agents cannot communicate with the Apex One server.
- Firewall profiles applied to online Security Agents also apply to Security Agents connected to reference servers.

Note

Only users using the built-in administrator account or those with full management permissions can see and configure the reference server list.

7. To save the current settings and assign the profiles to Security Agents:
   a. Select whether to **Overwrite agent security level/exception list**. This option overwrites all user-configured firewall settings.
   b. Click **Assign Profile to Agents**. Apex One assigns all profiles on the profile list to all the Security Agents.
8. To verify that you successfully assigned profiles to Security Agents:
   a. Go to **Agents** > **Agent Management**. In the agent tree view drop-down box, select **Firewall view**.
   b. Ensure that a green check mark exists under the **Firewall** column in the agent tree. If the policy associated with the profile enables the Intrusion Detection System, a green check mark also exists under the **IDS** column.
   c. Verify that the agent applied the correct firewall policy. The policy appears under the **Firewall Policy** column in the agent tree.

Adding and Editing a Firewall Profile

Security Agent endpoints may require different levels of protection. Firewall profiles allow you to specify the agent endpoints to which an associated policy applies. Generally, one profile is necessary for each policy in use.

Adding a Firewall Profile

Procedure

1. Go to **Agents** > **Firewall** > **Profiles**.
2. Click **Add**.
3. Click **Enable this profile** to allow Apex One to deploy the profile to Security Agents.
4. Type a name to identify the profile and an optional description.
5. Select a policy for this profile.
6. Specify the agent endpoints to which Apex One applies the policy. Select endpoints based on the following criteria:
   - IP address
   - Domain: Click the button to open and select domains from the agent tree.

     Note

     Only users with full domain permissions can select domains.
   - Endpoint name: Click the button to open, and select Security Agent endpoints from, the agent tree.
   - Platform
   - Logon name
   - NIC description: Type a full or partial description, without wildcards.

Tip

Trend Micro recommends typing the NIC card manufacturer because NIC descriptions typically start with the manufacturer's name. For example, if you typed "Intel", all Intel-manufactured NICs will satisfy the criteria. If you typed a particular NIC model, such as "Intel(R) Pro/100", only NIC descriptions that start with "Intel(R) Pro/100" will satisfy the criteria.

- Agent location: Select from the following:
  - **Internal - Security Agents can connect to a configured reference server**

    Note

    Click **Edit reference server list** to configure location settings.

    For more information, see *Reference Servers on page 14-36*.

  - **External - Security Agents cannot connect to a configured reference server**

7. Select whether to grant users the privilege to change the firewall security level or edit a configurable list of exceptions to allow specified types of traffic.

   For details, see *Firewall Policies on page 13-8*.

8. Click **Save**.

Modifying a Firewall Profile

Procedure

1. Go to **Agents** > **Firewall** > **Profiles**.
2. Click a profile.
3. Click **Enable this profile** to allow Apex One to deploy this profile to Security Agents. Modify the following:

- Profile name and description
- Policy assigned to the profile
- Security Agent endpoints, based on the following criteria:
  - IP address
  - Domain: Click the button to open the agent tree and select domains from there.
  - Endpoint name: Click the button to open the agent tree and select agent endpoints from there.
  - Platform
  - Logon name
  - NIC description: Type a full or partial description, without wildcards.

    Tip

    Trend Micro recommends typing the NIC card manufacturer because NIC descriptions typically start with the manufacturer's name. For example, if you typed "Intel", all Intel-manufactured NICs will satisfy the criteria. If you typed a particular NIC model, such as "Intel(R) Pro/100", only NIC descriptions that start with "Intel(R) Pro/100" will satisfy the criteria.

  - Agent connection status

4. Click **Save**.

Firewall Privileges

Allow users to configure their own firewall settings. All user-configured settings cannot be overridden by settings deployed from the Apex One server. For example, if the user disables Intrusion Detection System (IDS)

and you enable IDS on the Apex One server, IDS remains disabled on the Security Agent endpoint.

Enable the following settings to allow users to configure the firewall.

TABLE 13-2. Firewall Privileges

PRIVILEGE	DESCRIPTION
Display the Firewall settings on the Security Agent console	The **Firewall** option displays all Firewall settings on the Security Agent.
Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message	The Apex One Firewall protects agents and servers on the network using stateful inspection, high performance network virus scanning, and elimination. If you grant users the privilege to enable or disable the firewall and its features, warn them not to disable the firewall for an extended period of time to avoid exposing the endpoint to intrusions and hacker attacks. If you do not grant users the privileges, the Firewall settings you configure from the Apex One server web console display under Network card list on the Security Agent console.
Allow agents to send firewall logs to the Apex One server	Select this option to analyze traffic the Apex One firewall blocks and allows. For details about firewall logs, see *Firewall Logs on page 13-28*. If you select this option, configure the log sending schedule in **Agents** > **Global Agent Settings** on the **Security Settings** tab. Go to the **Firewall Settings** section. The schedule only applies to agents with the firewall log sending privilege. For instructions, see *Global Firewall Settings on page 13-24*.

Granting Firewall Privileges

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.

3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Firewall Privileges** section.
5. Select the following options:
   - *Display the Firewall settings on the Security Agent console on page 13-23*
   - *Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message on page 13-23*
   - *Allow agents to send firewall logs to the Apex One server on page 13-23*
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Global Firewall Settings

There are a number of ways global firewall settings get applied to Security Agents.

- A particular firewall setting can apply to all agents that the server manages.
- A setting can apply only to Security Agents with certain firewall privileges. For example, the firewall log sending schedule only applies to Security Agents with the privilege to send logs to the server.

Configuring Global Firewall Settings

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. On the **Security Settings** tab, go to the **Firewall Settings** section and configure the following:

Setting	Description
Enable the Apex One Firewall	You must enable the Apex One Firewall on all Security Agents before applying policies and profiles.
Send firewall logs to the server	You can grant certain Security Agents the privilege to send firewall logs to the Apex One server. Configure the log sending schedule in this section. Only agents with the privilege to send firewall logs use the schedule. See *Firewall Privileges on page 13-22* for information on firewall privileges available to selected agents.
Update the Apex One firewall driver only after a system restart	Enable the Security Agent to update the Common Firewall Driver only after the Security Agent endpoint restarts. Enable this option to avoid potential agent endpoint disruptions (such as temporary disconnection from the network) when the Common Firewall Driver updates during agent upgrade.
Send firewall log information to the Apex One server hourly to determine the possibility of a firewall outbreak	When you enable this option, Security Agents sends firewall log counts once every hour to the Apex One server. For details about firewall logs, see *Firewall Logs on page 13-28*. Apex One uses log counts and the firewall violation outbreak criteria to determine the possibility of a firewall violation outbreak. Apex One sends email notifications to Apex One administrators in the event of an outbreak.

3. On the **System** tab, go to the **Certified Safe Software Settings** section and select **Enable the Certified Safe Software Service for Behavior Monitoring, Firewall, and antivirus scans**.

   The Certified Safe Software Service queries Trend Micro datacenters to verify the safety of a program detected by Malware Behavior Blocking,

Event Monitoring, Firewall, or antivirus scans. Enable Certified Safe Software Service to reduce the likelihood of false positive detections.

Note

Ensure that Security Agents have the correct proxy settings (for details, see *Security Agent Proxy Settings on page 15-50*) before enabling Certified Safe Software Service. Incorrect proxy settings, along with an intermittent Internet connection, can result in delays or failure to receive a response from Trend Micro datacenters, causing monitored programs to appear unresponsive.

In addition, pure IPv6 Security Agents cannot query directly from Trend Micro datacenters. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Security Agents to connect to the Trend Micro datacenters.

4. Click **Save**.

Firewall Violation Notifications for Security Agent Users

Apex One can display a notification message on endpoints immediately after the Apex One firewall blocks outbound traffic that violated firewall policies. Grant users the privilege to enable/disable the notification message.

Note

You can also enable the notification when you configure a particular firewall policy. To configure a firewall policy, see *Adding a Firewall Policy on page 13-9*.

Granting Users the Privilege to Enable/Disable the Notification Message

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Firewall Privileges** section.
5. Select **Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message**.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Modifying the Content of the Firewall Notification Message

Procedure

1. Go to **Administration** > **Notifications** > **Agent**.
2. From the **Type** drop-down, select **Firewall Violations**.
3. Modify the default messages in the text box provided.

4. Click **Save**.

Firewall Logs

Firewall logs available on the server are sent by Security Agents with the privilege to send firewall logs. Grant specific agents this privilege to monitor and analyze traffic on the endpoints that the Apex One firewall is blocking.

For information about firewall privileges, see *Firewall Privileges on page 13-22*.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing Firewall Logs

The Security Agent generates logs after detecting firewall violations and then sends the logs to the server.

Procedure

1. Go to one of the following:
   - **Logs** > **Agents** > **Security Risks**
   - **Agents** > **Agent Management**
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Go to the **Firewall Log Criteria** screen:
   - From the **Security Risk Logs** screen, click **View Logs** > **Firewall Logs**.
   - From the **Agent Management** screen, click **Logs** > **Firewall Logs**.

4. To ensure that the most up-to-date logs are available, click **Notify Agents**. Allow some time for agents to send firewall logs before proceeding to the next step.

5. Specify the log criteria and then click **Display Logs**.

6. View logs. Logs contain the following information:

Item	Description
Date/Time	The time the detection occurred
Endpoint	The endpoint on which the detection occurred
Domain	The domain on which the detection occurred
Remote Host	The IP address of the remote host
Local Host	The IP address of the local host
Protocol	The protocol used
Port	The port number
Direction	• **Receive**: Indicates that the traffic was inbound • **Send**: Indicates that the traffic was outbound
Process	The executable program or service running on the endpoint that triggered the firewall violation
Description	Specifies the actual security risk (such as a network virus or IDS attack) or the firewall policy violation

7. To save logs to a comma-separated value (CSV) file, click **Export All to CSV**. Open the file or save it to a specific location.

Firewall Violation Outbreaks

Define a firewall violation outbreak by the number of firewall violations and the detection period.

Apex One comes with a default notification message that inform you and other Apex One administrators of an outbreak. You can modify the notification message to suit your requirements.

Note

Apex One can send firewall outbreak notifications through email. Configure email settings to allow Apex One to send emails successfully. For details, see *Administrator Notification Settings on page 14-38*.

Configuring the Firewall Violation Outbreak Criteria and Notifications

Procedure

1. Go to **Administration** > **Notifications** > **Outbreak**.
2. In the **Criteria** tab:
   a. Go to the **Firewall Violations** section.
   b. Select **Monitor firewall violations on Security Agents**.
   c. Specify the number of IDS logs, firewall logs, and network virus logs.
   d. Specify the detection period.

   Tip

   Trend Micro recommends accepting the default values in this screen.

   Apex One sends a notification message when the number of logs is exceeded. For example, if you specify 100 IDS logs, 100 firewall logs, 100 network virus logs, and a time period of 3 hours, Apex One sends the notification when the server receives 301 logs within a 3-hour period.
3. In the **Email** tab:

a. Go to the **Firewall Violation Outbreaks** section.

b. Select **Enable notification via email**.

c. Specify the email recipients.

d. Accept or modify the default email subject and message. You can use token variables to represent data in the **Subject** and **Message** fields.

TABLE 13-3. Token Variables for Firewall Violation Outbreak Notifications

VARIABLE	DESCRIPTION
%A	Log type exceeded
%C	Number of firewall violation logs
%T	Time period when firewall violation logs accumulated

4. Click **Save**.

Testing the Apex One Firewall

To ensure that the Apex One firewall works properly, perform a test on a single Security Agent or group of Security Agents.

WARNING!

Test Security Agent program settings in a controlled environment only. Do not perform tests on endpoints connected to the network or to the Internet. Doing so may expose Security Agent endpoints to viruses, hacker attacks, and other risks.

Procedure

1. Create and save a test policy. Configure the settings to block the types of traffic you want to test. For example, to prevent the Security Agent from accessing the Internet, do the following:

a. Set the security level to **Low** (allow all inbound/outbound traffic).

b. Select **Enable firewall and Notify users when a firewall violation occurs**.

c. Create an exception that blocks HTTP (or HTTPS) traffic.

2. Create and save a test profile, selecting the agents to which you will test firewall features. Associate the test policy with the test profile.

3. Click **Assign Profile to Agents**.

4. Verify the deployment.

a. Click **Agents** > **Agent Management**.

b. Select the domain to which the agent belongs.

c. Select **Firewall view** from the agent tree view.

d. Check if there is a green check mark under the **Firewall** column of the agent tree. If you enabled the Intrusion Detection System for that agent, check that a green check mark also exists under the **IDS** column.

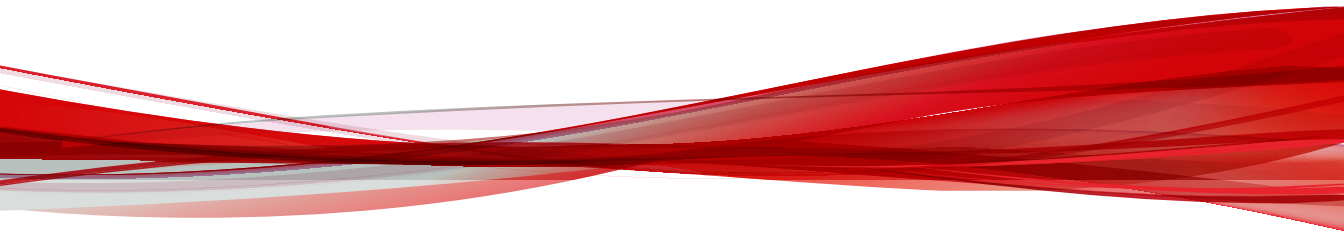
e. Verify that the agent applied the correct firewall policy. The policy appears under the **Firewall Policy** column in the agent tree.

5. Test the firewall on the agent endpoint by attempting to send or receive the type of traffic you configured in the policy.

6. To test a policy configured to prevent the agent from accessing the Internet, open a web browser on the agent endpoint. If you configured Apex One to display a notification message for firewall violations, the message displays on the agent endpoint when an outbound traffic violation occurs.

Part III

Managing the Apex One Server and Agents



Chapter 14

Managing the Apex One Server

This chapter describes Apex One server management and configurations.

Topics include:

Role-based Administration

Use Role-based Administration to grant and control access to the Apex One web console. If there are several Apex One administrators in your organization, you can use this feature to assign specific web console privileges to the administrators and present them with only the tools and permissions necessary to perform specific tasks. You can also control access to the agent tree by assigning them one or several domains to manage. In addition, you can grant non-administrators "view only" access to the web console.

Each user (administrator or non-administrator) is assigned a specific role. A role defines the level of access to the web console. Users log on to the web console using custom user accounts or Active Directory accounts.

Role-based administration involves the following tasks:

1. Define user roles. For details, see *User Roles on page 14-13*.
2. Configure user accounts and assign a particular role to each user account. For details, see *User Accounts on page 14-3*.

View web console activities for all users from the system event logs. The following activities are logged:

- Logging on to the console
- Password modification
- Logging off from the console
- Session timeout (user is automatically logged off)

User Accounts

Set up manual user accounts or use Active Directory accounts to assign permissions to view or configure the granular agent settings, tasks, and data that are available in the agent tree. You must assign a particular role to each user, which dermines the web console menu items that the user can view or

configure. You can use Apex One user accounts to perform "single sign-on" to Apex One from the Trend Micro Apex Central console.

During Apex One server installation, Setup automatically creates a built-in account called "root". Users who log on using the root account can access all menu items. You cannot delete the root account but you can modify account details, such as the password and account description. If you forget the root account password, contact your support provider for help in resetting the password.

Note

After upgrading the Apex One server, you must edit custom accounts and manually enable all new features on the **Step 3 Define Agent Tree Menu** screen for previously added custom accounts.

For details about permissions, see *Defining Permissions for Domains on page 14-11*.

The following table outline the tasks available on the **User Accounts** screen.

Task	Description
Add account	Click **Add** to create a new user account. For more information, see *Adding a User Account on page 14-7*.
Delete existing accounts	Select preexisting user accounts and click **Delete**.
Edit existing accounts	Click the name of a preexisting user account to view or modify the current account settings.

Agent Management Menu Items

The following table lists the available agent management menu items.

Note

Menu items display only after the activation of their respective plug-in program. For example, if the Data Loss Prevention module is not activated, none of the Data Loss Prevention menu items appear in the list.

TABLE 14-1. Agent Management Menu Items

MAIN MENU ITEM	SUBMENUS
Status	N/A
Tasks	• Scan Now • Agent Uninstallation • Central Quarantine Restore • Spyware/Grayware Restore

Main Menu Item	Submenus

Settings	• Scan Settings
	  • Scan Methods
	  • Manual Scan Settings
	  • Real-time Scan Settings
	  • Scheduled Scan Settings
	  • Scan Now Settings
	• Web Reputation Settings
	• Suspicious Connection Settings
	• Behavior Monitoring Settings
	• Device Control Settings
	• DLP Settings
	• Sample Submission
	• Update Agent Settings
	• Privileges and Other Settings
	• Additional Service Settings
	• Spyware/Grayware Approved List
	• Trusted Program List
	• Predictive Machine Learning Settings
	• Export Settings
	• Import Settings

Main Menu Item	Submenus
Logs	• Virus/Malware Logs • Spyware/Grayware Logs • Firewall Logs • Web Reputation Logs • Suspicious Connection Logs • Suspicious Files Logs • C&C Callback Logs • Behavior Monitoring Logs • Predictive Machine Learning Logs • Device Control Logs • Data Loss Prevention Logs • Scan Operation Logs • Delete Logs
Manage Agent Tree	• Add Domain • Rename Domain • Move Agent • Remove Domain/Agent
Export	N/A

Adding a User Account

Set up manual user accounts or use Active Directory accounts to assign permissions to view or configure the granular agent settings, tasks, and data that are available in the agent tree.

Procedure

1. Go to **Administration** > **Account Management** > **User Accounts**.

2. Click **Add**.

   The **Step 1 User Information** screen appears.

3. Select **Enable this account**.

4. Choose a previously configured role in the **Select role** drop-down.

   For more information, see *Adding a Custom Role on page 14-15*.

5. In the **User Information** section, configure the following:

   - **Custom account**: Select to create a manual user account and specify the required information
     - **User name**: Type a unique user name for the account
     - **Description**: Type a description for the account
     - **Password**: Type and confirm the password that the account uses to log on to the Apex One web console

       Important

       You cannot use the user name as the account password. Provide a password other than the user name.

     - **Email address**: Type the email address associated with the user account

       Note

       Apex One sends notifications to this email address. Notifications inform the recipient about security risk detections and digital asset transmissions.

       For details about notifications, see *Security Risk Notifications for Administrators on page 7-78*.

   - **Active Directory user or group**: Select if you want to use existing Active Directory accounts or groups to log on to the Apex One web console

Important

The Apex One server must be joined to the Active Directory domain in order to manage user accounts.

a. In the **User name or group** field, type the Active Directory account that you want to use.

b. In the **Domain** field, type the Active Directory domain to which the **User name or group** belongs.

c. Click **Search**.

d. From the **User and Groups** list, select from the search results and click **>** to add the account to the **Selected Users and Groups** list.

6. Click **Next**.

   The **Step 2 Agent Domain Control** screen appears.

7. Select the root account to grant allow the account to view all Apex One domains, or select specific Apex One domains that the user account can access in the agent tree.

Important

Apex One only displays the selected domains when the user account accesses the agent tree. If you do not select a domain, Apex One hides the domain on the agent tree.

8. Click **Next**.

   The **Step 3 Define Agent Tree Menu** screen appears.

9. Click the **Available Menu Items** controls and then specify the permission for each available menu item. For a list of available menu items, see *Agent Management Menu Items on page 14-4*.

   The agent tree scope you configured in step 8 determines the level of permission to the menu items and defines the targets for the

permission. The agent tree scope can either be the root domain (all agents) or specific agent tree domains.

TABLE 14-2. Agent Management Menu Items and Agent Tree Scope

CRITERIA	AGENT TREE SCOPE	
	ROOT DOMAIN	SPECIFIC DOMAINS
Menu item permission	Configure, View, or No Access	Configure, View, or No Access
Target	Root domain (all agents) or specific domains For example, you can grant a role "Configure" permission to the "Tasks" menu item in the agent tree. If the target is the root domain, the user can initiate the tasks on all agents. If the targets are Domains A and B, the tasks can only be initiated on agents in Domains A and B.	Only the selected domains For example, you can grant a role "Configure" permission to the "Settings" menu item in the agent tree. This means that the user can deploy the settings but only to the agents in the selected domains.
	The agent tree will only display if the permission to the Agent Management menu item in "Menu Items for Servers/Agents" is "View".	

- If you select the check box under **Configure**, the check box under **View** is automatically selected.
- If you do not select any check box, the permission is "No Access".
- If you are configuring permissions for a specific domain, you can copy the permissions to other domains by clicking **Copy settings of the selected domain to other domains**.

10. Click **Finish**.
11. Send the account details to the user.

Defining Permissions for Domains

When defining permissions for domains, Apex One automatically applies the permissions for a parent domain to all the subdomains that it manages. A subdomain cannot have lesser permissions than its parent domain. For example, if the System Administrator has permission to view and configure all Security Agents that Apex One manages (the "Apex One Server" domain), the permissions for the subdomains must allow the System Administrator access to these configuration features. Removing a permission on a subdomain would mean that the System Administrator does not have full configuration permissions for all Security Agents.

For the following procedure, the domain tree is as follows:

For example, to grant the user account "Chris" permissions to view and configure specific menu items for the subdomain "Employees" but only grant permission to view logs in the parent domain "Managers", perform the following procedure.

TABLE 14-3. Permissions for User Account "Chris"

DOMAIN	DESIRED PERMISSIONS
Apex One Server	No special permissions
Managers	View **Logs**
Employees	View and configure **Tasks** View and configure **Logs** View **Settings**
Sales	No special permissions

Procedure

1. Go to the **User Accounts: Step 3 Define Agent Tree Menu** screen.
2. Click the “Apex One Server” domain.
3. Clear all **View** and **Configure** check boxes.

   Note

   The “Apex One Server” domain is only configurable if you selected all of its subdomains on the **User Accounts: Step 2 Agent Domain Control** screen.

4. Click the “Sales” domain.
5. Clear all **View** and **Configure** check boxes.

   Note

   The “Sales” domain only displays if selected on the **User Accounts: Step 2 Agent Domain Control** screen.

6. Click the “Managers” domain.
7. Select to “View Logs” and clear all other **View** and **Configure** check boxes.
8. Click the “Employees” domain.
9. Select the following menu items for Chris:

   - **Tasks**: View and configure
   - **Logs**: View and configure
   - **Settings**: View

   Chris can now view and configure the selected menu items for the “Employees” domain and can only view **Logs** for the “Managers” domain.

If Chris has permission to view and configure the “Managers” domain, Apex One automatically grants the same permissions to the “Employees” subdomain as well. This occurs because the “Managers” domain manages all of its subdomains.

User Roles

Define and assign user roles to limit the access specific user accounts have to certain web console screens. You can define user roles to completely hide web console screens, limit access to “Read only”, or grant full configuration rights.

The following table outline the tasks available on the **User Roles** screen.

Task	Description
Add custom role	Click **Add** to create a new custom role. For more information, see *Adding a Custom Role on page 14-15*. **Important** Only the “root” account or users with the built-in administrator role can create and assign custom user roles to user accounts.
Copy settings from an existing custom role	Select a preexisting custom role and click **Copy**. The **Copy Role** screen appears allowing you to create a new custom role based off of the original settings.
Delete existing custom roles	Select preexisting custom roles and click **Delete**. **Important** You cannot delete roles currently assigned to user accounts.

Task	Description
Export custom roles	Select preexisting custom roles, click the **Export** button, and select one of the following: • **Export to DAT**: Exports the selected roles to a DAT file that you can import to another Apex One server • **Export to CSV**: Exports the selected roles to a CSV file that you can use to view role settings **Important** You cannot import the generated CSV file to the Apex One server.
Import custom roles	Click **Import** to import the user roles settings from a previously exported user role DAT file. For more information, see *Importing or Exporting Custom Roles on page 14-21*.
Edit existing custom roles	Click the name of a preexisting user role to view or modify the current role settings. **Note** You cannot modify the contents of any of the predefined user roles. For more information, see *Built-in User Roles on page 14-14*.

Built-in User Roles

Apex One comes with a set of built-in user roles that you cannot modify or delete. The built-in roles are as follows:

TABLE 14-4. Built-in User Roles

ROLE NAME	DESCRIPTION
Administrator	Delegate this role to other Apex One administrators or users with sufficient knowledge of Apex One. Users with this role have "Configure" permission to all menu items. **Note** Only users assigned the “Administrator (Built-in)” role have access to the Plug-ins menu item.

Guest User	Delegate this role to users who want to view the web console for reference purposes.
	
	• Users with this role have no access to the following menu items:
	  • Plug-ins
	  • **Administration** > **Account Management** > **User Roles**
	  • **Administration** > **Account Management** > **User Accounts**
	• Users have "View" permission to all other menu items.

Adding a Custom Role

Add new custom user roles if the available built-in roles do not satisfy your requirements.

For more information, see *Built-in User Roles on page 14-14*.

Procedure

1. Go to **Administration** > **Account Management** > **User Roles**.
2. Click **Add**.

   The **Add Role** screen appears.
3. In the **Role Information** section, specify the following:

- **Name**: Type a unique name for the role
- **Description**: (Optional)

4. In the **Role Permissions** section:

   a. Select the menu items that user accounts assigned with the role can access.

      - **Menu Items for Servers/Agents**: Includes global Security Agent and Apex One server settings, tasks, and data

        For more information, see *Menu Items for Servers and Agents on page 14-17*.

      - **Menu items for Managed Domains**: Includes granular Security Agent settings, tasks, and data that are available outside the agent tree

        For more information, see *Menu Items for Managed Domains on page 14-19*.

   b. Select the access permissions that user accounts assigned to the role have for the selected menu items.

      - **Configure**: Allows full access to a menu item

        Users can configure all settings, perform all tasks, and view data in a menu item.

      - **View**: Only allows users to view settings, tasks, and data in a menu item

      Note

      Clear both the **Configure** and **View** check boxes to completely hide a menu item from view. Menu items do not display for user accounts assigned to the role.

5. Click **Save**.

   The new role displays on the **User Roles** screen.

Menu Items for Servers and Agents

The following tables list the menu items available for servers/agents.

Note

Menu items display only after the activation of their respective plug-in program. For example, if the Data Loss Prevention module is not activated, none of the Data Loss Prevention menu items appear in the list. Any additional plug-in programs display under the Plug-ins menu item.

Only users assigned the "Administrator (Built-in)" role have access to the Plug-ins menu item.

TABLE 14-5. Agents Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM
Agents	• Agent Management • Agent Grouping • Global Agent Settings • Endpoint Location • Data Loss Prevention • Connection Verification • Outbreak Prevention

TABLE 14-6. Logs Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM

Logs	• Agents
	  • Security Risks
	  • Agent Component Update
	• Server Updates
	• System Events
	• Log Maintenance

TABLE 14-7. Updates Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM	SUBMENU ITEM
Updates	Server	• Scheduled Update • Manual Update • Update Source
	Agents	• Automatic Update • Update Source
	Rollback	N/A

TABLE 14-8. Administration Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM	SUBMENU ITEM
Administration	Account Management	• User Accounts • User Roles **Note** Only users using the built-in administrator account can access User Accounts and User Roles.
	Smart Protection	• Smart Protection Sources • Integrated Server • Smart Feedback
	Active Directory	• Active Directory Integration • Scheduled Synchronization
	Notifications	• General Settings • Outbreak • Agent

Top-level Menu Item	Menu Item	Submenu Item
	Settings	• Proxy • Agent Connection • Inactive Agents • Quarantine Manager • Product License • Apex Central • Web Console • Database Backup • Suspicious Object List • Edge Relay • Server Migration

Menu Items for Managed Domains

The following table lists the available menu items for managed domains.

Table 14-9. Dashboard Menu Item

Main Menu Item	Menu Item
Dashboard **Note** Any user can access this page, regardless of permission.	N/A

TABLE 14-10. Assessment Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM	SUBMENU ITEM
Assessment	Security Compliance	• Manual Report • Scheduled Report
	Unmanaged Endpoints	N/A

TABLE 14-11. Agents Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM	SUBMENU ITEM
Agents	Firewall	• Policies • Profiles
	Agent Installation	• Browser-based • Remote

TABLE 14-12. Logs Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM	SUBMENU ITEM
Logs	Agents	• Connection Verification • Central Quarantine Restore • Spyware/Grayware Restore

TABLE 14-13. Updates Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM	SUBMENU ITEM
Updates	Summary	N/A
	Agents	Manual Update

TABLE 14-14. Administration Menu Items

TOP-LEVEL MENU ITEM	MENU ITEM	SUBMENU ITEM
Administration	Notifications	Administrator

Importing or Exporting Custom Roles

Procedure

1. Go to **Administration** > **Account Management** > **User Roles**.
2. To export custom roles to a `.dat` file, which you can import back to another Apex One server:
   a. Select the roles and click **Export** > **Export to DAT**.
   b. Save the `.dat` file. If you are managing another Apex One server, use the `.dat` file to import custom roles to that server.

   Note
   Exporting roles can only be done between servers that have the same version.
3. To export custom roles to a `.csv` file:
   a. Select the roles and click **Export** > **Export to CSV**.
   b. Save the `.csv` file. Use this file to check the information and permissions for the selected roles.
4. If you have saved custom roles from a different Apex One server and want to import those roles into the current Apex One server, click **Import** and locate the `.dat` file containing the custom roles.
   - A role on the User Roles screen will be overwritten if you import a role with the same name.
   - Importing roles can only be done between servers that have the same version.

- A role imported from another Apex One server:
  - Retains the permissions for menu items for servers/agents and menu items for managed domains.
  - Applies the default permissions for agent management menu items. On the other server, record the role's permissions for agent management menu items and then re-apply them to the role that was imported.

Trend Micro Apex Central

Trend Micro Apex Central™ is a central management console that 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 managed products and services throughout the network.

Apex Central allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Apex Central allows both manual and pre-scheduled updates, and the configuration and administration of products as groups or as individuals for added flexibility.

Apex Central Integration in this Apex One Release

This Apex One release includes the following features and capabilities when managing Apex One servers from Apex Central:

- Create, manage, and deploy policies for Trend Micro Apex One Antivirus, Data Loss Prevention, and Device Control, and assign privileges directly to Security Agents from the Apex Central console.

  The following table lists the policy configurations available in Apex Central 2019 (or later).

TABLE 14-15. Apex One Policy Management Types in Apex Central

POLICY TYPE	FEATURES
Apex One Antivirus and Agent Settings	• Additional Service Settings • Application Control Settings • Behavior Monitoring Settings • Device Control Settings • Endpoint Sensor Settings • Manual Scan Settings • Predictive Machine Learning Settings • Privileges and Other Settings • Real-time Scan Settings • Sample Submission • Scan Methods • Scan Now Settings • Scheduled Scan Settings • Spyware/Grayware Approved List • Suspicious Connection Settings • Trusted Program List • Update Agent Settings • Vulnerability Protection Settings • Web Reputation Settings
Data Protection	Data Loss Prevention Policy Settings **Note** Manage the Device Control permissions for Data Protection in the Security Agent policies.

