Trend Micro Apex Central™

Patch 1

Widget and Policy Management Guide

Centralized Security Management for Endpoints

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

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

Document Part No.: APEM09004/200609

Release Date: June 2020

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Part I: Introduction

Chapter 1: The Dashboard

Chapter 2: Policy Management

Chapter 3: Policy Resources

Chapter 19: Apex One Data Loss Prevention Policy Settings

Part VII: Apex One (Mac) Widgets and Policies

Chapter 20: Apex One (Mac) Dashboard Widgets

Chapter 21: Apex One (Mac) Policy Settings

Part VIII: Deep Discovery Widgets and Policies

Chapter 22: Deep Discovery Analyzer and Email Inspector Dashboard Widgets

Chapter 23: Deep Discovery Inspector Integration and Policy Settings

Part IX: Deep Security Manager Widgets

Chapter 24: Deep Security Manager Dashboard Widgets

Part X: Endpoint Application Control Widgets and Policies

Chapter 25: Endpoint Application Control Dashboard Widgets

Chapter 26: Endpoint Application Control Policy Settings

Part XI: Endpoint Encryption Widgets and Policies

Chapter 27: Endpoint Encryption Dashboard Widgets

Chapter 31: InterScan Messaging Security Suite Policy Settings

Chapter 32: InterScan Messaging Security Virtual Appliance Policy Settings

Chapter 33: InterScan Web Security Suite Policy Settings

Chapter 34: InterScan Web Security Virtual Appliance Policy Settings

Part XIV: ScanMail for Microsoft Exchange Policies

Chapter 35: ScanMail for Microsoft Exchange Policy Settings

Part XV: Smart Protection Server Widgets

Chapter 36: Smart Protection Server Dashboard Widgets

Chapter 38: Trend Micro Mobile Security Policy Settings

Part XVII: Virtual Mobile Infrastructure Widgets

Chapter 39: Virtual Mobile Infrastructure Dashboard Widgets

Part XVIII: Vulnerability Protection Widgets

Chapter 40: Vulnerability Protection Dashboard Widgets

Index

Preface

Preface

Welcome to the Trend Micro Apex Central™ *Widget and Policy Management Guide*. This document explains how to configure **Dashboard** widgets and **Policy Management** settings on Apex Central.

Topics in this section:

Documentation

Apex Central documentation includes the following:

Document	Description
Readme file	Contains a list of known issues and may also contain late-breaking product information not found in the Online Help or printed documentation
Administrator's Guide	A PDF document that provides detailed instructions of how to configure and manage Apex Central and managed products, and explanations on Apex Central concepts and features
Online Help	HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. The Help is also accessible from the Apex Central console
Widget and Policy Management Guide	A PDF document that explains how to configure dashboard widgets and policy management settings in Apex Central
Automation Center	Online user guides and references that explain how to use the Apex Central Automation APIs: https://automation.trendmicro.com/apex-central/home
Data Protection Lists (Chapter 1 only)	A PDF document that lists predefined data identifiers and templates for Data Loss Prevention
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://success.trendmicro.com

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

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

Audience

Apex Central documentation is intended for the following users:

- Apex Central Administrators: Responsible for Apex Central installation, configuration, and management. These users are expected to have advanced networking and server management knowledge.
- Managed Product Administrators: Users who manage Trend Micro products that integrate with Apex Central. These users are expected to have advanced networking and server management knowledge.

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

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

Convention	Description
⚠ **WARNING!**	Critical actions and configuration options

Terminology

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

Terminology	Description
Administrator (or Apex Central administrator)	The person managing the Apex Central server
Security Agent	The managed product program installed on an endpoint
Components	Responsible for scanning, detecting, and taking actions against security risks
Apex Central console, web console, or management console	The web-based user interface for accessing, configuring, and managing a Apex Central **Note** Consoles for integrated managed products are indicated by the managed product name. For example, the Apex One web console.
Managed endpoint	The endpoint where the managed product Security Agent is installed
Managed product	A Trend Micro product that integrates with Apex Central
Managed server	The endpoint where the managed product is installed
Server	The endpoint where the Apex Central server is installed
Security risk	The collective term for virus/malware, spyware/grayware, and web threats

Terminology	Description
Dual-stack	Entities that have both IPv4 and IPv6 addresses
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address

Part I

Introduction

Chapter 1

The Dashboard

This section discusses how to use the Apex Central dashboard tabs and widgets.

Topics include:

About the Dashboard

The **Dashboard** appears when you open the Apex Central web console or click **Dashboard** on the main menu. Each Apex Central user account has a completely independent dashboard. Any changes to the dashboard belonging to a specific user account will not affect the dashboards of the other user accounts.

The **Dashboard** contains the following:

- Tabs
- Widgets

Tabs and Widgets

Widgets are the core components of the **Dashboard**. Widgets provide specific information about various security-related events.

The information that widgets display comes from:

- Apex Central database
- Registered managed products
- Trend Micro Smart Protection Network

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

Working with Tabs

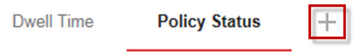
Manage tabs by adding, renaming, changing the layout, deleting, and automatically switching between tab views.

Procedure

1. Go to the **Dashboard**.

2. To add a tab:

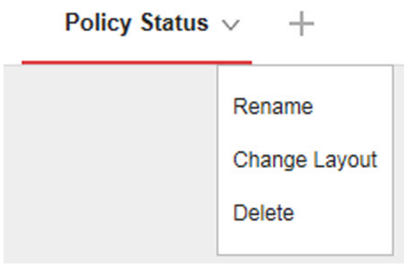
   a. Click the add icon (+).



   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**.

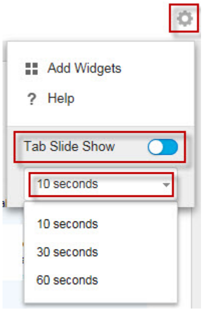
5. To delete a tab:

   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.

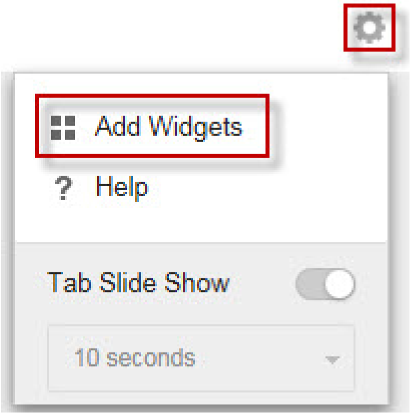
Working with Widgets

Manage widgets by adding, moving, resizing, renaming, and deleting items. You can also modify the products that contribute data for the widget.

Procedure

1. Go to the **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 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.

c. Click **Save**.

7. To modify the product scope of the widget:

a. Click the settings icon (⋮ > 🎚).

b. Click the double arrow button (») in the **Scope** field.

c. (Optional) Click the funnel icon (▽) to filter and search for products.

d. Select the products that contribute data for the widget and click **OK**.

e. Click **Save**.

8. To delete a widget, click the delete icon (⋮ > 🗑).

Security Posture Tab

The **Security Posture** tab provides a holistic summary of your network protection status by consolidating data about the compliance levels, critical threat detections, and detections stopped on your network. You can use the **Security Posture** chart to quickly identify high risk users and groups from an integrated Active Directory structure.

Note

To change the sample chart data and display sites or reporting lines based on your company network, enable Active Directory integration or create custom sites based on IP addresses.

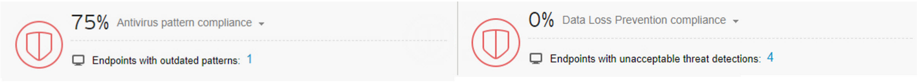
By default, the **Security Posture** tab is toggled to **Chart** view (◉). To display the chart nodes, critical threats, and antivirus pattern compliance information in a table, toggle the **Table** view (▦).

Click the settings icon (⋮ > 🎚) to change the following information that displays on the tab.

- **Organization**: Specify the display name of the organization.
- **Active Directory grouping**: Specify whether the nodes on the chart represent **Sites** or **Reporting Lines** from your Active Directory.

- **Groups to display**: Select the top number of groups at the highest risk
- **Period**: Specify the time range for the data that displays on the chart.

Compliance Indicators



75% Antivirus pattern compliance ▾

Endpoints with outdated patterns: 1

0% Data Loss Prevention compliance ▾

Endpoints with unacceptable threat detections: 4

This section of the **Security Posture** tab provides information about the antivirus pattern compliance level or the Data Loss Prevention compliance level of your network.

As your network compliance level changes, the color of the compliance indicator icon changes to reflect the thresholds configured on the **Active Directory and Compliance Settings** screen.

The default view displays information for the **Antivirus pattern compliance** indicator.

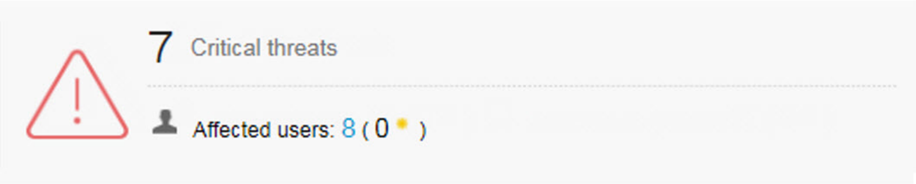
Note

Changing the compliance indicator also changes the compliance level information that displays in the **Security Posture** chart.

To change the compliance information that displays, click the name of the selected compliance indicator next to the down arrow icon (▾) and select one of the following indicators from the drop-down.

Indicator	Description
Antivirus pattern compliance	Displays the following information: • The percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions • The total number of endpoints with outdated antivirus patterns on your network Click the count for **Endpoints with outdated patterns** to view detailed information about the affected endpoints in the User/Endpoint Directory.
Data Loss Prevention compliance	Displays the following information: • The percentage of Data Loss Prevention enabled Security Agents with an acceptable number of threat detections • The total number of endpoints with Data Discovery threat detections Click the count for **Endpoints with unacceptable threat detections** to view detailed information about the affected endpoints in the User/Endpoint Directory.

Critical Threats



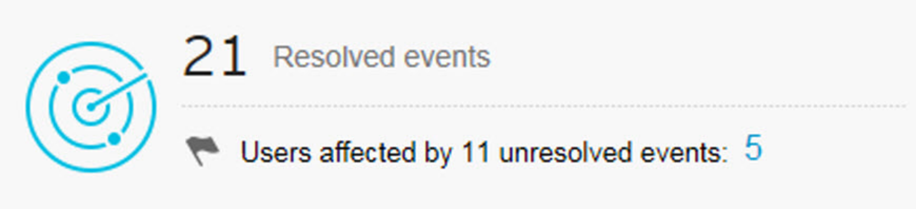
The **Critical Threats** section of the **Security Posture** tab displays the total number of unique critical threats (by threat type) detected on your network, the total number of affected users, and the number of affected important users (marked by the star).

Click the number of affected users to view additional details on the **User/Endpoint Directory** screen.

Critical threat detections include the following threat types.

Threat Type	Description
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid
Known Advanced Persistent Threat (APT)	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents
Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file
Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems
Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
C&C callback	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware

Resolved Events

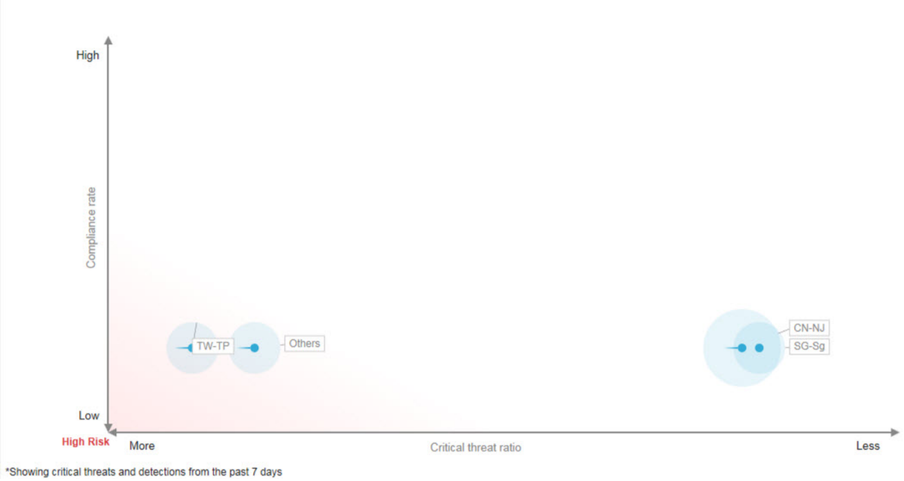

21 Resolved events

Users affected by 11 unresolved events: 5

This section of the **Security Posture** tab displays the total number of resolved and unresolved events on your network.

Click the count for the **Users affected by __ unresolved events** field to view detailed information about the users affected by unresolved events on your network.

Security Posture Chart



*Showing critical threats and detections from the past 7 days

The chart on the **Security Posture** tab displays the relationship between the critical threat ratio and compliance level of your network. The x-axis indicates the ratio of critical threats to total endpoints within a site or reporting line. The y-axis indicates the compliance levels of the sites or reporting lines for the selected compliance indicator. You can use this data to quickly identify high risk users and groups from an integrated Active Directory structure.

Note

To change the sample chart data and display sites or reporting lines based on your company network, enable Active Directory integration or create custom sites based on IP addresses.

Hover over a node to view compliance and critical threat information for particular sites or reporting lines. The tail on a node indicates the direction from which the security status has changed over the specified time period.

- Click the settings icon (⋮ > 🎚) to change the **Active Directory grouping** (**Sites**, **Reporting Lines**) represented by the node.
- You can also customize sites and reporting lines by using the **Active Directory and Compliance Settings** screen.

The default view displays the selected compliance indicator information for all nodes on your network for the last 7 days.

- Select a different compliance indicator to change the compliance information that displays.
- Click the settings icon (⋮ > 🎚) to change the **Period** for the data that displays.
- Click a node to view detailed information about the selected node in the summary panel on the right.

Security Posture Details Pane

The details pane on the **Security Posture** tab displays more detailed information about the compliance levels, critical threat detections, and total resolved/unresolved events on your network.

The default view displays the selected compliance indicator information for all nodes on your network for the last 7 days.

- Select a different compliance indicator to change the compliance information that displays.
- Click a node on the chart to display only the information for the selected node.
- Click the settings icon (⋮ > 🎚) to change the **Period** for the data that displays.

TABLE 1-1. Compliance Information

INDICATOR	DESCRIPTION
Antivirus pattern compliance	Displays the percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions You can also view the following details: • **Managed agents**: The number of endpoints that have Apex One or Worry-Free Business Security Services Security Agents installed • **With compliant virus patterns**: The number of managed agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions • **With outdated virus patterns**: The number of managed agents not using acceptable Virus Pattern and Smart Scan Agent Pattern versions • **Offline for 7 days**: The number of managed agents that have not communicated with the managed product server in 7 or more days • **Exceptions**: The number of users or endpoints excluded from the compliance calculations • **Unmanaged endpoints**: The number of endpoints that do not have Apex One or Worry-Free Business Security Services Security Agents installed Expand the categories and click a count to view additional details about the affected endpoints.

Indicator	Description
Data Loss Prevention compliance	Displays the percentage of Data Loss Prevention enabled Apex One agents with an acceptable number of threat detections You can also view the following details: • **Managed agents**: The number of endpoints that have Apex One or Worry-Free Business Security Services Security Agents installed • **With acceptable threat detections**: The number of managed agents with an acceptable number of threat detections • **With unacceptable threat detections**: The number of managed agents that exceeded the acceptable number of threat detections • **Offline for 7 days**: The number of managed agents that have not communicated with the managed product server in 7 or more days • **Exceptions**: The number of users or endpoints excluded from the compliance calculations • **Unmanaged endpoints**: The number of endpoints that do not have Apex One or Worry-Free Business Security Services Security Agents installed Expand the categories and click a count to view additional details about the affected endpoints.

Table 1-2. Critical Threats

Section	Description
Critical threats	Displays the total number of unique critical threats (by threat type) detected on your network Lists all the critical threat types affecting your network For threat types with detections: • Expand the threat type to view a list of detections. • Click a detection to view additional details on the **Threat Information** screen.

Section	Description
Affected users	Displays the total number of users affected by critical threats • Expand the section to view affected users. • Click an affected user to view additional details on the **User** information screen.
Affected endpoints	Displays the total number of endpoints affected by critical threats • Expand the section to view affected endpoints. • Click an affected endpoint to view additional details on the **Endpoint** information screen.

Table 1-3. Total Events

Data	Description
Total events	Displays the total number of events detected
Resolved events	Displays the number of resolved events on your network
Unresolved events	Displays the number of unresolved events on your network that require action
Affected users	Displays the number of users affected by unresolved events on your network Click the count to view details about the affected users.

Summary Tab

The **Summary** tab contains a predefined set of widgets that provides an overview of the security status of your network.

Note

You can add, delete, or modify the widgets that display on the **Summary** tab.

Available widgets:

- Critical Threats
- Users with Threats
- Endpoints with Threats
- Product Connection Status
- Product Component Status
- Ransomware Prevention

Critical Threats Widget

This widget displays the total number of unique critical threat types detected on your network and the number of affected users and threat detections for each threat type.

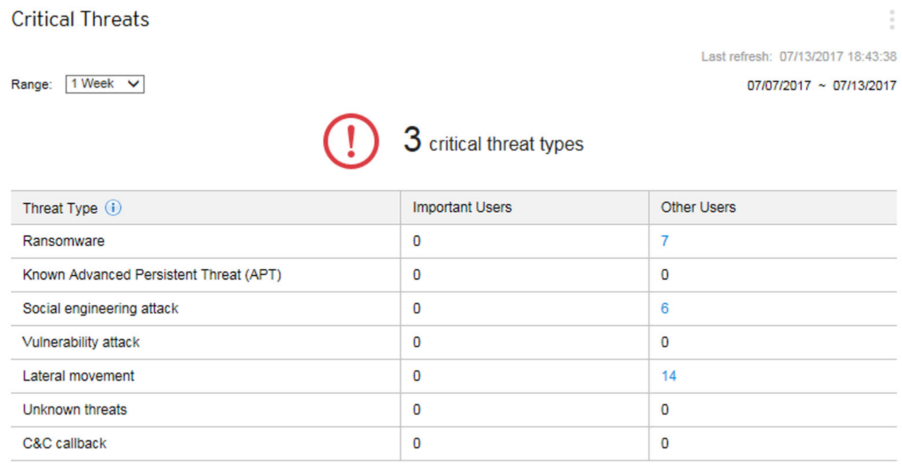
Click the settings icon (⋮ > 🎚) to change the default **View**.

- On the **Summary** tab or a custom tab, the **Affected users** view is selected by default.
- On the **Threat Investigation** tab, the **Threat detections** view is selected by default.

Note

- The widget lists critical threat types in order of severity.
- Individual users may be affected by more than one critical threat type.

Use the **Range** drop-down to select the time period for the data that displays.



Critical Threats

Last refresh: 07/13/2017 18:43:38

Range: 1 Week

07/07/2017 ~ 07/13/2017

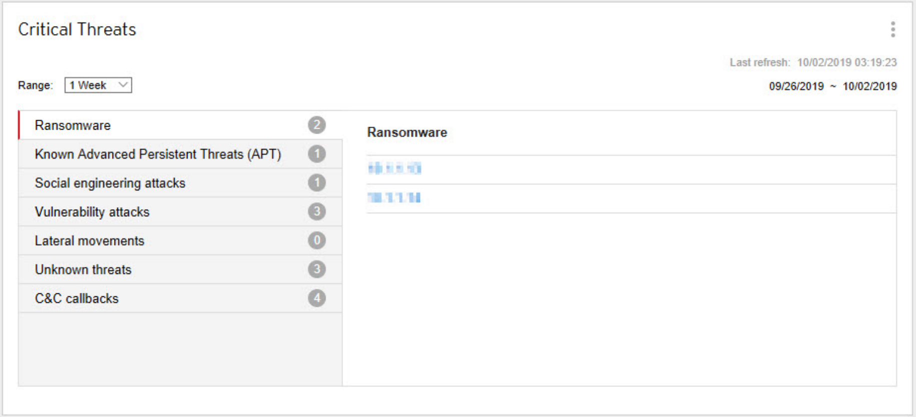
3 critical threat types

Threat Type	Important Users	Other Users
Ransomware	0	7
Known Advanced Persistent Threat (APT)	0	0
Social engineering attack	0	6
Vulnerability attack	0	0
Lateral movement	0	14
Unknown threats	0	0
C&C callback	0	0

FIGURE 1-1. Affected Users View

The **Affected users** view displays the number of **Important Users** and **Other Users** affected by each threat type.

- Click the count in the **Important Users** or **Other Users** column, and then click the affected user you want to view.
- You can define important users or endpoints on the **User/Endpoint Directory** screen.



Critical Threats

Last refresh: 10/02/2019 03:19:23

Range: 1 Week

09/26/2019 ~ 10/02/2019

Threat type	Count
Ransomware	2
Known Advanced Persistent Threats (APT)	1
Social engineering attacks	1
Vulnerability attacks	3
Lateral movements	0
Unknown threats	3
C&C callbacks	4

Ransomware

[redacted]

[redacted]

FIGURE 1-2. Threat Detections View

The **Threat detections** view displays the number of detections for each critical threat type.

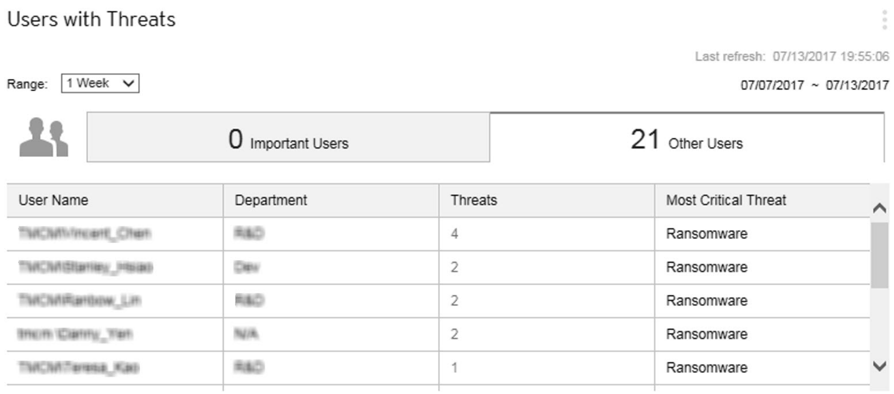
- Click a critical threat type to view the specific threat detections.
- Click the hyperlink for a specific threat detection to view details about the affected users and automatically start a Root Cause Analysis to determine whether the threat has affected other endpoints on your network.

Critical threat detections include the following threat types.

THREAT TYPE	DESCRIPTION
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid
Known Advanced Persistent Threats (APT)	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents
Social engineering attacks	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file

Threat Type	Description
Vulnerability attacks	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems
Lateral movements	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
C&C callbacks	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware

Users with Threats Widget



Users with Threats

Last refresh: 07/13/2017 19:55:06

Range: 1 Week

07/07/2017 ~ 07/13/2017

0 Important Users

21 Other Users

User Name	Department	Threats	Most Critical Threat
[redacted]	[redacted]	4	Ransomware
[redacted]	[redacted]	2	Ransomware
[redacted]	[redacted]	2	Ransomware
[redacted]	[redacted]	2	Ransomware
[redacted]	[redacted]	1	Ransomware

This widget displays information about users with security threat detections.

Use the **Range** drop-down to select the time period for the data that displays.

Click the **Important Users** or **Other Users** tabs to switch between the different views.

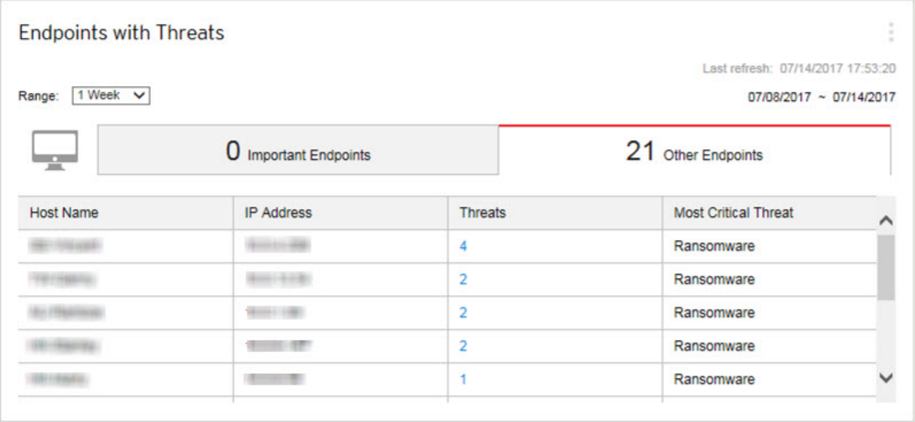
The table lists affected users in order by critical threat type severity first, and then by the number of threat detections for the user.

- Click the number in the **Threats** column for the user you want to view.

The **Most Critical Threat** column displays the following threat types.

Threat Type	Description
C&C callback	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware
Known Advanced Persistent Threat (APT)	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents
Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid
Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file
Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems

Endpoints with Threats Widget



Endpoints with Threats

Last refresh: 07/14/2017 17:53:20

Range: 1 Week

07/08/2017 ~ 07/14/2017

0 Important Endpoints

21 Other Endpoints

Host Name	IP Address	Threats	Most Critical Threat
[redacted]	[redacted]	4	Ransomware
[redacted]	[redacted]	2	Ransomware
[redacted]	[redacted]	2	Ransomware
[redacted]	[redacted]	2	Ransomware
[redacted]	[redacted]	1	Ransomware

This widget displays information about endpoints with security threat detections.

Use the **Range** drop-down to select the time period for the data that displays.

Click the **Important Users** or **Other Users** tabs to switch between the different views.

The table lists affected users in order by critical threat type severity first, and then by the number of threat detections for the user.

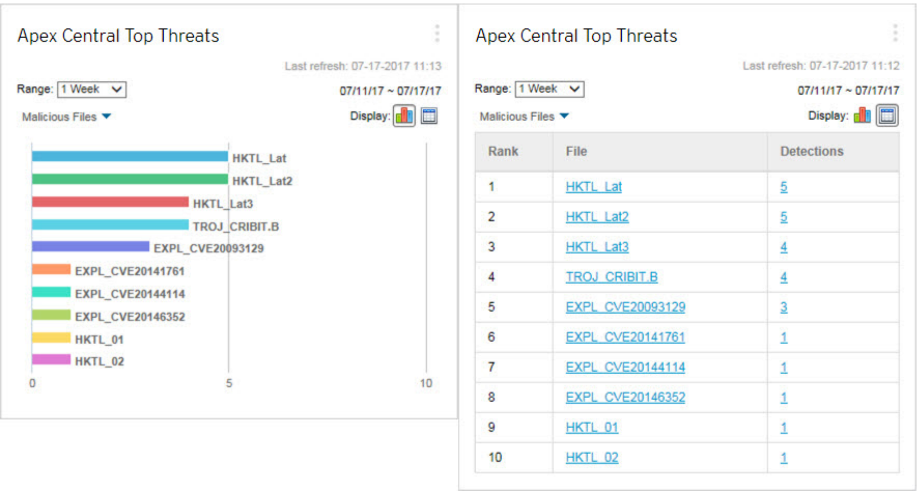
- Click the number in the **Threats** column for the user you want to view.

The **Most Critical Threat** column displays the following threat types.

Threat Type	Description
C&C callback	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware

THREAT TYPE	DESCRIPTION
Known Advanced Persistent Threat (APT)	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents
Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid
Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file
Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems

Apex Central Top Threats Widget



Apex Central Top Threats

Last refresh: 07-17-2017 11:12

Range: 1 Week

07/11/17 ~ 07/17/17

Malicious Files

Display:

Rank	File	Detections
1	HKTL_Lat	5
2	HKTL_Lat2	5
3	HKTL_Lat3	4
4	TROJ_CRIBIT.B	4
5	EXPL_CVE20093129	3
6	EXPL_CVE20141761	1
7	EXPL_CVE20144114	1
8	EXPL_CVE20146352	1
9	HKTL_01	1
10	HKTL_02	1

This widget displays information about the malicious files and malicious URLs detected for a specified time range.