For more information about migrating Security Agent policy settings to the Apex Central server, see *The Apex One Settings Export Tool on page 14-29*.

- Replicate the following settings from one Trend Micro Apex One server to another from the Apex Central console:
  - *Data Identifier Types on page 11-5*
  - *Data Loss Prevention Templates on page 11-19*

Note

If these settings are replicated to Trend Micro Apex One servers where the Data Protection license has not been activated, the settings will only take effect when the license is activated.

Enhanced Product Integration Through Apex Central

The Apex Central web console provides advanced Security Agent policy configuration setting that are not available from the Apex One web console. With the correct licensing, you can send the following enhanced security policies to Security Agents across your network.

Feature	Description
Application Control	Integration with Application Control provides Apex One users with advanced application blocking and endpoint lockdown capabilities. You can run application inventories and create policy rules that only allow specific applications to execute on your endpoints. You can also create application control rules based on application category, vendor, or version.
Endpoint Sensor	Integration with Endpoint Sensor allows you to monitor, record, and perform both current and historical security investigations on your Apex One endpoints. Use the Apex Central console and perform preliminary investigations to locate at-risk endpoints before executing an in-depth Root Cause Analysis to identify the attack vectors.

Feature	Description
Vulnerability Protection	Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with recommended Intrusion Prevention rules based on your network performance and security priorities.

For more information about the enhanced product integration, see the *Apex Central Administrator's Guide*.

Supported Apex Central Versions

This Apex One version supports the following Apex Central / Control Manager versions:

- Apex Central 2019 or later
- Control Manager 7.0 or later

For details on the IP addresses that the Apex One server and Security Agents report to Apex Central, see *Screens That Display IP Addresses on page A-6*.

Apply the latest patches and critical hot fixes for these Apex Central versions to enable Apex Central to manage Apex One. To obtain the latest patches and hot fixes, contact your support provider or visit the Trend Micro Update Center at:

http://downloadcenter.trendmicro.com

After installing Apex One, register it to Apex Central and then configure settings for Apex One on the Apex Central management console. See the *Apex Central documentation* for information on managing Apex One servers.

Registering Apex One to Apex Central

Procedure

1. Go to **Administration** > **Settings** > **Apex Central**.

2. Specify the entity display name, which is the name of the Apex One server that will display in Apex Central.

   By default, entity display name includes the server computer's host name and this product's name (for example, Server01_OSCE).

   Note

   In Apex Central, Apex One servers and other products managed by Apex Central are referred to as "entities".

3. Specify the Apex Central server FQDN or IP address and the port number to use to connect to this server. Optionally connect with increased security using HTTPS.

   - For a dual-stack Apex One server, type the Apex Central FQDN or IP address (IPv4 or IPv6, if available).
   - For a pure IPv4 Apex One server, type the Apex Central FQDN or IPv4 address.
   - For a pure IPv6 Apex One server, type the Apex Central FQDN or IPv6 address.

4. Beside **Apex Central certificate**, click **Browse...** and select the certificate file downloaded from the target Apex Central server.

   To obtain the Apex Central certificate file, go to the Apex Central server and copy the certificate file to the Apex One server from the following location:

   ```
   <Apex Central installation folder>\Certificate\CA
   \TMCM_CA_Cert.pem
   ```

Important

If your company uses a customized certificate on the Apex Central server, you must upload the Root CA certificate during the Apex Central registration.

For more information, see *Apex Central Certificate Authorization on page 14-28*.

5. If the IIS web server of Apex Central requires authentication, type the user name and password.

6. If you will use a proxy server to connect to the Apex Central server, specify the following proxy settings:

   - Proxy protocol
   - Server FQDN or IPv4/IPv6 address and port
   - Proxy server authentication user ID and password

7. Decide whether to use one-way communication or two-way communication port forwarding, and then specify the IPv4/IPv6 address and port.

8. To check whether Apex One can connect to the Apex Central server based on the settings you specified, click **Test Connection**.

   Click **Register** if a connection was successfully established.

9. If the Control Manager server is version 6.0 SP1 or later or you use the Apex Central server, a message appears prompting you to use the Apex Central server as the update source for the Apex One integrated Smart Protection Server. Click **OK** to use the Apex Central server as the integrated Smart Protection Server update source or **Cancel** to continue using the current update source (by default, the ActiveUpdate server).

10. If you change any of the settings on this screen after registration, click **Update Settings** after changing the settings to notify the Apex Central server of the changes.

Note

If the Apex Central server is connected to a Virtual Analyzer, the automatic subscription process starts after the registration is complete. For more information, see *Suspicious Object List Settings on page 14-34*.

11. If you no longer want the Apex Central server to manage Apex One, click **Unregister**.

Apex Central Certificate Authorization

Before registering Apex One to the Apex Central server, you must first obtain the Apex Central certificate file from the Apex Central server from the following location:

```
<Apex Central installation folder>\Certificate\CA
\TMCM_CA_Cert.pem
```

Apex One and Apex Central use the certificate and public key encryption to ensure that only authorized registration and policy management communication occurs between the servers. If either server detects unauthorized communication, the server rejects any registration or policy settings being received.

Important

If your company uses a customized certificate on the Apex Central server, you must upload the Root CA certificate during the Apex Central registration.

Checking the Apex One Status on the Apex Central Management Console

Procedure

1. Open the Apex Central management console.

   To open the Apex Central console, on any endpoint on the network, open a web browser and type the following:

```
https://<Apex Central server name>/Webapp/login.aspx
```

Where `<Apex Central server name>` is the IP address or host name of the Apex Central server

2. On the main menu, click **Directories** > **Products**.
3. In the tree that displays, go to the **[Apex Central Server]** > **Local Folder** > **New Entity** folder.
4. Check if the Apex One server icon displays.

The Apex One Settings Export Tool

Apex One provides the Apex One Settings Export Tool, which allows administrators to copy Apex One settings from previous OfficeScan versions to the current version. The Apex One Settings Export Tool migrates the following settings:

Feature	Migrated Settings
Agent Management **Note** The Apex One Settings Export Tool migrates the applicable Agent Management settings to the `ApexOne_Agent_DLP_Policies.zip` and `ApexOne_Agent_Policies.zip` packages for use during import to Apex Central.	• Manual Scan • Scheduled Scan • Real-time Scan • Scan Now • Scan Method • Web Reputation • Behavior Monitoring • Device Control • Data Loss Prevention • Privileges and Other Settings • Additional Service Settings • Spyware/Grayware Approved List • Predictive Machine Learning • Suspicious Connection • Trusted Program List **Note** • The Server Migration Tool does not migrate the backup directories for Manual Scan, Scheduled Scan, Real-time Scan, and Scan Now. • Settings retain the configurations at both the root and domain level.
Agent Grouping	All settings **Note** The Active Directory domain structures display after synchronizing with Active Directory the first time.
Global Agent Settings	All settings
Endpoint Location	• Location awareness settings • Gateway IP address and MAC lists
Data Loss Prevention	• Data Identifiers • Templates
Firewall	• Policies • Profiles

Feature	Migrated Settings
Log Maintenance	All settings
Agent Update Source	• Agent update source • Customized update source list
Smart Protection Sources	Customized smart protection source list
Notifications	• General notification settings • Administrator notification settings • Outbreak notification settings • Agent notification settings
Proxy	All settings
Inactive Agents	All settings
Quarantine Manager	All settings
Web Console	All settings
`ofcscan.ini` settings	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]: All settings
`ofcserver.ini` settings	[INI_SERVER_DISK_THRESHOLD]: All settings

Note

- The tool does not back up the Security Agent listings of the OfficeScan server; only the domain structures.
- The tool only migrates features available on the older version of the OfficeScan server. For features that are not available on the older server, the tool applies the default settings.

Using the Apex One Settings Export Tool

Note

This version of Apex One supports the following migrations:

- On-premises Apex One servers: From OfficeScan version 11.0 and later
- Apex One as a Service servers: From OfficeScan version XG Service Pack 1

For a complete list of the settings that the Apex One Settings Export Tool migrates, see *The Apex One Settings Export Tool on page 14-29*.

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

Procedure

1. Locate the Server Migration Tool package.
   - From the Apex One web console, go to **Administration** > **Settings** > **Server Migration** and click the **Download Apex One Settings Export Tool** link.
   - On the Apex One 2019 server computer, navigate to <*Server installation folder*>`\PCCSRV\Admin\Utility\PolicyExportTool`.
2. Copy the Apex One Settings Export Tool to the source OfficeScan server computer.

   Important

   You must use the Apex One 2019 Apex One Settings Export Tool on the source OfficeScan server version to ensure that all data is properly formatted for the new target server. Apex One 2019 is not compatible with older versions of the Server Migration Tool.
3. Double-click `ApexOneSettingsExportTool.exe` to start the Apex One Settings Export Tool.

   The Apex One Settings Export Tool runs.

Note

The default names of the export packages are:

- `ApexOne_Agent_DLP_Policies.zip` (used to import DLP policy settings into Apex Central)
- `ApexOne_Agent_Policies.zip` (used to import all other Security Agent policy settings into Apex Central)
- `Server_Settings_Migration.zip` (used to import all Security Agent policy settings and OfficeScan server settings to another Apex One server)

4. Copy the export package(s) to a location that the destination Apex One or Apex Central server can access.
5. To import the settings to the destination Apex One server:
   a. From the Apex One web console, go to **Administration** > **Settings** > **Server Migration** and click the **Import Settings...** button.
   b. Locate the `Server_Settings_Migration.zip` package and click **Open**.
   c. Verify that the server contains all the previous OfficeScan version settings.
6. To import the Security Agent policy settings to the destination Apex Central console:
   a. From the Apex Central web console, go to **Policies** > **Policy Management**.
   b. In the **Product** drop-down, select **Apex One Security Agent**.
   c. Click **Import Settings**.
   d. Locate the `ApexOne_Agent_Policies.zip` package and click **Open**.
7. To import the Security Agent DLP policy settings to the destination Apex Central console:
   a. From the Apex Central web console, go to **Policies** > **Policy Management**.

b. In the **Product** drop-down, select **Apex One Data Loss Prevention**.

c. Click **Import Settings**.

d. Locate the `ApexOne_Agent_DLP_Policies.zip` package and click **Open**.

8. Move the old Security Agents to the new Apex One server.

   For details about moving Security Agents, see *Moving Security Agents to Another Domain or Server on page 2-58* or *Agent Mover on page 15-24*.

Suspicious Object List Settings

Suspicious objects are digital artifacts resulting from an analysis completed by Trend Micro Deep Discovery products or other sources. Apex One can synchronize suspicious objects and retrieve actions against these objects from a Control Manager 7.0 (or later) or the Apex Central 2019 (or later) on-premises server (that is connected to Deep Discovery).

After subscribing to Control Manager or Apex Central, select the types of suspicious objects to monitor C&C callbacks or possible targeted attacks identified by agents on the network. Suspicious objects include:

- Suspicious URL List
- Suspicious IP List
- Suspicious File List
- Suspicious Domain List

Note

If Apex One is subscribed to Deep Discovery Analyzer, only the suspicious URL list is available. After you unsubscribe Apex One from Deep Discovery Analyzer, it is not possible to re-subscribe. Apex One must subscribe to Apex Central with a connected to Deep Discovery to synchronize suspicious objects.

For more information about how Apex Central manages suspicious objects, see the *Apex Central Administrator's Guide*.

Configuring Suspicious Object List Settings

During Apex One registration to an on-premises Apex Central, Apex Central deploys an API key to Apex One to start the subscription process. To enable this automatic subscription process, check with the Apex Central administrator to ensure that Apex Central is connected to a Virtual Analyzer or that the Suspicious Object Lists have been manually populated.

For details on registering to the Apex Central server, see *Registering Apex One to Apex Central on page 14-25*.

Procedure

1. Go to **Administration** > **Settings** > **Suspicious Object List**.
2. Select which list to enable on agents.
   - Suspicious URL List
   - Suspicious IP List (only available when subscribing to the registered Apex Central or Control Manager server)
   - Suspicious File List (only available when subscribing to the registered Apex Central or Control Manager server)
   - Suspicious Domain List (only available when subscribing to the registered Apex Central or Control Manager server)

   Administrators can manually synchronize the Suspicious Object lists at any time by clicking the **Sync Now** button.

3. Under **Update the Suspicious Object lists on Security Agents**, specify when agents update the Suspicious Object lists.

   - **Based on the Security Agent component update schedule**: Security Agents update the Suspicious Object lists based on the current update schedule.
   - **Automatically after updating the Suspicious Object lists on the server**: Security Agents automatically update the Suspicious Object lists after the Apex One server receives updated lists.

   Note

   Security Agents not configured to receive updates from Update Agents perform incremental updates of the subscribed Suspicious Object lists during synchronization.

4. Click **Save**.

Reference Servers

One of the ways the Security Agent determines which policy or profile to use is by checking its connection status with the Apex One server. If an internal Security Agent (or any agent within the corporate network) cannot connect to the server, the agent status becomes offline. The agent then applies a policy or profile intended for external agents. Reference servers address this issue.

Any Security Agent that loses connection with the Apex One server will try connecting to reference servers. If the agent successfully establishes connection with a reference server, it applies the policy or profile for internal agents.

Policies and profiles managed by reference servers include:

- Firewall profiles
- Web reputation policies

- Data Protection policies
- Device Control policies

Take note of the following:

- Assign computers with server capabilities, such as a web server, SQL server, or FTP server, as reference servers. You can specify a maximum of 320 reference servers.
- Security Agents connect to the first reference server on the reference server list. If connection cannot be established, the agent tries connecting to the next server on the list.
- Security Agents use reference servers when determining the antivirus (Behavior Monitoring, Device Control, firewall profiles, the web reputation policy) or Data Protection settings to use. Reference servers do not manage agents or deploy updates and agent settings. The Apex One server performs these tasks.
- The Security Agent cannot send logs to reference servers or use them as update sources

Managing the Reference Server List

Procedure

1. Go to **Agents** > **Firewall** > **Profiles** or **Agents** > **Endpoint Location**.
2. Depending on the displayed screen, do the following:
   - If you are on the **Firewall Profiles for Agents** screen, click **Edit Reference Server List**.
   - If you are on the **Endpoint Location** screen, click **reference server list**.
3. Select **Enable the Reference Server list**.

- **Exclude agents using VPN or PPP dial-up connections**: Select to define endpoints that use a VPN or PPP (Point-to-Point Protocol) dial-up connection to the reference servers as **External Agents**

4. To add any endpoint to the list, click **Add**.

   a. Specify the endpoint's IPv4/IPv6 address, name, or fully qualified domain name (FQDN), such as:

      - `computer.networkname`
      - `12.10.10.10`
      - `mycomputer.domain.com`

   b. Type the port through which agents communicate with this endpoint. Specify any open contact port (such as ports 20, 23 or 80) on the reference server.

      Note

      To specify another port number for the same reference server, repeat steps 2a and 2b. The Security Agent uses the first port number on the list and, if connection is unsuccessful, uses the next port number.

   c. Click **Save**.

5. To edit the settings of any endpoint on the list, click the endpoint name. Modify the endpoint name or port, and then click **Save**.

6. To remove any endpoint from the list, select the endpoint name and then click **Delete**.

7. To enable the endpoints to act as reference servers, click **Assign to Agents**.

Administrator Notification Settings

Configure administrator notification settings to allow Apex One to successfully send notifications through email, and SNMP Trap. Apex One can

also send notifications through Windows NT event log but no settings are configured for this notification channel.

Apex One can send notifications to you and other Apex One administrators when the following are detected:

TABLE 14-16. Detections that Trigger Administrator Notifications

DETECTIONS	NOTIFICATION CHANNELS		
	EMAIL	SNMP TRAP	WINDOWS NT EVENT LOGS
Viruses and malware	Yes	Yes	Yes
Spyware and grayware	Yes	Yes	Yes
Digital asset transmissions	Yes	Yes	Yes
C&C callbacks	Yes	Yes	Yes
Virus and malware outbreaks	Yes	Yes	Yes
Spyware and grayware outbreaks	Yes	Yes	Yes
Firewall violation outbreaks	Yes	No	No
Shared folder session outbreaks	Yes	No	No
C&C callback outbreaks	Yes	Yes	Yes

Configuring General Notification Settings

Procedure

1. Go to **Administration** > **Notifications** > **General Settings**.
2. Configure email notification settings.
   a. In the **SMTP server** field, specify the endpoint name, or IPv4 or IPv6 address of the SMTP server.

b. Specify the port used by the SMTP server.

   Valid port numbers are 1 to 65535.

c. In the **From** field, specify the email address that displays as the sender of the notification.

   If you want to enable ESMTP in the next step, specify a valid email address.

d. Optionally enable **ESMTP**.

e. Specify the user name and password for the email address you specified in the **From** field.

f. Choose a method for authenticating the agent to the server:

   - **Login**: Login is an older version of the mail user agent. The server and agent both use BASE64 to authenticate the user name and password.
   - **Plain Text**: Plain Text is the easiest to use but can also be unsafe because the user name and password are sent as one string and BASE64 encoded before being sent over the Internet.
   - **CRAM-MD5**: CRAM-MD5 uses a combination of a challenge-response authentication mechanism and a cryptographic Message Digest 5 algorithm to exchange and authenticate information.

3. Configure SNMP Trap notification settings.

   a. Specify either an IPv4/IPv6 address or endpoint name in the **Server IP address** field.

   b. Specify a community name that is difficult to guess.

Note

Due to security concerns, the Community Name displays as a masked value using the asterisk (*) character. The default value assigned is: “public”.

4. Click **Save**.

System Event Logs

Apex One records events related to the server program, such as shutdown and startup. Use these logs to verify that the Apex One server and services work properly.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing System Event Logs

Procedure

1. Go to **Logs** > **System Events**.
2. Under **Event**, check for logs that need further action. Apex One logs the following events:

TABLE 14-17. System Event Logs

LOG TYPE	EVENTS
Apex One Master Service and Database Server	• Master Service started • Master Service stopped successfully • Master Service stopped unsuccessfully
Outbreak Prevention	• Outbreak Prevention enabled • Outbreak Prevention disabled • Number of shared folder sessions in the last <number of minutes>

Log Type	Events
Database backup	• Database backup successful • Database backup unsuccessful
Role-based web console access	• Logging on to the console • Password modification • Logging off from the console • Session timeout (user automatically logged off)
Server authentication	• The Security Agent received invalid commands from the server • Authentication certificate invalid or expired
Virtual Analyzer	• Sample submitted for analysis • Sample analysis completed • The Virtual Analyzer reported a previous, duplicate sample submission from another connected Apex One server

3. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Log Management

Apex One keeps comprehensive logs about security risk detections, events, and updates. Use these logs to assess your organization's protection policies and to identify Security Agents at a higher risk of infection or attack. Also use these logs to check agent-server connection and verify that component updates were successful.

Apex One also uses a central time verification mechanism to ensure time consistency between Apex One server and agents. This prevents log inconsistencies caused by time zones, Daylight Saving Time, and time differences, which can cause confusion during log analysis.

Note

Apex One performs time verification for all logs except for Server Update and System Event logs.

The Apex One server receives the following logs from Security Agents:

- *Viewing Virus/Malware Logs on page 7-89*
- *Viewing Spyware/Grayware Logs on page 7-96*
- *Viewing Spyware/Grayware Restore Logs on page 7-100*
- *Viewing Firewall Logs on page 13-28*
- *Viewing Web Reputation Logs on page 12-20*
- *Viewing Suspicious Connection Logs on page 8-14*
- *Viewing Suspicious File Logs on page 7-100*
- *Viewing C&C Callback Logs on page 12-21*
- *Viewing Behavior Monitoring Logs on page 9-23*
- *Viewing Predictive Machine Learning Logs on page 8-11*
- *Viewing Device Control Logs on page 10-19*
- *Viewing Scan Operation Logs on page 7-101*
- *Viewing Data Loss Prevention Logs on page 11-57*
- *Viewing Security Agent Update Logs on page 6-50*
- *Viewing Connection Verification Logs on page 15-45*

The Apex One server generates the following logs:

- *Apex One Server Update Logs on page 6-26*
- *System Event Logs on page 14-41*

The following logs are also available on the Apex One server and Security Agents:

- *Windows Event Logs on page 18-22*
- *Apex One Server Logs on page 18-3*
- *Security Agent Logs on page 18-12*

Log Maintenance

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule from the web console.

Deleting Logs Based on a Schedule

Procedure

1. Go to **Logs** > **Log Maintenance**.
2. Select **Enable scheduled deletion of logs**.
3. Select the log types to delete. All Apex One-generated logs, except debug logs, can be deleted based on a schedule. For debug logs, disable debug logging to stop collecting logs.

   Note

   For virus/malware logs, you can delete logs generated from certain scan types and Damage Cleanup Services. For spyware/grayware logs, you can delete logs from certain scan types. For details about scan types, see *Scan Types on page 7-14*.

4. Select whether to delete logs for all the selected log types or only logs older than a certain number of days.
5. Specify the log deletion frequency and time.
6. Click **Save**.

Manually Deleting Logs

Procedure

1. Go to **Logs** > **Agents** > **Security Risks**, or **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Perform one of the following steps:
   - If you are accessing the **Security Risk Logs** screen, click **Delete Logs**.
   - If you are accessing the **Agent Management** screen, click **Logs** > **Delete Logs**.
4. Under **Log Types to Delete**, select the type of log data to remove:
   - Behavior Monitoring logs
   - C&C Callback logs
   - Data Loss Prevention logs
   - Device Control logs
   - Firewall logs
   - Predictive Machine Learning logs
   - Spyware/Grayware logs
   - Scan Operation logs
   - Suspicious Connection logs
   - Suspicious Files logs
   - Virus/Malware logs
   - Web Reputation logs

Note

For virus/malware logs, you can delete logs generated from certain scan types and Damage Cleanup Services. For spyware/grayware logs, you can delete logs from certain scan types.

For details about scan types, see *Scan Types on page 7-14*.

5. Under **Logs to Delete**, select one of the following:
   - **All logs for the selected log types**: Deletes all log data for the selected log types
   - **Logs older than XX days**: Deletes all log data older than the amount of days specified for the selected log types
6. Click **Delete**.

Licenses

View, activate, and renew Apex One licenses on the web console.

Note

Some native Apex One features, such as Data Protection and Virtual Desktop Support, have their own licenses. The licenses for these features are activated and managed from Plug-in Manager. For details about licensing for these features, see *Data Protection License on page 3-4* and *Virtual Desktop Support License on page 15-79*.

A pure IPv6 Apex One server cannot connect to the Trend Micro Online Registration Server to activate/renew the license. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Apex One server to connect to the registration server.

Managing License Information

The **License Information** screen allows you to view details about and renew your existing product license.

Procedure

1. Go to **Administration** > **Settings** > **Product License**.
2. View license information.

Item	Description
Product	The name of the product license
Status	The current license status
Type	Indicates either a **Full** or **Trial** subscription
Seats	The number of Security Agents licensed to report to the server
Expiration Date	The date the license expires
Activation Code	The current Activation Code registered to Trend Micro
Last Updated	The last time updated license information was retrieved from Trend Micro servers

3. Renew an expired or soon-to-expire license.
   a. Click **Specify Activation Code**.

      The **New Activation Code** screen appears.

   b. Paste or type the new **Activation Code**.
   c. Click **Save**.

      The **License Information** screen appears with the updated license information.

SQL Server Database Connection Settings

The SQL Server Database Configuration Tool allows you to connect the Apex One server to another existing Apex One SQL database and change the logon credentials used to connect to your existing database.

The SQL Server Database Configuration Tool allows you to perform the following:

- Switch to another preexisting Apex One SQL Server database instance
- Update logon credentials to the existing SQL Server database
- Configure alert settings for when the SQL Server database becomes unavailable

Configuring the SQL Server Database Connection

The SQL Server Database Configuration Tool allows you to connect the Apex One server to another existing Apex One SQL database and change the logon credentials used to connect to your existing database.

Procedure

1. On the Apex One server computer, browse to <*Server installation folder*>`\PCCSRV\Admin\Utility\SQL`.
2. Double-click `SQLTxfr.exe` to run the tool.

   The **Apex One SQL Server Database Configuration** console opens.
3. Specify the **Server name** as follows: `<host name or IP address of the SQL Server>,<port_number>\<instance name>`

   Important

   Apex One automatically creates an instance for the Apex One database when SQL Server installs. When migrating to an existing SQL Server or database, type the preexisting instance name for the Apex One instance on the SQL Server.
4. Provide the authentication credentials for the SQL Server database.
   - 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
- bulkadmin
- db_owner

5. Specify the Apex One **Database name** on the SQL Server.
6. Optionally, perform the following tasks:
   - Click **SQL Database Unavailable Alert...** to configure the SQL database notification settings.

     For details, see *Configuring the SQL Database Unavailable Alert on page 14-49*.
   - Click **Test Connection** to verify the authentication credentials for the existing SQL Server or database.
7. Click **Start** to apply the configuration changes.

Configuring the SQL Database Unavailable Alert

Apex One automatically sends this alert whenever the SQL database becomes unavailable.

WARNING!

Apex One automatically stops all services when the database becomes unavailable. Apex One cannot log agent or event information, perform updates, or configure agents when the database is unavailable.

Procedure

1. On the Apex One server computer, browse to <*Server installation folder*>`\PCCSRV\Admin\Utility\SQL`.
2. Double-click `SQLTxfr.exe` to run the tool.

   The **Apex One SQL Server Database Configuration** console opens.
3. Click **SQL Database Unavailable Alert...**.

   The **SQL Server Unavailable Alert** screen opens.
4. Type the email address(es) for the recipient(s) of the alert.

   Separate multiple entries using semicolons (;).
5. Modify the **Subject** and **Message** as necessary.

   Apex One provides the following token variables:

   TABLE 14-18. SQL Database Unavailable Alert Tokens

VARIABLE	DESCRIPTION
%x	The name of the Apex One SQL Server instance
%s	The name of the affected Apex One server

6. Click **OK**.

Apex One Web Server/Agent Connection Settings

During Apex One server installation, Setup automatically sets up a web server that enables networked computers to connect to the Apex One server. Configure the web server to which networked endpoint agents will connect.

If you modify the web server settings externally (for example, from the IIS management console), replicate the changes in Apex One. For example, if you change the IP address of the server for networked computers manually or if you assign a dynamic IP address to it, you need to reconfigure the server settings of Apex One.

WARNING!

Changing the connection settings may result in the permanent loss of connection between the server and agents and require the re-deployment of Security Agents.

Configuring Connection Settings

Procedure

1. Go to **Administration** > **Settings** > **Agent Connection**.
2. Type the domain name or IPv4/IPv6 address and port number of the web server.

   Note

   The port number is the trusted port that the Apex One server uses to communicate with Security Agents.

3. Click **Save**.

Server-Agent Communication

You can configure Apex One to ensure that all communication between the server and agents are valid. Apex One provides public-key cryptography and enhanced encryption features to protect all communication between the server and agents.

For details regarding the communication protection features, refer to the following:

- *Authentication of Server-initiated Communications on page 14-52*
- *Enhanced Encryption of Server-Agent Communication on page 14-56*

Authentication of Server-initiated Communications

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.

The public and private keys are associated with a Trend Micro certificate. During installation of the Apex One server, Setup stores the certificate on the host's certificate store. Use the Authentication Certificate Manager tool to manage Trend Micro certificates and keys.

When deciding on whether to use a single authentication key across all Apex One servers, take note of the following:

- Implementing a single certificate key is a common practice for standard levels of security. This approach balances the security level of your organization and reduces the overhead associated with maintaining multiple keys.

- Implementing multiple certificate keys across Apex One servers provides a maximum level of security. This approach increases the maintenance required when certificate keys expire and need to be redistributed across the servers.

Important

Before reinstalling the Apex One server, ensure that you back up the existing certificate. After the new installation completes, import the backed up certificate to allow communication authentication between the Apex One server and Security Agents to continue uninterrupted. If you create a new certificate during server installation, Security Agents cannot authenticate server communication because they are still using the old certificate (which no longer exists).

For details on backing up, restoring, exporting, and importing certificates, see *Using Authentication Certificate Manager on page 14-53*.

Using Authentication Certificate Manager

The Apex One server maintains expired certificates for agents with expired public keys. For example, agents that have not connected to the server for an extended period of time have expired public keys. When agents reconnect, they associate the expired public key with the expired certificate, allowing them to recognize server-initiated communications. The server then deploys the latest public key to the agents.

When configuring certificates, note the following:

- For the certificate path, mapped drives and UNC paths are accepted.
- Choose a strong password and then record it for future reference.

Important

When using the Authentication Certificate Manager tool, note the following requirements:

- The user must have administrator privileges
- The tool can only manage certificates located on the local endpoint

Procedure

1. On the Apex One server, open a command prompt and change the directory to <*Server installation folder*>\PCCSRV\Admin\Utility\CertificateManager.

2. Issue any of the following commands:

Command	Example	Description
CertificateManager.exe -c [Backup_Password]	`CertificateManager.exe -c strongpassword`	Generates a new Trend Micro certificate and replaces the existing certificate Do this if the existing certificate has expired or if it has been leaked to unauthorized parties.
CertificateManager.exe -b [Password] [Certificate path] **Note** The certificate is in ZIP format.	`CertificateManager.exe -b strongpassword D:\Test\TrendMicro.zip`	Backs up all Trend Micro certificates issued by the current Apex One server Do this to back up the certificate on the Apex One server. **Note** Backing up the Apex One server certificates allows you to use these certificates if you need to reinstall the Apex One server.
CertificateManager.exe -r [Password] [Certificate path] **Note** The certificate is in ZIP format.	`CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip`	Restores all Trend Micro certificates on the server Do this to restore the certificate on a reinstalled Apex One server.

COMMAND	EXAMPLE	DESCRIPTION
CertificateManager.exe -e [Certificate path]	`CertificateManager.exe -e <Agent_installation_folder>\OfcNTCer.dat`	Exports the Security Agent public key associated with the currently used certificate Do this if the public key used by agents becomes corrupted. Copy the `.dat` file to the agent's root folder, overwriting the existing file. **Important** The file path of the certificate on the Security Agent must be: `<Agent_installation_folder>\OfcNTCer.dat`
CertificateManager.exe -i [Password] [Certificate path] **Note** The default file name of the certificate is: `OfcNTCer.pfx`	`CertificateManager.exe -i strongpassword D:\Test\OfcNTCer.pfx`	Imports a Trend Micro certificate to the certificate store
CertificateManager.exe -l [CSV Path]	`CertificateManager.exe -l D:\Test\MismatchedAgentList.csv`	Lists agents (in CSV format) currently using a mismatched certificate

Enhanced Encryption of Server-Agent Communication

Apex One provides enhanced encryption of communication between the server and agents using Advanced Encryption Standard (AES) 256 to meet governmental compliance standards.

Important

Apex One only supports AES-256 encryption on servers and agents running OfficeScan 11.0 SP1 or later versions and Plug-in Manager 2.2 or later versions.

WARNING!

Ensure that you upgrade all agents that the server manages to version 11.0 SP1 before enabling AES-256 encryption. Older agents versions may be unable to decrypt the AES-256 encrypted communication. Enabling AES-256 encryption on older agent versions may result in a complete loss of communication with the Apex One server when using a proxy server.

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **Network** tab.
3. Go to the **Server-Agent Communication** section.
4. Click the **Change** button beside **AES-256 encryption for communication between the Apex One server and Security Agents**.

   A message appears.
5. Click **Verify Versions** to confirm that you have updated all agents to OfficeScan 11.0 SP1 or later.
6. Click **OK**.

Web Console Password

The screen for managing the web console password (or the password for the root account created during Apex One server installation) will only be accessible if the server computer does not have the resources required to use role-based administration. If resources are adequate, this screen does not display and the password can be managed by modifying the root account in the **User Accounts** screen.

If Apex One is not registered to Apex Central, contact your support provider for instructions on how to gain access to the web console.

Configuring Web Console Settings

Configure the Apex One web console settings to determine how users access the web console and how often a screen refresh occurs.

Procedure

1. Go to **Administration** > **Settings** > **Web Console**.
2. Configure the required settings.

Section	Settings
Automatic Refresh Settings	Select **Automatically refresh the web console** to enable the Apex One server to refresh screen data at the specified interval • **Refresh interval**: Select the frequency (in seconds) in which the web console refreshes the screen data
Time-out Settings	Select **Automatically log off inactive users** to enable the Apex One server to log off users at the specified interval • **Inactive interval**: Select the period of inactivity (in minutes) in which the web console automatically logs off users

3. Click **Save**.

Quarantine Manager

Whenever the Security Agent detects a security risk and the scan action is quarantine, it encrypts the infected file and then moves it to the local quarantine folder located in <*Agent installation folder*>\SUSPECT\Backup.

After moving the file to the local quarantine directory, the Security Agent sends it to the designated quarantine directory. Specify the directory in **Agents** > **Agent Management > Settings** > **{Scan Type} Settings** > **Action** tab. Files in the designated quarantine directory are encrypted to prevent them from infecting other files. See *Quarantine Directory on page 7-40* for more information.

If the designated quarantine directory is on the Apex One server computer, modify the server's quarantine directory settings from the web console. The server stores quarantined files in <*Server installation folder*>\PCCSRV\Virus.

Note

If the Security Agent is unable to send the encrypted file to the Apex One server for any reason, such as a network connection problem, the encrypted file remains in the Security Agent quarantine folder. The Security Agent will attempt to resend the file when it connects to the Apex One server.

Configuring Quarantine Directory Settings

Procedure

1. Go to **Administration** > **Settings** > **Quarantine Manager**.
2. Accept or modify the default capacity of the quarantine folder and the maximum size of an infected file that Apex One can store on the quarantine folder.

   The default values display on the screen.
3. Click **Save Quarantine Settings**.

4. To remove all existing files in the quarantine folder, click **Delete All Quarantined Files**.

Server Tuner

Use Server Tuner to optimize the performance of the Apex One server using parameters for the following server-related performance issues:

- **Download**

  When the number of Security Agents (including update agents) requesting updates from the Apex One server exceeds the server's available resources, the server moves the agent update request into a queue and processes the requests when resources become available. After the agent successfully updates components from the Apex One server, it notifies the server that the update is complete. Set the maximum number of minutes the Apex One server waits to receive an update notification from the agent. Also set the maximum number of times the server tries to notify the agent to perform an update and to apply new configuration settings. The server keeps trying only if it does not receive agent notification.

- **Network Traffic**

  The amount of network traffic varies throughout the day. To control the flow of network traffic to the Apex One server and to other update sources, specify the number of Security Agents that can simultaneously update at any given time of the day.

Server Tuner requires the following file: `SvrTune.exe`

Running Server Tuner

Procedure

1. On the Apex One server computer, go to <*Server installation folder*>`\PCCSRV\Admin\Utility\SvrTune`.

2. Double-click `SvrTune.exe` to start Server Tuner.

   The Server Tuner console opens.

3. Under **Download**, modify the following settings:

   - **Timeout for client**: Type the number of minutes for the Apex One server to wait to receive an update response from Security Agents. If the agent does not respond within this time, the Apex One server does not consider the Security Agent to have current components. When a notified Security Agent times out, a slot for another agent awaiting notification becomes available.
   - **Timeout for update agent**: Type the number of minutes for the Apex One server to wait to receive an update response from an Update Agent. When a notified Security Agent times out, a slot for another agent awaiting notification becomes available.
   - **Retry count**: Type the maximum number of times the Apex One server tries to notify the Security Agent to perform an update or to apply new configuration settings.
   - **Retry interval**: Type the number of minutes the Apex One server waits between notification attempts.

4. Under **Network Traffic**, modify the following settings:

   - **Normal hours**: Click the radio buttons that represent the hours of the day you consider network traffic to be normal.
   - **Off-peak hours**: Click the radio buttons that represent the hours of the day you consider network traffic to be at its lowest.
   - **Peak hours**: Click the radio buttons that represent the hours of the day you consider network traffic to be at its peak.
   - **Maximum client connections**: Type the maximum number of clients that can simultaneously update components from both "other update source" and from the Apex One server. Type a maximum number of clients for each of the time periods. When the maximum number of connections is reached, Security Agents can update components only after a current Security Agent connection

closes (due to either the completion of the update or the agent response reaching the timeout value you specified in the **Timeout for client** or **Timeout for Update Agent** field).

5. Click **OK**. A prompt appears asking you to restart the Apex One Master Service.

Note

Only the service restarts, not the computer.

6. Select from the following restart options:

   - Click **Yes** to save the Server Tuner settings and restart the service. The settings take effect immediately after restart.
   - Click **No** to save the Server Tuner settings but not restart the service. Restart the Apex One Master Service or restart the Apex One server computer for settings to take effect.

Smart Feedback

Trend Micro Smart Feedback shares anonymous threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. You can disable Smart Feedback anytime through this console.

Participating in the Smart Feedback Program

Procedure

1. Go to **Administration** > **Smart Protection**.
2. Click **Enable Trend Micro Smart Feedback**.
3. To help Trend Micro understand your organization, select the **Industry** type.

4. To send information about potential security threats in the files on your Security Agents, select the **Enable feedback of suspicious program files** check box.

   Note

   Files sent to Smart Feedback contain no user data and are submitted only for threat analysis.

5. To configure the criteria for sending feedback, select the number of detections for the specific amount of time that triggers the feedback.
6. Specify the maximum bandwidth Apex One can use when sending feedback to minimize network interruptions.
7. Click **Save**.

Chapter 15

Managing the Security Agent

This chapter describes Security Agent management and configurations.

Topics include:

Endpoint Location

Apex One provides a location awareness feature that determines whether the Security Agent is in the internal or external network. Location awareness is leveraged in the following Apex One features and services:

TABLE 15-1. Features and Services that Leverage Location Awareness

FEATURE/SERVICE	DESCRIPTION
File Reputation Services	For smart scan agents, the location of the Security Agentdetermines the smart protection source to which the Security Agent sends scan queries. External Security Agents send scan queries to the Smart Protection Network while internal Security Agents send scan queries to the sources defined in the smart protection source list. For more information, see *Smart Protection Sources on page 4-5*.
Web Reputation Data Loss Prevention Device Control	The location of the Security Agent determines whether the Security Agent applies internal or external policy settings. Administrators typically enforce a stricter policy for external Security Agents. For more information, see: • *Web Reputation Policies on page 12-5*. • *Data Loss Prevention Policies on page 11-3* • *Device Control on page 10-2*

Location Criteria

Specify whether location is based on the Security Agent endpoint's gateway IP address or the Security Agent's connection status with the Apex One server or any reference server.

- **Agent connection status**: If the Security Agent can connect to the Apex One server or any of the assigned reference servers on the intranet, the endpoint's location is internal. Additionally, if any endpoint outside the corporate network can establish connection with the Apex One server/ reference server, its location is also internal. If none of these conditions apply, the endpoint's location is external.

- **Gateway IP and MAC address**: If the Security Agent endpoint's gateway IP address matches any of the gateway IP addresses you specified on the **Endpoint Location** screen, the endpoint's location is internal. Otherwise, the endpoint's location is external.

Configuring Location Settings

Procedure

1. Go to **Agents** > **Endpoint Location**.
2. Choose whether location is based on **Agent connection status** or **Gateway IP and MAC address**.
3. If you choose **Agent connection status**, decide if you want to use a reference server.

   See *Reference Servers on page 14-36* for details.

   a. If you did not specify a reference server, the Security Agent checks the connection status with the Apex One server when the following events occur:

      - The Security Agent switches from Independent mode to normal (online/offline) mode.
      - The Security Agent switches from one scan method to another.

        See *Scan Method Types on page 7-8* for details.
      - The Security Agent detects an IP address change for the endpoint.
      - The Security Agent restarts.
      - Server initiates connection verification.

        See *Security Agent Icons on page 15-28* for details.
      - Web reputation location criteria changes while applying global settings.

- Outbreak prevention policy is no longer enforced and pre-outbreak settings are restored.

b. If you specified a reference server, the Security Agent checks its connection status with the Apex One server first, and then with the reference server if connection to the Apex One server is unsuccessful. The Security Agent checks the connection status every hour and when any of the above events occur.

4. If you choose **Gateway IP and MAC address**:

   a. Type the gateway IPv4/IPv6 address in the text box provided.

   b. Type the MAC address.

   c. Click **Add**.

      If you do not type a MAC address, Apex One will include all the MAC addresses belonging to the specified IP address.

   d. Repeat step a to step c until you have all the gateway IP addresses you want to add.

   e. Use the Gateway Settings Importer tool to import a list of gateway settings.

      See *Gateway Settings Importer on page 15-4* for details.

5. Click **Save**.

Gateway Settings Importer

Apex One checks the endpoint's location to determine the web reputation policy to use and the smart protection source to which to connect. One of the ways Apex One identifies the location is by checking the endpoint's gateway IP address and MAC address.

Configure the gateway settings on the **Endpoint Location** screen or use the Gateway Settings Importer tool to import a list of gateway settings to the **Endpoint Location** screen.

Using Gateway Settings Importer

Procedure

1. Prepare a text file (`.txt`) containing the list of gateway settings. On each line, type an IPv4 or IPv6 address and optionally type a MAC address.

   Separate IP addresses and MAC addresses by a comma. The maximum number of entries is 4096.

   For example:

   ```
   10.1.111.222,00:17:31:06:e6:e7

   2001:0db7:85a3:0000:0000:8a2e:0370:7334

   10.1.111.224,00:17:31:06:e6:e7
   ```

2. On the server computer, go to <*Server installation folder*>`\PCCSRV\Admin\Utility\GatewaySettingsImporter`.

3. Right-click `GSImporter.exe` and select **Run as administrator**.

   Note

   You cannot run the Gateway Settings Importer tool from Terminal Services.

4. On the **Gateway Settings Importer** screen, browse to the file created in step 1 and click **Import**.

5. Click **OK**.

   The gateway settings display on the **Endpoint Location** screen and the Apex One server deploys the settings to Security Agents.

6. To delete all entries, click **Clear All**.

   If you only need to delete a particular entry, remove it from the **Endpoint Location** screen.

7. To export the settings to a file, click **Export All** and then specify the file name and type.

Security Agent Program Management

The following topics discuss ways to manage and protect the Security Agent program:

- *Security Agent Services on page 15-6*
- *Security Agent Service Restart on page 15-13*
- *Security Agent Self-protection on page 15-14*
- *Security Agent Console Access Restriction on page 15-18*
- *Security Agent Unloading and Unlocking on page 15-19*
- *Security Agent Independent Mode Privilege on page 15-20*
- *Agent Mover on page 15-24*
- *Inactive Security Agents on page 15-27*

Security Agent Services

The Security Agent runs the services listed in the following table. You can view the status of these services from Microsoft Management Console.

Service	Features Controlled
Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)	• Behavior Monitoring • Device Control • Certified Safe Software Service
Apex One NT Firewall (`TmPfw.exe`)	Apex One Firewall

Service	Features Controlled
Apex One Data Protection Service (`dsagent.exe`)	• Data Loss Prevention • Device Control
Apex One NT Listener (`tmlisten.exe`)	Communication between the Security Agent and Apex One server
Apex One NT RealTime Scan (`ntrtscan.exe`)	• Real-time Scan • Scheduled Scan • Manual Scan/Scan Now
Apex One Common Client Solution Framework (`TmCCSF.exe`)	Advanced Protection Service • Browser Exploit Prevention • Memory Scanning
Trend Micro Advanced Threat Assessment Service (Agent) (`ATASAgent.exe`)	Advanced Managed Detection and Response tasks and communication
Trend Micro Application Control Service (Agent) (`TMiACAgentSvc.exe`)	Application Control
• Trend Micro Endpoint Sensor Engine Wrapper(TMESE.exe) • Trend Micro Endpoint Sensor Service (Agent) (`TMESC.exe`)	Endpoint Sensor
Trend Micro Vulnerability Protection Service (Agent) (`iVPAgent.exe`)	Vulnerability Protection

The following services provide robust protection but their monitoring mechanisms can strain system resources, especially on servers running system-intensive applications:

- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

- Apex One NT Firewall (`TmPfw.exe`)
- Apex One Data Protection Service (`dsagent.exe`)

For this reason, these services are disabled by default on Windows Server platforms. If you want to enable these services:

- Monitor the system's performance constantly and take the necessary action when you notice a drop in performance.
- For `TMBMSRV.exe`, you can enable the service if you exempt system-intensive applications from Behavior Monitoring policies. You can use a performance tuning tool to identify system intensive applications.

  For details, see *Using the Trend Micro Performance Tuning Tool on page 15-11*.

For desktop platforms, disable the services only if you notice a significant drop in performance.

Excluding Security Agent Services and Processes in Third-Party Applications

The following table lists the process names and full file locations of Security Agent processes that you may need to exclude from third-party applications.

Process	Location
TMCCSF.exe	<*Agent installation folder*>\CCSF\TmCCSF.exe
TmPfw.exe	<*Agent installation folder*>\TmPfw.exe
TmListen.exe	<*Agent installation folder*>\tmlisten.exe
Ntrtscan.exe	<*Agent installation folder*>\ntrtscan.exe
ATASAgent.exe	<%Program Files (x86) folder%>\Trend Micro\iService\iATAS \ATASAgent.exe
dsagent.exe	<%Windows directory%>\system32\dgagent\DSAGENT.exe

Process	Location
TMiACAgentSvc.exe	<%Program Files (x86) folder%>\Trend Micro\iService\iAC\ac_bin \TMiACAgentSvc.exe
ESEServiceShell.exe	<%Program Files (x86) folder%>\Trend Micro\iService\iES\ESE \ESEServiceShell.exe
ESClient.exe	<%Program Files (x86) folder%>\Trend Micro\iService\iES\ESE \ESClient.exe
TMBMSRV.exe	<%Program Files (x86) folder%>\Trend Micro\BM\TMBMSRV.exe
iVPAgent.exe	<%Program Files (x86) folder%>\Trend Micro\iService\iVP \iVPAgent.exe
ShowMsg.exe	<%Windows directory%>\System32\ShowMsg.exe
TmSSClient.exe	<*Agent installation folder*>\TmSSClient.exe
LogServer.exe	<*Agent installation folder*>\Temp\LogServer\LogServer.exe
TmsaInstance64.exe	<*Agent installation folder*>\CCSF\module\BES\TmsaInstance64.exe
CNTAoSMgr.exe	<*Agent installation folder*>\CNTAoSMgr.exe
PccNTMon.exe	<*Agent installation folder*>\PccNTMon.exe
ESEFrameworkHost.exe	<%Program Files (x86) folder%>\Trend Micro\iService\iES\ESE \ESEFrameworkHost.exe

Configuring Additional Security Agent Services

Important

Enabling additional services on Windows Server platforms may affect server performance. After enabling a service on a Windows Server platform, Trend Micro recommends that you monitor the server for some time to ensure that no performance impact occurred.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Additional Service Settings**.
4. Select to enable the required service on **Windows desktops** or **Windows Server platforms** in the following sections:
   - **Unauthorized Change Prevention Service**
     - For Windows Server platforms, select **Only enable services required by Security Agent Self-protection features** to ensure that the Security Agent program stays protected without affecting server performance.

       Important

       Selecting **Only enable services required by Security Agent Self-protection features** ensures that the service related to Behavior Monitoring, Device Control, Predictive Machine Learning (process detections), and the Certified Safe Software Service do not run. If you want to use any of the scanning features, do not enable this feature.
   - **Firewall Service**

     Important

     Enabling or disabling the service temporarily disconnects endpoints from the network. Ensure that you change the settings only during non-critical hours to minimize connection disruptions.
   - **Suspicious Connection Service**
   - **Data Protection Service**

Important

Enabling or disabling the service temporarily disconnects endpoints from the network. Ensure that you change the settings only during non-critical hours to minimize connection disruptions.

- **Advanced Protection Service**

5. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Using the Trend Micro Performance Tuning Tool

Procedure

1. Download Trend Micro Performance Tuning Tool from:

   http://esupport.trendmicro.com/solution/en-us/1056425.aspx

2. Unzip `TMPerfTool.zip` to extract `TMPerfTool.exe`.
3. Place `TMPerfTool.exe` in the <*Agent installation folder*> or in the same folder as `TMBMCLI.dll`.
4. Right-click `TMPerfTool.exe` and select **Run as administrator**.
5. Read and accept the end user agreement and then click **OK**.
6. Click **Analyze**.

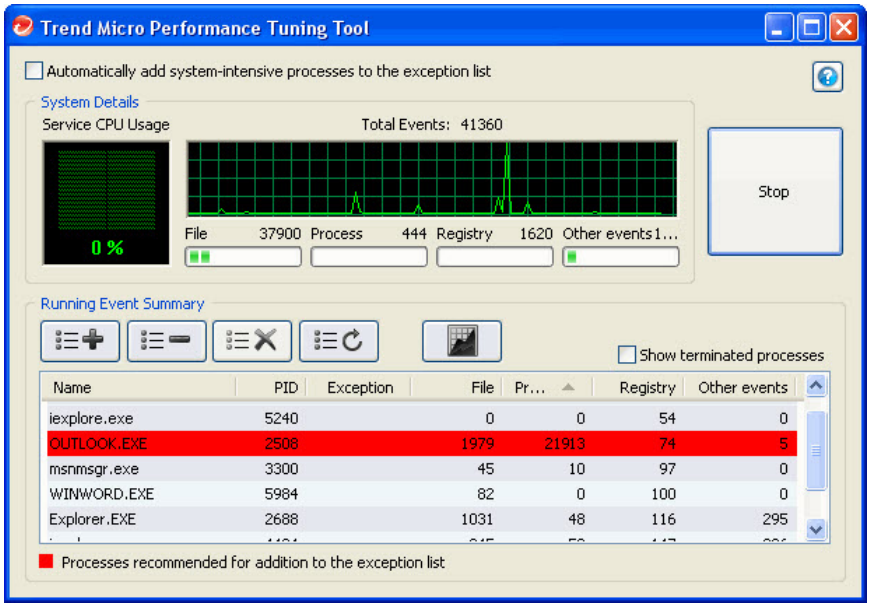


FIGURE 15-1. System-intensive process highlighted

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

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

8. Check if the system or application performance improves.

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

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

    a. Note the name of the application.

    b. Click **Stop**.

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

d. Review the applications that have been identified as conflicting and add them to the Behavior Monitoring exception list.

For details, see *Behavior Monitoring Exception List on page 9-9*.

Security Agent Service Restart

Apex One restarts Security Agent services that stopped responding unexpectedly and were not stopped by a normal system process. For details about agent services, see *Security Agent Services on page 15-6*.

Configure the necessary settings to enable Security Agent services to restart.

Configuring Service Restart Settings

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **System** tab.
3. Go to the **Services Restart** section.
4. Select **Automatically restart any Security Agent service if the service terminates unexpectedly**.
5. Configure the following:
   - **Restart the service after __ minutes**: Specify the amount of time (in number of minutes) that must elapse before Apex One restarts a service.
   - **If the first attempt to restart the service is unsuccessful, retry __ times**: Specify the maximum retry attempts for restarting a service. Manually restart a service if it remains stopped after the maximum retry attempts.
   - **Reset the unsuccessful restart count after_ hour(s)**: If a service remains stopped after exhausting the maximum retry attempts,

Apex One waits a certain number of hours to reset the failure count. If a service remains stopped after the number of hours elapses, Apex One restarts the service.

Security Agent Self-protection

Security Agent self-protection provides ways for the Security Agent to protect the processes and other resources required to function properly. Security Agent self-protection helps thwart attempts by programs or actual users to disable anti-malware protection.

Security Agent self-protection provides the following options:

- *Protect Security Agent Services on page 15-15*
- *Protect Files in the Security Agent Installation Folder on page 15-16*
- *Protect Security Agent Registry Keys on page 15-17*
- *Protect Security Agent Processes on page 15-17*

Configuring Security Agent Self-protection Settings

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Security Agent Self-protection** section.
5. Enable the following options:
   - *Protect Security Agent Services on page 15-15*

- *Protect Files in the Security Agent Installation Folder on page 15-16*
- *Protect Security Agent Registry Keys on page 15-17*
- *Protect Security Agent Processes on page 15-17*

6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Protect Security Agent Services

Apex One blocks all attempts to terminate the following Security Agent services:

- Apex One NT Listener (`TmListen.exe`)
- Apex One NT RealTime Scan (`NTRtScan.exe`)
- Apex One NT Firewall (`TmPfw.exe`)
- Trend Micro Apex One Data Protection Service (`dsagent.exe`)
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

Note

If this option is enabled, the Security Agent may prevent third-party products from installing successfully on endpoints. If you encounter this issue, you can temporarily disable the option and then re-enable it after the installation of the third-party product.

- Apex One Common Client Solution Framework (`TmCCSF.exe`)

Protect Files in the Security Agent Installation Folder

To prevent other programs and even the user from modifying or deleting Security Agent files, Apex One provides several enhanced protection capabilities.

After enabling **Protect files in the Security Agent installation folder**, Apex One locks the following files in the root <*Agent installation folder*>:

- All digitally-signed files with `.exe`, `.dll`, and `.sys` extensions
- Some files without digital signatures, including:
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`
  - `msvcp80.dll`
  - `msvcr80.dll`
  - `OfceSCV.dll`
  - `OFCESCVPack.exe`
  - `patchbld.dll`
  - `patchw32.dll`
  - `patchw64.dll`
  - `PiReg.exe`
  - `ssleay32.dll`
  - `Tmeng.dll`
  - `TMNotify.dll`
  - `zlibwapi.dll`

After enabling **Protect files in the Security Agent installation folder** and Real-time Scan for virus/malware threats, Apex One performs the following actions:

- File integrity checking before launching `.exe` files in the installation folder

  During ActiveUpdate updates, Apex One verifies that the issuer of the file triggering the update is Trend Micro. If the issuer is not recognized as Trend Micro and ActiveUpdate cannot replace the incorrect file, Apex One logs the incident in the Windows event logs and blocks the update.

- Prevents DLL hijacking

  Some malware writers copy dynamic link library files to the Security Agent installation folder or the Behavior Monitoring folder with the purpose of loading these files before the agent loads. These files attempt to disrupt the protection offered by Apex One. To prevent the copying of hijacked files to the Security Agent folders, Apex One prevents the copying of files to the installation folder and Behavior Monitoring folder.

- Prevents the locking of files using the "SHARE:NONE" setting in Windows

Protect Security Agent Registry Keys

The Security Agent blocks all attempts to modify, delete, or add new entries under the following registry keys and subkeys:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP`

Protect Security Agent Processes

The Security Agent blocks all attempts to terminate the processes in the following table.

Process	Description
`TmListen.exe`	Receives commands and notifications from the Apex One server and facilitates communication from the Security Agent to the server
`NTRtScan.exe`	Performs Real-time, Scheduled, and Manual Scan on Security Agents
`TmProxy.exe`	Scans network traffic before passing it to the target application

Process	Description
TmPfw.exe	Provides packet level firewall, network virus scanning, and intrusion detection capabilities
TMBMSRV.exe	Regulates access to external storage devices and prevents unauthorized changes to registry keys and processes
DSAgent.exe	Monitors the transmission of sensitive data and controls access to devices
PccNTMon.exe	This process is responsible for starting the Security Agent console
TmCCSF.exe	Performs Browser Exploit Prevention and memory scanning

The Security Agent can also protect against the addition of processes in the Microsoft Software Restriction Policies (SRP). Software Restriction Policies prevent the listed applications from running on the endpoint. To prevent the addition of Security Agent processes in the Software Restriction Policies list:

1. Enable **Protect Security Agent processes**.
2. Enable the **Unauthorized Change Prevention Service**.

   For details, see *Configuring Additional Security Agent Services on page 15-9*.

Security Agent Console Access Restriction

This setting disables Security Agent console access from the system tray or Windows Start menu. The only way users can access the Security Agent console is by double-clicking PccNTMon.exe from the <*Agent installation folder*>. After configuring this setting, reload the Security Agent for the setting to take effect.

This setting does not disable the Security Agent. The Security Agent runs in the background and continues to provide protection from security risks.

Restricting Access to the Security Agent Console

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. Click the **Other Settings** tab and go to the **Security Agent Access Restriction** section.
5. Select **Do not allow users to access the Security Agent console from the system tray or Windows Start menu**.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Security Agent Unloading and Unlocking

The Security Agent unloading and unlocking privilege allows users to temporarily stop the Security Agent or gain access to advanced web console features with or without a password.

Granting the Agent Unloading and Unlocking Privilege

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Unload and Unlock** section.
5. To allow Security Agent unloading without a password, select **Does not require a password**.
   - If a password is required, select **Requires a password**, type the password, and then confirm it.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Security Agent Independent Mode Privilege

Grant certain users the Security Agent Independent mode privilege if agent-server events are interfering with the users' tasks. For example, a user who frequently gives presentations can enable Independent mode before starting a presentation to prevent the Apex One server from deploying Security Agent settings and initiating scans on the Security Agent.

When Security Agents are in Independent mode:

- Security Agents do not send logs to the Apex One server, even if there is a functional connection between the server and agents.
- The Apex One server does not initiate tasks and deploy Security Agent settings to the agents, even if there is functional connection between the server and agents.
- Security Agents update components if they can connect to any of their update sources. Sources include the Apex One server, Update Agents, or a custom update source.

  The following events trigger an update on Independent agents:

  - The user performs a manual update.
  - Automatic agent update runs. You can disable automatic agent update on Independent agents.

    For details, see *Disabling Automatic Agent Update on Independent Agents on page 15-22*.
  - Scheduled update runs. Only agents with the required privileges can run scheduled updates. You can revoke this privilege anytime.

    For details, see *Revoking the Scheduled Update Privilege on Independent Agents on page 15-22*.

Granting the Agent Independent Mode Privilege

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Independent Mode** section.
5. Select **Enable Independent mode**.

6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Disabling Automatic Agent Update on Independent Agents

Procedure

1. Go to **Updates** > **Agents** > **Automatic Update**.
2. Go to the **Event-triggered Update** section.
3. Disable **Include Independent and offline agent(s)**.

Note

This option is automatically disabled if you disable **Initiate component update on agents immediately after the Apex One server downloads a new component**.

Revoking the Scheduled Update Privilege on Independent Agents

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.

4. On the **Privileges** tab, go to the **Component Updates** section.
5. Clear the **Enable/Disable schedule-based updates** option.
6. Click **Save**.

Security Agent Language Configuration

You can configure all Security Agents to display using the Apex One server language settings or the locally logged on user language settings. After installing or upgrading the Security Agent program, the agent applies the language settings configured on the **Global Settings** screen.

By default, if the Security Agent does not support the logged on user's language settings, the language settings default to the Apex One server language, and then to English.

Configuring Security Agent Language Settings

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **Agent Control** tab.
3. Go to the **Agent Language Configuration** section.
4. Specify how the Security Agent applies the language settings:
   - **Local language settings on the endpoint**: The Security Agent displays using the language settings of the logged on user.

Note

If the Security Agent does not support the logged on user language settings, the agent applies the Apex One server language. If the endpoint does not support the Apex One server language, English displays.

- **Apex One server language**: The Security Agent displays using the Apex One server language.

Note

If the endpoint does not support the Apex One server language, English displays.

5. Click **Save**.

Agent Mover

If you have more than one Apex One server on the network, use the Agent Mover tool to transfer Security Agents from one Apex One server to another. This is especially useful after adding a new Apex One server to the network and you want to transfer existing Security Agents to the new server.

Note

The two servers must be of the same language version. If you use Agent Mover to move any Security Agent running an earlier version to a server of the current version, the Security Agent will be upgraded automatically.

Ensure that the account you use has administrator privileges before using this tool.

Running Agent Mover

Procedure

1. On the Apex One server, go to <*Server installation folder*>`\PCCSRV\Admin\Utility\IpXfer`.
2. Copy `IpXfer.exe` to the Security Agent endpoint. If the Security Agent endpoint runs an x64 type platform, copy `IpXfer_x64.exe` instead.
3. On the Security Agent endpoint, open a command prompt and then go to the folder where you copied the executable file.

4. Run Agent Mover using the following syntax:

```
<executable file name> -s <server name> -p <server
listening port> -c <agent listening port> -d <domain or
domain hierarchy> -e <Certificate location and file name> -
pwd <agent unload and unlock privilege password>
```

TABLE 15-2. Agent Mover Parameters

PARAMETER	EXPLANATION
`<executable file name>`	`IpXfer.exe` or `IpXfer_x64.exe`
`-s <server name>`	The name of the destination Apex One server (the server to which the Security Agent will transfer)
`-p <server listening port>`	The listening port (or trusted port) of the destination Apex One server (for local servers only) To view the listening port on the Apex One web console, click **Administration** > **Settings** > **Agent Connection** in the main menu.
`-sp <server HTTPS listening port>`	The listening port (or trusted port) of the destination Apex One server for HTTPS communication
`-c <agent listening port>`	The port number used by the Security Agent endpoint to communicate with the server
`-d <domain or domain hierarchy>`	The agent tree domain or subdomain to which the agent will be grouped The domain hierarchy should indicate the subdomain.