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

Use the drop-down list above the chart/table to select the type of threat data to display.

- **Malicious Files**: Ranks the malicious files detected on your network by the number of detections
- **Malicious URLs**: Ranks the malicious URLs detected on your network by the number of detections

Click a bar, threat name, or detection number to open the **Log Query** screen that displays information about the affected endpoints, threat details, and detection count.

The default view displays the top 10 threats from all the managed products for which the logged on user account has access rights.

- Click the settings icon (⋮ > ⚙) to edit the widget title, product scope, or number of threats that displays.

Product Component Status Widget

This widget displays the component versions and compliance status of managed products or endpoints on your network. Use this widget to track managed products or endpoints with outdated components.

The default view displays the latest versions of components managed by Apex Central and the compliance status of managed products. The **Pattern** and **Engine** sections list components in order of the highest rate of non-compliance first. You can click the **Rate** column to change the sort order.

Click any of the components in the **Pattern** or **Engine** columns to view a pie chart that displays the number of managed products or endpoints using each component version.

Click the counts in the **Outdated/All** columns to view information about the component versions on outdated managed products, all managed products, outdated endpoints, or all endpoints.

Click the settings icon (⋮ > ⚙) to configure the following options:

Note

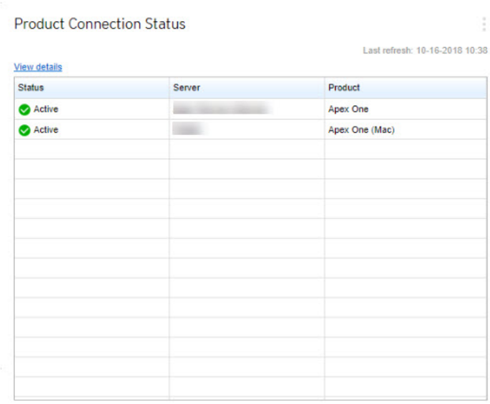
The settings icon (⚙) does not display for widgets on the **Summary** tab.

- To modify the product scope of the widget, click the double arrow button (») in the **Scope** field and select the products that contribute data.
- To edit the components that display in the widget, select or clear components from the **Pattern** or **Engine** fields.
- To display compliance information for managed products, endpoints, or both, specify the **Source**.

- To specify whether to view data from all components reported by managed products or to view data from only components managed by Apex Central, select the **View**.

DATA	DESCRIPTION
Pattern	Displays the name of the pattern file, template, or antispam rule
Engine	Displays the name of the scan engine
Latest Version	Displays the following information: • The latest version of the component downloaded by Apex Central • The latest version of the component that is available for download (reported by managed products)
Outdated/All	Displays the following information: • **Outdated**: The number of managed products or endpoints with outdated components Click the first count in the **Outdated/All** column to view information about the component versions on the outdated managed products or endpoints. • **All**: The total number of managed products or endpoints that use the component Click the second count in the **Outdated/All** column to view information about the component versions on all managed products or endpoints. **Note** This column displays when **Both** is selected for the **Source**.
Rate	Displays the percentage of managed products or endpoints with outdated components **Note** This column displays when **Both** is selected for the **Source**.

Product Connection Status Widget

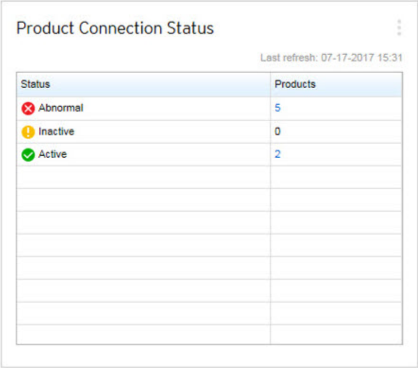


Product Connection Status

Last refresh: 10-16-2018 10:38

View details

Status	Server	Product
✓ Active	[redacted]	Apex One
✓ Active	[redacted]	Apex One (Mac)



Product Connection Status

Last refresh: 07-17-2017 15:31

Status	Products
✕ Abnormal	5
! Inactive	0
✓ Active	2

This widget displays the connection status of all managed products that register to the Apex Central server.

The default view lists the connection status and managed server name of each managed product for which the logged on user account has access rights.

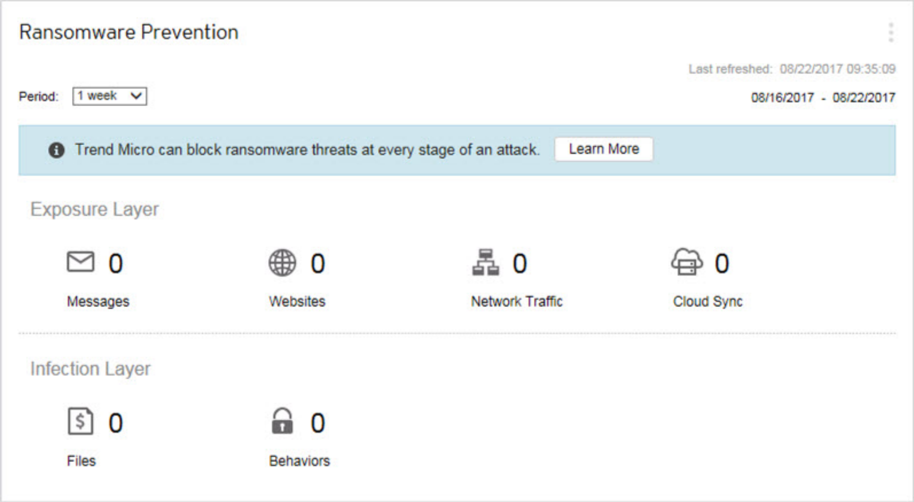
- To change the product scope, click the settings icon (⋮ > ⫶) and select a new **Scope**.
- To view a summary of the total number of managed products for each connection status, click the settings icon (⋮ > ⫶) and switch the **View** to **Summary**.

Click **View details** to view detailed information on the **Log Query** screen.

Status	Description
Active	Indicates that the product service is running and communication with the Apex Central server is established successfully

Status	Description
Inactive	Indicates that the product service is not running or is unable to establish communication with the Apex Central server
Abnormal	Indicates that the product service has not communicated with the Apex Central server within the user-defined agent communication time-out interval

Ransomware Prevention Widget


Ransomware Prevention

Last refreshed: 08/22/2017 09:35:09

Period: 1 week

08/16/2017 - 08/22/2017

Trend Micro can block ransomware threats at every stage of an attack.

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 categorizes all the attempts based on the infection channel.

- Click the ransomware detection count to view additional details.

CHANNEL	DESCRIPTION
Messages	Ransomware detected in email messages or email attachments
Websites	Ransomware detected by Web Reputation Services
Network traffic	Ransomware detected by Apex One Suspicious Connections and Deep Discovery Inspector
Cloud sync	Ransomware detected by Cloud App Security on cloud storage and Office 365 servers (Exchange Online, SharePoint Online, and OneDrive), or detected by Apex One in local folders on Apex One agents that sync with cloud storage
Files	Ransomware detected by File Reputation Services
Behaviors	Ransomware detected by Apex One Behavior Monitoring

Data Loss Prevention Tab

The **Data Loss Prevention** tab contains widgets that display information about DLP incidents, template matches, and incident sources.

The predefined widgets include:

- DLP Incidents by Severity and Status
- DLP Incident Trends by User
- DLP Incidents by User
- DLP Incidents by Channel
- DLP Template Matches
- Top DLP Incident Sources
- DLP Violated Policy

DLP Incident Trends by User Widget

This widget checks the number of DLP incident trends based on managed users. Data can be filtered by severity level, or filtered to show only the total number of incidents triggered by a specific user for a specified period of time. By default the widget displays data from all the managed products that a user's account privileges allow.

Use the **Range** drop-down to select the time period for the data that displays.

Click the sections from the graph to open the **Incident Information** screen and review the summary of incidents.

Click the widget settings icon on the widget to access additional settings.

Setting	Description
Title	Specify a new and meaningful title for the widget in the field.
Range	Specify the time range when the DLP incidents were triggered.
Scope	Specify the data scope displayed by the widget. • Directly managed users • All managed users: Data is collected from both directly managed users and people under the directly managed users.
Severity	Specify the severity levels to filter the data.
Users to display	Specify the number of managed users to display.

Click **Save** to apply changes and update the widget data.

DLP Incidents by Severity and Status Widget

This widget checks the number of DLP incidents based on severity levels and incident status. Data can be filtered by severity level, as well as display the total number of new and high severity incidents. By default the widget displays data from all the managed products that a user's account privileges allow.

Use the **Range** drop-down to select the time period for the data that displays.

Click the numbers in any column to open the **Incident Information** screen and review the summary of incidents.

To look up a specific incident, type an ID in the **Incident ID** field and click **Search**.

Tip

Each incident is assigned an ID number. ID numbers can be found by clicking a table link, in **Incident details updated** event notifications, or in **Data Loss Prevention** log query results.

Click the widget settings icon on the widget to access additional settings.

SETTING	DESCRIPTION
Title	Specify a new and meaningful title for the widget in the field.
Range	Specify the time range when the DLP incidents were triggered.
Scope	Specify the data scope displayed by the widget. • Directly managed users • All managed users: Data is collected from both directly managed users and people under the directly managed users
Severity	Specify the severity levels to filter the data.

Click **Save** to apply changes and update the widget data.

DLP Incidents by User Widget

This widget checks the number of DLP incidents based on severity levels and managed users. Data can be filtered by severity level, as well as display the total number of new and high severity incidents triggered by specific users. By default the widget displays data from all the managed products that a user's account privileges allow. The widget shows a maximum of 50 users.

Use the **Range** drop-down to select the time period for the data that displays.

Click the numbers in any column to open the **Incident Information** screen and review the summary of incidents.

To look up a specific user, type a few characters in the **User** field and click **Search**. For example typing `ke` shows all user names with `ke`, such as “Ken” and “Brooke”. You can also type a domain and user name, such as `domain1\chris`.

Note

User names must not contain the following characters: " [ ] : ; | = + * ? / \ < &> ,

Domain names must not contain the following characters: \ * + = | : ; " ? < &> ,

Click the widget settings icon on the widget to access additional settings.

Setting	Description
Title	Specify a new and meaningful title for the widget in the field.
Range	Specify the time range when the DLP incidents were triggered.
Scope	Specify the data scope displayed by the widget. • Directly managed users • All managed users: Data is collected from both directly managed users and people under the directly managed users.
Severity	Specify the severity levels to filter the data.
Users to display	Specify the number of managed users to display.

Click **Save** to apply changes and update the widget data.

DLP Incidents by Channel Widget

This widget displays the total number of DLP incidents. Data can be filtered by the type of channels where the incident is triggered.

Use the **Range** drop-down to select the time period for the data that displays.

Use the **Channel** drop-down to filter out the type of channels where the incident is triggered.

This widget displays the number of DLP incidents and the ratio of channels compared to the total number of incidents. This widget displays this data by:

Data	Description
P2P	Displays all peer-to-peer DLP incidents by any managed product that the Data Scope specifies
IM	Displays all instant messaging DLP incidents by any managed product that the Data Scope specifies
Webmail	Displays all webmail DLP incidents by any managed product that the Data Scope specifies
Email	Displays all email DLP incidents by any managed product that the Data Scope specifies
Web App	Displays all web application DLP incidents by any managed product that the Data Scope specifies
Others	Displays the remaining DLP incidents by any managed product that the Data Scope specifies

Clicking links in the **Channel** column or sections from the graphs opens a screen that displays detailed information.

Data	Description
Channel	Type of channels where the DLP incidents is triggered
Incidents	Number of DLP incidents triggered
Percentage (%)	DLP incidents percentage of total number of incidents

To change the information that the widget displays, click ⋮ > 🎚. On the dialog box that appears, specify the **Scope** by clicking >> and selecting the parent servers that the widget uses as its source.

DLP Template Matches Widget

This widget displays the type of DLP incidents on your network. Data can be filtered by template.

Use the **Range** drop-down to select the time period for the data that displays.

Clicking links in the **Template** column or sections from the graphs opens a screen that displays detailed information.

Data	Description
Template	Template triggered by DLP incidents
Incidents	Number of DLP incidents
Percentage (%)	DLP incidents percentage of total number of incidents

To change the information that the widget displays, click ⋮ > 🎚. On the dialog box that appears, specify the **Scope** by clicking >> and selecting the parent servers that the widget uses as its source.

Top DLP Incident Sources Widget

This widget displays the total number of top DLP incident sources on your network. This data includes users, email addresses, host names, and IP addresses, which can be filtered by incident source.

Use the **Range** drop-down to select the time period for the data that displays.

Use the **Show** drop-down to select the data to be displayed.

DLP Violated Policy Widget

This widget displays the DLP violated policy. Use this widget to check the total number of DLP incidents. By default data is sorted by the number of incidents. To sort data by policy name, click the **Policy** column title.

Use the **Range** drop-down to select the time period for the data that displays.

Clicking links in the **Incidents** column opens a screen that displays detailed information.

Data	Description
Policy	Name of the policy where the DLP incidents is triggered
Incidents	Number of DLP incidents triggered

Compliance Tab

The **Compliance** tab contains widgets that display information relating to component or connection compliance for managed products or endpoints.

The predefined widgets are as follows:

- Product Application Compliance
- Product Component Status
- Product Connection Status
- Agent Connection Status

Product Application Compliance Widget

This widget displays the product version, language, build, and update status for managed products. This provides administrators a quick way to discern which managed product's applications are up-to-date and which require updating.

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

Click the counts in the **Up-to-date** and **Out-of-date** columns to open a screen that displays detailed information. Apex Central performs a log query to provide the detailed information.

Data	Description
Product	The managed product registered to Apex Central

Data	Description
Version	Version of the managed product
Language	Language version of the managed product
Build	Build number of the managed product
Up-to-date	Number of products that are considered updated Edit the widget to specify the minimum product version that should still be considered "up-to-date". Click the count to view more details about the product.
Out-of-date	Number of products that are "out-of-date" Click the count to view more details about the product.
Up-to-date Rate (%)	Percentage of products that are "up-to-date"

By default the widget displays data from all the managed products that a user's account privileges allow.

Specify a bar graph or a table to display the data. By default, data is displayed as a bar graph.

Click **Edit** to access the following options:

- Click **Scope** > **Browse** to specify the products that contribute data for the widget.

  The data scope specifies the products which the widget uses to display data. This can have a drastic affect on the usefulness of the information that the widget displays.

- On the **Up-to-date range** drop-down, specify the number of product versions away from the latest build that should still be considered "up-to-date".

Click **Save** to apply changes and exit.

Product Component Status Widget

This widget displays the component versions and compliance status of managed products or endpoints on your network. Use this widget to track managed products or endpoints with outdated components.

The default view displays the latest versions of components managed by Apex Central and the compliance status of managed products. The **Pattern** and **Engine** sections list components in order of the highest rate of non-compliance first. You can click the **Rate** column to change the sort order.

Click any of the components in the **Pattern** or **Engine** columns to view a pie chart that displays the number of managed products or endpoints using each component version.

Click the counts in the **Outdated/All** columns to view information about the component versions on outdated managed products, all managed products, outdated endpoints, or all endpoints.

Click the settings icon (⋮ > ⚙) to configure the following options:

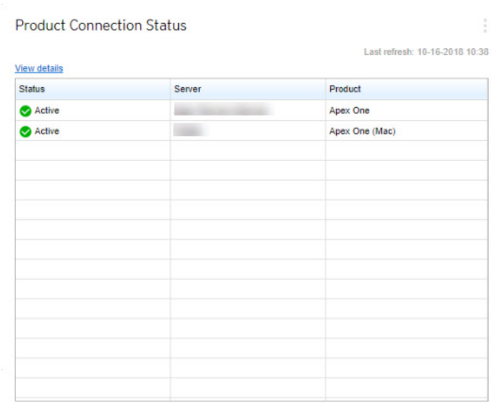
Note

The settings icon (⚙) does not display for widgets on the **Summary** tab.

- To modify the product scope of the widget, click the double arrow button (>>) in the **Scope** field and select the products that contribute data.
- To edit the components that display in the widget, select or clear components from the **Pattern** or **Engine** fields.
- To display compliance information for managed products, endpoints, or both, specify the **Source**.
- To specify whether to view data from all components reported by managed products or to view data from only components managed by Apex Central, select the **View**.

DATA	DESCRIPTION
Pattern	Displays the name of the pattern file, template, or antispam rule
Engine	Displays the name of the scan engine
Latest Version	Displays the following information: • The latest version of the component downloaded by Apex Central • The latest version of the component that is available for download (reported by managed products)
Outdated/All	Displays the following information: • **Outdated**: The number of managed products or endpoints with outdated components Click the first count in the **Outdated/All** column to view information about the component versions on the outdated managed products or endpoints. • **All**: The total number of managed products or endpoints that use the component Click the second count in the **Outdated/All** column to view information about the component versions on all managed products or endpoints. **Note** This column displays when **Both** is selected for the **Source**.
Rate	Displays the percentage of managed products or endpoints with outdated components **Note** This column displays when **Both** is selected for the **Source**.

Product Connection Status Widget

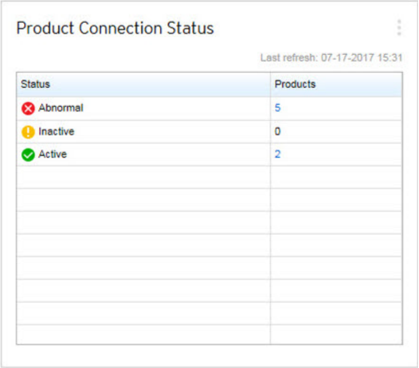


Product Connection Status

Last refresh: 10-16-2018 10:38

View details

Status	Server	Product
✓ Active	[redacted]	Apex One
✓ Active	[redacted]	Apex One (Mac)



Product Connection Status

Last refresh: 07-17-2017 15:31

Status	Products
✖ Abnormal	5
! Inactive	0
✓ Active	2

This widget displays the connection status of all managed products that register to the Apex Central server.

The default view lists the connection status and managed server name of each managed product for which the logged on user account has access rights.

- To change the product scope, click the settings icon (⋮ > 🎚) and select a new **Scope**.
- To view a summary of the total number of managed products for each connection status, click the settings icon (⋮ > 🎚) and switch the **View** to **Summary**.

Click **View details** to view detailed information on the **Log Query** screen.

Status	Description
Active	Indicates that the product service is running and communication with the Apex Central server is established successfully

Status	Description
Inactive	Indicates that the product service is not running or is unable to establish communication with the Apex Central server
Abnormal	Indicates that the product service has not communicated with the Apex Central server within the user-defined agent communication time-out interval

Agent Connection Status Widget

This widget displays the connection status of agents with their parent servers. Agents for the following managed products are displayed:

- Endpoint Sensor
- Endpoint Encryption
- Mobile Security
- Mobile Security (for Mac)
- Apex One
- Vulnerability Protection
- Worry-Free Business Security Services

By default the widget displays data from all the managed products that a user's account privileges allow.

Click the values in the **Online**, **Offline**, or **Total** columns to view more information. Apex Central performs a log query to provide the information.

Data	Description
Server	Parent servers
Online	Agents connected to their parent servers
Offline	Agents disconnected from their parent servers

Data	Description
Total	Total number of endpoints

To change the information that the widget displays, click ⋮ > ⫲. On the dialog box that appears, specify the **Scope** by clicking >> and selecting the parent servers that the widget uses as its source.

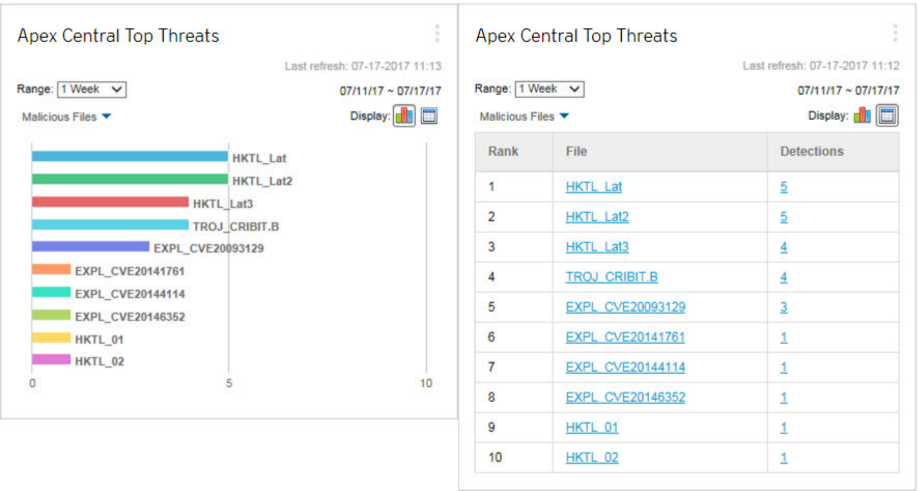
Threat Statistics Tab

The **Threat Statistics** tab contains widgets that display aggregated detections of security threats.

The predefined widgets include:

- Apex Central Top Threats
- Apex Central Threat Statistics
- Threat Detection Results
- Policy Violation Detections
- C&C Callback Events

Apex Central Top Threats Widget



Apex Central Top Threats

Last refresh: 07-17-2017 11:12

Range: 1 Week

07/11/17 ~ 07/17/17

Malicious Files

Display:

Rank	File	Detections
1	HKTL_Lat	5
2	HKTL_Lat2	5
3	HKTL_Lat3	4
4	TROJ_CRIBIT.B	4
5	EXPL_CVE20093129	3
6	EXPL_CVE20141761	1
7	EXPL_CVE20144114	1
8	EXPL_CVE20146352	1
9	HKTL_01	1
10	HKTL_02	1

This widget displays information about the malicious files and malicious URLs detected for a specified time range.

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

Use the drop-down list above the chart/table to select the type of threat data to display.

- **Malicious Files**: Ranks the malicious files detected on your network by the number of detections
- **Malicious URLs**: Ranks the malicious URLs detected on your network by the number of detections

Click a bar, threat name, or detection number to open the **Log Query** screen that displays information about the affected endpoints, threat details, and detection count.

The default view displays the top 10 threats from all the managed products for which the logged on user account has access rights.

- Click the settings icon (⋮ > 🎚) to edit the widget title, product scope, or number of threats that displays.

Apex Central Threat Statistics Widget

This widget displays the total number of security threat detections on your network. Data can be filtered by security threat type or by the location on your network where the threat is detected.

- Product Category

Data	Description
File server	Security threats on file servers detected by any managed product that the Data Scope specifies
Network	Security threats on your network detected by any managed product that the Data Scope specifies
Unknown	Unidentified security threats
Mail	Security threats on email servers detected by any managed product that the Data Scope specifies
Desktop	Security threats on desktops detected by any managed product that the Data Scope specifies
Gateway	Security threats at the gateway detected by any managed product that the Data Scope specifies
Apex Central server	Security threats on Apex Central servers detected by any managed product that the Data Scope specifies

- Violation Type

Data	Description
Behavior Monitoring	Behavior Monitoring violation detected by any managed product that the Data Scope specifies

Data	Description
Content Violation	Content security violations (spam, blocked keywords and expressions) detected by any managed product that the Data Scope specifies
Device Control	Device Control violation detected by any managed product that the Data Scope specifies
Firewall Violation	Firewall violation by any managed product that the Data Scope specifies
Network Content Inspection	Network Content Inspection violation detected by any managed product that the Data Scope specifies
Predictive Machine Learning	Predictive Machine Learning detection by any managed product that the Data Scope specifies
Spyware/Grayware	Spyware/grayware detected by any managed product that the Data Scope specifies
Suspicious Files	Suspicious file detection by any managed product that the Data Scope specifies
Virus/Malware	Viruses/malware detected by any managed product that the Data Scope specifies
Web Security	Web security violations (malicious URLs, blocked URLs) detected by any managed product that the Data Scope specifies

Note

The widget can display data for only one information type at a time.

Click the links in the **Detections** column to open a screen that displays detailed information. Apex Central performs a log query to provide the detailed information.

Data	Description
Type	Type of security threat or managed product where the threat is detected

Data	Description
Detections	Number of security threats detected
Percentage (%)	Security threat percentage of total number of detected threats

Specify the date range for the data that the widget displays:

- Today
- 1 Week
- 2 Weeks
- 1 Month

Specify how the widget displays the data:

- Pie chart
- Bar chart
- Tabular
- Line chart

By default the widget displays data from all the managed products that a user's account privileges allow.

To change the information that the widget displays, click ⋮ > ⚙. On the dialog box that appears, specify the **Scope** by clicking >> and selecting the parent servers that the widget uses as its source.

Threat Detection Results Widget

This widget displays the number of threat detections and the ratio of threats compared to the total number of detections. The widget can display data for only one information type at a time. Clicking links in the **Detections** column opens a screen that displays detailed information. Apex Central performs a log query to provide the detailed information.

Data	Description
Results	The action or result of the action performed by the managed product **Note** This column does not display for the **Web Security** threat type
Policy/Rule	The type of policy/rule applied under the **Web Security** threat type. **Note** This column does not display for other listed threat types.
Detections	The number of security threats detected
Percentage (%)	The percentage of total detections that are security threats

This widget displays threat detections for the following threat types:

Table 1-4. Threat Types

Threat Type	Description
Virus/Malware	Displays the action taken on all files by any managed product that the Data Scope specifies. For example: Cleaned, Access denied, and so on.
Spyware/Grayware	Displays the action taken on all files by any managed product that the Data Scope specifies. For example: Successful, Further action required, and so on.
Content Security	Displays the action taken on all email messages by any managed product that the Data Scope specifies. For example: Deleted, Attachments stripped, and so on.
Web Security	Displays all web security violations blocked using the policies by any managed product that the Data Scope specifies. For example: File blocking, File name, and so on.
Network Virus	Displays the action taken on all network viruses by any managed product that the Data Scope specifies

Click the settings icon (⋮ > 🎚) to edit the widget title, product scope, or type of threats that displays.

Policy Violation Detections Widget

This widget displays the policy violation detections for Network VirusWall Enforcer devices. Clicking links in the **Detections** column opens a screen that displays detailed information. Apex Central performs a log query to provide the detailed information.

Data	Description
Type	Lists **Service Violations** as a type of security threat
Updated	Last updated date
Detections	Number of service violations Network VirusWall Enforcer devices detect

Click the settings icon (⋮ > 🎚) to edit the widget title or product scope.

Note

This widget only displays policy violation detections for Network VirusWall Enforcer.

Click **Save** to apply changes and exit.

C&C Callback Events Widget

This widget displays the number of C&C callback attempts based on compromised hosts or callback addresses. The widget can display data for only one information type at a time. Clicking the numbers in any table cells opens the **C&C Callback Events** screen, which contains the following callback summary data:

Data	Description
Compromised Host	Affected host or email address
Callback Address	URL, IP address, or email address to which a compromised host attempts a callback
C&C Server Location	Region and country where the C&C server locates
Callback Attempts	Number of contacts made between callback addresses and compromised hosts
Latest Callback Address/ Compromised Host	URL, IP address, or email address to which the last callback attempt was logged
Callback Addresses/ Compromised Hosts (with numbers displayed in the columns)	Number of compromised hosts or callback addresses associated with the callback attempts
Logged By	Name of the managed product that logged the event

Click the settings icon (⋮ > 🎚) to edit the following:

- **Title**: Modify the title of the **C&C Callback Events** widget.
- **Scope**: Click >> and select the parent servers that the widget uses as the source.
- **C&C list source**: Select **Global Intelligence**, **Virtual Analyzer**, or **User-defined** as the C&C list sources.
- **Items to display**: Select the number of items to display on the widget.

Click **Save** to apply changes and exit.

Chapter 2

Policy Management

This section contains information about how to perform policy management on managed products and endpoints.

Important

Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the *Apex Central Widget and Policy Management Guide*.

You can download a PDF version of the guide using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

You can also view the guide online using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central-widget-and-policy-management-guide/introduction.aspx

Topics include:

Policy Management

Policy management allows administrators to enforce product settings on managed products and endpoints from a single management console. Administrators create a policy by selecting the targets and configuring a list of product settings.

To perform policy management on a new managed product or endpoint, move the managed product from the **New Entity** folder to another folder in the Product Directory structure.

Creating a New Policy

Important

Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the *Apex Central Widget and Policy Management Guide*.

You can download a PDF version of the guide using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

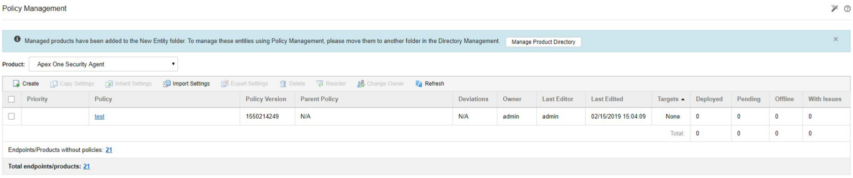
You can also view the guide online using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central-widget-and-policy-management-guide/introduction.aspx

Procedure

1. Go to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.



Policy Management

Managed products have been added to the New Entity folder. To manage these entities using Policy Management, please move them to another folder in the Directory Management. Manage Product Directory

Product: Apex One Security Agent

Create | Copy Settings | Inherit Settings | Import Settings | Export Settings | Delete | Reorder | Change Owner | Refresh

□	Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets ▲	Deployed	Pending	Offline	With Issues
□		test	1550214249	N/A	N/A	admin	admin	02/15/2019 15:04:09	None	0	0	0	0
									Total:	0	0	0	0

Endpoints/Products without policies: 21

Total endpoints/products: 21

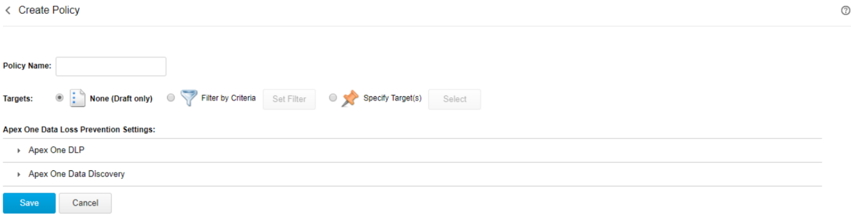
2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

   For more information about configuring policy settings for specific managed products, see the *Apex Central Widget and Policy Management Guide*.

3. Click **Create**.

   The **Create Policy** screen appears.



Create Policy

Policy Name:

Targets: ● None (Draft only) ○ Filter by Criteria ○ Specify Target(s)

Apex One Data Loss Prevention Settings:

- Apex One DLP
- Apex One Data Discovery

4. Type a policy name.

5. Specify targets.

   Apex Central provides several target selection methods that affect how a policy works.

   Note

   To include a managed product or endpoint as a target, make sure the product version of the managed product or endpoint supports policy management in Apex Central. The **Policy Template Settings** screen (**Policies** > **Policy Resources** > **Policy Template Settings**) contains information about supported product versions.

   The policy list arranges the policy targets in the following order:

   - **Specify Targets**: Use this option to select specific endpoints or managed products.

For details, see *Specifying Policy Targets on page 2-9*.

- **Filter by Criteria**: Use this option to allocate endpoints automatically based on the filtering criteria.

  For details, see *Filtering by Criteria on page 2-5*.

- **None (Draft only)**: Use this option to save the policy as a draft without choosing any targets.

For more information about the policy list, see *Understanding the Policy List on page 2-21*.

6. Click a managed product feature to expand it and configure its settings. Repeat this step to configure all features.

   - Each feature has a link to a Help topic that discusses the feature and how to use it.

   - For certain product settings, Apex Central needs to obtain specific setting options from the managed products. If administrators select multiple targets for a policy, Apex Central can only obtain the setting options from the first selected target. To ensure a successful policy deployment, make sure the product settings are synchronized across the targets.

   - If you are creating a policy for **Apex One Security Agent** that you want to act as a parent to a future child policy, configure settings that can be inherited, customized, or extended on the child policy.

     - For a list of Security Agent settings that can be inherited, customized, or extended, see *Working with Parent Policy Settings on page 2-11*.

     - For details on creating a child policy, see *Inheriting Policy Settings on page 2-14*.

7. Click **Deploy** or **Save**.

   If you clicked **Deploy**, Apex Central starts the deployment. The deployed policy appears in the list on the **Policy Management** screen. It usually takes a few minutes for Apex Central to deploy the policy to the targets.

Click **Refresh** on the **Policy Management** screen to update the status information in the policy list. If the status of the deployment remains pending after an extended period of time, there might be issues with the targets. Check if there is a connection between Apex Central and the targets. Also check if the targets are working properly.

Once Apex Central deploys a policy to the targets, the settings defined in the policy overwrite the existing settings in the targets. Apex Central enforces the policy settings in the targets every 24 hours. Although local administrators can make changes to the settings from the managed product console, the changes are overwritten every time Apex Central enforces the policy settings.

- Apex Central enforces the policy settings on the targets every 24 hours. Since policy enforcement only occurs every 24 hours, the product settings in the targets may not align with the policy settings if local administrators make changes through the managed product console between the enforcement period.
- Policy settings deployed to IMSVA servers take priority over the existing settings on the target servers instead of overwriting them. IMSVA servers save these policy settings on the top of the list.
- If an Apex One Security Agent assigned with a Apex Central policy has been moved to another Apex One domain, the agent settings will temporarily change to the ones defined by that Apex One domain. Once Apex Central enforces the policy again, the agent settings will comply with the policy settings.

Filtering by Criteria

Use this option to allocate endpoints automatically based on the filtering criteria.

This option:

- Is only available on the following managed products:
  - Apex One (Mac)

    - Apex One Data Loss Prevention
    - Apex One Security Agent
    - Mobile Security for Enterprise
    - Trend Micro Endpoint Application Control
- Uses a filter to automatically assign current and future targets to the policy
- Is useful for deploying standard settings to a group of targets

Administrators can change the priority of filtered policies in the policy list. When an administrator reorders the policy list, Apex Central re-assigns the targets to different filtered policies based on the target criteria and the user roles of each policy creator.

Apex Central can only assign endpoints without policies to a new filtered policy. To re-allocate an endpoint already assigned to a filtered policy, move another filtered policy with the matching criteria up the priority list.

See *Assigning Endpoints to Filtered Policies on page 2-8* for more information on how Apex Central assign targets to filtered policies.

Procedure

1. On the **Create Policy** screen, go to the **Targets** section, select **Filter by Criteria**, and then click **Set Filter**.

   The **Filter by Criteria** screen appears.

2. Select the following options and define the criteria.

Criteria	Description
Match keywords in	Define keywords based on the host name or Apex Central display name. **Note** Apex Central performs partial matching for single keyword searches. You can search multiple, comma-separated keywords, however,Apex Central only provides full string matches for each keyword provided.
IP addresses	Define a range of IP addresses and click **Add**. **Note** • Policy management only supports IPv4 addresses. • When a new managed product or endpoint registers to Apex Central, it takes about an hour for the managed product or endpoint to become available for searching by IP address.
Operating systems	Select one or more operation systems from the drop-down list.
Directories	Select one of the following directories and define the criteria. • **Product Directory**: Select folders from the Product Directory structure • **Active Directory**: Select organizational units from an integrated Active Directory structure • **Apex One domain hierarchy**: Type at least one Apex One domain hierarchy keyword

3. Click **Save**.

   The **Create Policy** screen reloads.

Assigning Endpoints to Filtered Policies

When a new endpoint registers to Apex Central, it goes through the filtered policies in the list in descending order. Apex Central assigns the new endpoint to a filtered policy when the following conditions are both satisfied:

- The new endpoint matches the target criteria in the policy
- The policy creator has the permission to manage the new endpoint

The same action applies to an endpoint already assigned to a policy, but the policy creator later deletes the policy.

Note

For endpoints just registered to Apex Central and for those just released from deleted policies, there is a three-minute grace period during which no endpoint allocation occurs. These endpoints are temporarily without policies during this period.

If an endpoint does not meet the target criteria in any filtered policies, the endpoint does not associate with any policies. Apex Central allocates these endpoints again when the following actions occur:

- Create a new filtered policy
- Edit a filtered policy
- Reorder the filtered policies
- Daily endpoint allocation schedule

  Apex Central uses a daily endpoint allocation schedule to ensure that endpoints are assigned to the correct policies. This action occurs once at 3:15 pm every day. When endpoint properties change, such as the operating system or IP address, these endpoints require the daily schedule to re-assign them to the correct policies.

Note

- If the endpoints are offline during the daily endpoint allocation schedule, the policy status for these endpoints will remain pending until they go online.
- If the Apex One domain of the endpoint is changed, Apex Central deploys the updated the policy after 10 minutes.

When the above actions occur, Apex Central allocate endpoints based on the following conditions:

TABLE 2-1. Endpoint Allocation for Filtered Policies

	New endpoints or endpoints from deleted policies	Endpoints without policies	Endpoints with policies
Create a new policy		●	
Edit a policy	●	●	●
Reorder the filtered policies	●	●	●
Daily endpoint allocation schedule	●	●	●

Specifying Policy Targets

Use this option to select specific endpoints or managed products.

This option:

- Uses the search or browse function to locate specific targets and manually assigns them to the policy
- Is useful when administrators plan to deploy specific settings only to a certain targets
- Remains static on the top of the policy list and takes priority over any filtered policies

Procedure

1. On the **Create Policy** screen, go to the **Targets** section, select **Specify Target(s)**, and then click **Select**.

   The **Specify Targets** screen appears.

2. Use **Search** or **Browse** to locate the targets.

   - **Search**: Use the following search criteria to find endpoints or managed products. The search results display the endpoints or managed products matching all of the selected criteria.

     - **Match keywords in**: Define keywords based on the host name or Apex Central display name.

     - **IP addresses**: Define a range of IP addresses and click **Add**.

       Note

       - Policy management only supports IPv4 addresses.

       - When a new managed product or endpoint registers to Apex Central, it takes about an hour for the managed product or endpoint to become available for search by IP address.

     - **Operating systems**: Select one or more operating systems from the drop-down.

   - **Browse**: Browse the Product Directory or Active Directory to locate endpoints or managed products to assign to the policy.

3. Select the endpoints or managed products and then click **Add Selected Targets**.

4. Wait for the numbers in **View Action List** and **View Results** to change.

5. Click **OK**.

   The **Create Policy** screen reloads.

Working with Parent Policy Settings

Apex Central administrators who create a parent policy for an **Apex One Agent** can configure certain policy settings to be inherited, customized, or extended.

> **Note**
>
> These options are not available on other managed products.

- **Inherit from parent**
  - A child policy administrator cannot change the setting at all. An Apex One administrator can manually change the setting from the Apex One server console. However, the setting will be overwritten when Apex Central deploys policies to the Apex One server.

    For example, a Apex Central administrator can create a parent policy that enforces the exclusion of PDF files from a Manual Scan.
  - Changes to the setting on the parent policy are always enforced on the child policy.
  - If the permission on the parent policy changes from "Inherit from parent" to "Are customizable" or "Extend from parent", the child policy administrator can customize or extend the current setting. Changes to the setting on the parent policy are no longer enforced.
- **Are customizable**
  - A child policy can deviate from the setting configured in the parent policy.

    For example, if Scheduled Scan on the parent policy runs weekly but is customizable, the child policy administrator can change the schedule to daily.
  - Changes to the setting on the parent policy are never enforced on the child policy.
  - If the permission on the parent policy changes from "Are customizable" to "Inherit from parent", the current setting on the

parent policy overwrites the setting on the child policy. Changes to the setting on the parent policy are always enforced.

- **Extend from parent**
    - A child policy administrator can add to the items configured in the parent policy.

      For example, if the parent policy excludes 20 file names from being scanned during a Manual Scan, the administrator can add 10 more safe and trustworthy files to the child policy.
    - Items added or removed from the parent policy are also added or removed from the child policy. A removed item can be added back to the child.
    - If the permission on the parent policy changes from "Extend from parent" to "Inherit from parent", items in the child policy that have no match in the parent are removed. Changes to the items on the parent policy are always enforced.

The following table lists the parent policy settings that can be inherited, customized, or extended.

Setting and Path	Available Options		
	Inherit From Parent	Are Customizable	Extend From Parent
Scan schedule **Scheduled Scan Settings** > **Target** tab > **Schedule** section	●	●	
File extensions to scan **Manual Scan / Real-time Scan / Scan Now / Scheduled Scan Settings** > **Target** tab > **Files to Scan** section > **Files with the following extensions** option	●		●

Setting and Path	Available Options		
	Inherit From Parent	Are Customizable	Extend From Parent
Scan exclusion lists (directories, files, and file extensions to exclude from scans) **Manual Scan / Real-time Scan / Scan Now / Scheduled Scan Settings** > **Scan Exclusion** tab	●		● Note When selecting **Extend from parent** from a scan exclusion list, the list expands to show a **Child Policy Restrictions** section where the parent policy creators can specify items that child policies cannot exclude from scans.

Copying Policy Settings

Administrators can copy the settings from an existing policy, create a new policy with the same settings, and deploy the settings to different endpoints or managed products.

Note

It is not possible to copy the settings of a child **Apex One Agent** policy. To determine whether the **Apex One Agent** policy is a child or a parent, check the **Parent Policy** column. A clickable value displays if the policy is a child, and N/A if otherwise.

Procedure

1. Go to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select the type of product settings from the Product list.

   The screen refreshes to display policies created for the selected managed product.

3. Select a policy from the list.

4. Click **Copy Settings**.

   The **Copy and Create Policy** screen appears.

5. In the **Policy Name** field, type a name for the policy.

6. Assign **Targets** to the policy.

7. (Optional) Change settings as necessary.

8. Click **Deploy**.

Note

- After clicking **Deploy**, please wait two minutes for Apex Central to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.
- Apex Central enforces the policy settings on the targets every 24 hours.

Inheriting Policy Settings

Create a new child policy by inheriting the settings of an existing parent policy. A child policy cannot be copied and its settings cannot be inherited.

This task requires a parent policy for the Apex One agent. A parent policy for the Apex One agent has the value **N/A** displayed under the **Parent Policy** column.

Procedure

1. Go to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select **Apex One Agent** from the Product list.

   The screen refreshes to display policies created for the selected managed product.

3. Select a parent policy that does not have locally managed settings.

4. Click **Inherit Settings**.

   The **Inherit and Create Policy** screen appears.

5. In the **Policy Name** field, type a name for the policy.

6. Assign **Targets** to the policy.

7. (Optional) Review the settings that can be customized or extended and then make changes as necessary. For a list of settings to review, see *Working with Parent Policy Settings on page 2-11*.

   Note

   A setting cannot be customized or extended if the option selected on the parent policy is **Inherit from parent**.

   For example:

   - If the Scheduled Scan setting is customizable, you can change the schedule from weekly to daily.

   - If the scan exclusion list for Real-time Scan can be extended, you can type additional file names that you deem safe and trustworthy. After the child policy is created, it will add those file names to the scan exclusion list.

8. Click **Deploy**.

Note

- After clicking **Deploy**, please wait two minutes for Apex Central to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.
- Apex Central enforces the policy settings on the targets every 24 hours.

Modifying a Policy

Administrators can modify policy targets and settings as necessary. The root account owner can modify every policy in the list, while other account owners can only modify the policies they created. After a policy is modified, Apex Central deploys the policy to the targets.

Important

Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the *Apex Central Widget and Policy Management Guide*.

You can download a PDF version of the guide, or view the guide online, using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

For a parent policy for the Apex One agent, if you modified the targets and settings for specific features, the modifications will apply to all child policies and deployed to the respective targets. Some settings on a parent policy support **permissions**, which control the changes allowed on child policies. Modifications to these parent policy permissions are also applied to child policies and deployed to targets. For a list of settings that support permissions, see *Working with Parent Policy Settings on page 2-11*.

For example:

- If you changed the scan schedule permission from "Inherit from parent" to "Are customizable", administrators can start to customize the existing schedule on their child policies.
- If you changed the Manual Scan file extensions permission from "Extend from parent" to "Inherit from parent", any file extensions that administrators added to child policies will be removed. In addition, administrators will no longer be able to add file extensions.

Procedure

1. Navigate to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

3. Click a policy name in the **Policy** column.

   The **Edit Policy** screen appears.

4. Modify the policy.

   Note

   Modifying the filtering criteria in a filtered policy can affect target allocation. Apex Central may re-assign some targets to other filtered policies, or add additional targets to the current policy.

5. Click **Deploy**.

   It usually takes a few minutes for Apex Central to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list. If the status of the deployment remains pending after an extended period of time, there might be issues with the targets. Check if there is a connection between Apex Central and the targets. Also check if the targets are working properly.

Apex Central enforces the policy settings on the targets every 24 hours.

Importing and Exporting Policies

Export policies for backup or to import to another Apex Central server of the same version.

Note

- Apex Central exports policy settings but not policy targets.
- A parent policy stays as a parent after the export or import.
- A child policy becomes a parent after the export. Consequently, it is a parent after the import.
- Apex Central cannot import a policy if its name is the same as an existing child policy. If the existing policy is not a child, Apex Central overwrites it after the import.
- For more information, see the following topics:
    - *Creating a New Policy on page 2-2*
    - *Inheriting Policy Settings on page 2-14*

Procedure

1. Go to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

3. To export, select one or several policies, click **Export Settings**, and then save the resulting policy file.

   - If you exported a single policy, the resulting file has the extension `*.cmpolicy`.

- If you exported several policies, the resulting file is a compressed (`*.zip`) file containing the individual `.cmpolicy` files.

4. To import, click **Import Settings** and then locate and load the policy file.

    - You can import an entire `*.zip` file or import individual `*.cmpolicy` files one by one.
    - If the policy already exists in the policy list, a confirmation prompt appears, asking if you want to overwrite the existing policy.

      Click **OK** to proceed.

    The screen refreshes and displays the imported policy at the top of the list.

    For more information about reordering the policy list, see *Reordering the Policy List on page 2-24*.

Deleting a Policy

Administrators can remove a policy from the list. Apex Central then re-allocates the targets associated with the deleted policy if the targets match the filtering criteria of another policy. Those without a match become endpoints without policies, and they keep the settings defined by the deleted policy unless a managed product administrator modifies the settings.

Apex Central only allows policy creators to delete their own policies. However, the root account can delete every policy in the list.

It is not possible to delete an Apex One Agent parent policy with settings *inherited* by an existing child policy.

Procedure

1. Go to **Policies** > **Policy Management**.

    The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

The screen refreshes to display policies created for the selected managed product.

3. Select the policy to delete.
4. Click **Delete**.

   A confirmation screen appears.
5. Click **OK**.

Changing the Policy Owner

The default owner of a policy is the user account that created the policy. You can use the **Policy Management** screen to change the owner of a policy to any Apex Central user account. You can also change the policy owner to an Active Directory group, which designates all Active Directory users within the group as owners of the policy.

Important

If you change the owner of a policy to a user account that does not have access rights to the specified targets, the new owner can modify the policy settings but cannot view the policy data.

Procedure

1. Go to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.
2. Select one or more policies to change the owner.
3. Click **Change Owner**.

   The **Change Policy Owner** screen appears.
4. Select a user account from the drop-down list.
5. Click **Save** to change the owner.

Apex Central sends an email notification to all user accounts assigned the “Administrator” role.

Understanding the Policy List

The policy list displays the information and status of policies created by all users. When a new endpoint registers to Apex Central, it goes through the filtered policies in the list in descending order. Apex Central assigns the new endpoint to a filtered policy when the following conditions are both satisfied:

- The new endpoint matches the target criteria of the policy
- The policy creator has the permission to manage the new endpoint

The following table describes the policy list columns that display on the **Policy Management** screen. Click a column to sort the data.

TABLE 2-2. Policy List

COLUMN	DESCRIPTION
Priority	Displays the priority of the policies • Apex Central lists policies from the highest to the lowest priority. • When administrators create a filtered policy, Apex Central saves the new policy as the lowest priority policy. • A specified policy takes priority over any filtered policies and remains on the top of the list. Administrators cannot reorder specified policies. • Apex Central places draft policies at the bottom of the list.
Policy	Displays the name of the policy

Column	Description
Policy Version	This column only appears if the selected product is **Apex One Security Agent**. Displays the latest policy version deployed **Note** Some targets might not have the latest policy version deployed. To view the current policy deployed on specific targets, click the number in the **Deployed** column.
Parent Policy	This column only appears if the selected product is **Apex One Security Agent**. If a policy is a child policy (that is, it inherited its settings from a parent policy), this column shows the name of the parent policy. Otherwise, N/A displays.
Deviations	This column only appears if the selected product is **Apex One Security Agent**. If a policy is a child policy, this column shows the number of settings that have been changed on the policy and are therefore inconsistent with settings on the parent policy. If settings are consistent between the policy and its parent, 0 (zero) displays. If a policy is not a child policy, N/A displays.

COLUMN	DESCRIPTION
Owner	Displays the user who is currently assigned the policy **Note** The default owner is the user who created the policy. • If you change the owner of a policy to a user account that does not have access rights to the specified targets, the new owner can modify the policy settings but cannot view the policy data. • You can also assign multiple owners by assigning the policy to an Active Directory group. For more information, see *Changing the Policy Owner on page 2-20*.
Last Editor	Displays the user who last edited the policy
Last Edited	This column only appears if the selected product is **Apex One Security Agent**. Displays when the policy was last edited
Targets	Displays how administrators select targets for the policy. • **Specified**: Uses the browse or search function to select specific targets for the policy. Specified policies remain static on the top of the policy list and take priority over filtered policies. • **Filtered**: Uses a filter to automatically assign current and future endpoints to the policy. Administrators can rearrange the priority of filtered policies. Hover over an item to conveniently view the filter criteria and make adjustments as necessary. • **None**: The policy creator saved the policy as a draft without selecting any targets.
Deployed	Displays the number of targets that have applied the policy settings or have unactivated product services Click the number to view the policy status.

Column	Description
Pending	Displays the number of targets that have not applied the policy settings Click the number to view the policy status.
Offline	Displays the number of targets that have offline agents Click the number to view the policy status.
With Issues	Displays the number of targets that have not applied the policy settings due to unsupported policy deployment, no policy configuration, system errors, endpoint communication errors with the product server, unsupported endpoints, locally changed settings, disabled product services, or partial deployment Click the number to view the policy status.

Note

The numbers in **Deployed** and **Pending** columns only reflect the endpoints or managed products that an administrator has permission to manage.

Reordering the Policy List

Administrators can use the **Reorder** button to change the order of the filtered policies. Rearranging the policy list can affect target allocation. Apex Central may re-assign some targets to different filtered policies.

Note

- Specified policies remain static and always take priority over filtered policies.
- This function is only available for managing Apex One settings.

Procedure

1. Go to **Policies** > **Policy Management**.

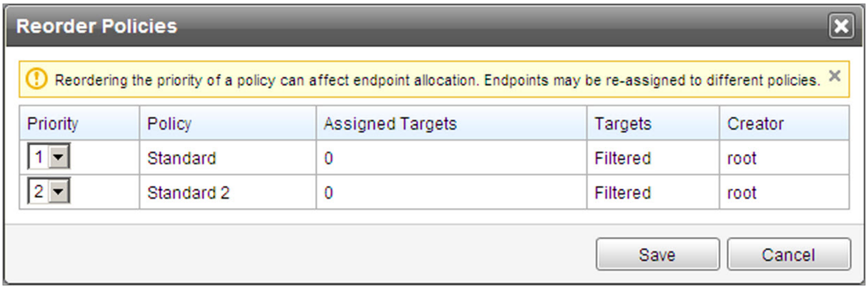
   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

3. Click **Reorder**.

   The **Reorder Policies** screen appears.



Reordering the priority of a policy can affect endpoint allocation. Endpoints may be re-assigned to different policies.

Priority	Policy	Assigned Targets	Targets	Creator
1	Standard	0	Filtered	root
2	Standard 2	0	Filtered	root

4. Rearrange the order of the **Priority** column.

5. Click **Save**.

Note

After clicking **Save**, please wait two minutes for Apex Central to re-assign the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.

Policy Status

Policy status allows administrators to check if Apex Central has successfully deployed a policy to its targets.

To check the policy deployment status, use one of the following methods:

- On the **Policy Management** screen, click a number in the policy list. The **Log Query** screen appears.

- On the dashboard, click a number in the **Policy Status** widget. The **Log Query** screen appears.
- Perform a log query

The following table provides the descriptions and suggestions about each policy status:

TABLE 2-3. Policy Status

POLICY STATUS	DESCRIPTION	SUGGESTIONS
Pending	Apex Central is processing the policy.	Wait a few minutes and then check the status again.
Without policy	Apex Central has not assigned a policy to this endpoint or managed product.	Assign a policy to the endpoint or managed product.
Deployed	Apex Central has successfully deployed the policy.	N/A
Endpoint unable to connect to server	• The endpoint did not receive the policy settings. • The server is currently busy.	• Check the connection status of the endpoint • Connect the endpoint to the company network • Wait for the updated policy status

Policy Status	Description	Suggestions
Inapplicable product settings	The managed product cannot process some of the policy settings.	- Verify the policy settings - Update to the latest policy template version - Check the settings on the managed product - Verify the IP address of the managed product on the **Managed Servers** screen If the IP address is incorrect, unregister and then register the managed product again to Apex Central. - Refer to the *Administrator's Guide* for the managed product
Unsupported endpoint	The endpoint does not support some features specified in the policy settings.	Upgrade the agent to a supported version.
Settings changed locally	Some settings on the endpoint or managed product do not comply with the settings specified in the policy because the managed product administrator has made some changes through the managed product console.	Verify the settings on the managed product console.
Unactivated licenses	The managed product has not activated the licenses for some of the services specified in the policy settings.	Activate the licenses for the related services from the **License Management** screen on the Apex Central console
Disabled product services	The managed product has disabled some of the services specified in the policy settings.	Enable the related services on the managed product.
Partially deployed	Apex Central has enforced a portion of the policy settings.	Wait a few minutes and then check the status again.

Policy Status	Description	Suggestions
Managed by [Apex Central server name]	Another Apex Central is currently managing the managed product.	Remove the managed product from the Managed Server list and add the managed product to the list again.
Invalid user name or password	The user name or password for authentication is incorrect.	Verify the user name or password.
Invalid product server or authentication information	The server name or the authentication information is incorrect.	Verify the server name and the authentication information.
Unable to automatically log on to product	Apex Central cannot use the single sign-on function to access the managed product.	• Check the single sign-on function in the Product Directory • Check the connection status of the MCP agent • Change the server connection type from **Automatic** to **Manual** in the **Managed Servers** list.
Web server configuration error	A web service error has occurred.	Check the IIS configuration.
Product communication error	Unable to access the product console.	• Check if you can connect to the managed product's web console. • Check the settings of the managed product.
Unable to connect to product	Apex Central cannot establish a connection with the managed product.	• Check the connection status of the managed product. • Check the network connection
Unsupported product version	The managed product version is not supported.	Upgrade the managed product to a supported version.

Policy Status	Description	Suggestions
Network configuration error	A network connection error has occurred.	Check the network connection.
System error. Error ID: [error ID number].	A system error has occurred.	Contact your Trend Micro support representative.

Chapter 3

Policy Resources

This section contains information about policy resources for integrated products/services.

Important

Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the *Apex Central Widget and Policy Management Guide*.

You can download a PDF version of the guide, or view the guide online, using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

Topics include:

Application Control Criteria

Configure Application Control criteria that you can then assign to Security Agent policy rules. You can create “Allow” and “Block” criteria to limit the applications that users can execute or install on protected endpoints. You can also create assessment criteria to monitor the applications executing on endpoints and then refine the criteria based on the usage results.

Important

You must configure Application Control criteria before deploying an Application Control policy to Security Agents.

Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the *Apex Central Widget and Policy Management Guide*.

You can download a PDF version of the guide, or view the guide online, using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

The following table outlines the tasks available on the **Application Control Criteria** screen.