Parameter	Explanation
`-e <Certificate location and file name>`	Imports a new authentication certificate for the Security Agent during the move process If this parameter is not used, the Security Agent automatically retrieves the current authentication certificate from its new managing server. **Note** The default certificate location on the Apex One server is: <*Server installation folder*>`\PCCSRV\Pccnt\Common\OfcNTCer.dat`. When using a certificate from a source other than Apex One, ensure that the certificate is in Distinguished Encoding Rules (DER) format.
`-pwd <agent unload and unlock privilege password>`	The unload and unlock privilege password configured in Privileges and Other Settings **Note** If the unload and unlock password is required and you do not provide the password, Agent Mover prompts you before attempting to move agents.
`-dbg`	Enables connection debug logging

Examples:

- For Apex One servers using HTTP communication:

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup -pwd unlock

ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup\Group01 -pwd unlock
```

- For Apex One servers using HTTPS communication:

```
ipXfer.exe -s Server01 -sp 443 -p 8080 -c 21112 -d
Workgroup -pwd unlock -dbg 1
```

5. To confirm the Security Agent now reports to the other server, do the following:

   a. On the Security Agent endpoint, right-click the Security Agent program icon in the system tray.

   b. Select **Component Versions**.

   c. Check the Apex One server that the Security Agent reports to in the **Server name/port** field.

Note

If the Security Agent does not appear in the agent tree of the new Apex One server managing it, restart the new server's Master Service (`ofservice.exe`).

Inactive Security Agents

When you use the Security Agent uninstallation program to remove the Security Agent program from endpoints, the program automatically notifies the server. When the server receives this notification, it removes the Security Agent icon in the agent tree to show that the agent does not exist anymore.

However, if you use other methods to remove the Security Agent, such as reformatting the endpoint hard drive or deleting the Security Agent files manually, Apex One will not be aware of the removal and it will display the Security Agent as inactive. If a user unloads or disables the Security Agent for an extended period of time, the server also displays the Security Agent as inactive.

To have the agent tree display active agents only, configure Apex One to automatically remove inactive agents from the agent tree.

Automatically Removing Inactive Agents

Procedure

1. Go to **Administration** > **Settings** > **Inactive Agents**.
2. Select **Enable automatic removal of inactive agents**.
3. Select how many days should pass before Apex One considers the Security Agent inactive.
4. Click **Save**.

Agent-Server Connection

The Security Agent must maintain a continuous connection with its parent server so that it can update components, receive notifications, and apply configuration changes in a timely manner. The following topics discuss how to check the Security Agent's connection status and resolve connection issues:

- *Agent IP Addresses on page 5-8*
- *Security Agent Icons on page 15-28*
- *Agent-Server Connection Verification on page 15-44*
- *Connection Verification Logs on page 15-45*
- *Unreachable Agents on page 15-45*

Security Agent Icons

The Security Agent icon in the system tray provide visual hints that indicate the current status of the Security Agent and prompt users to perform certain actions. At any given time, the icon will show a combination of the following visual hints.

TABLE 15-3. Security Agent Status as Indicated in the Security Agent Icon

AGENT STATUS	DESCRIPTION	VISUAL HINT
Agent connection with the Apex One server	Online agents are connected to the Apex One server. The server can initiate tasks and deploy settings to these agents	The icon contains a symbol resembling a heartbeat.  The background color is a shade of blue or red, depending on the status of the Real-time Scan Service.
	Offline agents are disconnected from the Apex One server. The server cannot manage these agents.	The icon contains a symbol resembling the loss of a heartbeat.  The background color is a shade of blue or red, depending on the status of the Real-time Scan Service. It is possible for the agent to become offline even if it is connected to the network. For details about this issue, see *Solutions to Issues Indicated in Security Agent Icons on page 15-41*.
	Independent agents may or may not be able to communicate with the Apex One server.	The icon contains the desktop and signal symbols.  The background color is a shade of blue or red, depending on the status of the Real-time Scan Service. For details about Independent mode agents, see *Security Agent Independent Mode Privilege on page 15-20*.

Agent Status	Description	Visual Hint
Availability of smart protection sources	Smart protection sources include Smart Protection Servers and Trend Micro Smart Protection Network. Conventional scan agents connect to smart protection sources for web reputation queries. Smart scan agents connect to smart protection sources for scan and web reputation queries.	The icon includes a check mark if a smart protection source is available. 
		The icon includes a progress bar if no smart protection source is available and the agent is attempting to establish connection with the sources.  For details about this issue, see *Solutions to Issues Indicated in Security Agent Icons on page 15-41*.
		For conventional scan agents, no check mark or progress bar appears if web reputation has been disabled on the agent.

Agent Status	Description	Visual Hint
Real-time Scan Service status	Apex One uses the Real-time Scan Service not only for Real-time Scan, but also for Manual Scan and Scheduled Scan. The service must be functional or the agent becomes vulnerable to security risks.	The entire icon is shaded blue if the Real-time Scan Service is functional. Two shades of blue are used to indicate the of the agent. • For conventional scan:  • For smart scan: 
		The entire icon is shaded red if the Real-time Scan Service has been disabled or is not functional. Two shades of red are used to indicate the scan method of the agent. • For conventional scan:  • For smart scan:  For details about this issue, see *Solutions to Issues Indicated in Security Agent Icons on page 15-41*.

Agent Status	Description	Visual Hint
Real-time Scan status	Real-time Scan provides proactive protection by scanning files for security risks as they are created, modified, or retrieved.	There are no visual hints if Real-time Scan is enabled.
		The entire icon is surrounded by a red circle and contains a red diagonal line if Real-time Scan is disabled.  For details about this issue, see *Solutions to Issues Indicated in Security Agent Icons on page 15-41*.
Pattern update status	Agents must update the pattern regularly to protect the agent from the latest threats.	There are no visual hints if the pattern is up-to-date or is slightly out-of-date.
		The icon includes an exclamation mark if the pattern is severely outdated. This means that the pattern been not been updated for a while.  For details on how to update agents, see *Security Agent Updates on page 6-27*.
Apex One server trial license status	Online agents are connected to an Apex One server that is using an expired trial license.	This icon indicates that the trial license on the Apex One server has expired. 

Smart Scan Icons

Any of the following icons displays when Security Agents use smart scan.

TABLE 15-4. Smart Scan Icons

ICON	CONNECTION WITH APEX ONE SERVER	AVAILABILITY OF SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN
	Online	Available	Functional	Enabled
	Online	Available	Functional	Disabled
	Online	Available	Disabled or not functional	Disabled or not functional
	Online	Unavailable, reconnecting to sources	Functional	Enabled
	Online	Unavailable, reconnecting to sources	Functional	Disabled
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional
	Offline	Available	Functional	Enabled
	Offline	Available	Functional	Disabled
	Offline	Available	Disabled or not functional	Disabled or not functional
	Offline	Unavailable, reconnecting to sources	Functional	Enabled
	Offline	Unavailable, reconnecting to sources	Functional	Disabled

Icon	Connection with Apex One Server	Availability of Smart Protection Sources	Real-time Scan Service	Real-time Scan
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional
	Independent	Available	Functional	Enabled
	Independent	Available	Functional	Disabled
	Independent	Available	Disabled or not functional	Disabled or not functional
	Independent	Unavailable, reconnecting to sources	Functional	Enabled
	Independent	Unavailable, reconnecting to sources	Functional	Disabled
	Independent	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional

Conventional Scan Icons

Any of the following icons displays when Security Agents use conventional scan.

TABLE 15-5. Conventional Scan Icons

ICON	CONNECTION WITH APEX ONE SERVER	WEB REPUTATION SERVICES PROVIDED BY SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN	VIRUS PATTERN
	Online	Available	Functional	Enabled	Up-to-date or slightly outdated
	Online	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated
	Online	Available	Functional	Enabled	Severely outdated
	Online	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated
	Online	Available	Functional	Disabled	Up-to-date or slightly outdated
	Online	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Online	Available	Functional	Disabled	Severely outdated
	Online	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated
	Online	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated

Icon	Connection with Apex One Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Online	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated
	Offline	Available	Functional	Enabled	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated
	Offline	Available	Functional	Enabled	Severely outdated
	Offline	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated
	Offline	Available	Functional	Disabled	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Offline	Available	Functional	Disabled	Severely outdated

Icon	Connection with Apex One Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Offline	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated
	Offline	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Offline	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated
	Independent	Available	Functional	Enabled	Up-to-date or slightly outdated
	Independent	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated
	Independent	Available	Functional	Enabled	Severely outdated
	Independent	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated
	Independent	Available	Functional	Disabled	Up-to-date or slightly outdated

Icon	Connection with Apex One Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Independent	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Independent	Available	Functional	Disabled	Severely outdated
	Independent	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated
	Independent	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Independent	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Independent	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Independent	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Severely outdated

Icon	Connection with Apex One Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Online	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Severely outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Severely outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Up-to-date or slightly outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Severely outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Up-to-date or slightly outdated

Icon	Connection with Apex One Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Offline	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Severely outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Severely outdated
	Independent	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Up-to-date or slightly outdated
	Independent	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Severely outdated
	Independent	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Up-to-date or slightly outdated
	Independent	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Severely outdated

Icon	Connection with Apex One Server	Web Reputation Services Provided by Smart Protection Sources	Real-time Scan Service	Real-time Scan	Virus Pattern
	Independent	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Independent	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Severely outdated

Solutions to Issues Indicated in Security Agent Icons

Perform the necessary actions if the Security Agent icon indicates any of the following conditions:

Condition	Description
Pattern file has not been updated for a while	Security Agent users need to update components. From the web console, configure component update settings in **Updates** > **Agents** > **Automatic Update**, or grant users the privilege to update in **Agents** > **Agent Management > Settings** > **Privileges and Other Settings** > **Privileges (tab)** > **Component Updates**.
Real-time Scan Service has been disabled or is not functional	If the Real-time Scan Service (Apex One NT RealTime Scan) has been disabled or becomes non-functional, users must start the service manually from Microsoft Management Console.
Real-time Scan was disabled	Enable Real-time Scan from the web console (**Agents** > **Agent Management > Settings** > **Scan Settings** > **Real-time Scan Settings**).
Real-time Scan was disabled and the	Users need to disable Independent mode first. After disabling Independent mode, enable Real-time Scan from the web console.

Condition	Description
Security Agent is in Independent mode	
The Security Agent is connected to the network but appears offline	Verify the connection from the web console (**Agents** > **Connection Verification**) and then check connection verification logs (**Logs** > **Agents** > **Connection Verification Logs**). If the Security Agent is still offline after verification: 1. If the connection status on both the server and Security Agent is offline, check the network connection. 2. If the connection status on the Security Agent is offline but online on the server, the server's domain name may have been changed and the Security Agent connects to the server using the domain name (if you select domain name during server installation). Register the Apex One server's domain name to the DNS or WINS server or add the domain name and IP information into the "hosts" file in the following folder on the agent endpoint: `<Windows folder>\system32\drivers\etc` 3. If the connection status on the Security Agent is online but offline on the server, check the Apex One firewall settings. The firewall may block server-to-agent communication, but allow agent-to-server communication. 4. If the connection status on the Security Agent is online but offline on the server, the Security Agent's IP address may have been changed but its status does not reflect on the server (for example, when the agent is reloaded). Try to redeploy the Security Agent.
Smart protection sources are unavailable	Perform these tasks if the agent loses connection with smart protection sources: 1. On the web console, go to the **Endpoint Location** screen (**Agents** > **Endpoint Location**) and check if the following endpoint location settings have been configured properly: • Reference servers and port numbers • Gateway IP addresses 2. On the web console, go to the Smart Protection Source screen (**Administration** > **Smart Protection** > **Smart Protection Sources**) and then perform the following tasks:

Condition	Description
	a. Check if the Smart Protection Server settings on the standard or custom list of sources are correct. b. Test if connection to the servers can be established. c. Click **Notify All Agents** after configuring the list of sources. 3. Check if the following configuration files on the Smart Protection Server and Security Agent are synchronized: • `sscfg.ini` • `ssnotify.ini` 4. Open Registry Editor and check if the agent is connected to the corporate network. Key: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server` • If `LocationProfile=1`, the Security Agent is connected to the network and should be able to connect to a Smart Protection Server. • If `LocationProfile=2`, the Security Agent is not connected to the network and should connect to the Smart Protection Network. From Internet Explorer, check if the Security Agent endpoint can browse Internet web pages. 5. Check internal and external proxy settings used to connect to Smart Protection Network and Smart Protection Servers. For more information, see *Configuring Internal Agent Proxy Settings on page 15-52* and *Configuring External Agent Proxy Settings on page 15-53*. 6. For conventional scan agents running Windows 7, Server 2012, and later versions, verify that the tmusa driver is running. If this driver stops, agents cannot connect to smart protection sources for web reputation.

Agent-Server Connection Verification

The Security Agent connection status with the Apex One server displays on the Apex One agent tree.

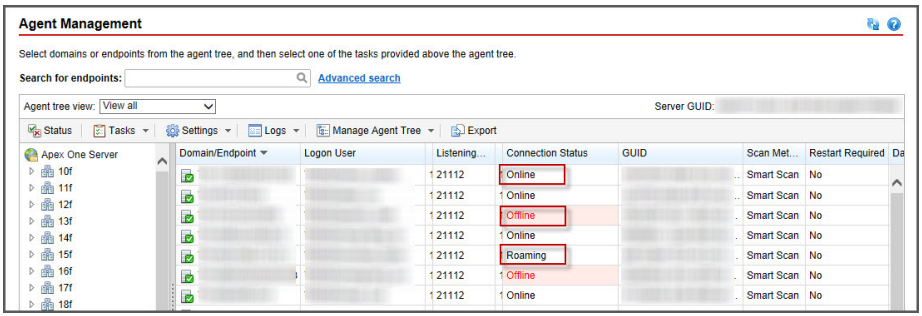


FIGURE 15-2. Agent tree displaying Security Agent connection status with the Apex One server

Certain conditions may prevent the agent tree from displaying the correct Security Agent connection status. For example, if you accidentally unplug the network cable of the Security Agent endpoint, the Security Agent will not be able to notify the server that it is now offline. This Security Agent will still appear as online in the agent tree.

Verify Security Agent-server connection manually or let Apex One perform scheduled verification. You cannot select specific domains or Security Agents and then verify their connection status. Apex One verifies the connection status of all its registered Security Agents.

Verifying Agent-Server Connections

Procedure

1. Go to **Agents** > **Connection Verification**.
2. To verify agent-server connection manually, go to the **Manual Verification** tab and click **Verify Now**.

3. To verify agent-server connection automatically, go to the **Scheduled Verification** tab.
   a. Select **Enable scheduled verification**.
   b. Select the verification frequency and start time.
   c. Click **Save** to save the verification schedule.
4. Check the agent tree to verify the status or view the connection verification logs.

Connection Verification Logs

Apex One keeps connection verification logs to allow you to determine whether or not the Apex One server can communicate with all of its registered agents. Apex One creates a log entry each time you verify agent-server connection from the web console.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Log Management on page 14-42*.

Viewing Connection Verification Logs

Procedure

1. Go to **Logs** > **Agents** > **Connection Verification Logs**.
2. View connection verification results by checking the **Status** column.
3. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Unreachable Agents

Security Agents on unreachable networks, such as those on network segments behind a NAT gateway, are almost always offline because the server

cannot establish direct connection with the agents. As a result, the server cannot notify the agents to:

- Download the latest components.
- Apply agent settings configured from the web console. For example, when you change the Scheduled Scan frequency from the web console, the server will immediately notify agents to apply the new setting.

Unreachable agents therefore cannot perform these tasks in a timely manner. They only perform the tasks when they initiate connection with the server, which happens when:

- They register to the server after installation.
- They restart or reload. This event does not occur frequently and usually requires user intervention.
- Manual or scheduled update is triggered on the agent. This event also does not occur frequently.

It is only during registration, restart, or reload that the server becomes "aware" of the agents' connectivity and treats them as online. However, because the server is still unable to establish connection with the agents, the server immediately changes the status to offline.

Apex One provides the "heartbeat" and server polling features to resolve issues regarding unreachable agents. With these features, the server stops notifying agents of component updates and setting changes. Instead, the server takes a passive role, always waiting for agents to send heartbeat or initiate polling. When the server detects any of these events, it treats the agents as online.

Note

Agent-initiated events not related to heartbeat and server polling, such as manual agent update and log sending, do not trigger the server to update the unreachable agents' status.

Heartbeat

Security Agents send heartbeat messages to notify the server that connection from the agent remains functional. Upon receiving a heartbeat message, the server treats the agent as online. In the agent tree, the agent's status can either be:

- **Online**: For regular online agents
- **Unreachable/Online**: For online agents in the unreachable network

Note

Security Agents do not update components or apply new settings when sending heartbeat messages. Regular agents perform these tasks during routine updates (see *Security Agent Updates on page 6-27*). Agents in the unreachable network perform these tasks during server polling.

The heartbeat feature addresses the issue of Security Agents in unreachable networks always appearing as offline even when they can connect to the server.

A setting in the web console controls how often agents send heartbeat messages. If the server did not receive a heartbeat, it does not immediately treat the agent as offline. Another setting controls how much time without a heartbeat must elapse before changing the agent's status to:

- **Offline**: For regular offline Security Agents
- **Unreachable/Offline**: For offline Security Agents in the unreachable network

When choosing a heartbeat setting, balance between the need to display the latest agent status information and the need to manage system resources. The default setting is satisfactory for most situations. However, consider the following points when you customize the heartbeat setting:

TABLE 15-6. Heartbeat Recommendations

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before the server reflects the agent's status on the web console.
Short-interval Heartbeats (below 60 minutes)	Short intervals present a more up-to-date agent status but may be bandwidth-intensive.

Server Polling

The server polling feature addresses the issue of unreachable Security Agents not receiving timely notifications about component updates and changes to agent settings. This feature is independent of the heartbeat feature.

With the server polling feature:

- Security Agents automatically initiate connection with the Apex One server at regular intervals. When the server detects that polling took place, it treats the agent as "Unreachable/Online".
- Security Agents connect to one or several of their update sources to download any updated components and apply new agent settings. If the Apex One server or an Update Agent is the primary update source, agents obtain both components and new settings. If the source is not the Apex One server or Update Agent, agents only obtain the updated components and then connect to the Apex One server or Update Agent to obtain the new settings.

Configuring the Heartbeat and Server Polling Features

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **Network** tab.

3. Go to the **Unreachable Network** section.

4. Configure server polling settings.

   For details about server polling, see *Server Polling on page 15-48*.

   a. If the Apex One server has both an IPv4 and IPv6 address, you can type an IPv4 address range and IPv6 prefix and length.

      Type an IPv4 address range if the server is pure IPv4, or an IPv6 prefix and length if the server is pure IPv6.

      When any agent's IP address matches an IP address in the range, the agent applies the heartbeat and server polling settings and the server treats the agent as part of the unreachable network.

      Note

      Agents with an IPv4 address can connect to a pure IPv4 or dual-stack Apex One server.

      Agents with an IPv6 address can connect to a pure IPv6 or dual-stack Apex One server.

      Dual-stack agents can connect to dual-stack, pure IPv4, or pure IPv6 Apex One server.

   b. In **Agents poll the server for updated components and settings every __ minute(s)**, specify the server polling frequency. Type a value between 1 and 129600 minutes.

      Tip

      Trend Micro recommends that the server polling frequency be at least three times the heartbeat sending frequency.

5. Configure heartbeat settings.

   For details about the heartbeat feature, see *Heartbeat on page 15-47*.

   a. Select **Allow agents to send heartbeat to the server**.

   b. Select **All agents** or **Only agents in the unreachable network**.

c. In **Agents send heartbeat every __ minute(s)**, specify how often agents send heartbeat. Type a value between 1 and 129600 minutes.

d. In **An agent is offline if there is no heartbeat after __ minute(s)**, specify how much time without a heartbeat must elapse before the Apex One server treats the agent as offline. Type a value between 1 and 129600 minutes.

6. Click **Save**.

Security Agent Proxy Settings

The following table outlines the Security Agent proxy settings available for connecting to internal and external servers.

Proxy Configuration	Description
Internal agents	Configure internal agent proxy settings for connections to the following servers: • Apex One server: The server computer hosts the Apex One server and the integrated Smart Protection Server. Security Agents connect to the Apex One server to update components, obtain configuration settings, and send logs. Security Agents connect to the integrated Smart Protection Server to send scan queries. • Smart Protection Servers: Smart Protection Servers include all standalone Smart Protection Servers and the integrated Smart Protection Server of other Apex One servers. Security Agents connect to the servers to send scan and web reputation queries. For more information, see *Configuring Internal Agent Proxy Settings on page 15-52*.
External agents	External Security Agents use the proxy settings configured in Internet Explorer to connect to the Trend Micro Smart Protection Network. For more information, see *Configuring External Agent Proxy Settings on page 15-53*.

Proxy Configuration	Description
Global Smart Protection Service	Security Agents use the configured Smart Protection Service Proxy settings when querying Smart Protection sources for the following features: • Predictive Machine Learning • Behavior Monitoring **Note** If the integrated Smart Protection Server is unavailable, Security Agents connect to the Trend Micro Smart Protection Network when performing queries. For more information, see *Configuring Global Smart Protection Service Proxy Settings on page 15-54*.
Agent user proxy privilege	You can grant agent users the privilege to configure proxy settings. Security Agents use user-configured proxy settings only on the following instances: • When Security Agents perform "Update Now". • When users disable, or the Security Agent cannot detect, automatic proxy settings. **WARNING!** Incorrect user-configured proxy settings can cause update problems. Exercise caution when allowing users to configure their own proxy settings. For more information, see *Granting Proxy Configuration Privileges on page 15-55*.

Configuring Internal Agent Proxy Settings

Procedure

1. Go to **Administration** > **Settings** > **Proxy**.
2. Click the **Agent** tab.
3. Go to the **Internal Proxy** section.
4. Select the type of proxy settings that internal Security Agents use when connecting to the Apex One server or Smart Protection Servers.
   - **No proxy**: Internal Security Agents do not require a proxy server to connect to the Apex One server or Smart Protection Servers
   - **Use Windows proxy settings**: Internal agents use the proxy server settings configured in Windows Internet Options when connecting to the Apex One server or Smart Protection Servers

     Note

     Specify proxy authentication credentials, if required.

   - **Use multiple proxy servers**: Internal agents use different proxy servers when connecting to the Apex One server or Smart Protection Servers

     For Apex One server connections:

     a. Select **Security Agent proxy for connection to the internal Apex One server**.

     b. Specify the proxy server name or IPv4/IPv6 address, and port number.

     c. Specify proxy authentication credentials, if required.

     For standalone Smart Protection Server connections:

     a. Select **Security Agent proxy for connection to standalone Smart Protection Servers**.

b. Specify the proxy server name or IPv4/IPv6 address, and port number.

c. Specify proxy authentication credentials, if required.

- **Use automatic proxy configuration (including PAC)**: Select to use administrator-configured proxy settings using DHCP, DNS, or an automatic configuration script
  - **Automatically detect network proxy settings**: Internal agents detect the administrator-configured proxy settings by DHCP or DNS
  - **Use specified proxy auto-configuration (PAC) script file**: Internal agents use the proxy auto-configuration (PAC) script set by the network administrator to detect the appropriate proxy server

Note

Type the URL address for the PAC script.

5. Click **Save**.

Configuring External Agent Proxy Settings

External agents can only use the proxy server settings configured in Windows Internet Options when connecting to the Apex One server or Smart Protection Servers.

Procedure

1. Go to **Administration** > **Settings** > **Proxy**.
2. Click the **Agent** tab.
3. Go to the **External Proxy** section.
4. Specify proxy authentication credentials, if required.

5. Click **Save**.

Configuring Global Smart Protection Service Proxy Settings

Security Agents use the configured Smart Protection Service Proxy settings when querying Smart Protection sources for the following features:

- Predictive Machine Learning
- Behavior Monitoring

Note

If the integrated Smart Protection Server is unavailable, Security Agents connect to the Trend Micro Smart Protection Network when performing queries.

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Click the **System** tab.
3. Go to the **Smart Protection Service Proxy** section.
4. Enable **Use configured Smart Protection Sources for service queries**.

Important

The Smart Protection Service Proxy only supports HTTPS protocol for File Reputation queries. You must ensure that all configured Smart Protection Servers that provide File Reputation Services use HTTPS protocol.

By default, the integrated Smart Protection Server does not use HTTPS communication. To change the communication method, see *Configuring Integrated Smart Protection Server Settings on page 4-22*.

To verify the communication method used by standalone Smart Protection Servers, see *Configuring Custom Lists of Smart Protection Sources on page 4-27*.

5. Click **Save**.

Granting Proxy Configuration Privileges

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, go to the **Proxy Settings** section.
5. Select **Allow users to configure proxy settings**.
6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Viewing Security Agent Information

The **View Status** screen displays important information about Security Agents, including privileges, endpoint software details and system events.

Procedure

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

2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Status**.
4. View status information by expanding the agent endpoint's name. If you selected multiple agents, click **Expand All** to view status information for all the selected agents.
5. (Optional) Use the **Reset** buttons to set the security risk count back to zero.

Importing and Exporting Agent Settings

Apex One allows you to export agent tree settings applied by a particular Security Agent or domain to a file. You can then import the file to apply the settings to other agents and domains or to another Apex One server of the same version.

All agent tree settings, except Update Agent settings, will be exported.

Exporting Agent Settings

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Export Settings**.
4. Click any of the links to view the settings for the Security Agent or domain you selected.
5. Click **Export** to save the settings.

   The settings are saved in a `.dat` file.

6. Click **Save** and then specify the location to which you want to save the `.dat` file.
7. Click **Save**.

Importing Agent Settings

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Settings** > **Import Settings**.
4. Click **Browse** to locate the `.dat` file on the endpoint and click **Import**.

   The **Import Settings** screen appears, showing a summary of the settings.
5. Click any of the links to view details about the scan settings or privileges to import.
6. Import the settings.
   - If you clicked the root domain icon, select **Apply to all domains** and then click **Apply to Target**.
   - If you selected domains, select **Apply to all computers belonging to the selected domain(s)**, and then click **Apply to Target**.
   - If you selected several agents, click **Apply to Target**.

Security Compliance

Use Security Compliance to determine flaws, deploy solutions, and maintain the security infrastructure. This feature helps reduce the time required to

secure the network environment and balance an organization's needs for security and functionality.

Enforce security compliance for two types of endpoints:

- **Managed**: Endpoints with Security Agents managed by the Apex One server. For details, see *Security Compliance for Managed Agents on page 15-58*.