Task	Description
Add criteria	Click the **Add Criteria** drop-down button and select from the following options: • **Allow**: Click to define “Allow” or “Lockdown” criteria For more information, see *Defining Allowed Application Criteria on page 3-4*. • **Block**: Click to define “Block” or “Assessment” criteria For more information, see *Defining Blocked Application Criteria on page 3-6*. • **Copy**: Select an existing criteria and click **Copy** to define new criteria based on the existing settings • **Import**: Click to select a ZIP package exported from a compatible Application Control source **Note** If the imported package contains criteria names that match preexisting criteria, you have the option to **Overwrite** existing criteria or **Skip** the import of the criteria with duplicated names.
Export criteria	Select the check box to the left of existing criteria and click **Export** to save the selected criteria to a ZIP package (`<timestamp>_iACRuleExport.zip`)
Delete criteria	Select the check box to the left of existing criteria and click **Delete** to remove the selected criteria from the list **WARNING!** If you selected criteria used by existing Apex One Security Agent policies, you must confirm that you want to delete and remove the criteria from all affected Security Agent policies. You cannot undo this action.

Task	Description
Modify criteria	Click a **Criteria Name** to modify the criteria settings **Note** Affected endpoints receive modified criteria settings the next time the Security Agents connect to the server.
View policy associations	Click the value in the **Target Policies** column to display a list of all Apex One Security Agent policies that implement the criteria. **Tip** Click a policy name to open a new browser tab on which you can view or modify the policy settings.

Defining Allowed Application Criteria

Application Control provides the ability to define criteria that specifically allow certain applications to execute. You can define allow criteria to ensure that Application Control never blocks a certain application, or you can create a complete list of applications allowed to execute on endpoints and then deploy a **Lockdown** policy to the endpoints. While in **Lockdown** mode, users cannot execute, access, or install any application that you did not include in the allow criteria.

For more information about Lockdown policies, see *Application Control Policy Settings*.

Procedure

1. Go to **Policies** > **Policy Resources** > **Application Control Criteria**.

   The **Application Control Criteria** screen appears.

2. Click **Add Criteria** and select **Allow**.

   The **Allow Criteria Settings** screen appears.

3. Type a unique **Name** for the criteria.

4. Select the level of **Trust permission** for the applications.

Permission	Description	Example Use
Application cannot execute external processes	Applications cannot access any external processes or start any other applications	Use when you want to allow standalone applications to run on endpoints but prevent access to other processes For example, this setting allows Microsoft Word to run but prevents embedded OLE objects from executing.
Application can execute other processes	Applications can start external processes and applications that users are unable to access directly	Use when you want to allow applications to run on endpoints and still allow access to required child processes or add-ons. For example, this setting allows Internet Explorer to run and also allows Internet Explorer to execute any installed plug-ins.
Inheritable execution rights (not recommended)	Applications can install and start external processes and applications, and the child applications can also install and start external processes and applications	Use when you want to allow installation packages to execute on the endpoint **Inheritable execution rights (not recommended)** allows the installation package to perform all installation tasks and then also allows the installed application to run all required processes.

5. Select the **Match method** used to identify applications and configure required settings.

Method	Description
Application Reputation List	Allows you to apply the criteria to applications that Trend Micro has tested and assigned a security score for For more information, see *Application Reputation List on page 3-8*.
File paths	Allows you to apply the criteria to any application installed in the specified location For more information, see *File Paths on page 3-9*.
Certificates	Allows you to apply the criteria to applications based on certificate validity and certificate attributes For more information, see *Certificates on page 3-12*.
Hash values	Allows you to apply the criteria to applications based on SHA-1 or SHA-256 hash values For more information, see *Hash Values on page 3-13*.
Gray Software List	Allows you to include applications to the criteria that Trend Micro has tested and found to be potentially harmful The Gray Software List is a subset of the Application Reputation List and contains applications that may be malicious if not used properly. Trend Micro recommends blocking or monitoring applications in the Gray Software List to ensure that your network remains secure.

6. Click **Save**.

Defining Blocked Application Criteria

Application Control provides the ability to define criteria that specifically block certain applications from executing. You can define block criteria to ensure that Application Control always blocks certain applications or you can create “Assessment” criteria to monitor the applications that users access.

Procedure

1. Go to **Policies** > **Policy Resources** > **Application Control Criteria**.

The **Application Control Criteria** screen appears.

2. Click **Add Criteria** and select **Block**.

   The **Block Criteria Settings** screen appears.

3. Type a unique **Name** for the criteria.

4. To create a monitoring rule, select **Enable assessment mode**.

   Note

   Application Control logs all applications that match the assessment criteria but takes no further action. Application Control allows the applications to execute normally.

5. Select the **Match method** used to identify applications and configure required settings.

Method	Description
Application Reputation List	Allows you to apply the criteria to applications that Trend Micro has tested and assigned a security score for For more information, see *Application Reputation List on page 3-8*.
File paths	Allows you to apply the criteria to any application installed in the specified location For more information, see *File Paths on page 3-9*.
Certificates	Allows you to apply the criteria to applications based on certificate validity and certificate attributes For more information, see *Certificates on page 3-12*.
Hash values	Allows you to apply the criteria to applications based on SHA-1 or SHA-256 hash values For more information, see *Hash Values on page 3-13*.

Method	Description
Gray Software List	Allows you to include applications to the criteria that Trend Micro has tested and found to be potentially harmful The Gray Software List is a subset of the Application Reputation List and contains applications that may be malicious if not used properly. Trend Micro recommends blocking or monitoring applications in the Gray Software List to ensure that your network remains secure.

6. Click **Save**.

Application Match Methods

Application Control provides multiple methods for identifying applications to include in the allow and block criteria.

Note

Application Control also provides the Gray Software List which you cannot modify.

The Gray Software List is a subset of the Application Reputation List and contains applications that may be malicious if not used properly. Trend Micro recommends blocking or monitoring applications in the Gray Software List to ensure that your network remains secure.

- *Application Reputation List on page 3-8*
- *File Paths on page 3-9*
- *Certificates on page 3-12*
- *Hash Values on page 3-13*

Application Reputation List

The Application Reputation List is a comprehensive list of applications tested by Trend Micro. The list includes most popular operating system files and binaries as well as applications for desktops, servers, and mobile devices. Trend Micro periodically provides updates to the list.

Important

Ensure that you have turned on regular updates to the Certified Safe Software Pattern to stay up-to-date with the latest application information.

You can search for applications by typing the name of **Vendors** or **Applications**. Select applications using the data provided.

Data	Description
Application	The name of the application
AIR Score	A comprehensive security score based on an application's popularity and reputation
Global Usage	The global prevalence of the application **Tip** Click the prevalence to view a regional breakdown of the application usage.

File Paths

You can configure Application Control to specifically target certain directory locations based on absolute path, storage type, and Perl Compatible Regular Expressions (PCRE).

Select whether to match by a specific path or a storage type, and specify the match string type (**String** or **Regular Expression (PCRE)**). Type the file paths that apply to the criteria.

Note

- Application Control supports the use of the asterisk (*) wildcard when specifying a **String** type match. The asterisk character can represent one or more characters in a subdirectory of the specified string location.
- You cannot use wildcard characters to indicate the entire contents of the selected storage location.
- You can specify up to 100 file paths.

Table 3-1. Supported Storage Locations

Storage Location	Environment Variable	Description
Specific path	Not applicable	Only applies to applications in the exact path specified **Note** Application Control does not check device type when using this location type.
Any built-in storage	$FixedDrives	Only applies to applications in the path specified and stored on an internal storage device (internal hard disk drive)
Any local storage	$LocalDrives	Only applies to applications in the path specified and stored on a non-removable local storage device (internal or external hard disk drive)
Any removable storage	$RemovableDrives	Only applies to applications in the path specified and stored on a removable storage device (USB drive, CD/DVD)
Network path	$RemoteDrives	Only applies to applications in the path specified and stored on a shared network resource
Program Files folder	$ProgramFiles	Only applies to applications in the path specified and stored in the Program Files folders (default folders `C:\Program Files` and `C:\Program Files (x86)`)
System volume	$SystemDrive	Only applies to applications in the path specified and stored in the default Windows system drive

File Path Example Usage

GOAL	ALLOW RULE	BLOCK RULE	RESULTS
Block all applications located in any folder under theMyApps subfolder of either Program Files directory	-	1. **Program Files folders** 2. **String** 3. `\MyApps*`	Blocks: • `C:\Program Files(x86)\MyApps\start.exe` • `C:\Program Files\MyApps\start.exe` • `C:\Program Files(x86)\MyApps\bin\start.exe` Allows: • `C:\Program Files(x86)\start.exe`
Allow all applications located in any folder under theMyApps subfolder of either Program Files directory but Block all other applications/ folders	1. **Program Files folders** 2. **String** 3. `\MyApps*`	1. **Any local storage** 2. **String** 3. `C:\Program Files\*` AND 1. **Any local storage** 2. **String** 3. `C:\Program Files (x86)\*`	Blocks: • `C:\Program Files(x86)\start.exe` Allows: • `C:\Program Files(x86)\MyApps\start.exe` • `C:\Program Files\MyApps\start.exe` • `C:\Program Files(x86)\MyApps\bin\start.exe`

Goal	Allow Rule	Block Rule	Results
Block only applications located in theMyApps subfolder of either Program Files directory but Allow all other applications/ folders	1. Allow the subfolders of the MyApps directory a. **Program Files folders** b. **String** c. `\MyApps\*\*`	1. **Program Files folders** 2. **String** 3. `\MyApps\*`	Blocks: - `C:\Program Files(x86)\MyApps\start.exe` - `C:\Program Files\MyApps\start.exe` Allows: - `C:\Program Files(x86)\start.exe` - `C:\Program Files(x86)\MyApps\bin\start.exe`

Certificates

You can configure Application Control to specifically target applications based on the “trust” level of a certificate and that contain specific certificate attributes.

Select the type of certificate “trust” level and then specify the required certificate “Issuer” or “Subject” information.

Note

Application Control supports the use of the asterisk (*) wildcard when specifying Certificate attributes, although you must use the wildcard in conjunction with other characters to limit the scope. For example, you cannot use only the wildcard character in any field.

The following table describes the different “trust” types.

Type	Description
Trusted (valid)	You must have included the certificate in the trusted certificates list and the certificate must not have expired
Trusted (expired)	You must have added the certificate in the trusted certificates list but the certificate has already expired
Untrusted	The certificate is unknown or you did not add the certificate to the trusted certificates list

Note

The “trust” level combinations for Allow and Block criteria differ.

Hash Values

You can configure Application Control to match applications using SHA-1 or SHA-256 hash value formats. You can choose to manually specify hash values or import a list of generated values.

Select your **Input method** and follow the on-screen instructions.

Input Method	Description
Manual	Allows you to manually specify up to 100 hash values (and descriptions)

Input Method	Description
Import	Allows you to import a ZIP package containing a properly formatted hash value list in CSV format You can choose to use the **Hash Generator tool** or manually create the CSV file using the **CSV sample format**. **WARNING!** You can only import one file into each set of criteria. If you attempt to import a new hash value list into the criteria, Application Control completely overwrites the existing values. • **Hash Generator tool**: Download and execute the tool on a target endpoint that you have installed with all necessary applications. The tool automatically creates a valid ZIP package containing the hash values of all applications found on the endpoint. • **CSV sample format**: Download the sample file and follow the instructions to properly populate the hash value list. Once you have completed the list, compress the file in ZIP format before importing into the set of criteria. **Important** The hash value list cannot contain a mixture of SHA-1 and SHA-256 formats. You must create separate hash value files and separate Application Control criteria for each type of hash value format.

Data Loss Prevention

Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data-referred to as digital assets-against accidental disclosure and intentional theft. DLP allows you to:

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

- Enforce compliance to established privacy standards

DLP evaluates data against a set of rules defined in policies. Policies determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission.

Important

Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the *Apex Central Widget and Policy Management Guide*.

You can download a PDF version of the guide, or view the guide online, using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

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 3-16*.

- **File attributes**: File properties such as file type and file size.

  For details, see *File Attributes on page 3-21*.

- **Keyword lists**: A list of special words or phrases.

  For details, see *Keywords on page 3-23*.

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 3-16* and *Customized Expressions on page 3-17*.

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 **Policies** > **Policy Resources** > **DLP 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 3-18*.

Criteria for Customized Expressions

TABLE 3-2. Criteria Options for Customized Expressions

<table>
<tr><th>CRITERIA</th><th>RULE</th><th>EXAMPLE</th></tr>
<tr><td>None</td><td>None</td><td>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]</td></tr>
<tr><td>Specific characters</td><td>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.</td><td>US - ABA Routing Number
• Expression: [^\d]([0123678]\d{8})[^\d]
• Characters: 0123456789
• Minimum characters: 9
• Maximum characters: 9</td></tr>
<tr><td>Suffix</td><td>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.</td><td>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</td></tr>
</table>

Criteria	**Rule**	**Example**
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address • Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Separator: @ • Minimum characters to the left: 3 • Maximum characters to the left: 15 • Maximum characters to the right: 30

Creating a Customized Expression

Procedure

1. Go to **Policies** > **Policy Resources** > **DLP 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 3-18*):

    - 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.

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 **Policies** > **Policy Resources** > **DLP 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.

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 Central 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.

Creating a File Attribute List

Procedure

1. Go to **Policies** > **Policy Resources** > **DLP 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**.

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 **Policies** > **Policy Resources** > **DLP 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.

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 3-24* and *Customized Keyword Lists on page 3-25*.

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 3-26*.

Customized Keyword List Criteria

TABLE 3-3. 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.
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 **Policies** > **Policy Resources** > **DLP 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**.

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 **Policies** > **Policy Resources** > **DLP 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.

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 3-30* and *Predefined DLP Templates on page 3-29*.

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 3-30*.

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 3-4. 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].

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
[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 **Policies** > **Policy Resources** > **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 3-30*.

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**.

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 **Policies** > **Policy Resources** > **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.

Intrusion Prevention Rules

The **Intrusion Prevention Rules** screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

- To filter the list of rules, use the **Search** box to specify full or partial strings that appear in any of the columns.
- To sort the list of Intrusion Prevention Rules by column data, click a column heading.
- To view detailed Intrusion Prevention Rule Properties, click the link in the **Rule Name** column of a rule.

Note

Apex Central automatically imports/updates Intrusion Prevention Rules from the Apex One server during manual or scheduled component updates.

Important

Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the *Apex Central Widget and Policy Management Guide*.

You can download a PDF version of the guide, or view the guide online, using the following link:

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

The following table outlines the rule information that displays on the **Intrusion Prevention Rules** screen.

COLUMN	DESCRIPTION
Identifier	The unique identifier tag for the Intrusion Prevention Rule
Rule Name	The name of the Intrusion Prevention Rule
Application Type	The Application Type this Intrusion Prevention Rule is grouped under
Severity	The severity level that Trend Micro assigns to the rule **Note** The severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of Intrusion Prevention Rules.
Mode	The network engine detection mode used by the Intrusion Prevention module

Column	Description
Type	The type of vulnerability detected: • **Smart**: Known or unknown (for example, zero-day) vulnerability • **Exploit**: Known exploit (usually signature based) for a known vulnerability • **Vulnerability**: Known vulnerability for which one or more exploits may exist
CVE	The Common Vulnerabilities and Exposures (CVE®) identifier that MITRE assigns to the vulnerability For more information, see http://cve.mitre.org/.
Microsoft	The Common Vulnerabilities and Exposures (CVE®) identifier that Microsoft assigns to the vulnerability
CVSS Score	The Common Vulnerability Scoring System (CVSS) severity score of the vulnerability according the National Vulnerability Database For more information, see http://nvd.nist.gov/cvss.cfm.
Last Updated	The date and time the rule was last modified

Intrusion Prevention Rule Properties

The **Intrusion Prevention Rule Properties** screen displays detailed information about a specific Intrusion Prevention Rule and vulnerability. Click the **General** tab or the **Vulnerability** to view details about the rule.

The following tables describe the information provided on the **General** tab and **Vulnerability** tab.

Table 3-5. General Information

Data	Description
Identifier	The unique identifier tag for the Intrusion Prevention Rule
Name	The name of the Intrusion Prevention Rule

Data	Description
Description	The description of the Intrusion Prevention Rule
Application Type	The Application Type this Intrusion Prevention Rule is grouped under
Priority	The priority level of the Intrusion Prevention Rule. Higher priority rules are applied before lower priority rules.
Severity	The severity level that Trend Micro assigns to the rule **Note** The severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of Intrusion Prevention Rules.
Mode	The network engine detection mode used by the Intrusion Prevention module
Type	The type of vulnerability detected: • **Smart**: Known or unknown (for example, zero-day) vulnerability • **Exploit**: Known exploit (usually signature based) for a known vulnerability • **Vulnerability**: Known vulnerability for which one or more exploits may exist
Issued	The date the rule was released (not downloaded)
Last Updated	The date and time the rule was last modified

Table 3-6. Vulnerability Information

Data	Description
Severity	The severity level of the vulnerability
CVSS Score	The Common Vulnerability Scoring System (CVSS) severity score of the vulnerability according the National Vulnerability Database For more information, see http://nvd.nist.gov/cvss.cfm.

Data	Description
Description	The description of the vulnerability
External References	Provides links to external references for more information about the vulnerability

Device Control Allowed Devices

Import or export lists of **Device Control Allow Devices** that apply to all Apex One Security Agent policy targets.

Item	Description
Import	Select a properly formatted CSV file containing a list of all the devices you want to allow on all Apex One Security Agent endpoints. **Important** Importing a new list overwrites the previous list completely. To retain the existing list, export the list before importing a new CSV file.
Last imported	The date/time the server imported the current list
Total allowed devices	The total number of allowed devices in the currently applied list
Export	Exports the current allowed list in CSV format

Part II

Apex Central Widgets

Chapter 4

Apex Central Dashboard Widgets

This section contains help topics for the dashboard widgets specific to the Apex Central management console dashboard.

Topics include:

Apex Central Top File-based Threats Widgets

This widget tracks the distribution of the top malicious files detected on endpoints across the network and displays the product-detected distribution as one of the top 10/25/50 file-based threats (viruses and spyware/grayware).

Click any node in the graph to open a screen that displays detailed information. Apex Central performs log query to provide the detailed information.

Specify the date range for the data that the widget displays:

- Today
- 1 Week
- 2 Weeks
- 1 Month

Specify the threat for the widget to display. The widget can display data for only one file-based threat at a time. By default the widget displays data from all the managed products that a user's account privileges allow.

Click the widget settings icon on the widget to access additional settings.

Setting	Description
Title	Specify a new and meaningful title for the widget in the field.
Scope	Specify the data scope displayed by the widget. The scope determines the products which the widget uses to display data.
Top Threats	Specify the number of threats to display.

Click **Save** to apply changes and update the widget data.

Endpoint Protection Verification Widget

This widget displays the Apex One and Deep Security protection status of endpoints from an integrated Active Directory structure.

Important

Before using this widget:

- Synchronize the Apex One client tree with the Active Directory tree.

  Refer to the Apex One documentation for further instructions.

- Go to **Administration** > **Settings** > **Endpoint Protection Verification** to enable the widget and configure Active Directory server, Apex One server, and Deep Security server connection settings.

Click the settings icon (⋮ > 🎚) to configure the following:

- **Apex One servers**: Click the browse button (...) to specify the Apex One servers that contribute data for the widget.
- **Deep Security servers**: Click the browse button (...) to specify the Deep Security servers that contribute data for the widget.
- **Columns**: Specify the columns for the widget to display in the data table.

Click an organization unit in the Active Directory structure to view the following the information.

Column	Description
Computer	Displays the endpoint name
Apex One	Displays whether the endpoint is protected by an Apex One or VDI client
Deep Security	Displays whether the endpoint is protected by a Deep Security agent
Physical Host	Displays the physical server where virtual endpoints reside

Column	Description
Pattern	Displays the version of the pattern file that the Apex One or VDI client uses
Scan Engine	Displays the version of the scan engine that the Apex One or VDI client uses
Client Version	Displays the client program version
Deep Security Profile	Displays the Deep Security profile in use
Server Name	Displays the Apex One and/or Deep Security server with which the endpoints connect

Hosts with C&C Callback Attempts Widget

This widget displays the total unique compromised hosts and groups them by C&C list source.

The default view displays data for the current day.

Use the **Range** drop-down to select the time period for the data that displays. You can view data for **Today**, **1 week**, **2 weeks**, or **1 month**.

Data	Description
Hosts matched with Global Intelligence	C&C callbacks detected by Trend Micro Global Intelligence network, including Smart Protection Network.
Hosts matched with dynamic analyzers	C&C callbacks detected by dynamic analyzers, including Virtual Analyzer and the Network Content Inspection Engine. Analyzers are built in to products such as Deep Discovery Inspector and Apex One.

Data	Description
Hosts matched with user-defined lists in managed products	C&C callbacks detected by products using a user-defined list. An example of a user-defined list is the Deny List in Deep Discovery Inspector.

Policy Status

This widget displays the deployment status of your policies.

Clicking the name of a policy or the number of targets opens a new **Log Query** screen to provide detailed information.

Data	Description
Policy	Displays the name of the policy
Deployment Status	Displays the percentage of targets that comply with the policy settings
Deployed	Displays the number of targets that have applied the policy settings or have unactivated product services
Pending	Displays the number of targets that have not applied the policy settings **Note** If Hotfix 2575 is not installed, the **Pending** column includes the number of targets that have offline agents.
Offline	Displays the number of targets that have offline agents **Important** This feature requires installing Hotfix 2575. Otherwise, the **Pending** column includes the number of targets that have offline agents and the **Offline** column does not display.

Data	Description
With Issues	Displays the number of targets that have not applied the policy settings due to unsupported policy deployment, no policy configuration, system errors, endpoint communication errors with the product server, unsupported endpoints, locally changed settings, disabled product services, or partial deployment
Endpoints/Products without policies	Displays the number of endpoints or managed products with no policy applied
Total endpoints/ products	Displays the number of endpoints or managed products the administrator can manage

Quick Launch

This widget displays shortcuts to the **Product Directory** and **Policy Management**.

Unique Compromised Hosts Over Time Widget

This widget displays the unique compromised hosts logged by managed products within the last 30 days.

This widget groups and displays the unique compromised hosts as circles. The circle size relatively represents the number of compromised hosts.

- Small: 1 to 5
- Medium: 6 to 10
- Large: 11 or more

Mouse-over a computer icon or host name to display additional compromised hosts.

Use the **Callback address** drop-down to display compromised hosts that had callback attempts to the selected callback address.

Note

The **Callback address** drop-down contains the top 25 callback addresses.

The widget only displays the first callback attempt from a compromised host to the selected callback address.

Change the managed products that the widget uses as its source by clicking the settings icon (⋮ > ⫶). In the dialog box that appears, specify the **Scope** by clicking >> and selecting the managed products to use as the source.

Part III

Apex One Widgets

Chapter 5

Apex One Dashboard Widgets

This section describes the available Apex One dashboard widgets in Apex Central.

Topics include:

Attack Discovery Detections Widget

This widget displays the detection logs generated by the Endpoint Sensor Attack Discovery feature based on the risk level for the specified period.

Important

This feature requires that you have valid Endpoint Sensor policies deployed to endpoints.

Click the **Rule Name** to display a detailed view of the detection and all the related objects. You can trigger a Historical Investigation on all related objects by clicking the **Assess Impact** button.

Note

A Historical Investigation can only perform an assessment based on specific criteria types. If you perform a Historical Investigation from the Attack Discovery Detections Widget, the investigation disregards objects for which no data is available.

Quick Investigation Widget

This widget allows you to start a basic Historical Investigation across your network using a single criterion type.

Important

This feature requires that you have valid Endpoint Sensor policies deployed to endpoints.

Select the type of criteria, specify the value, and click **Assess Impact**. The **Historical Investigation** screen appears with the assessment results.

Note

To perform a more complicated assessment, use the Historical Investigation or Live Investigation screens.

Top Blocked Applications

This widget provides an overview of the top applications that users attempted to access in violation of an Application Control policy.

Use the settings button to change the default number of applications that display.

Top Endpoints Affected by IPS Events Widget

This widget provides information about the endpoints affected by the most IPS events detected. IPS events are triggered by Intrusion Prevention Rules for Vulnerability Protection.

Use the **Period** drop-down to select the time range for the data that displays.

Use the settings icon (⋮ > 🎚) to change the default number of affected endpoints to display.

Data	Description
Endpoint	The name of the endpoint
IP Address	The IP address of the endpoint
Detections	The number of IPS events detected on the endpoint

Top IPS Attack Sources

This widget provides information about the top attack sources for IPS events detected on your network. IPS events are triggered by Intrusion Prevention Rules for Vulnerability Protection.

Use the **Period** drop-down to select the time range for the data that displays.

Use the settings icon (⋮ > 🎚) to change the default number of attack sources to display.

Data	Description
Attack Source	The IP address of the known attack source
Location	The location of the attack source
Detections	The number of IPS events detected on the endpoint

Top IPS Events

This widget provides information about the Intrusion Prevention Rules triggering the most IPS events on your network. IPS events are triggered by Intrusion Prevention Rules for Vulnerability Protection.

Use the **Period** drop-down to select the time range for the data that displays.

You can also use the second drop-down to display only the top **Detected** or **Prevented** IPS events.

Use the settings icon (⋮ > 🎚) to change the default number of triggered Intrusion Prevention Rules to display.

Data	Description
Rule Name	The name of the Intrusion Prevention Rule
Severity	The severity level that Trend Micro assigns to the rule

Data	Description
Total	The number of IPS events triggered by the Intrusion Prevention Rule

Top Violated Application Control Criteria

This widget provides an overview of the top Application Control criteria that users triggered while attempting to access unauthorized applications.

Use the settings button to change the default number of matches that display.

Part IV

Apex One Security Agent Policies

Chapter 6

Security Agent Program Settings

This section describes how you can manage the Security Agent program installed on endpoints.

Topics include:

Additional Service Settings

The Security Agent program requires that you enable additional services in order to allow certain features to function properly. The following table describes the available services and the features that require each service.

Service	Description	Features
Unauthorized Change Prevention Service (`TMBMSRV.exe`)	Regulates application behavior and verifies program trustworthiness	• Predictive Machine Learning • Behavior Monitoring • Device Control • Certified Safe Software Service • Agent Self-protection
Firewall Service (`TmPfw.exe`)	Regulates network connection access permissions	• Apex One Firewall
Suspicious Connection Service	Provides advanced protection against C&C callbacks	• User-defined IP Approved and Blocked Lists • Global C&C IP List (Network Content Inspection Engine) • Malware network fingerprinting (Relevance Rule Pattern)
Data Protection Service (`dsagent.exe`)	Provides advanced monitoring of sensitive data and restricts device access on endpoints	• Data Loss Prevention • Device Control (Block access) • Data Discovery (managed using the Apex Central console)
Advanced Protection Service (`TMCCSF.exe`))	Facilitates advanced scanning and protection features	• Predictive Machine Learning • Browser Exploit Prevention • Behavior Monitoring

Configuring Additional Security Agent Services

Procedure

1. 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**

> **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.

Privileges and Other Settings

Configure Security Agents to grant users rights to configure personalized settings, to display notification messages, and to protect critical Security Agent files and services.

Configuring Agent Privileges

Procedure

1. Configure settings as required.

Section	Settings
Independent Mode	**Enable Independent mode**: Allows users to disable the following features on the Security Agent to prevent the Security Agent from adversely affecting system performance: • 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 End users can manually initiate scans and updates on agents in Independent mode.

Section	Settings
Scans	• **Configure Manual Scan**: Allows users to configure the **Manual Scan** settings on the Security Agent console • **Configure Real-time Scan**: Allows users to configure the **Real-time Scan** settings on the Security Agent console • **Configure Scheduled Scan**: Allows users to configure the **Scheduled Scan** settings on the Security Agent console
Scheduled Scans	• **Postpone Scheduled Scan**: Allows users to postpone a Scheduled Scan before the scan starts or stop a currently running scan for a specified period **Note** Users can only stop a running scan once. Once the scan restarts, the Security Agent rescans all files on the endpoint. • **Skip and stop Scheduled Scan**: Allows users to skip or stop a running Scheduled Scan one time **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.

SECTION	SETTINGS
Firewall	• **Display the Firewall settings on the Security Agent console**: Allows users to configure the **Firewall** settings on the Security Agent console • **Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message**: Displays the **Enable/Disable Firewall** and **Enable/Disable IDS Mode** menu options on the Security Agent system tray icon **Note** 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. • **Allow Security Agents to send firewall logs to the Apex One server**: Configures the Security Agent to send Firewall logs to the server, allowing you to analyze network traffic
Behavior Monitoring	**Display the Behavior Monitoring settings on the Security Agent console**: Allows users to configure the **Behavior Monitoring** settings on the Security Agent console
Trusted Program List	**Display the Trusted Program List on the Security Agent console**: Allows users to configure the **Trusted Program List** on the Security Agent console
Mail Scan	**Display the Mail Scan settings on the Security Agent console**: Allows users to configure the **Mail Scan** settings on the Security Agent console If enabled, Real-time Scan can detect and take action on POP3 email messages retrieved from the mail server that contain malicious threats.

SECTION	SETTINGS
Proxy Settings	**Allow users to configure proxy settings**: Allows users to use user-configured proxy settings only in 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.
Component Updates	• **Perform "Update Now"**: Displays the **Update Now** menu option on the Security Agent system tray icon • **Enable/Disable schedule-based updates**: Displays the **Enable/ Disable Schedule-based Updates** menu option on the Security Agent system tray icon **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.

Section	Settings
Unload and Unlock	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. • **Does not require a password** • **Requires a password**: Type the required password and confirmation password **Note** Passwords must meet the following complexity requirements: • Length of 8 to 32 characters • At least one of each: uppercase (A-Z), lowercase (a-z), numeric (0-9), and special character • Cannot contain non-printable ASCII characters **Important** If you select **Requires a password** and do not specify a password, Apex Central applies the following default password: • For Apex One on-premises: The password provided during server installation • For Apex One as a Service: The account name used to provision the console

SECTION	SETTINGS
Uninstallation	The Security Agent uninstallation privilege allows users to uninstall the Security Agent program on local endpoints. • **Does not require a password** • **Requires a password**: Type the required password and confirmation password **Note** Passwords must meet the following complexity requirements: • Length of 8 to 32 characters • At least one of each: uppercase (A-Z), lowercase (a-z), numeric (0-9), and special character • Cannot contain non-printable ASCII characters **Important** If you select **Requires a password** and do not specify a password, Apex Central applies the following default password: • For Apex One on-premises: The password provided during server installation • For Apex One as a Service: The account name used to provision the console

Configuring Other Agent Settings

Procedure

1. Configure settings as required.

Section	Settings
Coexist Mode Conversion	**Permanently convert Security Agents using coexist mode into fully-functional Security Agents**: Activates all functions on Security Agents installed in “Co-exist mode” **Important** You cannot undo this action. After converting coexist mode Security Agents into fully-functional Security Agents, the agent program attempts to uninstall any incompatible third-party security software on the endpoint. After the conversion completes, Apex One enables all necessary services and functions related to normal Security Agent functionality. If you need to use a coexist mode Security Agent on a converted endpoint, you must unistall the Security Agent program and reinstall a coexist mode Security Agent.
Update Settings	• **Security Agents download updates from the Trend Micro ActiveUpdate Server**: Configures Security Agents that cannot connect to the specified update source to attempt to update from the Trend Micro ActiveUpdate server • **Enable schedule-based updates on Security Agents**: Configures all Security Agents to enable schedule-based updates by default • **Security Agents only update the following components**: Controls how component updates proceed on the Security Agents • **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 • **Pattern files**: Security Agents do not upgrade the Security Agent program, deploy hotfixes, or update engines and drivers
Web Reputation Settings	**Display a notification when a website is blocked**: Displays a notification message on the Security Agent after blocking a URL that violates a Web Reputation policy

Section	Settings
Behavior Monitoring Settings	**Display a notification when a program is blocked**: Displays a notification message on the Security Agent after blocking a program that violates a Behavior Monitoring policy
C&C Contact Alert Settings	**Display a notification when a C&C callback is detected**: Displays a notification message on the Security Agent after detecting a C&C callback
Central Quarantine Restore Settings	**Display a notification when a quarantined file is Restored**: Displays a notification message on the Security Agent after restoring a quarantined file
Predictive Machine Learning Settings	**Display a notification when a threat is detected**: Displays a notification message on the Security Agent after Predictive Machine Learning detects an unknown threat
Security Agent Self-protection	• **Protect Security Agent services**: Prevents users or applications from terminating Security Agent services • **Protect files in the Security Agent installation folder**: Prevents users or applications from modifying or deleting files in the Security Agent installation folder • **Protect Security Agent registry keys**: Prevents users or applications from modifying, deleting, or adding registry values used by the Security Agent program • **Protect Security Agent processes**: Prevents users or applications from terminating Security Agent processes For more information, see *Security Agent Self-protection on page 6-12*.
Scheduled Scan Settings	**Display a notification before a scheduled scan occurs**: Displays a notification message on the Security Agent before a configured Scheduled Scan starts

Section	Settings
Cache Settings for Scans	- **Enable the digital signature cache**: Configures the Security Agent to use the Behavior Monitoring Digital Signature Pattern to exclude files from Manual Scans, Scheduled Scans, and Scan Now - **Enable the on-demand scan cache**: Configures the Security Agent to maintain a local on-demand scan cache to exclude file during Manual Scan, Scheduled Scan, and Scan Now to improve scan performance For more information, see *Cache Settings for Scans on page 6-15*.
POP3 Email Scan Settings	**Scan POP3 email**: Enables POP3 mail scanning on the Security Agent For more information, see *POP3 Mail Scan on page 6-18*.
Security Agent Access Restriction	**Do not allow users to access the Security Agent console from the system tray or Windows Start menu**: Disables user access to the Security Agent console using the system tray or Windows Start menu **Note** This setting does not disable the Security Agent. The Security Agent runs in the background and continues to provide protection from security risks.
Restart Notification	**Display a notification if the endpoint needs to restart to finish cleaning infected files**: Displays a notification message on the Security Agent if the user needs to restart the endpoint to finish cleaning a malicious file

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.

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 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`

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

Process	Description
`NTRtScan.exe`	Performs Real-time, Scheduled, and Manual Scan on Security Agents
`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**.

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.

POP3 Mail Scan

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 6-1. 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** You must enable the **Display the Mail Scan settings on the Security Agent console** privilege to enable POP3 mail scanning. For more information, see *Configuring Agent Privileges on page 6-4*. • 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

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.

Assigning Security Agents as Update Agents

Procedure

1. Select the items that Update Agents can share.
   - Component updates
   - Domain settings
   - Security Agent programs and hot fixes

Chapter 7

Application Control Policy Settings

This section discusses how to configure Application Control policies on Security Agents.

Topics include:

Application Control

Application Control provides you with the ability to control which users have access to specific applications on certain endpoints. You have the option of creating an overall endpoint-based policy or, if integrated with Active Directory, very granular user-based policies per endpoint.

After determining the scope of the policy, you can create application matching criteria that define which applications to allow, block, or monitor. For experienced users, you can create "Lockdown" criteria that only allow trusted applications to execute and block all applications not explicitly allowed by the rules.

Configuring Application Control Settings (Agent)

Before configuring an Application Control policy, ensure that you define all required Application Control criteria. Application Control policies require the use of preconfigured criteria that define which applications you want to "Allow" or "Block" on an endpoint or for a particular user.

For more information, see *Application Control Criteria on page 3-2*.

Procedure

1. Select **Enable Application Control**.
2. In the **User-defined Rules** section, assign rules to the endpoint based on the logged on user account.

   Important

   - User-based Application Control is only available if you have integrated Active Directory. If you do not have Active Directory integration, you can only assign criteria to the default **All user accounts** rule.
   - You cannot delete the default **All user accounts** rule.

a. Add a new rule or modify an existing rule.

    - To add a new rule, click **Assign Rule**.
    - To modify an existing rule, click the value in the **User Accounts** column of the table.

    The **Assign Rule** screen appears.

b. Specify the **User Accounts** to which you want to apply specific Application Control criteria.

    Important

    - User-based Application Control is only available if you have integrated Active Directory. If you do not have Active Directory integration, you can only assign rules to the default **All user accounts** rule.
    - You can only assign 30 users or groups per rule. Create additional rules if you need to assign a greater number of users to a policy.

c. Move the necessary criteria to the **Selected criteria** table by clicking the criteria **Name**.

d. Click **Save**.

Note

To change the **Priority** order of rules, select and drag rules to different locations in the list. Application Control applies a first match rule to users included in multiple rules.

3. In the **Additional Actions** section, specify the action Application Control takes when a user attempts to execute an application that does not match any of the **User-defined Rule** criteria.

- **Allow: All other applications can execute**: Application Control takes no action on applications that do not match any of the **User-defined Rule** criteria. Choose when using Application Control to block or monitor application usage.

- **Lockdown: Block all applications not identified during the last inventory scan**: After endpoints receive this command, Application Control takes the following actions:

  a. Application Control scans the endpoint and creates a complete application inventory.

  b. Application Control “locks down” the endpoint and does not permit access to:

     - Any application that does not specifically match **Allow** criteria defined in the **User-defined Rule** table

     - Any application that does not specifically match assessment criteria defined in the **User-defined Rule** table

     - Any application not found in the inventory scan results for that particular endpoint

  - **Exclude applications by Trend Micro trusted vendors**: Select to automatically allow all applications that Trend Micro threat experts have determined come from trusted vendors

  - **Enable assessment mode**: Select to log access to applications not specifically allowed to execute during Lockdown but do not block the applications

    Tip

    Use assessment mode to determine which applications users may require before you completely block access to all applications you did not add to Allow Rules.

4. In the **Agent Notifications** section, select **Display a notification when an application is blocked** to display a notification on the endpoint when Application Control blocks an application.

5. In the **Log Maintenance** section:

   - **Maximum log age (in days)**: Specify the maximum number of days that the endpoint should keep log data

- **Maximum number of logs a Security Agent can send each hour per criteria**: Specify the maximum number of logs each Security Agent can send to the Apex One server every hour for each criteria rule

  Note

  Depending on the number of Security Agents and your network settings, the amount of network traffic that the server receives may cause performance issues.

Important

You must remember to **Deploy** or **Save** your Apex One Security Agent policy before leaving the screen. If you do not save the entire policy, you lose all changes.

Chapter 8

Behavior Monitoring Policy Settings

This section describes how to configure Behavior Monitoring policies on Security Agents.

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.

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.

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 8-1. Monitored System Events

EVENTS	DESCRIPTION
Duplicated System File	Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.
Hosts File Modification	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the web browser is redirected to infected, non-existent, or fake websites.

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 8-2. 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. **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.

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 more information, see *Configuring Agent Privileges on page 6-4*.

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`
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`

Exception Type	Wildcard Usage	Matched	Not Matched
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 Behavior Monitoring Rules and Exceptions

Configure Behavior Monitoring policies to protect endpoints against ransomware, exploit attacks, and emerging threats. Use the Event Monitoring feature to assess or block behaviors commonly associated with malware threats.

Note

By default, Behavior Monitoring is disabled on all versions of Windows Server platforms.

Procedure

1. 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 8-2*.

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 8-5*.

Important

Anti-exploit Protection works in conjunction with Real-time Scan (**Quarantine malware variants detected in memory**) to provide enhanced protection against Fileless Attacks.

For more information, see *Real-time Scan: Target Tab on page 9-12*.

---

2. 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.

3. In the **Event Monitoring** section:

    a. Select **Enable Event Monitoring**.

    b. Click **Specify detailed settings** to select the types of events to monitor.

c. Choose the system events to monitor and select an action for each of the selected events.

   For information about monitored system events and actions, see *Event Monitoring on page 8-6*.

4. Click the **Exceptions** tab to configure the exception lists.

   a. When configuring a parent policy, specify how other users can configure child policies.

      - **Inherit from parent**: Child policies must use the settings configured in the parent policy
      - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

      > **Note**
      >
      > If your child policies **Extend from parent**, you can also configure **Child Policy Restrictions**. Restrictions prevent the child policy from adding specific objects to the list.

   b. Type the full program path in the available text field.

      > **Note**
      >
      > - Separate multiple entries with semicolons (;).
      > - Use the **Import** and **Export** buttons to share the list with different policies.
      > - The **Approved List** supports the use of wildcard characters.
      >
      >   For more information, see *Exception List Wildcard Support on page 8-10*.

   c. Click **Add**.

   d. 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.

Chapter 9

Anti-malware Policy Settings

This section describes how to configure anti-malware scanning on Security Agents.

Topics include:

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.

Guidelines for Switching Scan Methods

The following table outlines some considerations you should be aware of before switching the scan method that Security Agents use.

TABLE 9-1. Considerations When Switching to Smart Scan

CONSIDERATION	DETAILS
Product license	Ensure that you have activated all required licenses for the new scan method.
Apex One server	Ensure that agents can connect to the Apex One server. Apex One only notifies online agents to switch scan methods. 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 to ensure that Security Agents can download the correct patterns from the server.

Consideration	Details
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.
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.
IPv6 support **Important** Only available for Security Agents reporting to an on-premises Apex One server.	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: • Smart Protection Server 2.0 (integrated or standalone) **Note** IPv6 support for Smart Protection Server starts in version 2.5. • Trend Micro Smart Protection Network Similarly, a pure IPv4 smart scan 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.

Consideration	Details
Smart Protection Services **Important** Only available for Security Agents reporting to an on-premises Apex One server.	If you are switching Security Agents from conventional scan to smart scan, ensure that you have set up Smart Protection Services.

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

Configure Manual Scan settings using the following tabs:

- *Manual Scan: Target Tab on page 9-5*
- *Manual Scan: Action Tab on page 9-7*
- *Manual Scan: Scan Exclusion Tab on page 9-9*

Manual Scan: Target Tab

Procedure

1. In the **Files to Scan** section, select from the following:

    - **All scannable files**: Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.

        Note

        This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.

    - **File types scanned by IntelliScan**: Scans files based on true-file type.

    - **Files with the following extensions (use commas to separate entries)**: Manually specify the files to scan based on their extensions. Separate multiple entries with commas.

        Note

        When configuring a parent policy, specify how other users can configure child policies.

        - **Inherit from parent**: Child policies must use the settings configured in the parent policy

        - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

2. In the **Scan Settings** section, configure the required settings.

Setting	Description
Scan hidden folders	Allows the Security Agent to detect and then scan hidden folders on the endpoint
Scan network drive	Scans directories physically located on other endpoints, but mapped to the local endpoint
Scan compressed files	Scans the specified number of compression layers within an archived file **Note** Scanning through more layers may detect malware intentionally buried within a compressed archive, however, the scan may affect system performance.
Scan OLE objects	Scans the specified number of Object Linking and Embedding (OLE) layers in a 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 the **Scan OLE objects** and **Detect exploit code in OLE files** options.
Scan boot area	Scans the boot sector of the hard disk on the endpoint for virus/ malware

3. In the **CPU Usage** section, select from the following:

   - **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

Manual Scan: Action Tab

Procedure

1. In the **Virus/Malware** section, configure the required settings.

   a. Select the type of action that the Security Agent takes after detecting a security threat.

      - **Use ActiveAction**: Select to use a set of pre-configured scan actions for viruses/malware

        For more information, see *ActiveAction on page 9-36*.

        - **Customize action for probable virus/malware**: Select and specify the action that the Security Agent takes on probable malware threats

      - **Use the same action for all virus/malware types**: Specify the action that the Security Agent takes on all malware threats

      - **Use a specific action for each virus/malware type**: Specify the action that the Security Agent takes on specific security threats

        For more information, see *Custom Scan Actions on page 9-38*.

   b. Select **Back up files before cleaning** to create an encrypted copy of the infected file on the endpoint in the `<Agent installation folder>\Backup` folder.

      Creating a backup copy of the file allows you to restore the original version of the file if necessary.

   c. Specify the location of the quarantine directory.

      - **Quarantine to the Security Agent's managing server**: The Security Agent sends an encrypted copy of all quarantined files to the managing Apex One server

      - **Quarantine directory**: The Security Agent sends an encrypted copy of all quarantined files to the specified location

      For more information, see *Quarantine Directory on page 9-39*.

d. In the **Damage Cleanup Services** section, configure the following:

  - **Cleanup type**

    - **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.

  - **Run cleanup when probable virus/malware is detected**: Performs the configured cleanup type on probable malware threats

> **Note**
>
> You can only select this option if the action on probable virus/malware is not **Pass** or **Deny Access**.

2. In the **Spyware/Grayware** section, select the action the Security Agent takes after detecting spyware or grayware programs.

   - **Clean**: Terminates all related processes and deletes associated registry values, files, cookies and shortcuts

   > **Note**
   >
   > After cleaning spyware/grayware, Security Agents back up spyware/grayware data, which you can restore if you consider the spyware/grayware safe to access.

- **Pass**: Logs the detection but allows the program to execute

Manual Scan: Scan Exclusion Tab

Procedure

1. Select **Enable scan exclusion**.

2. In the **Scan Exclusion List (Directories)** section, configure the required settings.

   a. Select **Exclude directories where Trend Micro products are installed** to automatically exclude directories associated with other Trend Micro products.

      For more information, see *Trend Micro Product Directory Exclusions on page 9-44*.

   b. When configuring a parent policy, specify how other users can configure child policies.

      - **Inherit from parent**: Child policies must use the settings configured in the parent policy

      - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

      Note

      If your child policies **Extend from parent**, you can also configure **Child Policy Restrictions**. Restrictions prevent the child policy from adding specific objects to the list.

   c. Type a directory path to exclude from scans and click the **+** button.

      The Security Agent does not scan files located in the specified directory (and sub-directories).

Note

- You can specify a maximum of 256 directories to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- Directory exclusions support the use of wildcard characters.

  For more information, see *Wildcard Exceptions on page 9-45*.

3. In the **Scan Exclusion List (Files)** section, configure the required settings.

   a. When configuring a parent policy, specify how other users can configure child policies.

   - **Inherit from parent**: Child policies must use the settings configured in the parent policy
   - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

   b. Type a file name or the file name with full directory path to exclude from scans and click the **+** button.

Note

- You can specify a maximum of 256 files to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- File exclusions support the use of wildcard characters.

  For more information, see *Wildcard Exceptions on page 9-45*.

4. In the **Scan Exclusion List (File Extensions)** section, configure the required settings.

   a. When configuring a parent policy, specify how other users can configure child policies.

- **Inherit from parent**: Child policies must use the settings configured in the parent policy
- **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

b. Select or type a file extension to exclude from scans and click the **Add >** button.

Note

- You can specify a maximum of 256 file extensions to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- 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??`.

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.

Configuring Real-time Scan Settings

Procedure

1. 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. During a virus outbreak, the Security Agent automatically enables Real-time Scan and you cannot disable scanning until the outbreak ends. Real-time Scan helps prevent the virus from modifying or deleting files and folders on endpoints.

2. Configure the **Target** settings.

   For more information, see *Real-time Scan: Target Tab on page 9-12*.

3. Configure the **Action** settings.

   For more information, see *Real-time Scan: Action Tab on page 9-15*.

4. Configure the **Scan Exclusion** settings.

   For more information, see *Real-time Scan: Scan Exclusion Tab on page 9-17*.

Real-time Scan: Target Tab

Procedure

1. In the **User Activity on Files** section, select which file operations trigger scanning from the **Scan files being** drop-down.
   - **created/modified and retrieved**: Scans all files created, modified, or opened on the endpoint

- **created/modified**: Scans all files created or modified on the endpoint
- **retrieved**: Scans all files opened on the endpoint

2. In the **Files to Scan** section, select from the following:

    - **All scannable files**: Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.

        Note

        This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.

    - **File types scanned by IntelliScan**: Scans files based on true-file type.
    - **Files with the following extensions (use commas to separate entries)**: Manually specify the files to scan based on their extensions. Separate multiple entries with commas.

        Note

        When configuring a parent policy, specify how other users can configure child policies.

        - **Inherit from parent**: Child policies must use the settings configured in the parent policy
        - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

3. In the **Scan Settings** section, configure the required settings.

SETTING	DESCRIPTION
Scan floppy disks during shutdown	Scans floppy disks during shutdown

Setting	Description
Scan network drive	Scans directories physically located on other endpoints, but mapped to the local endpoint
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
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
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** Memory scanning works in conjunction with Anti-exploit Protection in Behavior Monitoring to provide enhanced protection against Fileless Attacks. For more information, see *Configuring Behavior Monitoring Rules and Exceptions on page 8-15*.
Scan compressed files	Scans the specified number of compression layers within an archived file **Note** Scanning through more layers may detect malware intentionally buried within a compressed archive, however, the scan may affect system performance.

Setting	Description
Scan OLE objects	Scans the specified number of Object Linking and Embedding (OLE) layers in a 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 the **Scan OLE objects** and **Detect exploit code in OLE files** options.
Enable IntelliTrap	Detects malicious code, such as bots, in compressed files
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

Real-time Scan: Action Tab

Procedure

1. In the **Virus/Malware** section, configure the required settings.

    a. Select the type of action that the Security Agent takes after detecting a security threat.

    - **Use ActiveAction**: Select to use a set of pre-configured scan actions for viruses/malware

      For more information, see *ActiveAction on page 9-36*.

        - **Customize action for probable virus/malware**: Select and specify the action that the Security Agent takes on probable malware threats

- **Use the same action for all virus/malware types**: Specify the action that the Security Agent takes on all malware threats

- **Use a specific action for each virus/malware type**: Specify the action that the Security Agent takes on specific security threats

  For more information, see *Custom Scan Actions on page 9-38*.

b. Select the types of notification that display to end users.

   - **Display a notification when virus/malware is detected**: Select to display a notification informing the Security Agent user when a malware detection occurs

   - **Display a notification when probable virus/malware is detected**: Select to display a notification informing the Security Agent user when a probable malware detection occurs

c. Select **Back up files before cleaning** to create an encrypted copy of the infected file on the endpoint in the `<Agent installation folder>\Backup` folder.

   Creating a backup copy of the file allows you to restore the original version of the file if necessary.

d. Specify the location of the quarantine directory.

   - **Quarantine to the Security Agent's managing server**: The Security Agent sends an encrypted copy of all quarantined files to the managing Apex One server

   - **Quarantine directory**: The Security Agent sends an encrypted copy of all quarantined files to the specified location

   For more information, see *Quarantine Directory on page 9-39*.

e. In the **Damage Cleanup Services** section, configure the following:

   - **Run cleanup when probable virus/malware is detected**: Performs the configured cleanup type on probable malware threats

Note

You can only select this option if the action on probable virus/malware is not **Pass** or **Deny Access**.

2. In the **Spyware/Grayware** section, select the action the Security Agent takes after detecting spyware or grayware programs.

    - **Clean**: Terminates all related processes and deletes associated registry values, files, cookies and shortcuts

      Note

      After cleaning spyware/grayware, Security Agents back up spyware/grayware data, which you can restore if you consider the spyware/grayware safe to access.

    - **Deny access**: Prevents the end user from opening or copying the spyware or grayware components
    - **Display a notification on endpoints when spyware/grayware is detected**: Select to display a notification informing the Security Agent user when a spyware/grayware detection occurs

Real-time Scan: Scan Exclusion Tab

Procedure

1. Select **Enable scan exclusion**.
2. In the **Scan Exclusion List (Directories)** section, configure the required settings.

    a. Select **Exclude directories where Trend Micro products are installed** to automatically exclude directories associated with other Trend Micro products.

    For more information, see *Trend Micro Product Directory Exclusions on page 9-44*.

b. When configuring a parent policy, specify how other users can configure child policies.

   - **Inherit from parent**: Child policies must use the settings configured in the parent policy
   - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

   > **Note**
   >
   > If your child policies **Extend from parent**, you can also configure **Child Policy Restrictions**. Restrictions prevent the child policy from adding specific objects to the list.

c. Type a directory path to exclude from scans and click the **+** button.

   The Security Agent does not scan files located in the specified directory (and sub-directories).

   > **Note**
   >
   > - You can specify a maximum of 256 directories to exclude from scanning.
   > - Use the **Import** and **Export** buttons to share the list with different policies.
   > - Directory exclusions support the use of wildcard characters.
   >
   >   For more information, see *Wildcard Exceptions on page 9-45*.

3. In the **Scan Exclusion List (Files)** section, configure the required settings.

a. When configuring a parent policy, specify how other users can configure child policies.

   - **Inherit from parent**: Child policies must use the settings configured in the parent policy
   - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

b. Type a file name or the file name with full directory path to exclude from scans and click the **+** button.

Note

- You can specify a maximum of 256 files to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- File exclusions support the use of wildcard characters.

  For more information, see *Wildcard Exceptions on page 9-45*.

4. In the **Scan Exclusion List (File Extensions)** section, configure the required settings.

a. When configuring a parent policy, specify how other users can configure child policies.

- **Inherit from parent**: Child policies must use the settings configured in the parent policy
- **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

b. Select or type a file extension to exclude from scans and click the **Add >** button.

Note

- You can specify a maximum of 256 file extensions to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- Real-time Scan does not support the use of wildcard characters for file extension exclusions.

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. 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.

2. Configure the **Target** settings.

    For more information, see *Scan Now: Target Tab on page 9-21*.

3. Configure the **Action** settings.

    For more information, see *Scan Now: Action Tab on page 9-23*.

4. Configure the **Scan Exclusion** settings.

    For more information, see *Scan Now: Scan Exclusion Tab on page 9-25*.

Scan Now: Target Tab

Procedure

1. In the **Files to Scan** section, select from the following:

    - **All scannable files**: Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.

        Note

        This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.

    - **File types scanned by IntelliScan**: Scans files based on true-file type.

    - **Files with the following extensions (use commas to separate entries)**: Manually specify the files to scan based on their extensions. Separate multiple entries with commas.

        Note

        When configuring a parent policy, specify how other users can configure child policies.

        - **Inherit from parent**: Child policies must use the settings configured in the parent policy

        - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

2. In the **Scan Settings** section, configure the required settings.

Setting	Description
Scan compressed files	Scans the specified number of compression layers within an archived file **Note** Scanning through more layers may detect malware intentionally buried within a compressed archive, however, the scan may affect system performance.
Scan OLE objects	Scans the specified number of Object Linking and Embedding (OLE) layers in a 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 the **Scan OLE objects** and **Detect exploit code in OLE files** options.
Scan boot area	Scans the boot sector of the hard disk on the endpoint for virus/ malware

3. In the **CPU Usage** section, select from the following:

    - **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

Scan Now: Action Tab

Procedure

1. In the **Virus/Malware** section, configure the required settings.

   a. Select the type of action that the Security Agent takes after detecting a security threat.

      - **Use ActiveAction**: Select to use a set of pre-configured scan actions for viruses/malware

        For more information, see *ActiveAction on page 9-36*.

        - **Customize action for probable virus/malware**: Select and specify the action that the Security Agent takes on probable malware threats

      - **Use the same action for all virus/malware types**: Specify the action that the Security Agent takes on all malware threats

      - **Use a specific action for each virus/malware type**: Specify the action that the Security Agent takes on specific security threats

        For more information, see *Custom Scan Actions on page 9-38*.

   b. Select **Back up files before cleaning** to create an encrypted copy of the infected file on the endpoint in the `<Agent installation folder>\Backup` folder.

      Creating a backup copy of the file allows you to restore the original version of the file if necessary.

   c. Specify the location of the quarantine directory.

      - **Quarantine to the Security Agent's managing server**: The Security Agent sends an encrypted copy of all quarantined files to the managing Apex One server

      - **Quarantine directory**: The Security Agent sends an encrypted copy of all quarantined files to the specified location

      For more information, see *Quarantine Directory on page 9-39*.

d. In the **Damage Cleanup Services** section, configure the following:

- **Cleanup type**
    - **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.
- **Run cleanup when probable virus/malware is detected**: Performs the configured cleanup type on probable malware threats

> **Note**
>
> You can only select this option if the action on probable virus/malware is not **Pass** or **Deny Access**.

2. In the **Spyware/Grayware** section, select the action the Security Agent takes after detecting spyware or grayware programs.

- **Clean**: Terminates all related processes and deletes associated registry values, files, cookies and shortcuts

> **Note**
>
> After cleaning spyware/grayware, Security Agents back up spyware/grayware data, which you can restore if you consider the spyware/grayware safe to access.