- **Unmanaged**: Includes the following:
  - Security Agents not managed by the Apex One server
  - Endpoints without Security Agents installed
  - Endpoints that the Apex One server cannot reach
  - Endpoints whose security status cannot be verified

    For details, see *Security Compliance for Unmanaged Endpoints on page 15-71*.

Security Compliance for Managed Agents

Security Compliance generates a Compliance Report to help you assess the security status of Security Agents managed by the Apex One server. Security Compliance generates the report on demand or according to a schedule.

Note

Apex One only displays compliance reports for Security Agents operating with a full feature set. Coexist agents do not appear in the reports.

The **Manual Assessment** screen displays the following tabs:

- **Services**: Use this tab to check if agent services are functional.

  For details, see *Services on page 15-60*.
- **Components**: Use this tab to check if Security Agents have up-to-date components.

For details, see *Components on page 15-61*.

- **Scan Compliance**: Use this tab to check if Security Agents are running scans regularly.

  For details, see *Scan Compliance on page 15-63*.

- **Settings**: Use this tab to check if agent settings are consistent with the settings on the server.

  For details, see *Settings on page 15-65*.

Note

The **Components** tab can display Security Agents running the current and earlier versions of the product. The other tabs only display data for Security Agents running the latest version.

Important

- Security Compliance queries the connection status of Security Agents before generating a Compliance Report. It includes online and offline agents in the report, but not agents in Independent mode.
- For role-based user accounts:
  - Each web console user account has a completely independent set of Compliance Report settings. Any changes to a user account's Compliance Report settings will not affect the settings of the other user accounts.
  - The scope of the report depends on the agent domain permissions for the user account. For example, if you grant a user account permissions to manage domains A and B, the user account's reports will only show data from agents belonging to domains A and B.

    For details about user accounts, see *Role-based Administration on page 14-3*.

Services

Security Compliance checks whether the following Security Agent services are functional:

- Antivirus
- Anti-spyware
- Firewall
- Web Reputation
- Behavior Monitoring/Device Control (also referred to as Trend Micro Unauthorized Change Prevention Service)
- Data Protection
- Suspicious Connection

A non-compliant agent is counted at least twice in the Compliance Report.

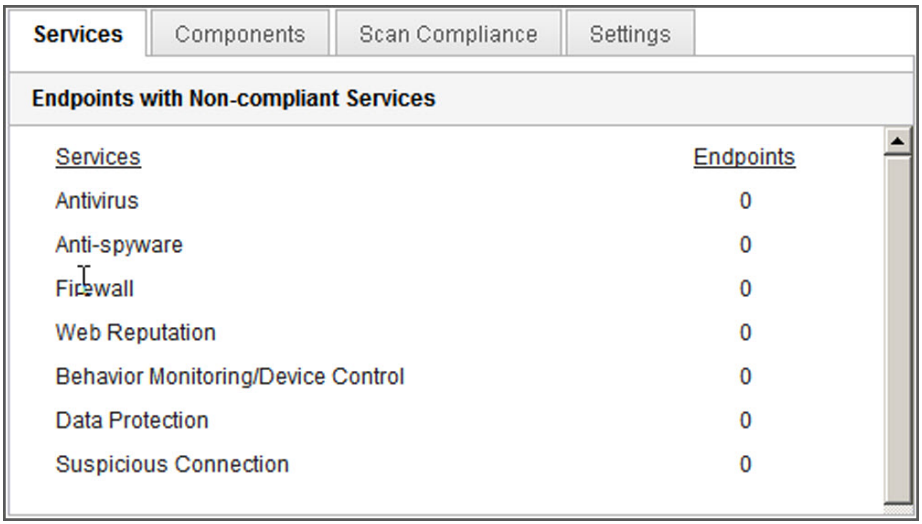


FIGURE 15-3. Compliance Report - Services tab

- In the **Endpoints with Non-compliant Services** category
- In the category for which the Security Agent is non-compliant. For example, if the Security Agent's Antivirus service is not functional, the agent is counted in the **Antivirus** category. If more than one service is not functional, the agent is counted in each category for which it is non-compliant.

Restart non-functional services from the web console or from the Security Agent. If the services are functional after the restart, the agent will no longer appear as non-compliant during the next assessment.

Components

Security Compliance determines component version inconsistencies between the Apex One server and Security Agents. Inconsistencies typically occur when agents cannot connect to the server to update components. If the agent obtains updates from another source (such as the Trend Micro ActiveUpdate server), it is possible for the agent component version to be newer than the version on the server.

Security Compliance checks the following components:

- Smart Scan Agent Pattern
- Virus Pattern
- IntelliTrap Pattern
- IntelliTrap Exception Pattern
- Virus Scan Engine 32/64-bit
- Spyware/Grayware Pattern
- Spyware Active-monitoring Pattern
- Spyware/Grayware Scan Engine 32/64-bit
- Damage Cleanup Template
- Damage Cleanup Engine 32/64-bit
- Common Firewall Pattern
- Common Firewall Driver 32/64-bit
- Behavior Monitoring Core Driver 32/64-bit
- Behavior Monitoring Core Service 32/64-bit
- Behavior Monitoring Configuration Pattern
- Digital Signature Pattern
- Policy Enforcement Pattern
- Behavior Monitoring Detection Pattern 32/64-bit
- Global C&C IP List
- Relevance Rule Pattern
- Early Boot Cleanup Driver 32/64-bit
- Memory Scan Trigger Pattern (32/64-bit)
- Memory Inspection Pattern
- Browser Exploit Prevention Pattern
- Script Analyzer Unified Pattern
- Program Inspection Monitoring Pattern
- Damage Recovery Pattern
- Early Launch Anti-Malware Pattern 32/64-bit
- Contextual Intelligence Engine 32/64-bit
- Contextual Intelligence Pattern
- Contextual Intelligence Query Handler 32/64-bit
- Advanced Threat Scan Engine 32/64-bit
- Advanced Threat Correlation Pattern
- Program Version

A non-compliant agent is counted at least twice in the Compliance Report.

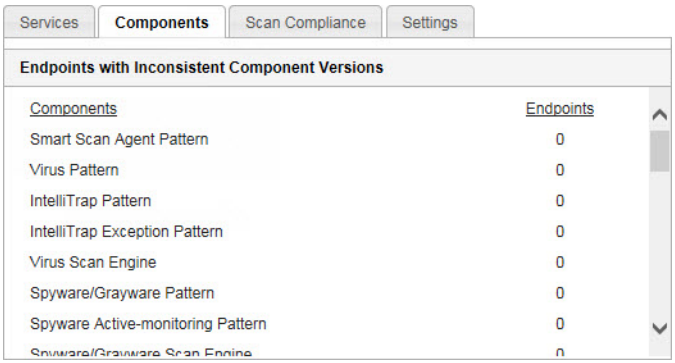


FIGURE 15-4. Compliance Report - Components tab

- In the **Endpoints with Inconsistent Component Versions** category
- In the category for which the agent is non-compliant. For example, if the agent Smart Scan Agent Pattern version is not consistent with the version on the server, the agent is counted in the **Smart Scan Agent Pattern** category. If more than one component version is inconsistent, the agent is counted in each category for which it is non-compliant.

To resolve component version inconsistencies, update outdated components on the agents or server.

Scan Compliance

Security Compliance checks if Scan Now or Scheduled Scan are run regularly and if these scans are completed within a reasonable amount of time.

Note

Security Compliance can only report the Scheduled Scan status if Scheduled Scan is enabled on agents.

Security Compliance uses the following scan compliance criteria:

- **No Scan Now or Scheduled Scan performed for the last (x) days**: The Security Agent is non-compliant if it did not run Scan Now or Scheduled Scan within the specified number of days.
- **Scan Now or Scheduled Scan exceeded (x) hours**: The Security Agent is non-compliant if the last Scan Now or Scheduled Scan lasted more than the specified number of hours.

A non-compliant agent is counted at least twice in the Compliance Report.

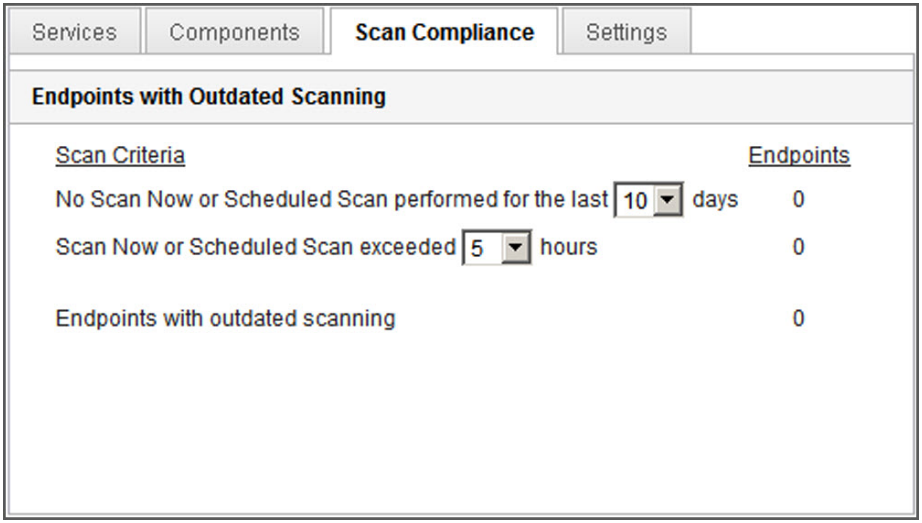


FIGURE 15-5. Compliance Report - Scan Compliance tab

- In the **Endpoints with Outdated Scanning** category
- In the category for which the agent is non-compliant. For example, if the last Scheduled Scan lasted more than the specified number of hours, the agent is counted in the **Scan Now or Scheduled Scan exceeded <x> hours** category. If the agent satisfies more than one scan compliance criteria, it is counted in each category for which it is non-compliant.

Run Scan Now or Scheduled Scan on agents that have not performed scan tasks or were unable to complete scanning.

Settings

Security Compliance determines whether agents and their parent domains in the agent tree have the same settings. The settings may not be consistent if you move any agents to another domain that is applying a different set of settings, or if any agent user with certain privileges manually configured settings on the Security Agent console.

Apex One verifies the following settings:

- Scan Method
- Manual Scan Settings
- Real-time Scan Settings
- Scheduled Scan Settings
- Scan Now Settings
- Privileges and Other Settings
- Additional Service Settings
- Web Reputation
- Behavior Monitoring
- Device Control
- Spyware/Grayware Approved List
- Data Loss Prevention Settings
- Suspicious Connection
- Trusted Program List
- Sample Submission
- Predictive Machine Learning

A non-compliant agent is counted at least twice in the Compliance Report.

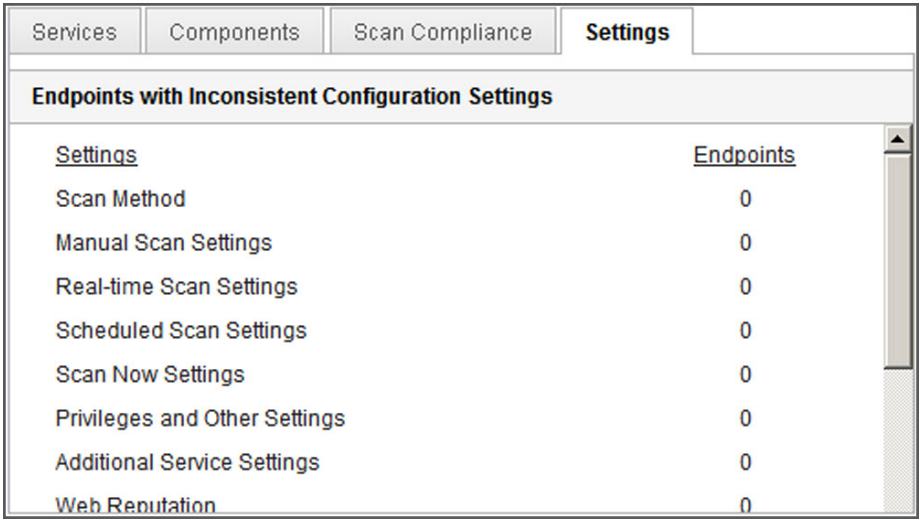


FIGURE 15-6. Compliance Report - Settings tab

- In the **Endpoints with Inconsistent Configuration Settings** category
- In the category for which the agent is non-compliant. For example, if the scan method settings in the agent and its parent domain are not consistent, the agent is counted in the **Scan Method** category. If more than one set of settings is inconsistent, the agent is counted in each category for which it is non-compliant.

To resolve the setting inconsistencies, apply domain settings to the agent.

On-demand Compliance Reports

Security Compliance can generate Compliance Reports on demand. Reports help you assess the security status of Security Agents managed by the Apex One server.

For more information on Compliance Reports, see *Security Compliance for Managed Agents on page 15-58*.

Generating an On-demand Compliance Report

Procedure

1. Go to **Assessment** > **Security Compliance** > **Manual Report**.
2. Go to the **Agent Tree Scope** section.
3. Select the root domain or a domain and click **Assess**.
4. View Compliance Report for agent services.

   For details about agent services, see *Services on page 15-60*.

   a. Click the **Services** tab.

   b. Under **Endpoints with Non-compliant Services**, check the number of agents with non-compliant services.

   c. Click a number link to display all affected agents in the agent tree.

   d. Select agents from the query result.

   e. Click **Restart Security Agent** to restart the service.

   Note

   After performing another assessment and the agent still appears as non-compliant, manually restart the service on the agent endpoint.

   f. To save the list of agents to a file, click **Export**.

5. View Compliance Report for agent components.

   For details about agent components, see *Components on page 15-61*.

   a. Click the **Components** tab.

b. Under **Endpoints with Inconsistent Component Versions**, check the number of agents with component versions that are inconsistent with the versions on the server.

c. Click a number link to display all affected agents in the agent tree.

Note

If at least one agent has a more up-to-date component than the Apex One server, manually update the Apex One server.

d. Select agents from the query result.

e. Click **Update Now** to force agents to download components.

Note

- To ensure that agents can upgrade the agent program:
  i. Go to **Agents** > **Agent Management**.
  ii. Click the **Settings** > **Privileges and Other Settings** > **Other Settings** tab.
  iii. Go to the **Update Settings** section.
  iv. In the **Security Agents only update the following components** drop-down, select **All components (including hotfixes and the agent program)**.
  v. Click **Apply to All Agents**.
- Restart the endpoint instead of clicking **Update Now** to update the Common Firewall Driver.

f. To save the list of agents to a file, click **Export**.

6. View Compliance Report for scans.

For details about scans, see *Scan Compliance on page 15-63*.

a. Click the **Scan Compliance** tab.

b. Under **Endpoints with Outdated Scanning**, configure the following:

- Number of days the agent has not performed Scan Now or Scheduled Scan
- Number of hours Scan Now or Scheduled Scan is running

Note

If the number of days or hours is exceeded, the agent is treated as non-compliant.

c. Click **Assess** next to the **Agent Tree Scope**.

d. Under **Endpoints with Outdated Scanning**, check the number of agents that satisfy the scan criteria.

e. Click a number link to display all affected agents in the agent tree.

f. Select agents from the query result.

g. Click **Scan Now** to initiate Scan Now on agents.

Note

To avoid repeating the scan, the **Scan Now** option will be disabled if Scan Now lasted more than the specified number of hours.

h. To save the list of agents to a file, click **Export**.

7. View Compliance Report for settings.

For details about settings, see *Settings on page 15-65*.

a. Click the **Settings** tab.

b. Under **Computers with Inconsistent Configuration Settings**, check the number of agents with settings inconsistent with the agent tree domain settings.

c. Click a number link to display all affected agents in the agent tree.

d. Select agents from the query result.

e. Click **Apply Domain Settings**.

f. To save the list of agents to a file, click **Export**.

Scheduled Compliance Reports

Security Compliance can generate Compliance Reports according to a schedule. Reports help you assess the security status of Security Agents managed by the Apex One server.

For more information on Compliance Reports, see *Security Compliance for Managed Agents on page 15-58*.

Configuring Settings for Scheduled Compliance Reports

Procedure

1. Go to **Assessment** > **Security Compliance** > **Scheduled Report**.
2. Select **Enable scheduled reporting**.
3. Specify a title for the report.
4. Select one or all of the following:
   - *Services on page 15-60*
   - *Components on page 15-61*
   - *Scan Compliance on page 15-63*
   - *Settings on page 15-65*
5. Specify the email address(es) that will receive notifications about scheduled Compliance Reports.

Note

Configure email notification settings to ensure that email notifications can be sent successfully. For details, see *Administrator Notification Settings on page 14-38*.

6. Specify the schedule.
7. Click **Save**.

Security Compliance for Unmanaged Endpoints

Security Compliance can query unmanaged endpoints in the network to which the Apex One server belongs. Use Active Directory and IP addresses to query endpoints.

The security status of unmanaged endpoints can be any of the following:

TABLE 15-7. Security Status of Unmanaged Endpoints

STATUS	DESCRIPTION
Managed by another Apex One server	The Security Agents installed on the computers are managed by another Apex One server. Security Agents are online and run either this Apex One version or an earlier version.
No Security Agent installed	The Security Agent is not installed on the endpoint.
Unreachable	The Apex One server cannot connect to the endpoint and determine its security status.
Unresolved Active Directory assessment	The endpoint belongs to an Active Directory domain but the Apex One server is unable to determine its security status. **Note** The Apex One server database contains a list of agents that the server manages. The server queries Active Directory for the computers' GUIDs and then compares them with GUIDs stored in the database. If a GUID is not in the database, the endpoint will fall under the Unresolved Active Directory Assessment category.

To run a security assessment, perform the following tasks:

1. Define the query scope. For details, see *Defining the Active Directory/IP Address Scope and Query on page 15-72*.

2. Check unprotected computers from the query result. For details, see *Viewing the Query Results on page 15-74*.
3. Install the Security Agent. For details, see *Installing with Security Compliance on page 5-52*.
4. Configure scheduled queries. For details, see *Configuring the Scheduled Query Assessment on page 15-75*.

Defining the Active Directory/IP Address Scope and Query

When querying for the first time, define the Active Directory/IP address scope, which includes Active Directory objects and IP addresses that the Apex One server will query on demand or periodically. After defining the scope, start the query process.

Note

To define an Active Directory scope, Apex One must first be integrated with Active Directory. For details about the integration, see *Active Directory Integration on page 2-32*.

Procedure

1. Go to **Assessment** > **Unmanaged Endpoints**.
2. On the **Active Directory/IP Address Scope** section, click **Define Scope**.

   A new screen opens.
3. To define an Active Directory scope:
   a. Go to the **Active Directory Scope** section.
   b. Select **Use on-demand assessment** to perform real-time queries and get more accurate results. Disabling this option causes Apex One to query the database instead of each Security Agent. Querying only the database can be quicker but is less accurate.
   c. Select the objects to query. If querying for the first time, select an object with less than 1,000 accounts and then record how much

time it took to complete the query. Use this data as your performance benchmark.

4. To define an IP address scope:

   a. Go to the **IP Address Scope** section.

   b. Select **Enable IP Address Scope**.

   c. Specify an IP address range. Click the plus or minus button to add or delete IP address ranges.

   - For a pure IPv4 Apex One server, type an IPv4 address range.
   - For a pure IPv6 Apex One server, type an IPv6 prefix and length.
   - For a dual-stack Apex One server, type an IPv4 address range and/or IPv6 prefix and length.

     The IPv6 address range limit is 16 bits, which is similar to the limit for IPv4 address ranges. The prefix length should therefore be between 112 and 128.

     TABLE 15-8. Prefix Lengths and Number of IPv6 Addresses

LENGTH	NUMBER OF IPV6 ADDRESSES
128	2
124	16
120	256
116	4,096
112	65,536

5. Under Advanced Setting, specify ports used by Apex One servers to communicate with agents.

   To view the communication port used by the Apex One server, go to **Agents** > **Agent Management** and select a domain. The port displays next to the IP address column. Trend Micro recommends keeping a record of port numbers for your reference.

a. Click **Specify ports**.

b. Type the port number and click **Add**. Repeat this step until you have all the port numbers you want to add.

c. Click **Save**.

6. To check the endpoints connectivity using a particular port number, select **Declare an endpoint unreachable by checking port <x>**. When connection is not established, Apex One immediately treats the endpoint as unreachable. The default port number is 135.

   Enabling this setting speeds up the query. When connection to endpoints cannot be established, the Apex One server no longer needs to perform all the other connection verification tasks before treating endpoints as unreachable.

7. To save the scope and start the query, click **Save and re-assess**. To save the settings only, click **Save only**.

   The **Outside Server Management** screen displays the result of the query.

Note

The query may take a long time to complete, especially if the query scope is broad. Do not perform another query until the Outside Server Management screen displays the result. Otherwise, the current query session terminates and the query process restarts.

Viewing the Query Results

The query result appears under the **Security Status** section. An unmanaged endpoint will have one of the following statuses:

- Managed by another Apex One server
- No Security Agent installed
- Unreachable

- Unresolved Active Directory assessment

Procedure

1. In the **Security Status** section, click a number link to display all affected computers.
2. Use the search and advanced search functions to search and display only the computers that meet the search criteria.

   If you use the advanced search function, specify the following items:

   - IPv4 address range
   - IPv6 prefix and length (prefix should be between 112 and 128)
   - Endpoint name
   - Apex One server name
   - Active Directory tree
   - Security status

   Apex One will not return a result if the name is incomplete. Use the wildcard character (*) if unsure of the complete name.
3. To save the list of computers to a file, click **Export**.
4. For Security Agents managed by another Apex One server, use the Agent Mover tool to have these Security Agents managed by the current Apex One server. For more information about this tool, see *Agent Mover on page 15-24*.

Configuring the Scheduled Query Assessment

Configure the Apex One server to periodically query the Active Directory and IP addresses to ensure that security guidelines are implemented.

Procedure

1. Go to **Assessment** > **Unmanaged Endpoints**.
2. Click **Define Schedule** on top of the agent tree.
3. Enable scheduled query.
4. Specify the schedule.
5. Click **Save**.

Trend Micro Virtual Desktop Support

Optimize virtual desktop protection by using Trend Micro Virtual Desktop Support. This feature regulates tasks on Security Agents residing in a single virtual server.

Running multiple desktops on a single server and performing on-demand scan or component updates consume significant amount of system resources. Use this feature to prohibit agents from running scans or updating components at the same time.

For example, if a VMware vCenter server has three virtual desktops running Security Agents, Apex One can initiate Scan Now and deploy updates simultaneously to all three agents. Virtual Desktop Support recognizes that the agents are on the same physical server. Virtual Desktop Support allows a task to run on the first agent and postpones the same task on the other two agents until the first agent finishes the task.

Virtual Desktop Support can be used on the following platforms:

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

For administrators using other virtualization applications, the Apex One server can also act as an emulated hypervisor to manage virtual agents.

Use the Apex One VDI Pre-Scan Template Generation Tool to optimize on-demand scan or remove GUIDs from base or golden images.

Virtual Desktop Support System Requirements

The following table lists the virtual platforms supported by Virtual Desktop Support.

Virtualization Provider	Supported Platforms
VMware	• VMware vCenter: 5.x, 6.x • VMware View: 4.x, 5.x, 6.x • VMware Horizon View: 6.x, 7.x
Citrix	• Citrix XenServer: 6.x, 7.x • Citrix XenDesktop: 5.x, 7.x
HyperV	Hyper-V Server: • Microsoft Hyper-V Server 2008/2008 R2 (64-bit) • Microsoft Hyper-V Server 2012/2012 R2 (64-bit) • Microsoft Hyper-V Server 2016 (64-bit) • Microsoft Hyper-V Server 2019 (64-bit) Windows Server Hyper-V: • Windows Server 2008/2008 R2 (64-bit) Hyper-V • Windows Server 2012/2012 R2 (64-bit) Hyper-V • Windows Server 2016 (64-bit) Hyper-V • Windows Server 2019 (64-bit) Hyper-V Windows Hyper-V: • Windows 8/8.1 Pro/Enterprise (64-bit) Hyper-V • Windows 10 Pro/Pro for Workstation/Enterprise (64-bit) Hyper-V

Virtual Desktop Support Installation

Virtual Desktop Support is a native Apex One feature but is licensed separately. After you install the Apex One server, this feature is available but is not functional. Installing this feature means downloading a file from the ActiveUpdate server (or a custom update source, if one has been set up). When the file has been incorporated into the Apex One server, you can activate Virtual Desktop Support to enable its full functionality. Installation and activation are performed from Plug-in Manager.

Note

Virtual Desktop Support is not fully supported in pure IPv6 environments. For details, see *Pure IPv6 Server Limitations on page A-2*.

Installing Virtual Desktop Support

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the **Trend Micro Virtual Desktop Support** section and click **Download**.

   The size of the package displays beside the **Download** button.

   Plug-in Manager stores the downloaded package to <*Server installation folder*>\PCCSRV\Download\Product.

   Note

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

3. Monitor the download progress. You can navigate away from the screen during the download.

If you encounter problems downloading the package, check the server update logs on the Apex One product console. On the main menu, click **Logs** > **Server Update**.

After Plug-in Manager downloads the file, Virtual Desktop Support displays in a new screen.

Note

If Virtual Desktop Support does not display, see the reasons and solutions in *Troubleshooting Plug-in Manager on page 17-12*.

4. To install Virtual Desktop Support immediately, click **Install Now**. To install at a later time:

   a. Click **Install Later**.

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

   c. Go to the **Trend Micro Virtual Desktop Support** section and click **Install**.

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

   The installation starts.

6. Monitor the installation progress. After the installation, the Virtual Desktop Support version displays.

Virtual Desktop Support License

View, activate, and renew the Virtual Desktop Support license from Plug-in Manager.

Obtain the Activation Code from Trend Micro and then use it to enable the full functionality of Virtual Desktop Support.

Activating or Renewing Virtual Desktop Support

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the **Trend Micro Virtual Desktop Support** section and click **Manage Program**.
3. Click **View License Information**.
4. On the **Product License Details** screen that opens, click **New Activation Code**.
5. On the screen that opens, type the Activation Code and click **Save**.
6. Back in the Product License Details screen, click **Update Information** to refresh the screen with the new license details and the status of the feature. This screen also provides a link to the Trend Micro website where you can view detailed information about your license.

Viewing License Information for Virtual Desktop Support

Procedure

1. Open the Apex One web console and click **Plug-ins** > **[Trend Micro Virtual Desktop Support] Manage Program** in the main menu.
2. Click **View License Information**.
3. View license details in the screen that opens.

   The Virtual Desktop Support License Details section provides the following information:

   - **Status**: Displays either "Activated", "Not Activated" or "Expired".
   - **Version**: Displays either "Full" or "Trial" version. If you have both full and trial versions, the version that displays is "Full".

- **Expiration Date**: If Virtual Desktop Support has multiple licenses, the latest expiration date displays. For example, if the license expiration dates are 12/31/2010 and 06/30/2010, 12/31/2010 displays.
- **Seats**: Displays how many Security Agents can use Virtual Desktop Support
- **Activation code**: Displays the activation code

Reminders about licenses display during the following instances:

If you have a full version license:

- During the feature's grace period. The duration of the grace period varies by region. Please verify the grace period with your Trend Micro representative.
- When the license expires and grace period elapses. During this time, you will not be able to obtain technical support.

If you have a trial version license

- When the license expires. During this time, you will not be able to obtain technical support.

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

Virtual Server Connections

Optimize on-demand scan or component updates by adding VMware vCenter 4 (VMware View 4), Citrix XenServer 5.5 (Citrix XenDesktop 4), or Microsoft Hyper-V Server. Apex One servers communicate with the specified virtual servers to determine Security Agents that are on the same physical server.

For other VDI servers, Apex One server provides an emulated virtual hypervisor to manage the virtual agents on other platforms. The Apex One hypervisor processes virtual agent requests in the order that the server

receives the requests. The Apex One server processes one request at a time and places the other requests in a queue.

Adding Server Connections

Procedure

1. Open the Apex One web console and click **Plug-ins** > **[Trend Micro Virtual Desktop Support] Manage Program** in the main menu.
2. Select **VMware vCenter Server**, **Citrix XenServer**, **Microsoft Hyper-V**, or **Other virtualization applications**.

   Note

   When selecting **Other virtualization applications**, no further information is necessary. The Apex One server responds to virtual agent requests in the order that the server receives the requests.

3. Enable the connection to the server.
4. Specify the following information:
   - For VMware vCenter and Citrix XenServer servers:
     - IP address
     - Port
     - Connection protocol (HTTP or HTTPS)
     - Username
     - Password
   - For Microsoft Hyper-V servers:
     - Host name or IP address
     - Domain\username

Note

The logon account must be a domain account in the Administrators group

- Password

5. Optionally enable proxy connection for VMware vCenter or Citrix XenServer.
   a. Specify the proxy server name or IP address and port.
   b. If the proxy server requires authentication, specify the user name and password.
6. Click **Test connection** to verify that the Apex One server can successfully connect to the server.

Note

For details on troubleshooting Microsoft Hyper-V connections, see *Troubleshooting Microsoft Hyper-V Connections on page 15-85*.

7. Click **Save**.

Adding Additional Server Connections

Procedure

1. Open the Apex One web console and click **Plug-ins** > **[Trend Micro Virtual Desktop Support] Manage Program** in the main menu.
2. Click **Add new vCenter connection**, **Add new XenServer connection**, or **Add new Hyper-V connection**.
3. Repeat the steps to provide the proper server information.
4. Click **Save**.

Deleting a Connection Setting

Procedure

1. Open the Apex One web console and go to **Plug-ins** > **[Trend Micro Virtual Desktop Support] Manage Program** in the main menu.
2. Click **Delete this connection**.
3. Click **OK** to confirm the deletion of this setting.
4. Click **Save**.

Changing the VDI Scan Capacity

Administrators can increase the number of VDI endpoints that run concurrent scanning by modifying the `vdi.ini` file. Trend Micro recommends strictly monitoring the effect of changing the VDI capacity to ensure that system resources can handle any increased scanning.

Procedure

1. On the Apex One server computer, go to <*Server installation folder*>`PCCSRV\Private\vdi.ini`.
2. Locate the `[TaskController]` settings.

   The default TaskController settings are as follows:

   - `[TaskController]`

     `Controller_02_MaxConcurrentGuests=1`

     `Controller_03_MaxConcurrentGuests=3`

     Where:

     - `Controller_02_MaxConcurrentGuests=1` equals the maximum number of clients that can perform scans concurrently.

- `Controller_03_MaxConcurrentGuests=3` equals the maximum number of clients that can perform updates concurrently.

3. Increase or decrease the count in each controller as necessary.

   The minimum value for all settings is 1.

   The maximum value for all settings is 65536.

4. Save and close the `vdi.ini` file.

5. Restart the Apex One Master Service.

6. Monitor the CPU, memory, and disk usage resources of the VDI endpoints. Modify the controller settings further to increase/decrease the number of concurrent scans to best suit the VDI environment by repeating steps 1 to 5.

Troubleshooting Microsoft Hyper-V Connections

The Microsoft Hyper-V connection uses Windows Management Instrumentation (WMI) and DCOM for agent-server communication. Firewall policies may block this communication, causing an unsuccessful connection to the Hyper-V server.

The Hyper-V server listening port defaults to port 135 and then chooses a randomly configured port for further communication. If the firewall blocks WMI traffic or either of these two ports, communication with the server is unsuccessful. Administrators can modify the firewall policy to allow successful communication with the Hyper-V server.

Verify that all connection settings, including IP address, domain\username, and password are correct before performing the following firewall modifications.

Allowing WMI Communication through the Windows Firewall

Procedure

1. On the Hyper-V server, open the **Windows Firewall Allowed Programs** screen.

   On Windows 2008 R2 systems, go to **Control Panel** > **System and Security** > **Windows Firewall** > **Allow a program or feature through Windows Firewall**.

2. Select **Windows Management Instrumentation (WMI)**.

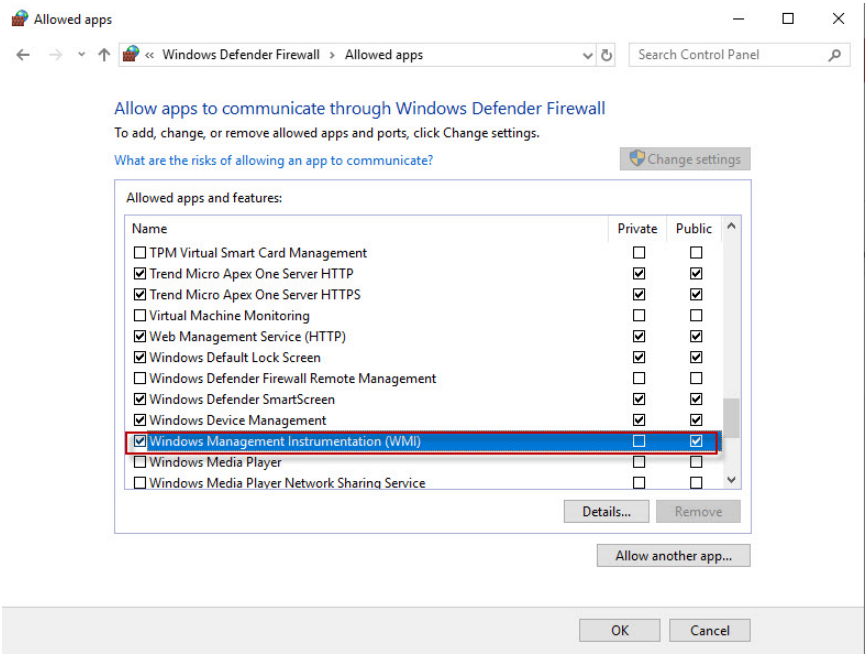


FIGURE 15-7. Windows Firewall Allowed Programs screen

3. Click **Save**.

4. Test the Hyper-V connection again.

Opening Port Communication through the Windows Firewall or a Third-party Firewall

Procedure

1. On the Hyper-V server, ensure that the firewall allows communication through port 135 and test the Hyper-V connection again.

   For details about opening ports, refer to your firewall documentation.

2. If the connection to the Hyper-V server is unsuccessful, configure WMI to use a fixed port.

   For details on *Setting Up a Fixed Port for WMI*, refer to:

   https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/setting-up-a-fixed-port-for-wmi

3. Open ports 135 and the newly created fixed port (24158) for communication through the firewall.

4. Test the Hyper-V connection again.

VDI Pre-Scan Template Generation Tool

Use the Apex One VDI Pre-Scan Template Generation Tool to optimize on-demand scans or remove GUIDs from base or golden images. This tool scans the base or golden image and certifies the image. When scanning duplicates of this image, Apex One only checks parts that have changed. This ensures shorter scanning time.

Tip

Trend Micro recommends generating the pre-scan template after applying a Windows update or installing a new application.

Creating a Pre-scan Template

Procedure

1. On the Apex One server computer, browse to <*Server installation folder*>`\PCCSRV\Admin\Utility\TCacheGen`.
2. Choose a version of the VDI Pre-Scan Template Generation Tool. The following versions are available:

TABLE 15-9. VDI Pre-Scan Template Generation Tool Versions

FILE NAME	INSTRUCTION
TCacheGen.exe	Choose this file if you want to run the tool directly on a 32-bit platform.
TCacheGen_x64.exe	Choose this file if you want to run the tool directly on a 64-bit platform.
TCacheGenCli.exe	Choose this file if you want to run the tool from the command line interface of a 32-bit platform.
TCacheGenCli_x64.exe	Choose this file if you want to run the tool from the command line interface of a 64-bit platform.

3. Copy the version of the tool that you chose in the previous step to the endpoint.
4. Run the tool.
   - To run the tool directly:
     a. Double-click `TCacheGen.exe` or `TCacheGen_x64.exe`.
     b. Select **Generate Pre-Scan Template** and click **Next**.
   - To run the tool from the command line interface:
     a. Open a command prompt and change the directory to `<Agent installation folder>`.
     b. Type the following command:

```
TCacheGenCli Generate_Template
```

Or

```
TcacheGenCli_x64 Generate_Template
```

Note

The tool scans the image for security threats before generating the pre-scan template and removing the GUID.

After generating the pre-scan template, the tool unloads the Security Agent. Do not reload the Security Agent. If the Security Agent reloads, you will need to create the pre-scan template again.

Removing GUIDs from Templates

Procedure

1. On the Apex One server computer, browse to <*Server installation folder*>`\PCCSRV\Admin\Utility\TCacheGen`.
2. Choose a version of the VDI Pre-Scan Template Generation Tool. The following versions are available:

TABLE 15-10. VDI Pre-Scan Template Generation Tool Versions

FILE NAME	INSTRUCTION
TCacheGen.exe	Choose this file if you want to run the tool directly on a 32-bit platform.
TCacheGen_x64.exe	Choose this file if you want to run the tool directly on a 64-bit platform.
TCacheGenCli.exe	Choose this file if you want to run the tool from the command line interface of a 32-bit platform.
TCacheGenCli_x64.exe	Choose this file if you want to run the tool from the command line interface of a 64-bit platform.

3. Copy the version of the tool that you chose in the previous step to the endpoint.
4. Run the tool.
   - To run the tool directly:
     a. Double-click `TCacheGen.exe` or `TCacheGen_x64.exe`.
     b. Select **Remove GUID from Template** and click **Next**.
   - To run the tool from the command line interface:
     a. Open a command prompt and change the directory to `<Agent installation folder>`.
     b. Type the following command:

        ```
        TCacheGenCli Remove GUID
        ```

        Or

        ```
        TcacheGenCli_x64 Remove GUID
        ```

Global Agent Settings

Apex One applies global agent settings to all agents or only to agents with certain privileges.

Procedure

1. Go to **Agents** > **Global Agent Settings**.
2. Configure the following settings:

TABLE 15-11. Global Agent Settings

TAB	SETTING	REFERENCE
Security Settings	Scan Settings	*Scan Settings Section on page 7-70*
	Scheduled Scan Settings	*Scheduled Scan Settings Section on page 7-75*
	Firewall Settings	*Global Firewall Settings on page 13-24*
	Suspicious Connection Settings	*Configuring Global User-defined IP List Settings on page 8-6*
	Behavior Monitoring Settings	*Configuring Global Behavior Monitoring Settings on page 9-18*
System	Certified Safe Software Service Settings	*Configuring Global Scan Settings on page 7-68*
	Smart Protection Service Proxy	*Configuring Global Smart Protection Service Proxy Settings on page 15-54*
	Updates	• *ActiveUpdate Server as the Security Agent Update Source on page 6-36* • *Configuring Reserved Disk Space for Security Agents Updates on page 6-48*
	Services Restart	*Security Agent Service Restart on page 15-13*
Network	Preferred IP Address	*Agent IP Addresses on page 5-8*
	Server-Agent Communication	*Enhanced Encryption of Server-Agent Communication on page 14-56*
	Virus/Malware Log Bandwidth Settings	*Configuring Global Scan Settings on page 7-68*
	Unreachable Network	*Unreachable Agents on page 15-45*

Tab	Setting	Reference
Agent Control	General Settings	*Configuring Global Scan Settings on page 7-68*
	Alert Settings	*Configuring Security Agent Update Notifications on page 6-49*
	Agent Language Configuration	*Security Agent Language Configuration on page 15-23*

3. Click **Save**.

Configuring Agent Privileges and Other Settings

Grant users the privileges to modify certain settings and perform high level tasks on the Security Agent.

Note

Antivirus settings only appear after activating the Apex One Antivirus feature.

Tip

To enforce uniform settings and policies throughout the organization, grant limited privileges to users.

Procedure

1. Go to **Agents** > **Agent Management**.
2. In the agent tree, click the root domain icon ( ) to include all agents or select specific domains or agents.
3. Click **Settings** > **Privileges and Other Settings**.
4. On the **Privileges** tab, configure the following user privileges:

TABLE 15-12. Agent Privileges

AGENT PRIVILEGES	REFERENCE
Independent Mode Privilege	*Security Agent Independent Mode Privilege on page 15-20*
Scan Privileges	*Scan Type Privileges on page 7-56*
Scheduled Scan Privileges	*Scheduled Scan Privileges and Other Settings on page 7-57*
Firewall Privileges	*Firewall Privileges on page 13-22*
Behavior Monitoring Privileges	*Behavior Monitoring Privileges on page 9-20*
Trusted Program List	*Trusted Program List Privilege on page 7-66*
Mail Scan Privileges	*Mail Scan Privileges and Other Settings on page 7-61*
Proxy Setting Privileges	*Granting Proxy Configuration Privileges on page 15-55*
Component Update Privileges	*Configuring Update Privileges and Other Settings on page 6-45*
Unloading and Unlocking	*Granting the Agent Unloading and Unlocking Privilege on page 15-20*
Uninstallation	*Granting the Security Agent Uninstallation Privilege on page 5-62*

5. Click the **Other Settings** tab and configure the following settings:

TABLE 15-13. Other Agent Settings

SETTING	REFERENCE
Update Settings	*Configuring Update Privileges and Other Settings on page 6-45*
Web Reputation Settings	*Web Threat Notifications for Agent Users on page 12-12*

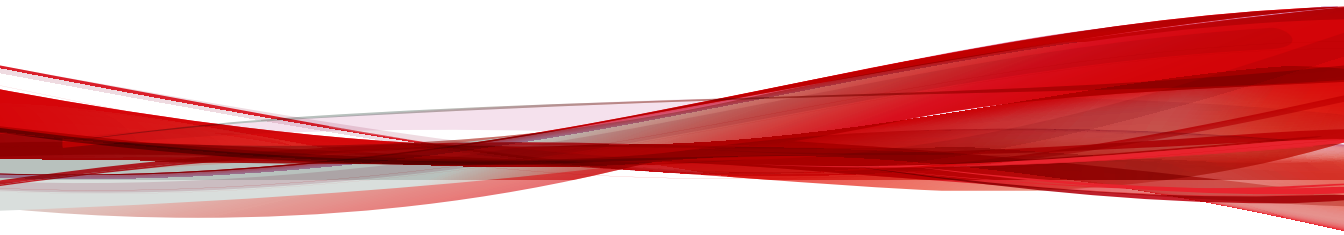
Setting	Reference
Behavior Monitoring Settings	*Behavior Monitoring Privileges on page 9-20*
C&C Contact Alert Settings	*C&C Contact Alert Notifications for Agent Users on page 12-16*
Central Quarantine Restore Alert Settings	Displays a notification message on the endpoint after restoring a quarantined file
Predictive Machine Learning Settings	Displays a notification message on the endpoint after detecting an unknown threat
Security Agent Self-protection	*Security Agent Self-protection on page 15-14*
Scheduled Scan Settings	*Granting Scheduled Scan Privileges and Displaying the Privilege Notification on page 7-59*
Cache Settings for Scans	*Cache Settings for Scans on page 7-62*
POP3 Email Scan Settings	*Granting Mail Scan Privileges and Enabling POP3 Mail Scan on page 7-62*
Security Agent Access Restriction	*Security Agent Console Access Restriction on page 15-18*
Restart Notification	*Security Risk Notifications for Security Agent Users on page 7-85*

6. If you selected domain(s) or agent(s) in the agent tree, click **Save**. If you clicked the root domain icon, choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future domain. Future domains are domains not yet created at the time you configured the settings.
   - **Apply to Future Domains Only**: Applies settings only to agents added to future domains. This option will not apply settings to new agents added to an existing domain.

Part IV

Providing Additional Protection



Chapter 16

Protecting Off-premises Agents

This chapter describes the Edge Relay Server installation and configuration steps necessary to protect Security Agents that leave the corporate intranet.

Topics include:

Edge Relay Server

The Apex One Edge Relay server provides administrators visibility and increased protection of endpoints that users take outside of the company's intranet. By installing the Edge Relay server in the Demilitarized Zone (DMZ), off-premises Security Agents that cannot establish a direct connection to the Apex One server can still poll the server in order to receive updated policy settings.

After configuring the Edge Relay server, Security Agents receive the settings and automatically begin to connect to the Edge Relay server once connection to the Apex One server is unavailable.

Communication between the Edge Relay server, Apex One server, and Security Agents is encrypted using certificate authentication.

For more information, see *Managing Edge Relay Server Certificates on page 16-19*.

Edge Relay Server System Requirements

Before installing the Edge Relay Server, ensure that the target server computer meets the minimum system requirements.

Resource	Requirements
Processor	2 GHz dual core
Memory	1 GB (exclusively for the Edge Relay Server)
Disk space	60 GB
Operating system	• Windows Server 2016 • Windows Server 2012 R2

Resource	Requirements

Network card	• 2 network cards
	  • One for intranet connection to the Apex One server
	  • One for external connection to off-premises Security Agents
	• 1 network card configured to use different ports for intranet and Internet connections

Installing the Edge Relay Server

Before installing the Edge Relay Server, ensure that the target server computer meets the minimum system requirements.

For more information, see *Edge Relay Server System Requirements on page 16-2*.

Procedure

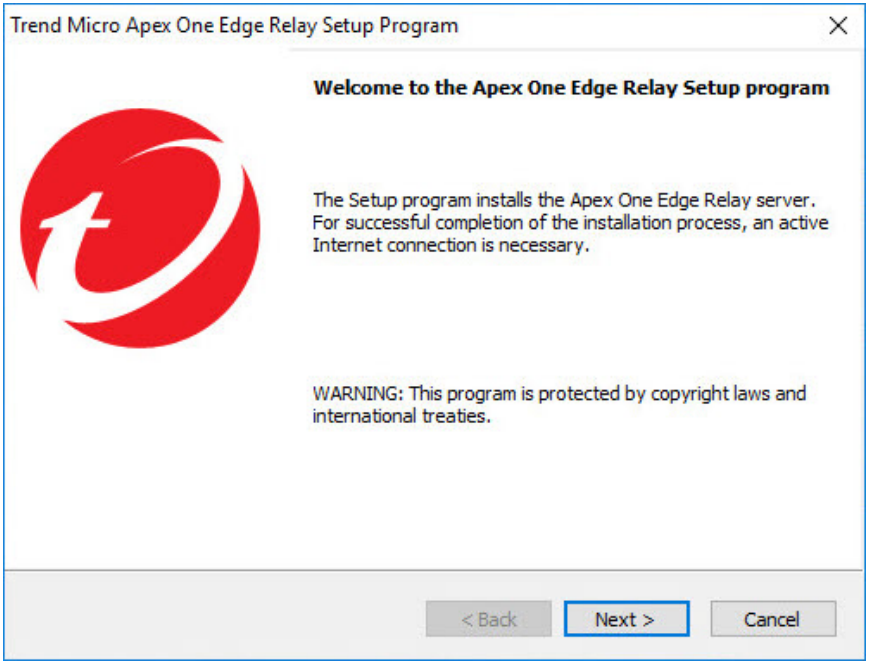
1. Locate the <*Server installation folder*>`\PCCSRV\Admin\Utility\EdgeServer` folder on the Apex One server computer, and copy the folder to the target Edge Relay Server computer.
2. On the target Edge Relay Server, open the `EdgeServer` folder and execute the `setup.exe` file to start the installation process.

   The setup package checks the server for required components.
3. If any of the following components do not exist on the server, click **Install** to allow the setup program to install the missing components during the Edge Relay Server installation process.
   - Microsoft Visual C++ 2017 Update 3 Redistributable Package (x86)
   - Microsoft Visual C++ 2017 Update 3 Redistributable Package (x64)
   - Microsoft .NET Framework 4.6.1
   - Microsoft URL Rewrite Module 2.0 for IIS (x64)

- Microsoft Application Request Routing 3.0 (x64)

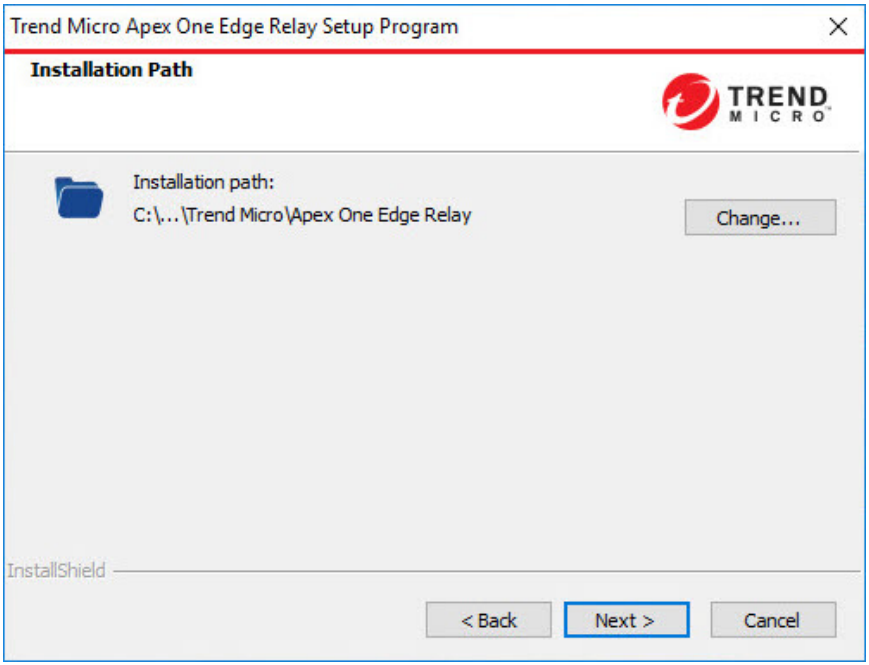
The Welcome screen appears.

4. Click **Next**.



The **Installation Path** screen appears.

5. Accept the default installation directory or click **Change...** to select a different location.



6. Click **Next >**.

   The **Edge Relay Server - Security Agent Connection** screen appears.

7. Specify the following settings that off-premises Security Agents use to connect to the Edge Relay server:

   - **Edge Relay server FQDN**: Type the FQDN of the Edge Relay server
   - **Certificate**: Select the Webhost certificate for the Edge Relay Server or allow the system to create a self-signed certificate after you click **Next >**.

Note

You can change the self-signed certificate using the Edge Relay Server Registration Tool after installation completes if you do not have custom certificates readily available.

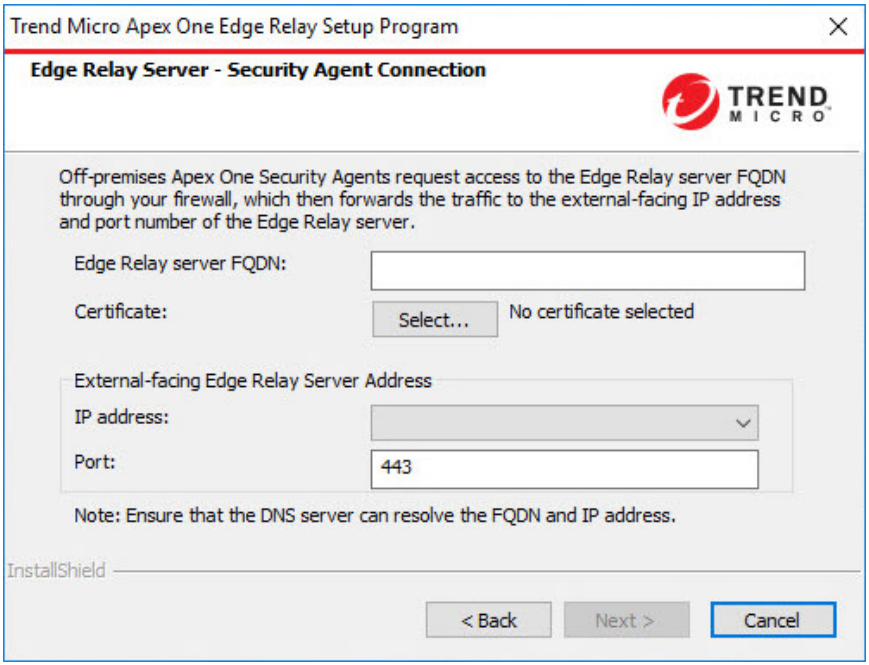
For more information, see *Binding Customer-Specific Certificates with the Edge Relay Server on page 16-17*.

- **IP address**: Select the IP address of the server
- **Port**: Accept the default port or specify a port

Important

You must configure your firewall and gateway to allow:

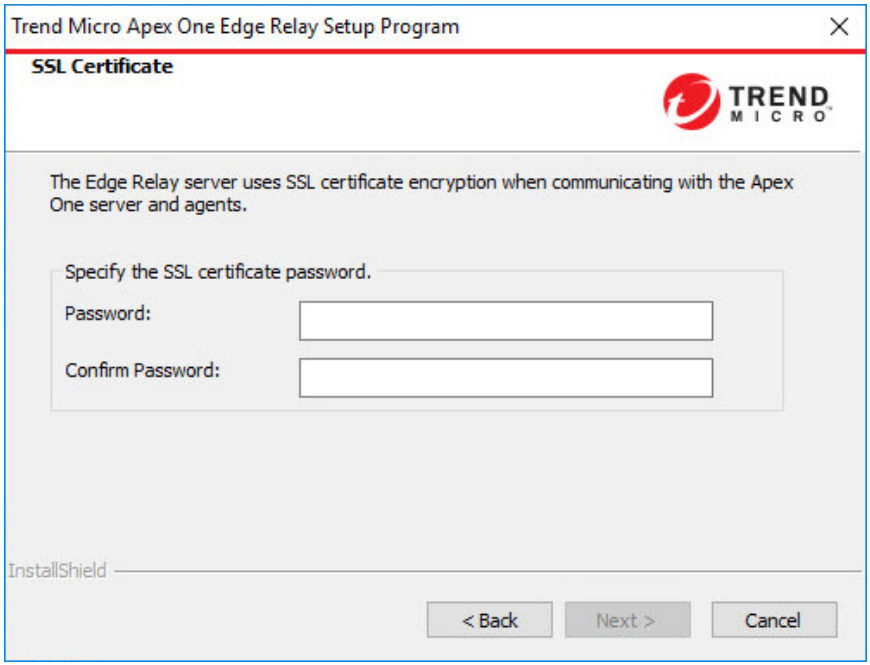
- Redirection of the Security Agent communication from the Internet to the Edge Relay server
- Communication through the port specified



8. Click **Next >**.

   The **SSL Certificate** screen appears.

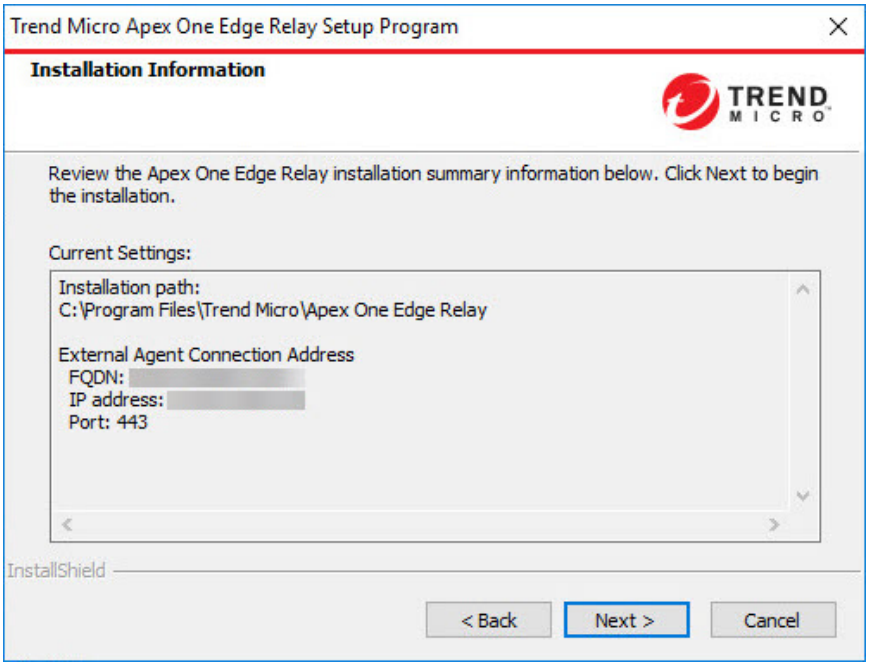
9. Specify and confirm the password used for the Edge Relay Server certificate (OsceOPA certificate).



10. Click **Next >**.

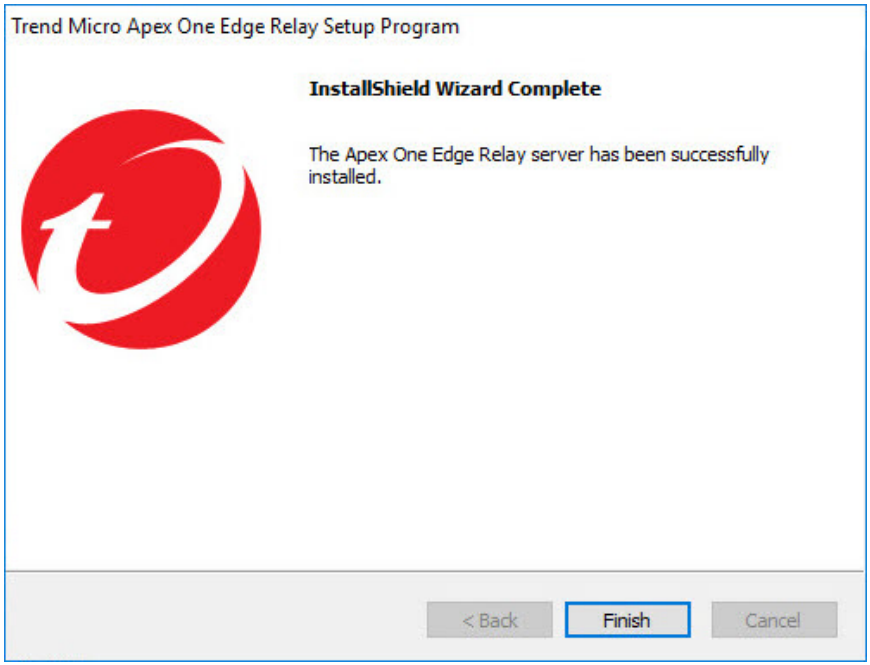
    The **Installation Information** screen appears.

11. Click **Next >** to begin the installation.



After the installation completes, the **InstallShield Wizard Complete** screen appears.

12. Click **Finish**.



The Edge Relay Server is ready for use. You can configure which Apex One servers the Edge Relay Server supports.

For more information, see *Edge Relay Server Registration Tool on page 16-12*.

Upgrading the Edge Relay Server

The Apex One Edge Relay Server supports upgrading from previous versions of the Edge Relay Server. During the upgrade process, the Setup program automatically applies the same server settings used by the previous version and transfers all certificates.

Important

This version of the Edge Relay Server does not support older versions of the agent program. If you want to manage off-premises endpoints, ensure that you upgrade all agents to the Apex One Security Agent and connect the Security Agents to the Apex One server to obtain the upgraded Edge Relay Settings.

Before upgrading the Edge Relay Server, ensure that the target server computer meets the minimum system requirements.

For more information, see *Edge Relay Server System Requirements on page 16-2*.

Procedure

1. Locate the <*Server installation folder*>`\PCCSRV\Admin\Utility \EdgeServer` folder on the Apex One server computer, and copy the folder to the target Edge Relay Server computer.
2. On the target Edge Relay Server, open the `EdgeServer` folder and execute the `setup.exe` file to start the upgrade process.

   The **Welcome** screen appears.
3. Click **Next >**

   The Setup program automatically retrieves the necessary settings from the previous Edge Relay Server and displays the **Installation Information** screen.
4. Click **Next >** to begin the upgrade.
5. After the upgrade completes, you must register the upgraded Edge Relay Server to the Apex One server using the Edge Relay Server Registration Tool.

   a. Locate the Edge Relay Server Registration Tool from the following location on the Edge Relay Server computer:

   ```
   <Apex One Edge Relay installation directory>\OfcEdgeSvc
   \ofcedgecfg.exe
   ```

b. Open a command line editor with administrator privileges.

   Right-click `cmd.exe` and click **Run as administrator**.

c. Change the directory to the location of the `ofcedgecfg.exe` file.

d. Execute the following command:

```
ofcedgecfg.exe --cmd reg --server <Apex One server
address> --port <Apex One server port> --pwd <Apex One
'root' account password>
```

Verify that the successful registration of the upgraded Edge Relay Server on the Apex One web console (**Administration** > **Settings** > **Edge Relay**).

6. Ensure that all Security Agents that you want to manage using the Edge Relay Server can connect directly to the Apex One server to obtain the latest Edge Relay Server settings.

Edge Relay Server Registration Tool

After installing the Edge Relay Server, you must use the Edge Relay Server Registration Tool to register the Edge Relay Server with each Apex One server that off-premises Security Agents report to. Security Agents reporting to the Apex One server receive the registered connection settings and can automatically use the Edge Relay Server to poll the Apex One server after leaving the corporate intranet.

The Edge Relay Server Registration Tool allows you to perform the following tasks using a command line editor:

- *Register to an Apex One Server on page 16-14*
- *Unregister from an Apex One Server on page 16-14*
- *Renew a Self-Signed Certificate (includes OsceEdgeRoot CA, webhost, and OsceOPA) on page 16-15*
- *Bind Customer-Specific Certificates with Webhost and OsceOPA Certificates on page 16-16*

- *Delete All IIS Rules (after unregistering from all Apex One servers) on page 16-17*

Using the Edge Relay Server Registration Tool

The Edge Relay Server Registration Tool allows you to perform the following tasks using a command line editor:

- *Register to an Apex One Server on page 16-14*
- *Unregister from an Apex One Server on page 16-14*
- *Renew a Self-Signed Certificate (includes OsceEdgeRoot CA, webhost, and OsceOPA) on page 16-15*
- *Bind Customer-Specific Certificates with Webhost and OsceOPA Certificates on page 16-16*
- *Delete All IIS Rules (after unregistering from all Apex One servers) on page 16-17*

Note

You can register the Edge Relay Server to multiple Apex One servers. Execute a separate registration command for each required Apex One connection.

Procedure

1. Locate the Edge Relay Server Registration Tool from the following location on the Edge Relay Server computer:

   `<Apex One Edge Relay installation directory>\OfcEdgeSvc\ofcedgecfg.exe`

2. Open a command line editor with administrator privileges.

   Right-click `cmd.exe` and click **Run as administrator**.

3. Change the directory to the location of the `ofcedgecfg.exe` file.

4. Execute the required task.

Register to an Apex One Server

Command	`--cmd reg`	
Parameters	`--server <VALUE>`	Apex One server IP address
	`--port <VALUE>`	Apex One server port number
	`--pwd <VALUE>`	Apex One server 'root' account password
Example	`ofcedgecfg.exe --cmd reg --server <server address> --port <port> --pwd <root password>`	

Unregister from an Apex One Server

Command	`--cmd unreg`	
Parameters	`--server <VALUE>`	Apex One server IP address
	`--port <VALUE>`	Apex One server port number
	`--pwd <VALUE>`	Apex One server 'root' account password
Example	`ofcedgecfg.exe --cmd unreg --server <server address> --port <port> --pwd <root password>`	

Renew a Self-Signed Certificate (includes OsceEdgeRoot CA, webhost, and OsceOPA)

WARNING!

You should only use the **renewcert** command if you are using certificates created by the Edge Relay Setup program. If you run the **renewcert** on an Edge Relay Server that uses customer-specific certificates, the command deletes and replaces the customer-specific certificates with self-signed versions.

Command	**--cmd renewcert**	
Parameters	**--opacertpwd <VALUE>**	OsceOPA certificate password
	--keeprootca	Keep root CA after certificate renewal (optional)
Example	**ofcedgecfg.exe --cmd renewcert --opacertpwd <OsceOPA certificate password> [--keeprootca]**	
Post-requisite command	After renewing your certificates, you must re-register the Edge Relay Server to the Apex One server. For more information, see *Register to an Apex One Server on page 16-14*. **Important** After re-registering to the Apex One server, you must ensure that all off-premises Security Agents reconnect to the Apex One server to obtain the updated certificates. Any off-premises Security Agent that does not receive the latest certificates is unable to connect to the Edge Relay Server.	

Bind Customer-Specific Certificates with Webhost and OsceOPA Certificates

Important

Binding customer-specific certificates to the Edge Relay server requires that you prepare and properly configure your Webhost and OsceOPA certificates.

For more information and detailed instructions about preparing and binding customer-specific certificates, see *Binding Customer-Specific Certificates with the Edge Relay Server on page 16-17*.

Command	**`--cmd bindwebsite`**	
Parameters	**`--certsubject <VALUE>`**	Webhost certificate subject
	`--certstore <VALUE>`	Webhost certificate store name: `My | webhosting`
	`--certissuer <VALUE>`	Webhost certificate issuer
	`--opacertpwd <VALUE>`	OsceOPA certificate password
Example	**`ofcedgecfg.exe --cmd bindwebsite --certsubject <certificate subject name> --certstore <certificate store name> --certissuer <certificate_issuer> --opacertpwd <OsceOPA certificate password>`**	
Post-requisite command	After binding your customer-specific certificates, you must re-register the Edge Relay Server to the Apex One server. For more information, see *Register to an Apex One Server on page 16-14*. **Important** After re-registering to the Apex One server, you must ensure that all off-premises Security Agents reconnect to the Apex One server to obtain the updated certificates. Any off-premises Security Agent that does not receive the latest certificates is unable to connect to the Edge Relay Server.	

Delete All IIS Rules (after unregistering from all Apex One servers)

Command	`--cmd delrule`
Parameters	None
Example	`ofcedgecfg.exe --cmd delrule`

Binding Customer-Specific Certificates with the Edge Relay Server

You can create and bind customer-specific certificates to validate Apex One server and Security Agent communication with the Edge Relay Server.

Important

When using customer-specific certificates, the certificates must include both public and private keys in order to sign out other certificates.

Due to the public and private key requirement, you may not be able to utilize most third-party commercial CAs.

Procedure

1. Prepare the customized Webhost certificate:
   - Must be issued by a CA that is included in the trusted store
   - Store in the “Web hosting” certificate store: “My” or “webhosting”
   - Record the following information required during binding:
     - Certificate subject
     - Certificate issuer

Important

When using customer-specific certificates, the certificates must include both public and private keys in order to sign out other certificates.

Due to the public and private key requirement, you may not be able to utilize most third-party commercial CAs.

2. Prepare a valid certificate to replace the self-signed OsceOPA certificate.
   - Must be issued by a CA that is included in the trusted store
   - Required certificate subject: `OsceOPA`

     Important

     The certificate subject is case-sensitive.

   - Store in the "OfcEdge" certificate store and remove any other certificates from the store
3. Locate the Edge Relay Server Registration Tool from the following location on the Edge Relay Server computer:

   ```
   <Apex One Edge Relay installation directory>\OfcEdgeSvc
   \ofcedgecfg.exe
   ```

4. Open a command line editor with administrator privileges.

   Right-click `cmd.exe` and click **Run as administrator**.

5. Change the directory to the location of the `ofcedgecfg.exe` file.
6. Execute the following command:

   ```
   ofcedgecfg.exe --cmd bindwebsite --certsubject <Webhost
   certificate subject name> --certstore <My | webhosting> --
   certissuer <Webhost certificate_issuer> --opacertpwd
   <OsceOPA certificate password>
   ```

7. Run the following command to re-register the Edge Relay Server to the Apex One server:

```
ofcedgecfg.exe --cmd reg --server <server address> --port
<port> --pwd <root password>
```

8. Instruct all off-premises users to connect directly to the local intranet to allow the Security Agent to receive the updated certificates and reconnect to the Edge Relay Server.

Viewing the Edge Relay Server Connection in Apex One

After connecting to the Edge Relay Server, Security Agents reporting to the Apex One server receive the connection settings and can automatically communicate to the Edge Relay Server after leaving the corporate intranet. You can then monitor the Edge Relay Server connection status from the **Edge Relay Settings** screen.

Procedure

1. On the Apex One web console, go to **Administration** > **Settings** > **Edge Relay**.

   The **Edge Relay Settings** screen appears.

2. View the Edge Relay Server currently registered to the Apex One server.

Managing Edge Relay Server Certificates

Apex One provides a command line tool that allows you to create or renew the Edge Relay Server certificate that agents use for communication. After creating a new certificate, the Edge Relay Server sends the new certificate to the Apex One server which then deploys the certificate to agents the next time agents connect to the Apex One server.

Important

Off-premises Security Agents must connect to the Apex One server to obtain the new Edge Relay Server certificate. Any off-premises agents that do not receive the updated certificate can no longer communicate with the Edge Relay Server until connection with the Apex One server is established.

Procedure

1. On the Edge Relay Server, open a command line editor and go to the following directory:

   ```
   C:\Program Files\Trend Micro\Apex One Edge Relay\OfcEdgeSvc
   \
   ```

2. Execute the certificate tool by running the following command:

   `ofcedgecfg.exe --cmd renewcert --opacertpwd <OsceOPA certificate password> [--keeprootca]`

   Where:

   - **`--renewcert`**: Creates the new certificate
   - **`--opacertpwd <password>`**: Specifies the password for the certificate package

   The Edge Relay Server creates the new certificate package and automatically sends the certificate to the Apex One server. The Apex One server deploys the new certificate to Security Agents the next time the Security Agents report to the Apex One server.

Chapter 17

Using Plug-in Manager

This chapter discusses how to set up Plug-in Manager and provides an overview of plug-in solutions delivered through Plug-in Manager.

Topics include:

About Plug-in Manager

Apex One includes a framework called Plug-in Manager that integrates new solutions into the existing Apex One environment. To help ease the management of these solutions, Plug-in Manager provides at-a-glance data for the solutions in the form of widgets.

Note

None of the plug-in solutions currently support IPv6. The server can download these solutions but is not able to deploy the solutions to pure IPv6 Security Agents or pure IPv6 hosts.

Plug-in Manager delivers the following:

- **Native Product Features**

  Some native Apex One features are licensed separately and activated through Plug-in Manager. In this release, two features fall under this category, namely, **Trend Micro Virtual Desktop Support** and **Apex One Data Protection**.

- **Plug-in programs**

  Plug-in programs are not part of the Apex One program. The plug-in programs have separate licenses and management consoles. Access the management consoles from within the Apex One web console. Examples of plug-in programs are **Trend Micro Apex One ToolBox** and **Trend Micro Apex One (Mac)**.

- **Dashboard tabs and widgets**

  The Apex One **Dashboard** screen requires Plug-in Manager to display the tabs and widgets used to monitor the Apex One server and agent protection status.

This document provides a general overview of plug-in program installation and management and discusses plug-in program data available in widgets.

Refer to specific plug-in program documentation for details on configuring and managing the program.

Plug-in Program Agents on Endpoints

Some plug-in programs (such as Apex One (Mac)) have agents that install on the endpoint's Windows operating systems. Security Agent Plug-in Manager running under the process name `CNTAoSMgr.exe` manages these agents.

Apex One install `CNTAoSMgr.exe` with Security Agent. The only additional system requirement for `CNTAoSMgr.exe` is Microsoft XML Parser (MSXML) version 3.0 or later.

Note

Other plug-in program have agents that do not install on Windows operating systems are not managed from the Security Agent Plug-in Manager. The Apex One (Mac) Security Agent is an example of these agents.

Widgets

Use widgets to view at-a-glance data for deployed plug-in solutions. Widgets are available on the Apex One server's **Dashboard** screen. A special widget, called **Apex One and Plug-ins Mashup**, combines data from Security Agents and plug-in solutions and then presents the data in the agent tree.

This Administrator's Guide provides an overview of widgets and the solutions that support widgets.

Plug-in Manager Installation

In previous Plug-in Manager versions, the Plug-in Manager installation package is downloaded from the Trend Micro ActiveUpdate server and then installed on the computer that hosts the Apex One server. In this version, the installation package is included in the Apex One server installation package in the following location:

<*Server installation folder*>\PCCSRV\Admin\Utility\PLM\PLMSetup.exe

Execute the PLMSetup.exe file to install Plug-in Manager.

Users who are new to Apex One have both the Apex One server and Plug-in Manager installed after completing the Apex One installation. Users who are upgrading to this Apex One version and have used Plug-in Manager previously need to stop the Plug-in Manager service before running the installation package.

Performing Post-installation Tasks

Perform the following after installing Plug-in Manager:

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. Manage plug-in solutions.
3. Access the **Dashboard** screen on the Apex One web console to manage widgets for the plug-in solutions.

Native Apex One Feature Management

Native Apex One features install with Apex One and administrators activate each feature from Plug-in Manager. Manage some features, such as Trend Micro Virtual Desktop Support, from Plug-in Manager and others, such as Apex One Data Protection, from the Apex One web console.

Managing Plug-in Programs

Install and activate plug-in programs independently of Apex One. Each plug-in provides a separate console for product management. The management consoles are accessible from the Apex One web console.

Plug-in Program Installation

Plug-in programs display on the **Plug-in Manager** console. Use the console to download, install, and manage the programs. Plug-in Manager downloads the installation package for the plug-in program from the Trend Micro ActiveUpdate server or from a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-in Manager downloads an installation package or starts the installation, Plug-in Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-in Manager does not support plug-in program installation or management from the Trend Micro Apex Central single sign-on function.

Installing Plug-in Programs

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Download**.

   The size of the plug-in program package displays beside the **Download** button. Plug-in Manager stores the downloaded package to `<Server installation folder>\PCCSRV\Download\Product`.

   Plug-in Manager stores the downloaded package to `<Server installation folder>\PCCSRV\Download\Product`

Monitor the progress or navigate away from the screen during the download.

Note

If Apex One encounters problems downloading or installing the package, check the server update logs on the Apex One web console. On the main menu, click **Logs** > **Server Updates**.

3. Click **Install Now** or **Install Later**.

   - After clicking **Install Now**, the installation begins and an installation progress screen appears.
   - After clicking **Install Later**, the **Plug-in Manager** screen appears.

     Install the plug-in program by clicking the **Install** button located in the plug-in program's section on the **Plug-in Manager** screen.

   The **Trend Micro End User License Agreement** screen appears.

   Note

   Not all plug-in programs require this screen. If this screen does not appear, the plug-in program installation begins.

4. Click **Agree** to install the plug-in program.

   Monitor the progress or navigate away from the screen during the installation.

   Note

   If Apex One encounters problems downloading or installing the package, check the server update logs on the Apex One web console. On the main menu, click **Logs** > **Server Updates**.

After the installation, the current plug-in program version displays on the **Plug-in Manager** screen.

Activating the Plug-in Program License

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.

   The **Product License New Activation Code** screen appears.
3. Type or copy-and-paste the Activation Code into the text fields.
4. Click **Save**.

   The plug-in console appears.

Viewing and Renewing the License Information

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.
3. Navigate the plug-in console to the **View License Information** hyperlink.

   Not all plug-in programs display the **View License Information** hyperlink in the same location. Refer to the plug-in program's user documentation for more details.
4. View the following license details in the screen that opens.

Option	Description
Status	Displays either "Activated", "Not Activated" or "Expired"
Version	Displays either "Full" or "Trial" version

Option	Description
	Note Activation of both the full and trial versions displays only as "Full".
Seats	Displays how many endpoints the plug-in program can manage
License expires on	If the plug-in program has multiple licenses, the latest expiration date displays. For example, if the license expiration dates are 12/31/2011 and 06/30/2011, 12/31/2011 displays.
Activation Code	Displays the Activation Code
Reminders	Depending on the current license version, the plug-in displays reminders about the license expiration date either during the grace period (full versions only), or when the license expires

Note

The duration of the grace period varies by region. Verify the grace period of a plug-in program with a Trend Micro representative.

After a plug-in program license expires, the plug-in continues to function but updates and support are no longer available.

5. Click **View detailed license online** to view information about the current license on the Trend Micro website.
6. To update the screen with the latest license information, click **Update Information**.
7. Click **New Activation Code** to open the **Product License New Activation Code** screen.

   For details, see *Activating the Plug-in Program License on page 3-4*.

Plug-in Program Management

Configure settings and perform program-related tasks from the plug-in program's management console, which is accessible from the Apex One web console. Tasks include activating the program and possibly deploying the plug-in program agent to endpoints. Consult the documentation for the specific plug-in program for details on configuring and managing the program.

Managing Plug-in Programs

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.

   When managing the plug-in program for the first time, the plug-in program may require activation. For details, see *Activating the Plug-in Program License on page 3-4*.

Plug-in Program Upgrades

A new version of an installed plug-in program displays on the Plug-in Manager console. Download the package and upgrade the plug-in program on the console. Plug-in Manager downloads the package from the Trend Micro ActiveUpdate server or a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-in Manager downloads an installation package or starts an upgrade, Plug-in Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-in Manager does not support plug-in program upgrading using the Trend Micro Apex Central single sign-on function.

Upgrading Plug-in Programs

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Download**.

   The size of the upgrade package displays beside the **Download** button.

   Monitor the progress or navigate away from the screen during the download.

   Note

   If Apex One encounters problems downloading or installing the package, check the server update logs on the Apex One web console. On the main menu, click **Logs** > **Server Updates**.
3. After Plug-in Manager downloads the package, a new screen displays.
4. Click **Upgrade Now** or **Upgrade Later**.
   - After clicking **Upgrade Now**, the upgrade begins and an upgrade progress screen appears.
   - After clicking **Upgrade Later**, the **Plug-in Manager** screen appears.

     Upgrade the plug-in program by clicking the **Upgrade** button located in the plug-in program's section on the **Plug-in Manager** screen.

After the upgrade, the Plug-in Manager service may need to restart, causing the **Plug-in Manager** screen to be temporarily unavailable. When the screen becomes available, the current plug-in program version displays.

Plug-in Program Uninstallation

Uninstall a plug-in program in the following ways:

- Uninstall the plug-in program from the Plug-in Manager console.
- Uninstall the Apex One server, which uninstalls Plug-in Manager and all installed plug-in programs. For instructions on uninstalling the Apex One server, see the *Apex One Installation and Upgrade Guide*.

For plug-in programs with agents on the endpoint:

- Consult the documentation for the plug-in program to see if uninstalling the plug-in program also uninstalls the plug-in agent.
- For plug-in agents installed on the same endpoint as the Security Agent, uninstalling the Security Agent uninstalls the plug-in agents and the Security Agent Plug-in Manager (`CNTAoSMgr.exe`).

Uninstalling Plug-in Programs from the Plug-in Manager Console

Procedure

1. Open the Apex One web console and click **Plug-ins** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Uninstall**.
3. Monitor the uninstallation progress or navigate away from the screen during the uninstallation.
4. Refresh the **Plug-in Manager** screen after the uninstallation.

   The plug-in program is again available for installation.

Uninstalling Plug-in Manager

Uninstall the Apex One server to uninstall Plug-in Manager and all installed plug-in programs. For instructions on uninstalling the Apex One server, see the *Apex One Installation and Upgrade Guide*.

Troubleshooting Plug-in Manager

Check the Apex One server and Security Agent debug logs for Plug-in Manager and plug-in program debug information.

Plug-in Program Does not Display on the Plug-in Manager Console

Any plug-in program available for download and installation may not display on the Plug-in Manager console for the following reasons:

Procedure

1. Plug-in Manager is still downloading the plug-in program, which may take some time if the program package size is large. Check the screen from time to time to see if the plug-in program displays.

   Note

   If Plug-in Manager is unable to download the plug-in program, it automatically re-downloads after 24 hours. To manually trigger Plug-in Manager to download the plug-in program, restart the Apex One Plug-in Manager service.

2. The server computer cannot connect to the Internet. If the server connects to the Internet through a proxy server, ensure that Internet connection can be established using the proxy settings.

3. The Apex One update source is not the ActiveUpdate server. On the Apex One web console, go to **Updates** > **Server** > **Update Source** and check the

update source. If the update source is not the ActiveUpdate server, you have the following options:

- Select the ActiveUpdate server as the update source.
- If you select **Other Update Source**, select the first entry in the **Other update source** list as update source and verify that it can successfully connect to the ActiveUpdate server. Plug-in Manager only supports the first entry in the list.
- If you select **Intranet location containing a copy of the current file**, ensure the endpoint in the Intranet can also connect to the ActiveUpdate server.

Plug-in Agent Installation and Display Issues on Endpoints

Installation of the plug-in program's agent on the endpoint may fail or the agent may not display in the Security Agent console for the following reasons:

Procedure

1. Plug-in Manager (`CNTAosMgr.exe`) on the endpoint is not running. In the Security Agent endpoint, open Windows Task Manager and run the `CNTAosMgr.exe` process.
2. The installation package for the plug-in agent was not downloaded to the Security Agent endpoint folder located in `<Agent installation folder>\AU_Data\AU_Temp\{xxx}AU_Down\Product`. Check `Tmudump.txt` located in `\AU_Data\AU_Log\` for the download failure reasons.

   Note

   If an agent successfully installs, agent information is available in `<Agent installation folder>\AOSSvcInfo.xml`.

3. The agent installation was unsuccessful or requires further action. You can check the installation status from the plug-in program's

management console and perform actions such as restarting the Security Agent endpoint after installation or installing required operating system patches before installation.

Agents on the Endpoints Cannot be Launched if the Automatic Configuration Script Setting on Internet Explorer Redirects to a Proxy Server

The Security Agent Plug-in Manager (`CNTAosMgr.exe`) is unable to launch agents on endpoints because the agent launch command redirects to a proxy server. This problem only occurs if the proxy setting redirects the user's HTTP traffic to 127.0.0.1.

To resolve this issue, use a well-defined proxy server policy. For example, do not reroute HTTP traffic to 127.0.0.1.

If you need to use the proxy configuration that controls the 127.0.0.1 HTTP requests, perform the following tasks.

Procedure

1. Configure Apex One firewall settings on the Apex One web console.

   Note

   Perform this step only if you enable the Apex One firewall on Security Agents.

   a. On the web console, go to **Agents** > **Firewall** > **Policies** and click **Edit Exception Template**.

   b. On the Edit Exception Template screen, click **Add**.

   c. Use the following information:

      - **Name**: Your preferred name

- **Action**: Allow network traffic
- **Direction**: Inbound
- **Protocol**: TCP
- **Port(s)**: Any port number between 5000 and 49151

d. **IP address(es)**: Select **Single IP address** and specify your proxy server's IP address (recommended) or select **All IP addresses**.

e. Click **Save**.

f. Back on the Edit Exception Template screen, click **Save and Apply to Existing Policies**.

g. Go to **Agents** > **Firewall** > **Profiles** and click **Assign Profile to Agents**.

If there is no firewall profile, create one by clicking Add. Use the following settings:

- **Name**: Your preferred name
- **Description**: Your preferred description
- **Policy**: All Access Policy

After saving the new profile, click **Assign Profile to Agents**.

2. Modify the `ofcscan.ini` file.

a. Open the `ofcscan.ini` file in `<Server installation folder>` using a text editor.

b. Search for **`[Global Setting]`** and add `FWPortNum=21212` to the next line. Change "21212" to the port number you specified in step c above.

For example:

```
[Global Setting]

FWPortNum=5000
```

c. Save the file.

3. On the web console, go to **Agents** > **Global Agent Settings** and click **Save**.

An Error in the System, Update Module, or Plug-in Manager Program occurred and the Error Message Provides a Certain Error Code

Plug-in Manager displays any of the following error codes in an error message. If you are unable to troubleshoot a problem after referring to the solutions provided in the table below, contact your support provider.

TABLE 17-1. Plug-in Manager Error Codes

ERROR CODE	MESSAGE, CAUSE, AND SOLUTION
001	An error in the Plug-in Manager program occurred. The Plug-in Manager update module does not respond when querying the progress of an update task. The module or command handler may not have been not initialized. Restart the Apex One Plug-in Manager service and perform the task again.
002	A system error occurred. The Plug-in Manager update module is unable to open the registry key `SOFTWARE\TrendMicro\OfficeScan\service\AoS` because it may have been deleted. Perform the following steps: 1. Open Registry Editor and go to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`. Reset the value to 1.0.1000. 2. Restart the Apex One Plug-in Manager service. 3. Download/Uninstall the plug-in program.

Error Code	Message, Cause, and Solution
028	An update error occurred. Possible causes: • Plug-in Manager update module was unable to download a plug-in program. Verify that the network connection is functional, and then try again. • Plug-in Manager update module cannot install the plug-in program because the AU patch agent has returned an error. The AU patch agent is the program that launches installation of new plug-in programs. For the exact cause of the error, check the ActiveUpdate module debug log "`TmuDump.txt`" in `\PCCSRV\Web\Service\AU_Data\AU_Log`. Perform the following steps: 1. Open Registry Editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`. Reset the value to 1.0.1000. 2. Delete the plug-in program registry key `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_ADDON_xxxx`. 3. Restart the Apex One Plug-in Manager service. 4. Download and install the plug-in program.
170	A system error occurred. Plug-in Manager update module cannot process an incoming operation because it is currently handling another operation. Perform the task at a later time.
202	An error in the Plug-in Manager program occurred. The Plug-in Manager program cannot handle the task being executed on the web console. Refresh the web console or upgrade Plug-in Manager if an upgrade to the program is available.

Error Code	Message, Cause, and Solution
203	An error in the Plug-in Manager program occurred. The Plug-in Manager program encountered an interprocess communication (IPC) error when attempting to communicate with Plug-in Manager backend services. Restart the Apex One Plug-in Manager service and perform the task again.
Other error codes	A system error occurred. When downloading a new plug-in program, Plug-in Manager checks the plug-in program list from the ActiveUpdate server. Plug-in Manager was unable to obtain the list. Perform the following steps: 1. Open Registry Editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`. Reset the value to `1.0.1000`. 2. Restart the Apex One Plug-in Manager service. 3. Download and install the plug-in program.

Chapter 18

Troubleshooting Resources

This chapter provides a list of resources you can use to troubleshoot Apex One server and Security Agent issues.

Topics include:

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 Apex One server GUID ensures that Trend Micro can provide feedback regarding the files sent for assessment.

Case Diagnostic Tool

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

Run the tool on all platforms that Apex One supports. To obtain this tool and relevant documentation, contact your support provider.

Trend Micro Performance Tuning Tool

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

Note

Performance issues are often due to a more complex problem. If you are unable to determine the root cause of your performance decrease, contact your support provider.

Apex One Server Logs

Aside from logs available on the web console, you can use other types of logs (such as debug logs) to troubleshoot product issues.

WARNING!

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

Server Debug Logs Using LogServer.exe

Use `LogServer.exe` to collect debug logs for the following:

- Apex One server basic logs
- Trend Micro Vulnerability Scanner
- Active Directory integration logs
- Agent grouping logs
- Security compliance logs
- Role-based administration
- Smart scan

Debug Logging

Apex One automatically collects debug logs related to “Error” events. If you attempt to disable the collection of debug logs, Apex One automatically restarts the collection of “Error” logs.

Procedure

1. Log on to the web console.
2. On the banner of the web console, click the "T" in "Trend Micro Apex One".
3. Select **Enable debug log**.

   Note

   If you attempt to disable the collection of debug logs, Apex One automatically restarts the collection of “Error” logs.

4. Specify debug log settings.

   Note

   Apex One automatically collects debug logs related to “Error” events. If you attempt to disable the collection of debug logs, Apex One automatically restarts the collection of “Error” logs.

5. Click **Save**.
6. Check the log file (`ofcdebug.log`) in the default location: <*Server installation folder*>`\PCCSRV\Log`.

Enabling Debug Logging for Server Installation and Upgrade

Enable debug logging before performing the following tasks:

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

Procedure

1. Copy the `LogServer` folder located in <*Server installation folder*>`\PCCSRV\Private` to `C:\`.
2. Create a file named ofcdebug`.ini` with the following content:

   ```
   [debug]

   debuglevel=9

   debuglog=c:\LogServer\ofcdebug.log

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
   ```

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

Installation Logs

- Local Installation/Upgrade Logs

  File name: `OFCMAS.LOG`

  Location: `%windir%`

Active Directory Logs

- File name: `ofcdebug.log`

- File name: `ofcserver.ini`

  Location: <*Server installation folder*>`\PCCSRV\Private\`

Role-based Administration Logs

To get detailed role-based administration information, do one of the following:

- Run the Trend Micro Case Diagnostics Tool. For information, see *Case Diagnostic Tool on page 18-2*.
- Gather the following logs:
  - All files in the <*Server installation folder*>`\PCCSRV\Private\AuthorStore` folder.
  - *Apex One Server Logs on page 18-3*

Security Agent Grouping Logs

- File name: `ofcdebug.log`
- File name: `ofcserver.ini`

  Location: <*Server installation folder*>`\PCCSRV\Private\`
- File name: `SortingRule.xml`

  Location: `<Server installation folder>\PCCSRV\Private\SortingRuleStore\`

Component Update Logs

File name: `TmuDump.txt`

Location: <*Server installation folder*>`\PCCSRV\Web\Service\AU_Data\AU_Log`

Getting Detailed Server Update Information

Procedure

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

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. Save the file to <*Server installation folder*>`\PCCSRV\Web\Service`.

3. Restart the Apex One Master Service.

Stopping the Collection of Detailed Server Update Information

Procedure

1. Delete `aucfg.ini`.

2. Restart the Apex One Master Service.

Agent Packager Logs

Enabling Logging for Agent Packager Creation

Procedure

1. Modify `ClnExtor.ini` in <*Server installation folder*>`\PCCSRV\Admin\Utility\ClientPackager` as follows:

   ```
   [Common]
   ```

```
DebugMode=1
```

2. Check `ClnPack.log` in `C:\`.

Disabling Logging for Agent Packager Creation

Procedure

1. Open `ClnExtor.ini`.
2. Change the "DebugMode" value from 1 to 0.

Security Compliance Report Logs

To get detailed Security Compliance information, gather the following:

- File name: `RBAUserProfile.ini`

  Location: <*Server installation folder*>`\PCCSRV\Private\AuthorStore\`

- All files in the `<Server installation folder>\PCCSRV\Log\Security Compliance Report` folder.
- *Apex One Server Logs on page 18-3*

Outside Server Management Logs

- File name: `ofcdebug.log`
- File name: `ofcserver.ini`

  Location: <*Server installation folder*>`\PCCSRV\Private\`
- All files in the `<Server installation folder>\PCCSRV\Log\Outside Server Management Report\` folder.

Device Control Exception Logs

To get detailed Device Control Exception information, gather the following:

- File name: `ofcscan.ini`

  Location: <*Server installation folder*>\

- Device Control Exception List from the Apex One web console.

Integrated Smart Protection Server Web Reputation Logs

File name: `diagnostic.log`

Location: <*Server installation folder*>\PCCSRV\LWCS\

ServerProtect Normal Server Migration Tool Logs

To enable debug logging for ServerProtect Normal Server Migration Tool:

Procedure

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

   ```
   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9
   ```

2. Save the file to `C:\`.
3. Check `ofcdebug.log` in `C:\`.

Note

To disable debug logging, delete the `ofcdebug.ini` file.

VSEncrypt Logs

Apex One automatically creates the debug log (`VSEncrypt.log`) in the user account's temporary folder. For example, `C:\Documents and Settings \<User name>\Local Settings\Temp`.

Apex Central MCP Agent Logs

Debug Files on the <*Server installation folder*>`\PCCSRV\CMAgent` folder

- `Agent.ini`
- `Product.ini`
- The screen shot of the Apex Central Settings page
- `ProductUI.zip`

Enabling Debug Logging for the MCP Agent

Procedure

1. Modify `product.ini` in <*Server installation folder*>`\PCCSRV\CmAgent` as follows:

```
[Debug]

debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Restart the Apex One Apex Central Agent service from Microsoft Management Console.

3. Check `CMAgent_debug.log` in `C:\`.

Disabling Debug Logging for the MCP Agent

Procedure

1. Open `product.ini` and delete the following:

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Restart the Apex One Apex Central Agent service.

Outbreak Logs

Log Type	File
Current Firewall Violation Outbreak Logs	File name: `Cfw_Outbreak_Current.log` Location: <*Server installation folder*>`\PCCSRV\Log\`
Last Firewall Violation Outbreak Logs	File name: `Cfw_Outbreak_Last.log` Location: <*Server installation folder*>`\PCCSRV\Log\`
Current Virus /Malware Outbreak Logs	File name: `Outbreak_Current.log` Location: <*Server installation folder*>`\PCCSRV\Log\`
Last Virus /Malware Outbreak Logs	File name: `Outbreak_Last.log` Location: <*Server installation folder*>`\PCCSRV\Log\`

Log Type	File
Current Spyware/Grayware Outbreak Logs	File name: `Spyware_Outbreak_Current.log` Location: <*Server installation folder*>`\PCCSRV\Log\`
Last Spyware/Grayware Outbreak Logs	File name: `Spyware_Outbreak_Last.log` Location: <*Server installation folder*>`\PCCSRV\Log\`

Virtual Desktop Support Logs

- File name: `vdi_list.ini`

  Location: <*Server installation folder*>`\PCCSRV\TEMP\`

- File name: `vdi.ini`

  Location: `<Server installation folder>\PCCSRV\Private\`

- File name: `ofcdebug.txt`

  Location: `<Server installation folder>\PCCSRV\Log`

To generate `ofcdebug.txt`, enable debug logging. For instructions on enabling debug logging, see *Debug Logging on page 18-3*.

Security Agent Logs

Use Security Agent logs (such as debug logs) to troubleshoot Security Agent issues.

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.

Security Agent Debug Logs Using LogServer.exe

To enabling debug logging for 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 users, instructing them to save the file to `C:\`.

   Note

   `LogServer.exe` automatically runs each time the Security Agent endpoint starts. 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 <*Agent installation folder*>.

3. For each Security Agent endpoint, check ofcdebug.log in C:\.

Note

Disable debug logging for the Security Agent by deleting `ofcdebug.ini`.

Fresh Installation Logs

For MSI package installations:

- File name: `OFCNT.LOG`
- Location: In a temporary system file, for example in Windows 7:

  `C:\Users\Administrator\AppData\Local\Trend Micro\Security Agent\OFCNT.LOG`

For web installations:

- File name: `WebInstall.log`
- Location: `C:\`

For remote installations:

- File name: `RemoteInstall.LOG`
- Location: `C:\`

For Autopcc and EXE package installations:

- File name: `OFCNT.LOG`
- Location: `%windir%\`

Upgrade/Hot Fix Logs

File name: `upgrade_yyyymmddhhmmss.log`

Location: <*Agent installation folder*>`\Temp`

Damage Cleanup Services Logs

Enabling Debug Logging for Damage Cleanup Services

Procedure

1. Open `TSC.ini` in <*Agent installation folder*>.
2. Modify the following line as follows:

   `DebugInfoLevel=5`
3. Check `TSCDebug.log` in `<Agent installation folder>\debug`.

Disabling Debug Logging for Damage Cleanup Services

Open `TSC.ini` and change the "`DebugInfoLevel`" value from 5 to 0.

Cleanup Log

File name: `yyyymmdd.log`

Location: <*Agent installation folder*>`\report\`

Mail Scan Logs

File name: `SmolDbg.txt`

Location: <*Agent installation folder*>

Security Agent Connection Logs

File name: `Conn_YYYYMMDD.log`

Location: <*Agent installation folder*>`\ConnLog`

Security Agent Update Logs

File name: `Tmudump.txt`

Location: <*Agent installation folder*>`\AU_Data\AU_Log`

Getting Detailed Security Agent Update Information

Procedure

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

   ```
   [Debug]
   level=-1
   [Downloader]
   ProxyCache=0
   ```

2. Save the file to <*Agent installation folder*>.
3. Reload the Security Agent.

Note

Stop collecting detailed agent update information by deleting the `aucfg.ini` file and reloading the Security Agent.

Virus Scan Engine Logs

To enable debug logging for the Virus Scan Engine:

Procedure

1. Open Registry Editor (`regedit.exe`).
2. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`.

3. Change the value of "DebugLogFlags" to "00003eff".
4. Perform the steps that led to the scanning issue you encountered.
5. Check TMFilter.log in %windir%.

Note

Disable debug logging by restoring the value of "DebugLogFlags" to "00000000".

Outbreak Prevention Logs

File name: OPPLogs.log

Location: <*Agent installation folder*>\OppLog

Outbreak Prevention Restore Logs

File names:

- TmOPP.ini
- TmOPPRestore.ini

Location: <*Agent installation folder*>\

Behavior Monitoring Debug Logs

To enable debug logging for Behavior Monitoring:

Procedure

1. Open Registry Editor (regedit.exe).
2. Go to HKLM\SOFTWARE\TrendMicro\Aegis.

3. Add the key "`DebugLogFlags`" as "`dword:00000032`".
4. Perform the steps that led to the issue you encountered.
5. Check the following logs in the `C:\Program Files (x86)\Trend Micro \BM\log\` folder:
   - `TmCommengyyyymmdd_nn.log`
   - `TMPEMyyyymmdd_nn.log`

Apex One Firewall Logs

Enabling Debug Logging for the Common Firewall Driver (all operating systems)

Procedure

1. Modify the following registry values:

Registry Key	Values
`HKEY_LOCAL_MACHINE\System\CurrentControlSet \Services\tmwfp\Parameters`	Type: `DWORD` value `(REG_DWORD)` Name: `DebugCtrl` Value: `0x00001111`
`HKEY_LOCAL_MACHINE\System\CurrentControlSet \Services\tmlwf\Parameters`	Type: `DWORD` value `(REG_DWORD)` Name: `DebugCtrl` Value: `0x00001111`

2. Restart the endpoint.
3. Check `wfp_log.txt` and `lwf_log.txt` in `C:\`.

Disabling Debug Logging for the Common Firewall Driver (all operating systems)

Procedure

1. Delete "`DebugCtrl`" in the registry key.
2. Restart the endpoint.

Enabling Debug Logging for the Apex One NT Firewall Service

Procedure

1. Edit `TmPfw.ini` located in <*Agent installation folder*> as follows:

   ```
   [ServiceSession]

   Enable=1
   ```

2. Reload the Security Agent.
3. Check `ddmmyyyy_NSC_TmPfw.log` in `C:\temp`.

Disabling Debug Logging for the Apex One NT Firewall Service

Procedure

1. Open `TmPfw.ini` and change the "`Enable`" value from 1 to 0.
2. Reload the Security Agent.

Web Reputation and POP3 Mail Scan Logs

Enabling Debug Logging for the Web Reputation and POP3 Mail Scan Features

Procedure

1. Edit `TmOsprey.ini` located in <*Agent installation folder*> as follows:

   ```
   [InteractiveSession]
   Enable=1
   LogFolder=C:\temp
   [ServiceSession]
   Enable=1
   LogFolder=C:\temp
   ```

2. Reload the Security Agent.
3. Check the `yyyy-mm-dd_hh-mm-ss_EE_TmOsprey1.etl` in `C:\temp`.

Disabling Debug Logging for the Web Reputation and POP3 Mail Scan Features

Procedure

1. Edit `TmOsprey.ini` located in <*Agent installation folder*> as follows:

   ```
   [InteractiveSession]
   Enable=0
   LogFolder=C:\temp
   [ServiceSession]
   ```

```
Enable=0

LogFolder=C:\temp
```

2. Reload the Security Agent.

Device Control Exception List Logs

File name: `DAC_ELIST`

Location: <*Agent installation folder*>\

Note

In order to access the encrypted log data, contact your support representative.