- **Pass**: Logs the detection but allows the program to execute

Scan Now: Scan Exclusion Tab

Procedure

1. Select **Enable scan exclusion**.
2. In the **Scan Exclusion List (Directories)** section, configure the required settings.

   a. Select **Exclude directories where Trend Micro products are installed** to automatically exclude directories associated with other Trend Micro products.

   For more information, see *Trend Micro Product Directory Exclusions on page 9-44*.

   b. When configuring a parent policy, specify how other users can configure child policies.

   - **Inherit from parent**: Child policies must use the settings configured in the parent policy
   - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

   Note

   If your child policies **Extend from parent**, you can also configure **Child Policy Restrictions**. Restrictions prevent the child policy from adding specific objects to the list.

   c. Type a directory path to exclude from scans and click the **+** button.

   The Security Agent does not scan files located in the specified directory (and sub-directories).

Note

- You can specify a maximum of 256 directories to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- Directory exclusions support the use of wildcard characters.

  For more information, see *Wildcard Exceptions on page 9-45*.

3. In the **Scan Exclusion List (Files)** section, configure the required settings.

   a. When configuring a parent policy, specify how other users can configure child policies.

   - **Inherit from parent**: Child policies must use the settings configured in the parent policy
   - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

   b. Type a file name or the file name with full directory path to exclude from scans and click the **+** button.

Note

- You can specify a maximum of 256 files to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- File exclusions support the use of wildcard characters.

  For more information, see *Wildcard Exceptions on page 9-45*.

4. In the **Scan Exclusion List (File Extensions)** section, configure the required settings.

   a. When configuring a parent policy, specify how other users can configure child policies.

- **Inherit from parent**: Child policies must use the settings configured in the parent policy
- **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

b. Select or type a file extension to exclude from scans and click the **Add >** button.

Note

- You can specify a maximum of 256 file extensions to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- 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??`.

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. 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.

2. Configure the **Target** settings.

   For more information, see *Scheduled Scan: Target Tab on page 9-28*.

3. Configure the **Action** settings.

   For more information, see *Scheduled Scan: Action Tab on page 9-31*.

4. Configure the **Scan Exclusion** settings.

   For more information, see *Scheduled Scan: Scan Exclusion Tab on page 9-33*.

Scheduled Scan: Target Tab

Procedure

1. In the **Schedule** section, specify the Scheduled Scan frequency:

   - **Daily**: Scans every day at the specified time
   - **Weekly, every <day_of_week>**: Scans once a week on the specified day at the specified time
   - **Monthly, on day <number>**: Scans once a month on the specified day at the specified time
   - **Monthly, on the <ordinal> <day_of_week>**: Scans once a month on the specified weekday at the specified time

Important

If you select a day that does not exist within a given month (for example, day “30” does not exist in February), the Scheduled Scan occurs on the last day of that month.

Note

When configuring a parent policy, specify how other users can configure child policies.

- **Inherit from parent**: Child policies must use the settings configured in the parent policy
- **Are customizable**: Other administrators can configure child policies to be different than the parent policy settings.

2. In the **Files to Scan** section, select from the following:

- **All scannable files**: Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.

  Note

  This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.

- **File types scanned by IntelliScan**: Scans files based on true-file type.
- **Files with the following extensions (use commas to separate entries)**: Manually specify the files to scan based on their extensions. Separate multiple entries with commas.

Note

When configuring a parent policy, specify how other users can configure child policies.

- **Inherit from parent**: Child policies must use the settings configured in the parent policy
- **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

3. In the **Scan Settings** section, configure the required settings.

Setting	Description
Scan compressed files	Scans the specified number of compression layers within an archived file **Note** Scanning through more layers may detect malware intentionally buried within a compressed archive, however, the scan may affect system performance.
Scan OLE objects	Scans the specified number of Object Linking and Embedding (OLE) layers in a 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 the **Scan OLE objects** and **Detect exploit code in OLE files** options.
Scan boot area	Scans the boot sector of the hard disk on the endpoint for virus/ malware

4. In the **CPU Usage** section, select from the following:

- **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

Scheduled Scan: Action Tab

Procedure

1. In the **Virus/Malware** section, configure the required settings.

    a. Select the type of action that the Security Agent takes after detecting a security threat.

    - **Use ActiveAction**: Select to use a set of pre-configured scan actions for viruses/malware

      For more information, see *ActiveAction on page 9-36*.

        - **Customize action for probable virus/malware**: Select and specify the action that the Security Agent takes on probable malware threats

    - **Use the same action for all virus/malware types**: Specify the action that the Security Agent takes on all malware threats
    - **Use a specific action for each virus/malware type**: Specify the action that the Security Agent takes on specific security threats

      For more information, see *Custom Scan Actions on page 9-38*.

    b. Select the types of notification that display to end users.

    - **Display a notification when virus/malware is detected**: Select to display a notification informing the Security Agent user when a malware detection occurs
    - **Display a notification when probable virus/malware is detected**: Select to display a notification informing the Security Agent user when a probable malware detection occurs

c. Select **Back up files before cleaning** to create an encrypted copy of the infected file on the endpoint in the `<Agent installation folder>\Backup` folder.

   Creating a backup copy of the file allows you to restore the original version of the file if necessary.

d. Specify the location of the quarantine directory.

   - **Quarantine to the Security Agent's managing server**: The Security Agent sends an encrypted copy of all quarantined files to the managing Apex One server

   - **Quarantine directory**: The Security Agent sends an encrypted copy of all quarantined files to the specified location

   For more information, see *Quarantine Directory on page 9-39*.

e. In the **Damage Cleanup Services** section, configure the following:

   - **Cleanup type**

     - **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.

   - **Run cleanup when probable virus/malware is detected**: Performs the configured cleanup type on probable malware threats

Note

You can only select this option if the action on probable virus/malware is not **Pass** or **Deny Access**.

2. In the **Spyware/Grayware** section, select the action the Security Agent takes after detecting spyware or grayware programs.

    - **Clean**: Terminates all related processes and deletes associated registry values, files, cookies and shortcuts

        Note

        After cleaning spyware/grayware, Security Agents back up spyware/grayware data, which you can restore if you consider the spyware/grayware safe to access.

    - **Pass**: Logs the detection but allows the program to execute

    - **Display a notification on endpoints when spyware/grayware is detected**: Select to display a notification informing the Security Agent user when a spyware/grayware detection occurs

Scheduled Scan: Scan Exclusion Tab

Procedure

1. Select **Enable scan exclusion**.

2. In the **Scan Exclusion List (Directories)** section, configure the required settings.

    a. Select **Exclude directories where Trend Micro products are installed** to automatically exclude directories associated with other Trend Micro products.

    For more information, see *Trend Micro Product Directory Exclusions on page 9-44*.

b. When configuring a parent policy, specify how other users can configure child policies.

  - **Inherit from parent**: Child policies must use the settings configured in the parent policy
  - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

> **Note**
>
> If your child policies **Extend from parent**, you can also configure **Child Policy Restrictions**. Restrictions prevent the child policy from adding specific objects to the list.

c. Type a directory path to exclude from scans and click the **+** button.

   The Security Agent does not scan files located in the specified directory (and sub-directories).

> **Note**
>
> - You can specify a maximum of 256 directories to exclude from scanning.
> - Use the **Import** and **Export** buttons to share the list with different policies.
> - Directory exclusions support the use of wildcard characters.
>
>   For more information, see *Wildcard Exceptions on page 9-45*.

3. In the **Scan Exclusion List (Files)** section, configure the required settings.

   a. When configuring a parent policy, specify how other users can configure child policies.

     - **Inherit from parent**: Child policies must use the settings configured in the parent policy
     - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

b. Type a file name or the file name with full directory path to exclude from scans and click the **+** button.

Note

- You can specify a maximum of 256 files to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- File exclusions support the use of wildcard characters.

  For more information, see *Wildcard Exceptions on page 9-45*.

4. In the **Scan Exclusion List (File Extensions)** section, configure the required settings.

a. When configuring a parent policy, specify how other users can configure child policies.

- **Inherit from parent**: Child policies must use the settings configured in the parent policy
- **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

b. Select or type a file extension to exclude from scans and click the **Add >** button.

Note

- You can specify a maximum of 256 file extensions to exclude from scanning.
- Use the **Import** and **Export** buttons to share the list with different policies.
- 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??`.

Scan Actions

You can configure Security Agents to use a set of predefined scan actions or custom actions based on the detected malware type.

Important

Some files are uncleanable.

For more information, see:

- *ActiveAction on page 9-36*
- *Custom Scan Actions on page 9-38*
- *Uncleanable Files on page 9-40*

ActiveAction

Different types of virus/malware require different scan actions. Customizing scan actions requires knowledge about virus/malware and can be a tedious task. The Security Agent 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 endpoints. ActiveAction settings are updated to protect against the latest threats and the latest methods of virus/malware attacks.

The following table illustrates how ActiveAction handles each type of virus/malware.

TABLE 9-2. Trend Micro Recommended Scan Actions Against Viruses and Malware

Virus/Malware Type	Real-time Scan		Manual Scan/Scheduled Scan	
	First Action	Second Action	First Action	Second Action
CVE exploit	Pass	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
Others	Clean	Quarantine	Clean	Quarantine
Probable malware	Deny Access or user-configured action	N/A	Pass or user-configured action	N/A

Note

- For probable virus/malware, the default action is “Deny Access” during Real-time Scan and “Pass” during Manual Scan and Scheduled Scan. If these are not your preferred actions, you can change them to “Quarantine”, “Delete”, or “Rename”.
- Some files are uncleanable.
- ActiveAction is not available for spyware/grayware scan.

Custom Scan Actions

Action	Description
Delete	Deletes the infected file.
Quarantine	Renames and then moves the infected file to a temporary quarantine directory on the endpoint. The Security Agent then sends quarantined files to the designated quarantine directory, which is on the managing server by default. The Security Agent encrypts quarantined files sent to this directory. For more information, see *Quarantine Directory on page 9-39*.
Clean	Cleans the infected file before allowing full access to the file. If the file is uncleanable, the Security Agent performs a second action, which can be one of the following actions: “Quarantine”, “Delete”, “Rename”, and “Pass”. This action can be performed on all types of security threats except probable virus/malware. **Note** Some files are uncleanable. For details, see *Uncleanable Files on page 9-40*.

Action	Description
Rename	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	Performs no action on detected threats but records the detection in the logs.
Deny Access	When the Security Agent detects an attempt to open or execute an infected file, it immediately blocks the operation. Users can manually delete the infected file.

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.

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 9-3. 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.
	UNC path	`\\<osceserver>\ofcscan\Virus`	
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`	

Uncleanable Files

The Virus Scan Engine is unable to clean the following files:

TABLE 9-4. 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. 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:

Uncleanable File	Explanation and Solution
	`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 .\*`
	The last command deletes all files in the Internet Explorer temporary folder.
	c. Restart the endpoint in normal mode.

Files compressed using an	Solution: Uncompress the files.

Uncleanable File	Explanation and Solution
unsupported compression format	
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.

Scan Exclusion Support

When excluding directories and file names from anti-malware scanning, refer to the following support information:

- *Trend Micro Product Directory Exclusions on page 9-44*
- *Wildcard Exceptions on page 9-45*

Trend Micro Product Directory Exclusions

If you select **Exclude directories where Trend Micro products are installed** in the **Scan Exclusion List (Directories)** section, the Security Agent automatically excludes following product directories:

- <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

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 9-5. 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`

Value	Excluded	Not Excluded
`c:\*.txt`	All `.txt` files in the `C:\` directory	All other file types in the `C:\` directory
`[]`	Not supported	Not supported

Chapter 10

Web Reputation Policy Settings

This section describes how to configure Web Reputation policies on Security Agents.

Topics include:

- *Web Reputation on page 10-2*
- *Configuring a Web Reputation Policy on page 10-2*

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.

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.

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.

Procedure

1. Click the **External Agents** tab to configure a policy for external agents or the **Internal Agents** tab to configure a policy for internal agents.

2. 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.

3. 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.

4. 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 10-6*.

5. Select **Scan common HTTP ports only** to restrict web reputation scanning to traffic through ports 80, 81, and 8080. By default, Web Reputation scans all traffic through all ports.

Note

Not supported on Windows 7, 8, 8.1, 10, or Windows Server 2008 R2, 2012 or later platforms.

6. 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.
    - 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.
    - 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.
    - Agents can block untested websites if you select the **Block pages that have not been tested by Trend Micro** option.

Note

You can only configure internal on-premises Security Agents to send web reputation queries to local Smart Protection Servers.

7. 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.

8. 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.

9. 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, Microsoft Edge Chromium, Mozilla Firefox, and Chrome browsers.
   - The Browser Exploit Prevention feature requires that you enable the Advanced Protection Service.

10. 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**.

Important

Web Reputation does not perform any scanning on addresses located in the Approved and Blocked lists.

11. To submit Web Reputation feedback, click the URL provided under **Reassess URL**. The Trend Micro Web Reputation Query system opens in a browser window.

12. 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.

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 10-1. 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 • Chromium	

For more information on configuring Internet Explorer settings for Web Reputation, see the following Knowledge Base articles:

- http://success.trendmicro.com/solution/1060643
- http://success.trendmicro.com/solution/1095350

Chapter 11

Unknown Threat Protection

This section describes how you can configure Security Agents to detect and protect against previously unidentified, targeted, or low prevalence threats.

Topics include:

- *Predictive Machine Learning on page 11-2*
- *Configuring Sample Submission Settings on page 11-5*
- *Configuring Suspicious Connection Settings on page 11-6*

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

Procedure

1. Select **Enable Predictive Machine Learning**.

2. 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

3. Under **Exceptions**, configure the global Predictive Machine Learning file exceptions to prevent all agents from detecting a file as malicious.

   a. When configuring a parent policy, specify how other users can configure child policies.

      - **Inherit from parent**: Child policies must use the settings configured in the parent policy

      - **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

Note

If your child policies **Extend from parent**, you can also configure **Child Policy Restrictions**. Restrictions prevent the child policy from adding specific objects to the list.

b. Click **Add File Hash**.

The **Add File to Exception List** screen appears.

Note

Use the **Import** and **Export** buttons to share the list with different policies.

c. Specify the file SHA-1 hash value to exclude from scanning.

d. Optionally provide a note regarding the reason for the exception or to describe the file name(s) associated with the hash value.

e. Click **Add**.

Predictive Machine Learning adds the file hash to the Exceptions list.

Configuring Sample Submission Settings

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.

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.

Procedure

1. Select **Enable suspicious file submission to Virtual Analyzer**.

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. 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.

2. Enable the **Detect connections using malware network fingerprinting** setting and select to **Log only** or **Block** connections.

    - 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.

Chapter 12

Device Control Policy Settings

This section describes how to configure Device Control policies on Security Agents.

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.

Apex Central provides both endpoint-based and user-based Device Control policy configuration.

Configuring Device Control Settings

Procedure

1. Select **Enable Device Control**.

    - 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**.

2. Add or edit a Device Control rule:

    - For user-based rules:

        - To create a rule based on Active Directory user or group accounts, click **Add**.

        - To edit a rule based on Active Directory user or group accounts, click the link in the **User Accounts** column.

    > **Important**
    >
    > User-based Device Control rules are only available after integrating Active Directory with Apex Central.

- To edit the default endpoint-based rule:
    - Click the **All users (default)** link in the **User Accounts** column.

    Note

    You cannot delete the default endpoint-based rule.

The **Device Control Rule** screen appears.

3. In the **User Accounts** section, type and select the Active Directory user(s) or group account(s) to which the rule applies.

    Note

    You cannot specify user or group accounts when editing the default **All users (default)** endpoint-based rule.

4. In the **Storage Devices** section:

    a. Select a permission for each storage device.

    Important

    - Only Security Agents with Data Protection enabled can take the “Block” action. If you deploy a policy to Security Agents that do not have Data Protection enabled, Apex One applies the action configured in the drop-down box.
    - Apex One automatically applies the access permission configured for any USB device in the **Allowed USB List** even if you do not enable Data Protection.

    For details about permissions, see *Permissions for Devices on page 12-5*.

    If you selected to restrict access to any storage device, the **Allowed Programs** button appears. For **USB storage devices**, if you selected **Block (Data Protection)**, the **Allowed USB Devices** button appears.

    b. (Optional) Click **Allowed Programs** to configure a list of programs that Device Control does not restrict access on any device type.

The **Allowed Programs** screen appears.

i. Type the full path or the trusted Digital Signature Provider information of programs that Device Control allows users to access.

Note

- When specifying a Digital Signature Provider, Device Control only allows programs signed by the publisher to **Execute**.

  For more information, see *Specifying a Digital Signature Provider on page 12-8*.

- When specifying the full path of a program, the Device Control Allowed Programs list supports the use of wildcard characters.

  For more information, see *Wildcard Support for the Device Control Allowed Programs List on page 12-7*.

ii. Click **Add**.

The the full path of the program or the trusted Digital Signature Provider information appears in the list.

iii. Select whether to allow the program to **Execute** or **Read/Write**.

iv. Click **OK**.

c. (Optional) Click **Allowed USB Devices** to configure a list of USB devices that Device Control does not block.

The **Allowed USB Devices** screen appears.

i. Type the device vendor, model, and serial ID in the list.

ii. To add more devices, click the plus (+) icon.

iii. In the **Permissions** drop-down, specify the access level Device Control permits to users accessing the specified USB devices.

iv. Click **OK**.

d. Select **Block the AutoRun function on USB storage devices** to prevent programs saved on USB devices from executing automatically.

e. Select **Display a notification message on the endpoint when Apex One detects unauthorized device access** to inform end users that Device Control restricted access to a device.

5. For Security Agents with the Data Protection feature installed, select to **Allow** or **Block** access to the devices listed under **Mobile Devices** and **Non-Storage Devices**.

6. Click **OK**.

Note

Device Control automatically assigns all user-based rules a higher priority than the default endpoint-based rule (**All users (default)**).

7. (Optional) Manage the Device Control rule list.

- **Priority**: Click the arrows to change the priority of user-based rules.
- **Copy**: Select a rule, click **Copy**, and modify the rule contents.
- **Delete**: Select a rule and click **Delete** to permanently remove the rule from the list.

Permissions for 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 12-1. 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.

The following table lists the permissions for mobile and non-storage devices managed by Data Protection.

TABLE 12-2. Device Control Permissions for Mobile and Non-storage Devices

PERMISSIONS	FILES ON THE DEVICE	INCOMING FILES
Allow	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.
Block	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

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.

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 12-3. 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 12-4. 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	

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**).

Chapter 13

Scan Exclusion Lists

This section describes how to configure scan exclusion lists that apply to multiple scan features.

Topics include:

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.

Managing the Spyware/Grayware Approved List

Procedure

1. 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.

2. Click **Add**.

    The names move to the **Approved List** table.

3. To remove names from the approved list, select the names and click **Remove**. To select multiple names, hold the CTRL key while selecting.

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
- 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. When configuring a parent policy, specify how other users can configure child policies.

    - **Inherit from parent**: Child policies must use the settings configured in the parent policy

- **Extend from parent**: Child policies can append additional settings to the settings inherited from the parent policy

> **Note**
>
> If your child policies **Extend from parent**, you can also configure **Child Policy Restrictions**. Restrictions prevent the child policy from adding specific objects to the list.

2. Type the full program path of the program to exclude from the list.
3. Click **Add to Trusted Program List**.
4. To remove a program from the list, click the **Delete** icon.

Chapter 14

Endpoint Sensor Policy Settings

This section discusses how to configure Endpoint Sensor policies on Security Agents.

Topics include:

Endpoint Sensor

Endpoint Sensor is a powerful monitoring and investigation tool used to identify the presence, location, and entry point of threats. Through the use of detailed system event recording and historical analysis, you can perform Historical Investigations to discover hidden threats throughout your network and locate all affected endpoints. Generate Root Cause Analysis reports to understand the nature and activity of the malware since the threat entered the endpoint.

You can also perform Live Investigations through the use of shared IOC files and YARA rules. Live Investigations conduct in-depth searches of endpoints to locate previously unidentified threats and possible Advanced Persistent Threat attacks.

Configuring Endpoint Sensor Settings

Important

The Endpoint Sensor feature requires special licensing and additional system requirements. Ensure that you have the correct license before deploying Endpoint Sensor policies to endpoints. For more information on how to obtain licenses, contact your support provider.

If your environment manages both Apex One on-premises and Apex One as a Service Security Agents, some features may be different compared to Apex One as a Service. Apex One as a Service Security Agents continue to send data to Trend Micro servers but investigation capabilities may differ from the Apex Central as a Service console.

Procedure

1. Select **Enable Endpoint Sensor**.

2. Select **Enable event recording** to begin collecting system event logs on the agent endpoint. (on-premises only)

   Endpoint Sensor uses the real-time event logs to identify at-risk endpoints when performing investigations. After identifying affected

Windows endpoints, you can perform an in-depth root cause analysis to better understand possible attack vectors.

Option	Description
Maximum database size (on-premises only)	Specify the maximum database size that Endpoint Sensor can use to store event logs on the endpoint. Once the agent database reaches the maximum size limit, Endpoint Sensor purges the oldest logs to make space for new event entries.
Send a subset of log data to perform Historical Investigations (on-premises only)	The information sent to the server consists of metadata, such as domain, files, or processes on the endpoint. Endpoint Sensor utilizes the data during Historical Investigations to identify affected endpoints. • **Upload frequency**: Specify how often the agent uploads the metadata to the server. **Note** Depending on your network, more frequent uploads may affect network performance. • **Additional hash types**: Specify if Endpoint Sensor also calculates and sends SHA-256 and MD5 hashes to the server. By default, Endpoint Sensor sends SHA1 hashes only. **Note** Selecting additional hash types takes up more database space.
Enable Attack Discovery to detect known attack indicators on endpoints	Attack Discovery uses Trend Micro threat intelligence based on Indicators of Attack (IoA) behaviors. After detecting a known IoA, Attack Discovery logs the detection.

Chapter 15

Vulnerability Protection Policy Settings

This section discusses how to configure Vulnerability Protection policies on Security Agents.

Topics include:

- *Vulnerability Protection on page 15-2*
- *Configuring Vulnerability Protection Settings on page 15-2*

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.

Configuring Vulnerability Protection Settings

Procedure

1. Select **Enable Vulnerability Protection**.
2. Configure intrusion prevention settings:
    a. Click the **Intrusion Prevention Rules** tab.

    b. Select one of the following scanning profiles:

    - **Recommended**: Ensures protection against known vulnerability issues, provides more relevant data, and reduces performance impact on endpoints
    - **Aggressive**: Applies additional Intrusion Prevention Rules for suspicious network activities to the **Recommended** scanning profile

    Important

    Aggressive scanning may generate a large number of nonessential logs and impact endpoint performance. Trend Micro strongly advises using the **Recommended** profile.

    c. (Optional) Select a view to filter the list of Intrusion Prevention Rules by status.

View	Description
All	Displays all Intrusion Prevention Rules
Default (Enabled)	Displays only the Intrusion Prevention Rules that the selected scanning profile enables by default
Default (Disabled)	Displays only the Intrusion Prevention Rules that the selected scanning profile disables by default
User-defined (Enabled)	Displays only the Intrusion Prevention Rules enabled by the user
User-defined (Disabled)	Displays only the Intrusion Prevention Rules disabled by the user

d. Modify the status of a rule by selecting from the **Status** drop-down control.

- **Default (Enabled)**: The selected scanning profile enables the corresponding rule by default. Select to apply the rule status defined by the scanning profile.
- **Default (Disabled)**: The selected scanning profile disables the corresponding rule by default. Select to apply the rule status defined by the scanning profile.
- **User-defined (Enabled)**: Select to enable the rule.
- **User-defined (Disabled)**: Select to disable the rule.

3. Configure network engine settings:

a. Click the **Network Engine Settings** tab.

b. Select the **Network Engine Detection Mode***.

Note

You can also use the selected Network Engine Detection Mode to configure the Advanced Logging Policy.

- **Inline**: Live packet streams pass directly through the Vulnerability Protection network engine. All rules are applied to the network traffic before the packets proceed up the protocol stack.
- **Tap (Detect-only)**: Live packet streams are replicated and diverted from the main stream.

c. Configure the following settings:

Setting	Description
ESTABLISHED Timeout	How long to stay in the ESTABLISHED state before closing the connection
LAST_ACK Timeout	How long to stay in the LAST-ACK state before closing the connection
Cold Start Timeout	The amount of time to allow non-SYN packets that could belong to a connection that was established before the stateful mechanism was started
UDP Timeout	The maximum duration of a UDP connection
Maximum TCP Connections	The maximum number of simultaneous TCP connections
Maximum UDP Connections	The maximum number of simultaneous UDP connections
Ignore Status Code	Select up to 3 types of events to ignore

Setting	Description
Advanced Logging Policy	Select from the following settings: - **Bypass**: No filtering of events. Overrides the **Ignore Status Code** settings (above) and other advanced settings, but does not override logging settings defined on the Apex One server - **Network Engine Detection Mode***: Uses **Tap Mode** if **Tap (Detect-only)** is selected for the Network Engine Detection Mode, or **Normal** if **Inline** is selected for the Network Engine Detection Mode - **Normal**: All events are logged except dropped retransmits - **Backwards Compatibility Mode**: For support use only - **Verbose Mode**: Same as **Normal** but including dropped retransmits - **Stateful and Normalization Suppression**: Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, unsolicited udp, unsolicited ICMP, out of allowed policy - **Stateful, Normalization, and Frag Suppression**: Ignores everything that **Stateful and Normalization Suppression** ignores as well as events related to fragmentation - **Stateful, Frag, and Verifier Suppression**: Ignores everything **Stateful, Normalization, and Frag Suppression** ignores as well as verifier-related events - **Tap Mode**: Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, max ack retransmit, packet on closed connection For a more comprehensive list of which events are ignored for **Stateful and Normalization Suppression**, **Stateful, Normalization, and Frag Suppression**, **Stateful, Frag, and Verifier Suppression**, and **Tap Mode**, see *Advanced Logging Policy Modes on page 15-6*.

4. Click **Save** to apply settings.

Advanced Logging Policy Modes

The following table lists the types of Events that are ignored in four of the more complex Advanced Logging Policy modes.

MODE	IGNORED EVENTS
Stateful and Normalization Suppression	Out Of Connection
	Invalid Flags
	Invalid Sequence
	Invalid ACK
	Unsolicited UDP
	Unsolicited ICMP
	Out Of Allowed Policy
	Dropped Retransmit

Mode	Ignored Events
Stateful, Normalization, and Frag Suppression	Out Of Connection
	Invalid Flags
	Invalid Sequence
	Invalid ACK
	Unsolicited UDP
	Unsolicited ICMP
	Out Of Allowed Policy
	CE Flags
	Invalid IP
	Invalid IP Datagram Length
	Fragmented
	Invalid Fragment Offset
	First Fragment Too Small
	Fragment Out Of Bounds
	Fragment Offset Too Small
	IPv6 Packet
	Max Incoming Connections
	Max Outgoing Connections
	Max SYN Sent
	License Expired
	IP Version Unknown
	Invalid Packet Info
	Maximum ACK Retransmit
	Packet on Closed Connection
	Dropped Retransmit

Mode	Ignored Events
Stateful, Frag, and Verifier Suppression	Out Of Connection
	Invalid Flags
	Invalid Sequence
	Invalid ACK
	Unsolicited UDP
	Unsolicited ICMP
	Out Of Allowed Policy
	CE Flags
	Invalid IP
	Invalid IP Datagram Length
	Fragmented
	Invalid Fragment Offset
	First Fragment Too Small
	Fragment Out Of Bounds
	Fragment Offset Too Small
	IPv6 Packet
	Max Incoming Connections
	Max Outgoing Connections
	Max SYN Sent
	License Expired
	IP Version Unknown
	Invalid Packet Info
	Invalid Data Offset
	No IP Header

Mode	Ignored Events
Stateful, Frag, and Verifier Suppression	Unreadable Ethernet Header
	Undefined
	Same Source and Destination IP
	Invalid TCP Header Length
	Unreadable Protocol Header
	Unreadable IPv4 Header
	Unknown IP Version
	Maximum ACK Retransmit
	Packet on Closed Connection
	Dropped Retransmit
Tap Mode	Out Of Connection
	Invalid Flags
	Invalid Sequence
	Invalid ACK
	Maximum ACK Retransmit
	Packet on Closed Connection
	Dropped Retransmit

Part V

Apex One Server Policies

Chapter 16

Apex One Server Policy Settings

This section describes how you can manage Apex One server policy settings.