Data Protection Debug Logs

To enable Data Protection debug logs:

Procedure

1. Obtain the `logger.cfg` file from your support provider.
2. Add the following data in `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`:
   - Type: `String`
   - Name: `debugcfg`
   - Value: `C:\Log\logger.cfg`
3. Create a folder named "Log" in the `C:\ directory`.
4. Copy `logger.cfg` to the `Log` folder.
5. Deploy Data Loss Prevention and Device Control settings from the web console to start collecting logs.

Note

Disable debug logging for the Data Protection module by deleting `debugcfg` in the registry key and restarting the endpoint.

Windows Event Logs

Windows Event Viewer records successful application events such as logging on or changing account settings.

Procedure

1. Do one of the following:
   - Click **Start** > **Control Panel** > **Performance and Maintenance** > **Administrative Tools** > **Computer Management**.
   - Open the MMC containing the Event Viewer snap-in.
2. Click **Event Viewer**.

Transport Driver Interface (TDI) Logs

To enable Transport Driver Interface (TDI) logs:

Procedure

1. Add the following data in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters`:

Parameter	Values
Key 1	Type: `DWORD` value `(REG_DWORD)` Name: `Debug` Value: `1111 (Hexadecimal)`

PARAMETER	VALUES
Key 2	Type: `String value (REG_SZ)` Name: `LogFile` Value: `C:\tmtdi.log`

2. Restart the endpoint.
3. Check `tmtdi.log` in `C:\`.

Note

Disable debug logging for TDI by deleting `Debug` and `LogFile` in the registry key and restarting the endpoint.

Chapter 19

Technical Support

Learn about the following topics:

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://www.ers.trendmicro.com/

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

Appendices

Appendices

Appendix A

IPv6 Support in Apex One

This appendix is required reading for users who plan to deploy Apex One in an environment that supports IPv6 addressing. This appendix contains information on the extent of IPv6 support in Apex One.

Trend Micro assumes that the reader is familiar with IPv6 concepts and the tasks involved in setting up a network that supports IPv6 addressing.

IPv6 Support for Apex One Server and Agents

IPv6 support is automatically enabled after installing or upgrading the Apex One server and Security Agents that satisfy the IPv6 requirements.

Apex One Server Requirements

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

- If the server will manage IPv4 and IPv6 Security Agents, it must have both IPv4 and IPv6 addresses and must be identified by its host name. If a server is identified by its IPv4 address, IPv6 Security Agents cannot connect to the server. The same issue occurs if pure IPv4 agents connect to a server identified by its IPv6 address.
- If the server will manage only IPv6 agents, the minimum requirement is an IPv6 address. The server can be identified by its host name or IPv6 address. When the server is identified by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.

Note

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

Pure IPv6 Server Limitations

The following table lists the limitations when the Apex One server only has an IPv6 address.

TABLE A-1. Pure IPv6 Server Limitations

ITEM	LIMITATION
Agent management	A pure IPv6 server cannot: • Deploy Security Agents to pure IPv4 endpoints. • Manage pure IPv4 Security Agents.
Updates and centralized management	A pure IPv6 server cannot update from pure IPv4 update sources, such as: • Trend Micro ActiveUpdate Server • Any pure IPv4 custom update source
Product registration, activation, and renewal	A pure IPv6 server cannot connect to the Trend Micro Online Registration Server to register the product, obtain the license, and activate/renew the license.
Proxy connection	A pure IPv6 server cannot connect through a pure IPv4 proxy server.
Plug-in solutions	A pure IPv6 server will have Plug-in Manager but will not be able to deploy any of the plug-in solutions to: • Pure IPv4 Security Agents or pure IPv4 hosts (because of the absence of a direct connection) • Pure IPv6 Security Agents or pure IPv6 hosts because none of the plug-in solutions support IPv6.

Most of these limitations can be overcome by setting up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the Apex One server and the entities to which it connects or the entities that it serves.

Pure IPv6 Security Agent Limitations

The following table lists the limitations when the Security Agent only has an IPv6 address.

TABLE A-2. Pure IPv6 Security Agent Limitations

ITEM	LIMITATION
Parent Apex One server	Pure IPv6 Security Agents cannot be managed by a pure IPv4 Apex One server.
Updates	A pure IPv6 Security Agent cannot update from pure IPv4 update sources, such as: • Trend Micro ActiveUpdate Server • A pure IPv4 Apex One server • A pure IPv4 Update Agent • Any pure IPv4 custom update source
Scan queries, web reputation queries, and Smart Feedback	A pure IPv6 Security Agent cannot send queries to smart protection sources, such as: • Trend Micro Smart Protection Network (also for Smart Feedback)
Software safety	Pure IPv6 Security Agents cannot connect to the Trend Micro-hosted Certified Safe Software Service.
Plug-in solutions	Pure IPv6 Security Agents cannot install plug-in solutions because none of the plug-in solutions support IPv6.
Proxy connection	A pure IPv6 Security Agent cannot connect through a pure IPv4 proxy server.

Most of these limitations can be overcome by setting up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the Security Agents and the entities to which they connect.

Configuring IPv6 Addresses

The web console allows you to configure an IPv6 address or an IPv6 address range. The following are some configuration guidelines.

- Apex One accepts standard IPv6 address presentations.

  For example:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- Apex One also accepts link-local IPv6 addresses, such as:

  `fe80::210:5aff:feaa:20a2`

  WARNING!

  Exercise caution when specifying a link-local IPv6 address because even though Apex One can accept the address, it might not work as expected under certain circumstances. For example, Security Agents cannot update from an update source if the source is on another network segment and is identified by its link-local IPv6 address.

- When the IPv6 address is part of a URL, enclose the address in square brackets ([]).

- For IPv6 address ranges, a prefix and prefix length are usually required. For configurations that require the server to query IP addresses, prefix length restrictions apply to prevent performance issues that may occur when the server queries a significant number of IP addresses. For example, for the Outside Server Management feature, the prefix length can only be between 112 (65,536 IP addresses) and 128 (2 IP addresses).

- Some settings that involve IPv6 addresses or address ranges will be deployed to Security Agents but Security Agents will ignore them. For example, if you configured the smart protection source list and included a Smart Protection Server identified by its IPv6 address, pure IPv4 Security Agents will ignore the server and connect to the other smart protection sources.

Screens That Display IP Addresses

This topic enumerates places in the web console where IP addresses are shown.

Location	Description
Agent Tree	Whenever the agent tree displays, the IPv6 addresses of pure IPv6 Security Agents display under the **IP address** column. For dual-stack Security Agents, their IPv6 addresses display if they used their IPv6 address to register to the server. **Note** The IP address that dual-stack Security Agents use when registering to the server can be controlled from **Agents** > **Global Agent Settings > Network** > **Preferred IP Address**. When you export agent tree settings to a file, the IPv6 addresses also display in the exported file.
Agent Status	Detailed agent information is available when you go to **Agents** > **Agent Management > Status**. In this screen, you will see the IPv6 addresses of pure IPv6 Security Agents and dual-stack Security Agents that used their IPv6 addresses to register to the server.
Logs	The IPv6 addresses of dual-stack and pure IPv6 Security Agents display on the following logs: • Virus/Malware logs • Spyware/Grayware logs • Firewall logs • Connection verification logs

Location	Description
Apex Central Console	The following lists which of the Apex One server and Security Agents' IP addresses display on the Apex Central console. • Dual-stack server: IPv4 and IPv6 • Pure IPv4 server: IPv4 • Pure IPv6 server: IPv6 • Dual-stack Security Agent: The IP address used when the Security Agent registered to the Apex One server • Pure IPv4 Security Agent: IPv4 • Pure IPv6 Security Agent: IPv6

Appendix B

Windows Server Core Support

This appendix discusses Apex One support for Windows Server Core.

Windows Server Core Support

Windows Server Core is a "minimal" installation of a Windows Server version. In a Server Core:

- Many of the Windows Server options and features are removed.
- The server runs a much thinner core operating system.
- Tasks are performed mostly from the command line interface.
- The operating system runs fewer services and requires less resources during startup.

Apex One supports Security Agent installations on the following Windows Server Core versions:

- Windows Server Core 2008 R2
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016
- Windows Server Core 2019

The Security Agent supports Server Core. This section contains information on the extent of support for Server Core.

The Apex One server does not support Server Core.

Installation Methods for Windows Server Core

The following installation methods are not or are partially supported:

- Web install page: This method is not supported because Server Core does not support web browsers.

- Trend Micro Vulnerability Scanner: The Vulnerability Scanner tool cannot be run locally on the Server Core. Run the tool from the Apex One server or another endpoint.

The following installation methods are supported:

- Remote installation. For details, see *Installing Remotely from the Apex One Web Console on page 5-15*.
- Login Script Setup
- Agent Packager

Installing the Security Agent Using Login Script Setup

Procedure

1. On the target endpoint, open a command prompt.
2. Map the location of `AutoPcc.exe` file on the Apex One server by typing the following command:

   ```
   net use <mapped drive letter> \\<Apex One server host name or IP address>\ofcscan
   ```

   For example:

   ```
   net use P: \\10.1.1.1\ofcscan
   ```

3. Provide the user name and password for the target server.

   A message appears, informing you if the location of `AutoPcc.exe` was mapped successfully.

4. Change to the location of `AutoPcc.exe` by typing the mapped drive letter and a colon. For example:

   ```
   P:
   ```

5. Type the following to launch the installation:

   ```
   AutoPcc.exe
   ```

A new command prompt appears once the installation completes.

Installing the Security Agent Using the Security Agent Package

Procedure

1. Create the package.

   For details, see *Installing with Agent Packager on page 5-19*.

2. Open a command prompt.

3. Map the location of the Security Agent package by typing the following command:

   ```
   net use <mapped drive letter> \\<Location of the agent package>
   ```

   For example:

   ```
   net use P: \\10.1.1.1\Package
   ```

   A message appears, informing you if the location of the Security Agent package was mapped successfully.

4. Change to the location of the Security Agent package by typing the mapped drive letter and a colon. For example:

   ```
   P:
   ```

5. Copy the Security Agent package to a local directory on the Server Core endpoint by typing the following command:

   ```
   copy <package file name> <directory on the Server Core endpoint where you want to copy the package>
   ```

   For example:

   ```
   copy securityagent.msi C:\Agent Package
   ```

   A message appears, informing you if the Security Agent package was copied successfully.

6. Change to the local directory. For example:

   ```
   C:
   ```

   ```
   cd C:\Agent Package
   ```

7. Type the package file name to launch the installation. For example:

   ```
   securityagent.msi
   ```

   The following shows the commands and results on the command prompt from the example.

   ```
   C:\WINDOWS>net use P: \\10.1.1.1\Package
   C:\Windows>P:
   P:\>copy securityagent.msi C:\Agent Package
           1 file(s) copied.
   P:\>C:
   C:\WINDOWS>cd C:\Agent Package
   C:\Agent Package>securityagent.msi
   ```

Security Agent Features on Windows Server Core

Most Security Agent features available on supported Windows Server version work on Server Core. The only feature that is not supported is Independent mode.

For a list of features available on Windows Server, see *Security Agent Features on page 5-3*.

The Security Agent console is only accessible from the command line interface.

Note

Some Security Agent console screens include a Help button, which, when clicked, opens context-sensitive, HTML-based Help. Because Windows Server Core lacks a browser, the Help will not be available to the user. To view the Help, the user must install a browser.

Windows Server Core Commands

Perform Security Agent tasks by issuing commands from the command line interface.

To run the commands, go to the location of `PccNTMon.exe`. This process is responsible for starting the Security Agent console. This process is found under the <*Agent installation folder*>.

The following table lists the available commands.

TABLE B-1. Windows Server Core Commands

COMMAND	ACTION
`pccnt <drive or folder path>`	Scans the specified drive or folder for security risks Guidelines: • If the folder path contains a space, enclose the entire path in quotes. • Scanning of individual files is not supported. Correct commands: • `pccnt C:\` • `pccnt D:\Files` • `pccnt "C:\Documents and Settings"` Incorrect commands: • `pccnt C:\Documents and Settings` • `pccnt D:\Files\example.doc`
`pccntmon -r`	Opens Real-time Monitor
`pccntmon -v`	Lists the agent components and their versions
`pccntmon -u`	Updates the Security Agent components

COMMAND	ACTION
`pccntmon -n <unload_password>`	Unloads the Security Agent To reload the Security Agent, type the following command: `pccntmon`
`pccntmon -m <uninstall_password>`	Uninstalls the Security Agent

`pccntmon -c`	Shows the following information in the command line:
	• Scan method
	  • Smart scan
	  • Conventional scan
	• Pattern status
	  • Updated
	  • Outdated
	• Real-time scan service
	  • Functional
	  • Disabled or Not Functional
	• Agent connection status
	  • Online
	  • Independent
	  • Offline
	• Web Reputation Services
	  • Available
	  • Reconnecting
	• File Reputation Services
	  • Available
	  • Reconnecting

COMMAND	ACTION
`pccntmon -h`	Shows all the available commands

Appendix C

Apex One Rollback

This appendix discusses Apex One server and agent rollback support.

Rolling Back the Apex One Server and Security Agents Using the Server Backup Package

The Apex One rollback procedure involves rolling back Security Agents and then rolling back the Apex One server.

Important

- Administrators can only roll back the Apex One server and agents using the following procedure if the administrator chose to back up the server during the installation process. If the server backup files are not available, refer to the previously installed OfficeScan version's *Installation and Upgrade Guide* for manual rollback procedures.
- This version of Apex One only supports rollbacks to the following OfficeScan versions:
  - OfficeScan XG Service Pack 1
  - OfficeScan XG
  - OfficeScan 11.0 Service Pack 1 with a Critical Patch
  - OfficeScan 11.0 Service Pack 1
  - OfficeScan 11.0

Rolling Back the Security Agents

Apex One can only rollback Security Agents to the same version of the server being restored. You cannot rollback Security Agents to an older version than the server.

Important

Ensure that you roll back Security Agents before rolling back the Apex One server.

Procedure

1. Ensure that Security Agents cannot upgrade the agent program.

   a. On the Apex One 2019 web console, go to **Agents** > **Agent Management**.

   b. Select the Security Agents to be rolled back.

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

   d. In the **Security Agents only update the following components** drop-down, select **Pattern files, engines, drivers**.

2. On the Apex One 2019 web console, go to **Updates** > **Agents** > **Update Source**.

3. Select **Customized Update Source**.

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

   A new screen opens.

5. Type the IP addresses of the Security Agents to be rolled back.

6. Type the update source URL.

   For example, type:

   ```
   http://<IP address of the Apex One server>:<port>/
   officescan/download/Rollback
   ```

7. Click **Save**.

8. Click **Notify All Agents**.

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

Tip

Administrators can speed up the rollback process by initiating a Manual Update on Security Agents. For details, see *Updating Security Agents Manually on page 6-44*.

9. After the previous Security Agent version is installed, inform the user to restart the endpoint.

   After the rollback process is complete, the Security Agent continues to report to the same Apex One server.

Note

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

Restoring the Previous OfficeScan Server Version

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

Important

Ensure that you roll back Security Agents before restoring the OfficeScan server.

Procedure

1. Uninstall the Apex One server.
2. Remove the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows \CurrentVersion\Uninstall\InstallShield Uninstall Information\OfficeScan Management Console-<server host name or IP address>`

3. Install the previous OfficeScan server version.

Tip

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

To verify the previous version of the server, go to the <*Server installation folder*> and view the restoration folder created during the Apex One server installation. The folder name (referred to as <Restore_folder_version>) is one of the following:

- OSCEXG_SP1: OfficeScan XG Service Pack 1
- OSCEXG: OfficeScan XG
- OSCE11_SP1: OfficeScan 11.0 Service Pack 1
- OSCE11: OfficeScan 11.0

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

6. Restore the OfficeScan registry.

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

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

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

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

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

      The registry file name follows this format:

      `RegBak_<Restore_folder_version>.reg`

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

7. Optionally restore the database backup schedule.

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

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

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

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

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

      The registry file name follows this format:

```
RegBak_DBBak_<Restore_folder_version>.reg
```

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

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

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

regsvr32.exe /u /s perfLWCSPerfMonMgr.dll

regsvr32.exe /s perfLWCSPerfMonMgr.dll
```

9. Restart the following services:
   - Intrusion Defense Firewall (if installed)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - Apache 2 (if using the Apache web server)
   - World Wide Web Publishing Service (if using the IIS web server)
10. Clean the Internet Explorer cache and remove ActiveX controls manually. For details on removing ActiveX controls in Internet Explorer 9, see http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9.

    The previous OfficeScan server version settings have been restored.

Tip

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

11. Optionally register the OfficeScan server to the Apex Central/Control Manager server using the web console.

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

Appendix D

Glossary

The terms contained in this glossary provide further information about commonly referenced endpoint terms, as well as Trend Micro products and technologies.

ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides up-to-date downloads of pattern files, scan engines, programs, and other Trend Micro component files through the Internet.

Compressed File

A single file containing one or more separate files plus information for extraction by a suitable program, such as WinZip.

Cookie

A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in the web browser for later use. The next time you access a website for which your browser has a cookie, the browser sends the cookie to the web server, which the web server can then use to present you with customized web pages. For example, you might enter a website that welcomes you by name.

Denial of Service Attack

A Denial of Service (DoS) attack refers to an attack on the endpoint or network that causes a loss of "service", namely a network connection. Typically, DoS attacks negatively affect network bandwidth or overload system resources such as the endpoint's memory.

DHCP

Dynamic Host control Protocol (DHCP) is a protocol for assigning dynamic IP addresses to devices in a network. With dynamic addressing, a device can

have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

DNS

Domain Name system (DNS) is a general-purpose data query service chiefly used in the Internet for translating host names into IP addresses.

When a DNS agent requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data in a machine in the current zone. Agent software in the remote server queries the resolver, which answers the request from its database files.

Domain Name

The full name of a system, consisting of its local host name and its domain name, for example, `tellsitall.com`. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).

Dynamic IP Address

A Dynamic IP address is an IP address assigned by a DHCP server. The MAC address of the endpoint will remain the same, however, the DHCP server may assign a new IP address to the endpoint depending on availability.

ESMTP

Enhanced Simple Mail Transport Protocol (ESMTP) includes security, authentication and other devices to save bandwidth and protect servers.

End User License Agreement

An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product.

Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.

False Positive

A false positive occurs when a file is incorrectly detected by security software as infected.

FTP

File Transfer Protocol (FTP) is a standard protocol used for transporting files from a server to a client over the Internet. Refer to Network Working Group RFC 959 for more information.

GeneriClean

GeneriClean, also known as referential cleaning, is a new technology for cleaning viruses/malware even without the availability of virus cleanup

components. Using a detected file as basis, GeneriClean determines if the detected file has a corresponding process/service in memory and a registry entry, and then removes them altogether.

Hot Fix

A hot fix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes do not (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).

By default, the Security Agents can install hot fixes. If you do not want Security Agents to install hot fixes, change agent update settings in the web console by going to **Agents** > **Agent Management**, click **Settings** > **Privileges and Other Settings** > **Other Settings** tab.

If you unsuccessfully attempt to deploy a hot fix on the Apex One server, use the Touch Tool to change the time stamp of the hot fix. This causes Apex One to interpret the hot fix file as new, which makes the server attempt to automatically deploy the hot fix again. For details about this tool, see *Running the Touch Tool for Security Agent Hot Fixes on page 6-52*.

HTTP

Hypertext Transfer Protocol (HTTP) is a standard protocol used for transporting web pages (including graphics and multimedia content) from a server to a client over the Internet.

HTTPS

Hypertext Transfer Protocol using Secure Socket Layer (SSL). HTTPS is a variant of HTTP used for handling secure transactions.

ICMP

Occasionally a gateway or destination host uses Internet Control Message Protocol (ICMP) to communicate with a source host, for example, to report an error in datagram processing. ICMP uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and implemented by every IP module. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.

IntelliScan

IntelliScan is a method of identifying files to scan. For executable files (for example, `.exe`), the true file type is determined based on the file content. For non-executable files (for example, `.txt`), the true file type is determined based on the file header.

Using IntelliScan provides the following benefits:

- Performance optimization: IntelliScan does not affect applications on the agent because it uses minimal system resources.
- Shorter scanning period: Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

IntelliTrap

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering the network by blocking real-time compressed executable files and

pairing them with other malware characteristics. Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files after enabling IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap.

IntelliTrap uses the following components:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

IP

"The internet protocol (IP) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)

Java File

Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets". An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet transfers its code to your endpoint and the browser's Java Virtual Machine executes the applet.

LDAP

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP.

Listening Port

A listening port is utilized for agent connection requests for data exchange.

MCP Agent

Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP replaces Trend Micro Management Infrastructure (TMI) as the way Apex Central communicates with Apex One. MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and two-way communication support
- Single sign-on (SSO) support
- Cluster node support

Mixed Threat Attack

Mixed threat attacks take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.

NAT

Network Address Translation (NAT) is a standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows trusted networks with privately assigned IP addresses to

have access to the Internet. This also means that you do not have to get a registered IP address for every machine in the network.

NetBIOS

Network Basic Input Output System (NetBIOS) is an application program interface (API) that adds functionality such as network capabilities to disk operating system (DOS) basic input/output system (BIOS).

One-way Communication

NAT traversal has become an increasingly more significant issue in the current real-world network environment. To address this issue, MCP uses one-way communication. One-way communication has the MCP agent initiating the connection to, and polling of commands from, the server. Each request is a CGI-like command query or log transmission. To reduce the network impact, the MCP agent keeps connection alive and open as much as possible. A subsequent request uses an existing open connection. If the connection breaks, all SSL connections to the same host benefit from session ID cache that drastically reduces re-connection time.

Patch

A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program, while non-Windows patches commonly have a setup script.

Phish Attack

Phish, or phishing, is a rapidly growing form of fraud that seeks to fool web users into divulging private information by mimicking a legitimate website.

In a typical scenario, unsuspecting users get an urgent sounding (and authentic looking) email telling them there is a problem with their account that they must immediately fix to avoid account termination. The email will include a URL to a website that looks exactly like the real thing. It is simple to copy a legitimate email and a legitimate website but then change the so-called backend, which receives the collected data.

The email tells the user to log on to the site and confirm some account information. A hacker receives data a user provides, such as a logon name, password, credit card number, or social security number.

Phish fraud is fast, cheap, and easy to perpetuate. It is also potentially quite lucrative for those criminals who practice it. Phish is hard for even computer-savvy users to detect. And it is hard for law enforcement to track down. Worse, it is almost impossible to prosecute.

Please report to Trend Micro any website you suspect to be a phishing site.

Ping

Ping is a utility that sends an ICMP echo request to an IP address and waits for a response. The Ping utility can determine if the endpoint with the specified IP address is online or not.

POP3

Post Office Protocol 3 (POP3) is a standard protocol for storing and transporting email messages from a server to a client email application.

Proxy Server

A proxy server is a World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.

RPC

Remote procedure call (RPC) is a network protocol that allows a program running on one host to cause code to be executed on another host.

Security Patch

A security patch focuses on security issues suitable for deployment to all customers. Windows security patches include a Setup program, while non-Windows patches commonly have a setup script.

Service Pack

A service pack is a consolidation of hot fixes, patches, and feature enhancements significant enough to be a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

SMTP

Simple Mail Transport Protocol (SMTP) is a standard protocol used to transport email messages from server to server, and agent to server, over the Internet.

SNMP

Simple Network Management Protocol (SNMP) is a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.

SNMP Trap

A Small Network Management Protocol (SNMP) trap is a method of sending notifications to network administrators that use management consoles that support this protocol.

Apex One can store notification in Management Information Bases (MIBs). You can use the MIBs browser to view SNMP trap notification.

SSL

Secure Socket Layer (SSL) is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional agent authentication for a TCP/IP connection.

SSL Certificate

This digital certificate establishes secure HTTPS communication.

TCP

Transmission Control Protocol (TCP) is a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols that support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.

Telnet

Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.

Trojan Port

Trojan ports are commonly used by Trojan horse programs to connect to endpoints. During an outbreak, Apex One blocks the following port numbers that Trojan programs may use.

TABLE D-1. Trojan Ports

PORT NUMBER	TROJAN HORSE PROGRAM	PORT NUMBER	TROJAN HORSE PROGRAM
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy

Port Number	Trojan Horse Program	Port Number	Trojan Horse Program
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Trusted Port

The server and the Security Agent use trusted ports to communicate with each other.

If you block the trusted ports and then restore network settings to normal after an outbreak, Security Agents will not immediately resume communication with the server. Agent-server communication will only be restored after the number of hours you have specified in the Outbreak Prevention Settings screen elapses.

Apex One uses the HTTP port (by default, 8080) as the trusted port on the server. During installation, you may enter a different port number. To block this trusted port and the trusted port on the Security Agent, select the Block trusted ports check box on the Port Blocking screen.

The master installer randomly generates the Security Agent trusted port during installation.

Determining the Trusted Ports

Procedure

1. Access <Server installation folder>\PCCSRV.
2. Open the ofcscan.ini file using a text editor such as Notepad.
3. For the server trusted port, search for the string "Master_DomainPort" and then check the value next to it.

   For example, if the string appears as Master_DomainPort=80, this means that the trusted port on the server is port 80.
4. For the agent trusted port, search for the string "Client_LocalServer_Port" and then check the value next to it.

   For example, if the string appears as Client_LocalServer_Port=41375, this means that the trusted port on the agent is port 41375.

Two-way Communication

Two-way communication is an alternative to one-way communication. Based on one-way communication but with an extra HTTP-based channel that receives server notifications, two-way communication can improve real time dispatching and processing of commands from the server by the MCP agent.

UDP

User Datagram Protocol (UDP) is a connectionless communication protocol used with IP for application programs to send messages to other programs. Refer to DARPA Internet Program RFC 768 for information.

Uncleanable Files

The Virus Scan Engine is unable to clean the following files:

TABLE D-2. Uncleanable File Solutions

UNCLEANABLE FILE	EXPLANATION AND SOLUTION
Files infected with Trojans	Trojans are programs that perform unexpected or unauthorized, usually malicious, actions such as displaying messages, erasing files, or formatting disks. Trojans do not infect files, thus cleaning is not necessary. Solution: The Damage Cleanup Engine and Damage Cleanup Template remove Trojans.
Files infected with worms	A worm is a self-contained program (or set of programs) able to spread functional copies of itself or its segments to other endpoint systems. The propagation usually takes place through network connections or email attachments. Worms are uncleanable because the file is a self-contained program. Solution: Trend Micro recommends deleting worms.
Write-protected infected files	Solution: Remove the write-protection which allows for the cleaning of the file.
Password-protected files	Password-protected files include password-protected compressed files or password-protected Microsoft Office files. Solution: Remove the password protection which allows for the cleaning of the file.
Backup files	Files with the RB0~RB9 extensions are backup copies of infected files. The cleaning process creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process. Solution: If successfully cleaned, you do not need to keep the backup copy of the infected file. If the endpoint functions normally, you can delete the backup file.
Infected files in the Recycle Bin	The system may not allow the removal of infected files from the Recycle Bin because the system is running.
	1. Log on to the endpoint with Administrator privilege.

Uncleanable File	Explanation and Solution
	2. Close all running applications to prevent applications from locking the file, which would make Windows unable to delete it. 3. Open the command prompt. 4. Type the following to delete the files: `del /s \$Recycle.Bin\*` 5. Check if the files were removed.
Infected files in Windows Temp Folder or Internet Explorer Temporary Folder	The system may not allow the cleaning of infected files in the Windows Temp folder or the Internet Explorer temporary folder because the endpoint uses them. The files to clean may be temporary files needed for Windows operation.

	1. Log on to the endpoint with Administrator privilege.
	2. Close all running applications to prevent applications from locking the file, which would make Windows unable to delete it.
	3. If the infected file is in the Windows Temp folder:
	a. Open the command prompt.
	b. Type the following to delete the files:
	`del /s \Windows\Temp\*`
	c. Restart the endpoint in normal mode.
	4. If the infected file is in the Internet Explorer temporary folder:
	a. Open a command prompt and go to the Internet Explorer Temp folder.
	• For Windows 7: `%LocalAppData%\Microsoft\Windows\Temporary Internet Files`
	• For Windows 8/8.1: `%LocalAppData%\Microsoft\Windows\INetCache`
	• For Windows 10: `%LocalAppData%\Microsoft\Windows\INetCache\IE`
	b. Type the following to delete the files:
	`del /s .\*`

Uncleanable File	Explanation and Solution
	The last command deletes all files in the Internet Explorer temporary folder. c. Restart the endpoint in normal mode.
Files compressed using an unsupported compression format	Solution: Uncompress the files.
Locked files or files that are currently executing	Solution: Unlock the files or wait until the files have been executed.
Corrupted files	Solution: Delete the files.

Files Infected with Trojans

Trojans are programs that perform unexpected or unauthorized, usually malicious, actions such as displaying messages, erasing files, or formatting disks. Trojans do not infect files, thus cleaning is not necessary.

Solution: The Security Agent uses the Damage Cleanup Engine and Damage Cleanup Template to remove Trojans.

Files Infected with Worms

A worm is a self-contained program (or set of programs) able to spread functional copies of itself or its segments to other endpoint systems. The propagation usually takes place through network connections or email attachments. Worms are uncleanable because the file is a self-contained program.

Solution: Trend Micro recommends deleting worms.

Write-protected Infected Files

Solution: Remove the write-protection to allow the Security Agent to clean the file.

Password-protected Files

Includes password-protected compressed files or password-protected Microsoft Office files.

Solution: Remove the password protection to allow the Security Agent to clean these files.

Backup Files

Files with the RB0~RB9 extensions are backup copies of infected files. The Security Agent creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.

Solution: If the Security Agent successfully cleans the infected file, you do not need to keep the backup copy. If the endpoint functions normally, you can delete the backup file.

Index

B

E

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: APEMS8589/190219