Topics include:

- *Configuring Endpoint Sensor Server Settings on page 16-2*

Configuring Endpoint Sensor Server Settings

Important

- The Endpoint Sensor feature requires special licensing and additional system requirements. Ensure that you have the correct license before deploying Endpoint Sensor policies to endpoints. For more information on how to obtain licenses, contact your support provider.
- Server policies only apply to on-premises Apex One servers.

Procedure

1. Select **Apex One Server** as the **Product**.
2. Create or Edit a policy.
   a. To create a policy, click **Create**.
   b. To edit a policy, click a policy name in the **Policy** column.
3. Configure **Endpoint Sensor settings**.

OPTION	DESCRIPTION
Maximum metadata storage	Specify the maximum size allowed for metadata storage. Specify a size between 20 to 20480 GB. The default storage size is 1024 GB. Once the metadata storage reaches this size, the server purges old records to accommodate new ones.
Maximum memory allocation	Specify the maximum amount of memory allocated to the metadata cache. Specify a size between 4 GB and 48 GB. The new size specified must be higher than the current size. The default allocation size is 4 GB. **Note** Memory size affects the performance of data uploads and investigation speed. To improve performance, increase the memory size of the affected server.

4. Click **Deploy** or **Save**.

Part VI

Apex One Data Loss Prevention Policies

Chapter 17

Apex One Data Discovery Dashboard Widgets

This section contains help topics for the Apex One Data Discovery dashboard widgets supported in Apex Central.

Topics include:

Top Sensitive File Policy Detections Widget

This widget displays information about Data Discovery policy violation detections and the sensitive files that triggered the rules.

Note

By default, the widget displays data from all the managed products that a user account has privileges to view.

Use the **Range** drop-down to select the time period for the data that displays.

- To specify a custom time range or time interval, click the settings icon (⋮ > 🎚) and select **Customized** for the **Range**.

Use the **Rule** drop-down to specify the rule that triggered the detection.

- To specify the number of rules that display, click the settings icon (⋮ > 🎚) and select from the **Rules to display** drop-down.
- To aggregate the remaining data, click the settings icon (⋮ > 🎚) and select **Display the remaining data as "Others"**.

You can choose to display the data in a table, bar chart, pie chart, or line chart by clicking the display icons (▦📊◔📈).

The default view displays the following information in a table.

Column Name	Description
Rule Name	Displays the rules triggered by sensitive files.
Detections	Displays the number of times the rule is triggered Click the **Detections** column name to sort the table by the number of detections. Click the number to view detailed information about the detection (when the detection occurs, the sensitive files detected).

Column Name	Description
Percentage	Displays the number of times that the rule is triggered as a percentage of the total number of detections

Click a number in the **Detections** column or click a chart section to view detailed information.

Data	Description
Received	The time and date Apex Central received the data
Generated	The time and date the detection occurred
Rule	The rule that is triggered
Endpoint	The endpoint that triggered the rule
Domain	The domain that triggered the rule
User	The user that triggered the rule
User Domain	The domain that the user belongs to
File Path	The file path for the sensitive file
File	The name of the sensitive file
Template	The template that the rule belongs to
Action	The action taken on the sensitive file

Top Endpoints with Sensitive Files Widget

This widget displays information about endpoints with sensitive files that triggered Data Discovery policy violation detections.

Note

By default, the widget displays data from all the managed products that a user account has privileges to view.

Use the **Range** drop-down to select the time period for the data that displays.

- To specify a custom time range or time interval, click the settings icon (⋮ > 🎚) and select **Customized** for the **Range**.

Use the **Rule** drop-down to specify the rule that triggered the detection.

- To specify the number of templates that display, click the settings icon (⋮ > 🎚) and select from the **Endpoints to display** drop-down.
- To aggregate the remaining data, click the settings icon (⋮ > 🎚) and select **Display the remaining data as "Others"**.

You can choose to display the data in a table, bar chart, or pie chart by clicking the display icons (▦📊◔).

The default view displays the following information in a table.

Column Name	Description
Endpoints	Displays the endpoint with sensitive files that triggered the rule
Detections	Displays the number of times the rule is triggered Click the **Detections** column name to sort the table by the number of detections.
Percentage	Displays the number of times that the rule is triggered as a percentage of the total number of detections

Click a number in the **Detections** column or click a chart section to view detailed information.

Data	Description
Received	The time and date Apex Central received the data
Generated	The time and date the detection occurred
Rule	The rule that is triggered
Endpoint	The endpoint that triggered the rule

Data	Description
Domain	The domain that triggered the rule
User	The user that triggered the rule
User Domain	The domain that the user belongs to
File Path	The file path for the sensitive file
File	The name of the sensitive file
Template	The template that the rule belongs to
Action	The action taken on the sensitive file

Top Data Discovery Template Matches Widget

This widget displays information about the top Data Discovery template policy violations over time.

Note

By default, the widget displays data from all the managed products that a user account has privileges to view.

Use the **Range** drop-down to select the time period for the data that displays.

- To specify a custom time range or time interval, click the settings icon (⋮ > 🎚) and select **Customized** for the **Range**.

Use the **Rule** drop-down to specify the rule that triggered the detection.

- To specify the number of templates that display, click the settings icon (⋮ > 🎚) and select from the **Templates to display** drop-down.
- To aggregate the remaining data, click the settings icon (⋮ > 🎚) and select **Display the remaining data as "Others"**.

You can choose to display the data in a table, bar chart, or pie chart by clicking the display icons (▦📊◔).

The default view displays the following information in a table.

Column Name	Description
Templates	Displays the template triggered by sensitive files
Detections	Displays the number of times that the template is triggered Click the **Detections** column name to sort the table by the number of detections.
Percentage	Displays the number of times that the template is triggered as a percentage of the total number of detections

Click a number in the **Detections** column or click a chart section to view detailed information.

Data	Description
Received	The time and date Apex Central received the data
Generated	The time and date the detection occurred
Rule	The rule that is triggered
Endpoint	The endpoint that triggered the rule
Domain	The domain that triggered the rule
User	The user that triggered the rule
User Domain	The domain that the user belongs to
File Path	The file path for the sensitive file
File	The name of the sensitive file
Template	The template that the rule belongs to
Action	The action taken on the sensitive file

Top Sensitive Files Widget

This widget displays information about the top sensitive files that triggered Data Discovery policy violations over time.

Note

By default, the widget displays data from all the managed products that a user account has privileges to view.

Use the **Range** drop-down to select the time period for the data that displays.

- To specify a custom time range or time interval, click the settings icon (⋮ >) and select **Customized** for the **Range**.

Use the **Rule** drop-down to specify the rule that triggered the detection.

- To specify the number of detections that display, click the settings icon (⋮ >) and select from the **Sensitive files to display** drop-down.
- To aggregate the remaining data, click the settings icon (⋮ >) and select **Display the remaining data as "Others"**.

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

The default view displays the following information in a table.

Column Name	Description
File	Displays the sensitive files potentially leaked
Detections	Displays the number of times that the sensitive file has been potentially leaked Click the **Detections** column name to sort the table by the number of detections.
Percentage	Displays the number of times that the sensitive file has been potentially leaked as a percentage of the total number of detections

Click a number in the **Detections** column or click a chart section to view detailed information.

Data	Description
Received	The time and date Apex Central received the data
Generated	The time and date the detection occurred
Rule	The rule that is triggered
Endpoint	The endpoint that triggered the rule
Domain	The domain that triggered the rule
User	The user that triggered the rule
User Domain	The domain that the user belongs to
File Path	The file path for the sensitive file
File	The name of the sensitive file
Template	The template that the rule belongs to
Action	The action taken on the sensitive file

Chapter 18

Apex One Data Discovery Policy Settings

This section discusses how to configure Apex One Data Discovery policy settings in Apex Central.

Topics include:

- *Creating Data Discovery Policies on page 18-2*

Creating Data Discovery Policies

Data Discovery searches databases, endpoints, and document management systems for the presence of sensitive information. Data Discovery widgets display data loss prevention compliance with an enterprise's policy. Using Data Discovery policies and widgets allows administrators to perform remediation actions on their network.

Note

Performing a full scan of an endpoint drive or directory can cause significant system slowdown for end users.

Procedure

1. Select **Enable Data Discovery**.
2. Click **Add**.

   The **Data Discovery Policy Settings** screen appears.
3. Select **Enable this rule**.
4. Specify a name for the rule.
5. Configure the target folder settings:
   a. Click the **Target Folder** tab.

      Note

      The root folder cannot be a Windows shared folder or removable device (USB device or DVD).

   b. In the **File Path** section, specify the scan location for files.

Note

Data Discovery does not scan `autoexec.bat` files located in the following directories:

- `\Documents and Settings\*\Application Data\`
- `\Documents and Settings\*\Local Settings\`
- `\Documents and Settings\*\Cookies\`
- `\Program Files\`
- `\Windows\`
- `\Winnt\`
- `\Users\*\AppData\`
- `\ProgramData\`

c. In the **File Type Exceptions** section, specify scanning exceptions.

- **Scan**: Specify specific files or file types to scan.
- **Do not scan**: Specify specific files, file types, or folders that Data Discovery will not scan.

Note

- Data Discovery supports the following wildcard characters:
  - `*`: Substitute for any and all characters before or after the *
  - `?`: Substitute for a single character or a single double-byte character
- Separate multiple entries with pipes (|) and use the following format:
  - For files: *.<file extension> (for example: *.exe|*.doc)
  - For folders: Specify a file path (for example: *\Test*|C:\My-Docs\)

Configure the template settings:

6. Configure the template settings:

    a. Click the **Template** tab.

    b. 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 500 templates.
    - your preferred template is not found in the **Available templates** list, go to **Policies** > **Policy Resources** > **DLP Templates** and create a new template.

7. Configure the action settings:

    a. Click the **Action** tab.

    b. Select **Monitor** to record detections for analysis.

    c. (Optional) Select **Encrypt** to encrypt sensitive files using one of the following methods:

    - **User key**
    - **Group key**
    - **Encryption password**: The encryption password is a global password for all Apex One servers. Click **Create encryption password** to configure a password.

8. Configure the schedule for the scan:

    a. Click the **Schedule** tab.

   b. Specify the frequency of the scan.

   c. Specify the time that the scan starts.

9. Click **Save** to apply settings.

Chapter 19

Apex One Data Loss Prevention Policy Settings

This section describes how to configure Data Loss Prevention policies for Security Agents.

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.

Configuring a Data Loss Prevention Policy

Procedure

1. 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.

2. Select **Enable Data Loss Prevention**.

3. 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**.

4. Manage the rules that Data Loss Prevention applies to the policy un the **Rules** tab.

TASK	DESCRIPTION
Add a new rule	Click **Add** to create a rule that applies to the policy. For more information, see *Configuring Data Loss Prevention Rules on page 19-4*.
Copy existing rule settings	Select an existing rule and click **Copy** to open the **Data Loss Prevention Policy Settings** screen. Modify the rule settings as required.
Delete existing rules	Select an existing rule and click **Delete** to remove the rule from the list.
Modify existing rules	Click the **Rule** name of an existing rule to modify settings.
Enable/Disable existing rules	Click the button under the **Enable** column to enable or disable a rule for the policy.

Note

A policy can contain a maximum of 40 rules.

5. Click the **Exceptions** tab and configure any necessary exception settings.

   For more information, see *Data Loss Prevention Exceptions on page 19-12*.

Configuring 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.

   Configure the channel settings:

5. Click the **Channel** tab.

6. Select the channels for the rule.

   For details about channels, see *Network Channels on page 19-7* and *System and Application Channels on page 19-9*.

7. 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 19-6* for details on transmission scope, how targets work depending on the transmission scope, and how to define targets correctly.

8. 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 19-7*.

9. 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.

    Configure the action settings:

10. Click the **Action** tab.

11. Select a primary action and any additional actions. For details about actions, see *Data Loss Prevention Actions on page 19-10*.

12. After configuring the **Template**, **Channel**, and **Action** settings, click **Save**.

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.

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).

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
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

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

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 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. On the endpoint, run `listDeviceInfo.exe`.

3. 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)

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 19-1. Data Loss Prevention Actions

ACTION	DESCRIPTION
Actions	
Pass	Data Loss Prevention allows and logs the transmission.

Action	Description
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 Encryption creates a self-extracting package that users can access on any endpoint after providing the decryption password.

Action	Description
	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 19-14*. 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 19-15*.

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.

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 19-13*.

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 19-13*.

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)**

Part VII

Apex One (Mac) Widgets and Policies

Chapter 20

Apex One (Mac) Dashboard Widgets

This section contains help topics for the Apex One (Mac) dashboard widgets supported in Apex Central.

Topics include:

Key Performance Indicators Widget

Use this widget on the Apex Central **Dashboard** screen to display Apex One (Mac) key performance indicators (KPIs) based on selected criteria.

For information on how to add a widget to the **Dashboard** screen, see the Apex Central or Control Manager documentation.

Tip

By default, the widget marks events as “Important” (⚠) at 15 occurrences and “Critical” (⚠) at 30 occurrences. Optionally, mark events as Important or Critical by customizing event thresholds.

Configuring Key Performance Indicators

In Apex Central or Control Manager, access the **Apex One (Mac) Key Performance Indicators** widget on the **Dashboard** to perform the following indicator-related tasks.

TABLE 20-1. KPI Widget Indicator Tasks

TASK	STEPS
Add a new indicator	1. Click **Add Indicator**. The **Add Indicator** screen appears. 2. Select an option from the **Name** drop-down list and optionally customize settings. 3. Click **Save**.
Edit an indicator	1. Click the indicator in the list. The **Edit Indicator** screen appears. 2. Customize settings. 3. Click **Save**.

TASK	STEPS
Delete an indicator	1. Click the indicator in the list. The **Edit Indicator** screen appears. 2. Click **Delete**. 3. Click **OK**.
Configure event threshold settings	1. On the **Add Indicator** or **Edit Indicator** screen, select **Enable alerts at the following thresholds**. 2. Type the minimum number of event occurrences for each event type. 3. Click **Save**. **Note** The important or critical icon displays in the **Occurrences** column if both of the following are true: • The number of event occurrences that match this indicator is equal to or more than the threshold. • **Enable alerts at the following threshold** is selected.

Configuring Widget Settings

On the Apex Central or Control Manager **Dashboard** screen, select **Widget Settings** from the menu on the top-right of the widget to perform the following tasks.

TABLE 20-2. KPI Widget Settings

TASK	STEPS
Edit widget title	Type the widget title in the text field.

Task	Steps
Configure daily update time	From the drop-down list, select the hour to generate the widget data every day. **Tip** To manually refresh the widget data, click the refresh (⟳) icon.

Chapter 21

Apex One (Mac) Policy Settings

This section discusses how to configure Trend Micro Apex One (Mac) policy settings in Apex Central.

Topics include:

Cache Settings for Scans

Each time scanning runs, the agent checks the modified files cache to see if a file has been modified since the last agent startup.

- If a file has been modified, the agent scans the file and adds it to the scanned files cache.
- If a file has not been modified, the agent checks if the file is in the scanned files cache.
    - If the file is in the scanned files cache, the agent skips scanning the file.
    - If the file is not in the scanned files cache, the agent checks the approved files cache.

      Note

      The approved files cache contains files that Apex One (Mac) deems trustworthy. Trustworthy files have been scanned by successive versions of the pattern and declared threat-free each time, or threat-free files that have remained unmodified for an extended period of time.

        - If the file is in the approved files cache, the agent skips scanning the file.
        - If the file is not in the approved files cache, the agent scans the file and adds it to the scanned files cache.

All or some of the caches are cleared whenever the scan engine or pattern is updated.

If scans are run frequently and many files hit the caches, the scanning time reduces significantly.

If scans are seldom run, disable the caches so that files can be checked for threats with each scan.

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.

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 agent tree. You can enforce specific policies to agent groups or individual Security Agents. You can also enforce a single policy to all Security Agents.

Configuring Device Control Settings

Procedure

1. Click the **External Agents** tab to configure settings for external agents or the **Internal Agents** tab to configure settings for internal agents.

2. Select **Enable Device Control**.

3. Under **Devices**, select a permission for each storage device.

   For details about permissions, see *Permissions for Storage Devices on page 21-4*.

4. (Optional) If the permission for USB storage devices is **Block**, you can configure a list of approved devices under **USB Storage Device Approved List**. Users can access these devices and you can control the level of access using permissions.

   a. Type the device vendor.

   b. Type the device model and serial ID.

   c. Select the permission for the device.

For details about permissions, see *Permissions for Storage Devices on page 21-4*.

Note

USB storage devices on the approved list must have a higher permission level than the permission setting for USB storage devices in the **Devices** section.

5. Under **Notification**, select the **Display a notification message on the agent endpoint when a new device is detected** option to display a notification when a new storage device is connected to the endpoint. The notification indicates the access permission for the new storage device.

6. Click **Deploy**.

Permissions for Storage Devices

Device Control permissions for storage devices are used when you:

- Allow access to USB storage devices, CD/DVD, SD cards, network drives, and Thunderbolt SATA storage devices. 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 21-1. 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.
Read only	Permitted operations: Copy, Open Prohibited operations: Save, Move, Delete, Execute	Prohibited operations: Save, Move, Copy
Block	Prohibited operations: All operations The device and the files it contains are not visible to the user (for example, from Finder).	Prohibited operations: Save, Move, Copy

Note

The read-only permission is not available for network drives.

Endpoint Sensor

Endpoint Sensor is a powerful monitoring and investigation tool used to identify the presence, location, and entry point of threats. Through the use of detailed system event recording and historical analysis, you can perform Historical Investigations to discover hidden threats throughout your network and locate all affected endpoints. Generate Root Cause Analysis reports to understand the nature and activity of the malware since the threat entered the endpoint.

Configuring Endpoint Sensor Settings

Important

The Endpoint Sensor feature requires special licensing and additional system requirements. Ensure that you have the correct license before deploying Endpoint Sensor policies to endpoints. For more information on how to obtain licenses, contact your support provider.

Procedure

1. Select **Enable Endpoint Sensor**.

Predictive Machine Learning Settings

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.

To enable this feature, select **Enable Predictive Machine Learning**.

Privileges and Other Settings

Configure Security Agents to protect critical Security Agent files and folders.

Section	Description
Security Agent Self-protection	Select **Protect files used by the Security Agent** to prevent other programs and even the user from modifying or deleting files that the Security Agent uses. For the list of files and folders this feature protects, see *Protected Security Agent Files on page 21-7*.

Protected Security Agent Files

When you enable the Security Agent self-protection feature, Apex One (Mac) locks the following files and folders to prevent other programs and even the user from modifying or deleting Security Agent files:

- /Library/Application Support/TrendMicro/common
- /Library/Application Support/TrendMicro/Kext
- /Library/Application Support/TrendMicro/TmccMac
- /Library/Application Support/TrendMicro/TmccUpdate
- /Library/Application Support/TrendMicro/Plug-in
- /Library/Application Support/TrendMicro/Tools
- /Library/LaunchDaemons/com.trendmicro.icore.*
- /Library/LaunchDaemons/com.trendmicro.tmsm.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.launcher.plist
- /Application/TrendMicroSecurity.app

Note

Apex One (Mac) allows files to be added in the `/Library/Application Support/TrendMicro/Tools` folder, files cannot be deleted from the folder.

Scan Method Types

Apex One (Mac) 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.

  This is the default scan method type.

- **Conventional Scan**

  Agents that do not use smart scan are called “conventional scan agents”. A conventional scan agent stores all Apex One (Mac) components on the agent endpoint and scans all files locally.

Scan Methods Compared

The following table provides a comparison between the two scan methods:

TABLE 21-2. Conventional Scan and Smart Scan Compared

BASIS OF COMPARISON	CONVENTIONAL SCAN	SMART SCAN
Scanning behavior	The conventional scan agent performs scanning on the local endpoint.	• The smart scan 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 Mac Heuristic Pattern and 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 (Mac) server	Apex One (Mac) server

Switching from Smart Scan to Conventional Scan

The following table provides other considerations when switching agents to conventional scan.

TABLE 21-3. Considerations When Switching to Conventional Scan

CONSIDERATION	DETAILS
Number of Security Agents to switch	Switching a relatively small number of Security Agents at a time allows efficient use of the Apex One (Mac) server and Smart Protection Server resources. These servers can perform other critical tasks while Security Agents change their scan methods.

CONSIDERATION	DETAILS
Timing	When switching back to conventional scan, Security Agents will likely download the full version of the Virus Pattern and Spyware-active Monitoring Pattern from the Apex One (Mac) server. These pattern files are only used by conventional 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 Security Agent is scheduled to update from the server.
Agent tree settings	Scan method is a granular setting that can be set on the root, domain, or individual agent level. When switching to conventional scan, you can: • Create a new group and assign conventional scan as its scan method. Any Security Agent you move to this group will use conventional scan. When you move the Security Agent, enable the setting **Apply settings of new group to selected agent(s)**. • Select a group and configure it to use conventional scan. Smart scan agents belonging to the group will switch to conventional scan. • Select one or several smart scan agents from a group and then switch them to conventional scan. **Note** Any changes to the group's scan method overrides the scan method you have configured for individual Security Agents.

Switching from Conventional Scan to Smart Scan

If you are switching Security Agents from conventional scan to smart scan, ensure that you have set up Smart Protection Services on the Apex One server. For details, see the Apex One documentation.

The following table provides other considerations when switching Security Agent to smart scan.

TABLE 21-4. 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 on the Apex One server and that the licenses are not expired: • Antivirus • Web Reputation and Anti-spyware
Apex One (Mac) server	Ensure that Security Agents can connect to the Apex One (Mac) server. Only online Security Agents will be notified to switch to smart scan. Offline Security Agents get notified when they become online. Roaming Security Agents are notified when they become online or, if the Security Agent has scheduled update privileges, when scheduled update runs.
Number of Security Agents to switch	Switching a relatively small number of Security Agents at a time allows efficient use of Apex One (Mac) server resources. The Apex One (Mac) server can perform other critical tasks while Security Agents change their scan methods.
Timing	When switching to smart scan for the first time, Security Agents need to download the full version of the Mac Heuristic Pattern and Smart Scan Agent Pattern from the Apex One (Mac) 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 Security Agent is scheduled to update from the server.

Consideration	Details
Agent tree settings	Scan method is a granular setting that can be set on the root, group, or individual agent level. When switching to smart scan, you can: • Create a new group and assign smart scan as its scan method. Any Security Agent you move to this group will use smart scan. When you move the Security Agent, enable the setting **Apply settings of new group to selected agent(s)**. • Select a group and configure it to use smart scan. Conventional scan agents belonging to the group will switch to smart scan. • Select one or several conventional scan agents from a group and then switch them to smart scan. **Note** Any changes to the group's scan method overrides the scan method you have configured for individual Security 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: • Smart Protection Server 3.0 (integrated or standalone) • 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 (Mac) provides the following scan types to protect endpoints from security risks:

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 21-13*.
Manual Scan	A user-initiated scan that scans a file or a set of files requested by the user See *Manual Scan on page 21-17*.
Scheduled Scan	Automatically scans files on the endpoint based on the schedule configured by the administrator See *Scheduled Scan on page 21-22*.
Scan Now	An administrator-initiated scan that scans files on one or several target endpoints

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 Apex One (Mac) does not detect a security risk, the file remains in its location and users can proceed to access the file. If Apex One (Mac) detects a security risk, it displays a notification message, showing the name of the infected file and the specific security risk.

Configure and apply Real-time Scan settings to one or several agents and groups, or to all Security Agents that the server manages.

Configuring Real-time Scan Settings

Procedure

1. Select the check box to enable Real-time Scan.
2. Click the **Target** tab to configure file activities and scan settings.

   For more information, see *Real-time Scan: Target Tab on page 21-14*.

3. Click the **Action** tab to configure the scan actions Apex One (Mac) performs on detected security threats.

   For more information, see *Real-time Scan: Action Tab on page 21-15*.

Real-time Scan: Target Tab

Procedure

1. Under **User Activity on Files**, choose activities on files that will trigger Real-time Scan. Select from the following options:

   - **Scan files being created/modified**: Scan new files introduced into the endpoint (for example, after downloading a file) or files being modified
   - **Scan files being retrieved/executed**: Scan files as they are opened
   - **Scan files being created/modified and retrieved/executed**
   - **Scan files being created/modified/executed**

   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.

2. Under **Scan Settings**, select one or more from the following options:

   - **Scan compressed files**: Scan individual files within an archive file

     For more information, see *Supported Compressed File Types on page 21-15*.

   - **Scan network drive**: Scan directories physically located on other endpoints, but mapped to the local endpoint

Real-time Scan: Action Tab

On the **Actions** tab, configure the scan actions Apex One (Mac) performs on detected security threats.

Procedure

1. Under **Action**, specify the scan actions.

Option	Description
Use ActiveAction	ActiveAction is a set of pre-configured scan actions for different types of security risks. If you are unsure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction. ActiveAction settings are constantly updated in the pattern files to protect endpoints against the latest security risks and the latest methods of attacks.
Use the same action for all security risk types	Select this option if you want the same action performed on all types of security risks, except probable virus/malware. For Probable Virus/ Malware, the action is always "Pass". If you choose "Clean" as the first action, select a second action that Apex One (Mac) performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable. For details about scan actions, see *Scan Actions on page 21-16*.

2. Select **Display a notification message on the agent endpoint when virus/malware is detected** to display a notification message when Apex One (Mac) detects a security risk during Real-time Scan.

Supported Compressed File Types

Apex One (Mac) supports the following compression types.

Extension	Type
.zip	Archive created by Pkzip
.rar	Archive created by RAR
.tar	Archive created by Tar
.arj	ARJ Compressed archive
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/Compressed 16bits
.bin	MacBinary
.cab	Microsoft Cabinet file
Microsoft Compressed/MSCOMP	
.eml; .mht	MIME
.td0	Teledisk format
.bz2	Unix BZ2 Bzip compressed file
.uu	UUEncode
.ace	WinAce

Scan Actions

Specify the action Apex One (Mac) performs when a particular scan type detects a security risk.

The action Apex One (Mac) performs depends on the scan type that detected the security risk. For example, when Apex One (Mac) detects a security risk during Manual Scan (scan type), it cleans (action) the infected file.

The following are the actions Apex One (Mac) can perform against security risks:

Scan Action	Details
Delete	Apex One (Mac) removes the infected file from the endpoint.
Quarantine	Apex One (Mac) renames and then moves the infected file to the quarantine directory on the endpoint located in `<Agent installation folder>/common/lib/vsapi/quarantine`. Once in the quarantine directory, Apex One (Mac) can perform another action on the quarantined file, depending on the action specified by the user. Apex One (Mac) can delete, clean, or restore the file. Restoring a file means moving it back to its original location without performing any action. Users may restore the file if it is actually harmless. Cleaning a file means removing the security risk from the quarantined file and then moving it to its original location if cleaning is successful.
Clean	Apex One (Mac) removes the security risk from an infected file before allowing users to access it. If the file is uncleanable, Apex One (Mac) performs a second action, which can be one of the following actions: Quarantine, Delete, and Pass. To configure the second action, navigate to **Agent Management** > **Settings** > **{Scan Type}** and click the **Action** tab.
Pass	Apex One (Mac) performs no action on the infected file but records the detected security risk in the logs. The file stays where it is located. Apex One (Mac) always performs "Pass" on files infected with the Probable Virus/Malware type to mitigate a False Positive. If further analysis confirms that probable virus/malware is indeed a security risk, a new pattern will be released to allow Apex One (Mac) to perform the appropriate scan action. If actually harmless, probable virus/malware will no longer be detected. For example: Apex One (Mac) detects "x_probable_virus" on a file named "123.pdf" and performs no action at the time of detection. Trend Micro then confirms that "x_probable_virus" is a Trojan horse program and releases a new Virus Pattern version. After loading the new pattern, Apex One (Mac) will detect "x_probable_virus" as a Trojan program and, if the action against such programs is "Delete", will delete "123.pdf".

Manual Scan

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the agent console. The time it takes to complete scanning depends on the number of files to scan and the endpoint's hardware resources.

Configure and apply Manual Scan settings to one or several Security Agents and groups, or to all Security Agents that the server manages.

Configuring Manual Scan Settings

Procedure

1. Click the **Target** tab to configure the general scan and CPU usage settings.

   For more information, see *Manual Scan: Target Tab on page 21-18*.

2. Click the **Action** tab to configure the scan actions Apex One (Mac) performs on detected security threats.

   For more information, see *Manual Scan: Action Tab on page 21-19*.

Manual Scan: Target Tab

Procedure

1. In the **Files to Scan** section, select from the following:

   - **All scannable files**: Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.

     Note

     Scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the Security Agent includes in the scan.

   - **Scan only Mach-O files**: Only scan Mach-O files on endpoints. Apex One (Mac) Security Agents do not scan other file types for malware.

Note

If you select this option, you must enable the smart scan feature to ensure protection against the latest malware attacks targeting OS X and macOS platforms.

2. Under **Scan Settings**, select one or more from the following options:

    - **Scan compressed files**: Scan individual files within an archive file

      For more information, see *Supported Compressed File Types on page 21-15*.

    - **Scan network drive**: Scan directories physically located on other endpoints, but mapped to the local endpoint

    - **Scan Time Machine**: Only scan files on Time Machine drives

    Note

    After enabling the **Scan Time Machine** option for Manual and Scheduled Scan, Apex One (Mac) can only detect malware threats but not take any action (clean, quarantine, or delete) due to a permission limitation in Mac OS. Configured scan actions display as unsuccessful in the product logs.

3. In the **CPU Usage** section, configure the required settings.

    - **High**: No pausing between scans

    - **Low**: Pause between file scans if CPU consumption is higher than 20%, and do not pause if 20% or lower

Manual Scan: Action Tab

On the **Actions** tab, configure the scan actions Apex One (Mac) performs on detected security threats.

Option	Description
Use ActiveAction	ActiveAction is a set of pre-configured scan actions for different types of security risks. If you are unsure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction. ActiveAction settings are constantly updated in the pattern files to protect endpoints against the latest security risks and the latest methods of attacks.
Use the same action for all security risk types	Select this option if you want the same action performed on all types of security risks, except probable virus/malware. For Probable Virus/Malware, the action is always "Pass". If you choose "Clean" as the first action, select a second action that Apex One (Mac) performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable. For details about scan actions, see *Scan Actions on page 21-16*.

Supported Compressed File Types

Apex One (Mac) supports the following compression types.

Extension	Type
.zip	Archive created by Pkzip
.rar	Archive created by RAR
.tar	Archive created by Tar
.arj	ARJ Compressed archive
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/Compressed 16bits

Extension	Type
.bin	MacBinary
.cab	Microsoft Cabinet file
Microsoft Compressed/MSCOMP	
.eml; .mht	MIME
.td0	Teledisk format
.bz2	Unix BZ2 Bzip compressed file
.uu	UUEncode
.ace	WinAce

Scan Actions

Specify the action Apex One (Mac) performs when a particular scan type detects a security risk.

The action Apex One (Mac) performs depends on the scan type that detected the security risk. For example, when Apex One (Mac) detects a security risk during Manual Scan (scan type), it cleans (action) the infected file.

The following are the actions Apex One (Mac) can perform against security risks:

Scan Action	Details
Delete	Apex One (Mac) removes the infected file from the endpoint.

Scan Action	Details
Quarantine	Apex One (Mac) renames and then moves the infected file to the quarantine directory on the endpoint located in `<Agent installation folder>/common/lib/vsapi/quarantine`. Once in the quarantine directory, Apex One (Mac) can perform another action on the quarantined file, depending on the action specified by the user. Apex One (Mac) can delete, clean, or restore the file. Restoring a file means moving it back to its original location without performing any action. Users may restore the file if it is actually harmless. Cleaning a file means removing the security risk from the quarantined file and then moving it to its original location if cleaning is successful.
Clean	Apex One (Mac) removes the security risk from an infected file before allowing users to access it. If the file is uncleanable, Apex One (Mac) performs a second action, which can be one of the following actions: Quarantine, Delete, and Pass. To configure the second action, navigate to **Agent Management** > **Settings** > **{Scan Type}** and click the **Action** tab.
Pass	Apex One (Mac) performs no action on the infected file but records the detected security risk in the logs. The file stays where it is located. Apex One (Mac) always performs "Pass" on files infected with the Probable Virus/Malware type to mitigate a False Positive. If further analysis confirms that probable virus/malware is indeed a security risk, a new pattern will be released to allow Apex One (Mac) to perform the appropriate scan action. If actually harmless, probable virus/malware will no longer be detected. For example: Apex One (Mac) detects "x_probable_virus" on a file named "123.pdf" and performs no action at the time of detection. Trend Micro then confirms that "x_probable_virus" is a Trojan horse program and releases a new Virus Pattern version. After loading the new pattern, Apex One (Mac) will detect "x_probable_virus" as a Trojan program and, if the action against such programs is "Delete", will delete "123.pdf".

Scheduled Scan

Scheduled Scan runs automatically on the appointed date and time. Use Scheduled Scan to automate routine scans on the Security Agent and improve scan management efficiency.

Configure and apply Scheduled Scan settings to one or several Security Agents and groups, or to all Security Agents that the server manages.

Configuring Scheduled Scan Settings

Procedure

1. Select the check box to enable Scheduled Scan.

2. Click the **Target** tab to configure the general scan and CPU usage settings, and the scan schedule.

   For more information, see *Scheduled Scan: Target Tab on page 21-23*.

3. Click the **Action** tab to configure the scan actions Apex One (Mac) performs on detected security threats.

   For more information, see *Scheduled Scan: Action Tab on page 21-24*.

Scheduled Scan: Target Tab

Procedure

1. Under **Schedule**, configure how often (daily, weekly, or monthly) and what time Scheduled Scan will run.

   For monthly Scheduled Scans, if you selected the 29th, 30th, or 31st day and a month does not have this day, Apex One (Mac) runs Scheduled Scan on the last day of the month.

2. In the **Files to Scan** section, select from the following:

   - **All scannable files**: Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.

Note

Scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the Security Agent includes in the scan.

- **File types scanned by IntelliScan**: Only scan files known to potentially harbor malicious code, including files disguised by a harmless extension name.
- **Specify path or full path** : Manually specify the files or directories to scan. For example, `/Shared/Files/mytext.txt` or `/Shared/Files`.

3. Under **Scan Settings**, select one or more from the following options:

   - **Scan compressed files**: Scan individual files within an archive file

     For more information, see *Supported Compressed File Types on page 21-15*.

   - **Scan Time Machine**: Only scan files on Time Machine drives

   Note

   After enabling the **Scan Time Machine** option for Manual and Scheduled Scan, Apex One (Mac) can only detect malware threats but not take any action (clean, quarantine, or delete) due to a permission limitation in Mac OS. Configured scan actions display as unsuccessful in the product logs.

4. In the **CPU Usage** section, configure the required settings.

   - **High**: No pausing between scans
   - **Low**: Pause between file scans if CPU consumption is higher than 20%, and do not pause if 20% or lower

Scheduled Scan: Action Tab

On the **Actions** tab, configure the scan actions Apex One (Mac) performs on detected security threats.

Procedure

1. Under **Action**, specify the scan actions.

Option	Description
Use ActiveAction	ActiveAction is a set of pre-configured scan actions for different types of security risks. If you are unsure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction. ActiveAction settings are constantly updated in the pattern files to protect endpoints against the latest security risks and the latest methods of attacks.
Use the same action for all security risk types	Select this option if you want the same action performed on all types of security risks, except probable virus/malware. For Probable Virus/ Malware, the action is always "Pass". If you choose "Clean" as the first action, select a second action that Apex One (Mac) performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable. For details about scan actions, see *Scan Actions on page 21-16*.

2. Under **Scheduled Scan Privileges**, specify whether users can postpone or skip a scheduled scan.

Privilege	Description
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. Configure the number of hours and minutes, which corresponds to: • The maximum postpone duration • The maximum amount of time that should elapse before scanning restarts
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

3. Under **Scheduled Scan Settings**, specify the notification and battery power settings.

Setting	Description
Display a notification before Scheduled Scan runs	When you enable this option, a notification message displays on the endpoint several 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. Configure the timing for displaying the notification message, in number of minutes.

Setting	Description
Automatically stop Scheduled Scan when scanning lasts more than __ hours and __ minutes	The Security Agent stops scanning when the specified amount of time is exceeded and scanning is not yet complete. The Security Agent 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 (Mac) skips a Scheduled Scan 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. If a scan is in progress when the battery life is low, the scan is not terminated.

Supported Compressed File Types

Apex One (Mac) supports the following compression types.

Extension	Type
.zip	Archive created by Pkzip
.rar	Archive created by RAR
.tar	Archive created by Tar
.arj	ARJ Compressed archive
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/Compressed 16bits
.bin	MacBinary
.cab	Microsoft Cabinet file
Microsoft Compressed/MSCOMP	
.eml; .mht	MIME
.td0	Teledisk format

Extension	Type
.bz2	Unix BZ2 Bzip compressed file
.uu	UUEncode
.ace	WinAce

Scan Actions

Specify the action Apex One (Mac) performs when a particular scan type detects a security risk.

The action Apex One (Mac) performs depends on the scan type that detected the security risk. For example, when Apex One (Mac) detects a security risk during Manual Scan (scan type), it cleans (action) the infected file.

The following are the actions Apex One (Mac) can perform against security risks:

Scan Action	Details
Delete	Apex One (Mac) removes the infected file from the endpoint.
Quarantine	Apex One (Mac) renames and then moves the infected file to the quarantine directory on the endpoint located in `<Agent installation folder>/common/lib/vsapi/quarantine`. Once in the quarantine directory, Apex One (Mac) can perform another action on the quarantined file, depending on the action specified by the user. Apex One (Mac) can delete, clean, or restore the file. Restoring a file means moving it back to its original location without performing any action. Users may restore the file if it is actually harmless. Cleaning a file means removing the security risk from the quarantined file and then moving it to its original location if cleaning is successful.
Clean	Apex One (Mac) removes the security risk from an infected file before allowing users to access it. If the file is uncleanable, Apex One (Mac) performs a second action, which can be one of the following actions: Quarantine, Delete, and Pass. To configure the second action, navigate to **Agent Management** > **Settings** > **{Scan Type}** and click the **Action** tab.

Scan Action	Details
Pass	Apex One (Mac) performs no action on the infected file but records the detected security risk in the logs. The file stays where it is located. Apex One (Mac) always performs "Pass" on files infected with the Probable Virus/Malware type to mitigate a False Positive. If further analysis confirms that probable virus/malware is indeed a security risk, a new pattern will be released to allow Apex One (Mac) to perform the appropriate scan action. If actually harmless, probable virus/malware will no longer be detected. For example: Apex One (Mac) detects "x_probable_virus" on a file named "123.pdf" and performs no action at the time of detection. Trend Micro then confirms that "x_probable_virus" is a Trojan horse program and releases a new Virus Pattern version. After loading the new pattern, Apex One (Mac) will detect "x_probable_virus" as a Trojan program and, if the action against such programs is "Delete", will delete "123.pdf".

Scan Exclusions

Configure scan exclusions to increase the scanning performance and skip scanning files that are known to be harmless. When a particular scan type runs, Apex One (Mac) checks the scan exclusion list to determine which files on the endpoint will be excluded from scanning.

Scan Exclusion List	Details
Files	Apex One (Mac) will not scan a file if: • The file is located under the directory path specified in the scan exclusion list • The file matches the full file path (directory path and file name) specified in the scan exclusion list
File extensions	Apex One (Mac) will not scan a file if its file extension matches any of the extensions included in this exclusion list.

Configuring Scan Exclusion Lists

For details about Scan Exclusion Lists, see *Scan Exclusions on page 21-29*.

Procedure

1. Select the check box to enable scan exclusion.
2. To configure the **Scan Exclusion List (Files)**:

    a. Type a full file path or directory path and click **Add**.

    Reminders:

    - It is not possible to type only a file name.
    - You can specify a maximum of 64 paths. See the following table for examples.

PATH	DETAILS	EXAMPLES

Full file path	Excludes a specific file on the endpoint	• Example 1:
		`/file.log`
		• Example 2:
		`/System/file.log`

PATH	DETAILS	EXAMPLES

Directory path	Excludes all files located on a specific folder and all its subfolders	- Example 1:
		`/System/`
		Examples of files excluded from scans:
		- `/System/file.log`
		- `/System/Library/file.log`
		Examples of files that will be scanned:
		- `/Applications/file.log`
		- Example 2:
		`/System/Library`
		Examples of files excluded from scans:
		- `/System/Library/file.log`
		- `/System/Library/Filters/file.log`
		Examples of files that will be scanned:
		- `/System/file.log`

- Use the asterisk wildcard (*) in place of folder names.

  See the following table for examples.

Path	Wildcard Usage Examples
Full file path	`/Users/Mac/*/file.log` Examples of files excluded from scans: • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` Examples of files that will be scanned: • `/Users/file.log` • `/Users/Mac/file.log`

Directory path	• Example 1:
	`/Users/Mac/*`
	Examples of files excluded from scans:
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	Examples of files that will be scanned:
	• `/Users/doc.html`
	• Example 2:
	`/*/Components`
	Examples of files excluded from scans:
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	Examples of files that will be scanned:
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

- Partial matching of folder names is not supported. For example, it is not possible to type `/Users/*user/temp` to exclude files on folder names ending in “user”, such as “end_user” or “new_user”.

b. To delete a path, select it and click **Remove**.

3. To configure the **Scan Exclusion List (File Extensions)**:

   a. Type a file extension without a period (.) and click **Add**. For example, type `pdf`. You can specify a maximum of 64 file extensions.

   b. To delete a file extension, select it and click **Remove**.

Trusted Program List

You can configure Security Agents to skip scanning of trusted processes during Real-time Scan and event recording. After adding a program to the Trusted Program List, the Security Agent does not subject the program or any processes initiated by the program to Real-time Scan and event recording. Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints.

Note

You can add files to the Trusted Program List if the following requirements are met:

- The file is not located in the system directory.
- The file has a valid digital signature.

After adding a program to the Trusted Program List, the Security Agent automatically excludes the program from the following:

- Real-time Scan file checking
- Real-time Scan process scanning
- Event recording

Configuring the Trusted Program List

The Trusted Program List excludes programs and all child processes called by the program from Real-time Scan.

Procedure

1. Type the full program path of the program to exclude from the list.
2. Click **+ Add**.
3. To remove a program from the list, click the **Delete** icon.

Update Settings

To ensure that Security Agents stay protected from the latest security risks, update agent components regularly. Also update Security Agents with severely out-of-date components and whenever there is an outbreak. Components become severely out-of-date when the Security Agent is unable to update from the Apex One (Mac) server or the ActiveUpdate server for an extended period of time.

Agent Update Methods

There are several ways to update Security Agents.

Update Method	Description
Administrator-initiated manual update	Initiate an update from the following web console screens: • Agent Management screen. • Summary screen.

Update Method	Description
Automatic update	- After the server finishes an update, it immediately notifies Security Agents to update. - Updates can run according to the schedule that you configured. You can configure a schedule that applies to one or several Security Agents and domains, or to all the Security Agents that the server manages. For details, see *Configuring Agent Update Settings on page 21-37*.
User-initiated manual update	Users launch the update from their endpoints.

Agent Update Source

By default, Security Agents download components from the Apex One (Mac) server. In addition to components, Security Agents also receive updated configuration files when updating from the Apex One (Mac) server. Security Agents need the configuration files to apply new settings. Each time you modify Apex One (Mac) settings on the web console, the configuration files change.

Before updating the Security Agents, check if the Apex One (Mac) server has the latest components.

Configure one, several, or all Security Agents to download from the Trend Micro ActiveUpdate server if the Apex One (Mac) server is unavailable.

For details, see *Configuring Agent Update Settings on page 21-37*.

Note

If an agent only has an IPv6 address, read the IPv6 limitations for agent updates in *Pure IPv6 Agent Limitations on page 21-36*.

Agent Update Notes and Reminders

- Security Agents can use proxy settings during an update. Proxy settings are configured on the agent console.

- During an update, the Security Agent icon on the menu bar of the endpoint indicates that the product is updating. If an upgrade to the Security Agent program is available, Security Agents update and then upgrade to the latest program version or build. Users cannot run any task from the console until the update is complete.
- Access the Summary screen to check if all Security Agents have been updated.

Pure IPv6 Agent Limitations

The following table lists the limitations when Security Agents only have an IPv6 address.

TABLE 21-5. Pure IPv6 Agent Limitations

ITEM	LIMITATION
Parent server	Pure IPv6 agents cannot be managed by a pure IPv4 server.
Updates	A pure IPv6 agent cannot update from pure IPv4 update sources, such as: • Trend Micro ActiveUpdate Server • A pure IPv4 Apex One (Mac) server
Web Reputation queries	A pure IPv6 agent cannot send Web Reputation queries to Trend Micro Smart Protection Network.
Proxy connection	A pure IPv6 agent cannot connect through a pure IPv4 proxy server.
Agent deployment	Apple Remote Desktop is unable to deploy the agent to pure IPv6 endpoints because these endpoints always appear as offline.

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 agents and the entities to which they connect.

Configuring Agent Update Settings

For a detailed explanation of agent updates, see *Update Settings on page 21-34*.

Procedure

1. Select **Agents download updates from the Trend Micro ActiveUpdate server when unable to connect to the Apex One (Mac) server** to allow agents to download updates from the Trend Micro ActiveUpdate server.

   Note

   If a Security Agent only has an IPv6 address, read the IPv6 limitations for agent updates in *Pure IPv6 Agent Limitations on page 21-36*.

2. Select **Agents can update the components but not upgrade the agent program or install hot fixes** to allow component updates to proceed but prevents agent upgrade.

3. To set up scheduled updates, complete the following steps:

   a. Select **Enable scheduled update**.

   b. Configure the schedule.

   c. If you select **Daily** or **Weekly**, specify the time of the update and the time period the Apex One (Mac) server will notify Security Agents to update components. For example, if the start time is 12pm and the time period is 2 hours, the server randomly notifies all online Security Agents to update components from 12pm until 2pm. This setting prevents all online Security Agents from simultaneously connecting to the server at the specified start time, significantly reducing the amount of traffic directed to the server.

Web Reputation

Web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. It will then continue to scan sites and block users from accessing infected ones.

Security Agents send queries to smart protection sources to determine the reputation of websites that users are attempting to access. A website's reputation is correlated with the specific web reputation policy enforced on the endpoint. Depending on the policy in use, the Security Agents will either block or allow access to the website.

Note

This feature supports the latest Safari™, Mozilla™ Firefox™, Google Chrome™, and Microsoft™ Edge Chromium browsers.

Configuring Web Reputation Settings

Web Reputation settings include policies that dictate whether Apex One (Mac) will block or allow access to a website. To determine the appropriate policy to use, Apex One (Mac) checks the location of the Security Agent. The location of a Security Agent is "internal" if the Security Agent can connect to the Apex One (Mac) server. Otherwise, the location for the Security Agent is "external".

Procedure

1. To configure a policy for external Security Agents:

    a. Click the **External Agents** tab.

    b. Select **Enable Web Reputation policy**.

    When the policy is enabled, external Security Agents send web reputation queries to the Smart Protection Network.

    Note

    If an agent only has an IPv6 address, read the IPv6 limitations for Web Reputation queries in *Pure IPv6 Agent Limitations on page 21-36*.

c. Select from the available web reputation security levels: **High**, **Medium** or **Low**

Note

The security levels determine whether Apex One (Mac) will allow or block access to a URL. For example, if you set the security level to Low, Apex One (Mac) 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.

d. To submit web reputation feedback, click the URL provided. The Trend Micro Web Reputation Query system opens in a browser window.

2. To configure a policy for internal Security Agents:

a. Click the **Internal Agents** tab.

b. Select **Enable Web Reputation policy**.

When the policy is enabled, internal Security 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.

Note

If an agent only has an IPv6 address, read the IPv6 limitations for Web Reputation queries in *Pure IPv6 Agent Limitations on page 21-36*.

c. Select **Send queries to Smart Protection Servers** if you want internal Security Agents to send web reputation queries to Smart Protection Servers.

- If you enable this option, Security Agents refer to the same smart protection source list used by Apex One Security Agents to determine the Smart Protection Servers to which they send queries.

- If you disable this option, Security Agents send web reputation queries to Smart Protection Network. Endpoints must have Internet connection to send queries successfully.

d. Select from the available web reputation security levels: **High**, **Medium** or **Low**

Note

The security levels determine whether Apex One (Mac) will allow or block access to a URL. For example, if you set the security level to Low, Apex One (Mac) 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.

Security Agents do not block untested websites, regardless of the security level.

e. To submit web reputation feedback, click the URL provided. The Trend Micro Web Reputation Query system opens in a browser window.

f. Select whether to allow the Security Agents to send web reputation logs to the server. Allow Security Agents to send logs if you want to analyze URLs being blocked by Apex One (Mac) and take the appropriate action on URLs you think are safe to access.

Configuring the Approved and Blocked URL Lists

Add websites that you consider safe or dangerous to the approved or blocked list. When Apex One (Mac) detects access to any of these websites, it automatically allows or blocks the access and no longer sends a query to smart protection sources.

Procedure

1. Access the Apex One (Mac) web console.
2. Navigate to **Agents** > **Global Agent Settings** > **Web Reputation Approved/Blocked URL List**.
3. Specify a URL in the text box. You can add a wildcard character (*) anywhere on the URL.

   Examples:

   - `www.trendmicro.com/*` means all pages on the www.trendmicro.com domain.
   - `*.trendmicro.com/*` means 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 square brackets.
4. Click **Add to Approved List** or **Add to Blocked List**.
5. To delete an entry, select an option from the **View** drop-down list and click the icon next to a URL.
6. Click **Deploy**.

Part VIII

Deep Discovery Widgets and Policies

Chapter 22

Deep Discovery Analyzer and Email Inspector Dashboard Widgets

This section contains help topics for the Deep Discovery Analyzer and Deep Discovery Email Inspector dashboard widgets supported in Apex Central.

Topics include:

Deep Discovery Analyzer Widgets

This section contains help topics for all the Deep Discovery Analyzer widgets supported in Apex Central.

Virtual Analyzer Summary Widget

This widget displays the total number of samples submitted to Virtual Analyzer and the number of these samples with risk. The widget may display data from one or more Deep Discovery Analyzer appliances. The widget presents data in a table and an associated pie chart.

Label	Description
Submissions	The total number of submissions to Virtual Analyzer.
Identified risks	The total number of submissions with identified risks.
High risk	The total number of high-risk submissions.
Medium risk	The total number of medium-risk submissions.
Low risk	The total number of low-risk submissions.
% of submissions that are risks	The percentage of the total submissions that are risks.
Malicious Events Distribution	A pie chart that shows the percentage of identified risks that are high-risk, medium-risk, and low-risk.

Change the time range by selecting an option in the **Range** drop-down list at the top left section of the widget.

Change whether the data shown is from all registered Deep Discovery Analyzer appliances or a specific appliance by selecting the option in the **Show** drop-down list at the top left section of the widget.

After selecting an appliance, view more details by clicking the total number of submissions, the number of submissions with high-/medium-/low-risk, or a section in the pie chart.

Deep Discovery Email Inspector Widgets

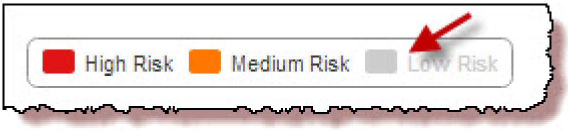
This section contains help topics for all the Deep Discovery Email Inspector widgets supported in Apex Central.

Email Messages with Advanced Threats Widget

The **Email Messages with Advanced Threats** widget shows all email messages with malicious and suspicious characteristics that Deep Discovery Email Inspector detects. Suspicious characteristics includes anomalous behavior, false or misleading data, suspicious and malicious behavior patterns, and strings that indicate system compromise but require further investigation.

The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click an item in the widget legend to show or hide data related to that metric.



Click **View detected messages** to view all detections.

Top Email Recipients of Advanced Threats Widget

The **Top Email Recipients of Advanced Threats** widget shows the recipients who received the highest volume of suspicious messages on Deep Discovery Email Inspector.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Chapter 23

Deep Discovery Inspector Integration and Policy Settings

This section discusses how to integrate Deep Discovery Inspector with Apex Central and manage policies from the Apex Central console.

Topics include:

Deep Discovery Inspector Integration Summary

This topic discusses the extent of integration between Apex Central and supported Deep Discovery Inspector versions.

Integration Feature/Function	5.0
Registration	From the Deep Discovery Inspector management console (through the MCP Agent)
Single sign-on	Supported
License management	None
Command tracking	Supported
Components deployed from Apex Central	All components
Policies managed and deployed from Apex Central	• *Deny List/Allow List on page 23-9* • *Adding Monitored Network Groups on page 23-10* • *Adding Registered Services on page 23-12* • *Configuring Virtual Analyzer Settings on page 23-13*
Information shown in User/Endpoint Directory	None
Ad-hoc query	Select any of the following data views while performing an ad-hoc query to view product information and logs: • Product Status Information • Deep Discovery Information
Dashboard widgets specific to product	• *Deep Discovery Inspector System Status Widget on page 23-6* • *Deep Discovery Inspector Affected Hosts Widget on page 23-3*

Integration Feature/Function	5.0
Dashboard widgets shared with other managed products	None
Static report templates	Trend Micro Deep Discovery Inspector reports
Custom report templates (predefined)	• TM-Deep Discovery Inspector Host Severity Summary • TM-Deep Discovery Inspector Suspicious Threat Detection Summary
Event notifications	Advanced Threat Activity • C&C callback alert • C&C callback outbreak alert • High risk Virtual Analyzer detections • High risk host detections • Known targeted attack behavior detections • Potential document exploit detections • Rootkit or hacking tool detections • SHA-1 Deny List detections • Worm or file infector propagation detections • Correlated incident detections
Data Loss Prevention (DLP) incident management	Not applicable
Suspicious object and IOC file management	• Sends suspicious objects to Apex Central • Synchronizes suspicious objects with Apex Central

Deep Discovery Inspector Affected Hosts Widget

This widget displays information about the Deep Discovery Inspector detections found on affected hosts.

The default view displays only the top 10 high severity hosts by **Detection count**.

To change whether the widget displays hosts by detection count or by detection time, click the settings icon (⋮ > 🎚) and select one of the following:

- **Detection count**: Select the number of hosts (Top 10, Top 25, Top 50) from the drop-down.
- **Detection time**: Select the number of hosts (Latest 10, Latest 25, Latest 50, Latest 100) from the drop-down.

Use the **Range** drop-down to select the time period for the data that displays.

- If you display hosts by **Detection count**, you can view data for Today, 1 Week, 2 Weeks, or 1 Month.
- If you display hosts by **Detection time**, you can only view data for Today or 1 Week.

You can also use the **Severity** drop-down to specify the severity level when displaying hosts by **Detection time**.

Column	Description
IP Address	Displays the IP address of the affected host
Host Name	Displays the name of the affected host.
Network Group	Displays the name of the group of monitored networks that allow Deep Discovery Inspector to determine whether attacks originate from within or outside the network

Column	Description
Detections	Displays the number of events found on affected hosts - Click a number in the **Detections** column to view additional information on the **Detections** screen. - Click the **View** link in the **Details** column to log on to Deep Discovery Inspector using single sign-on and display the **Detections Log Query Detail** screen. If the log is purged, the console displays a message informing you of the action.
Latest Detection	Displays the time and date that Deep Discovery Inspector last detected a potential/known risk.

Deep Discovery Inspector Affected Hosts Detections

Clicking a value in the **Detections** column of the Deep Discovery Inspector Affected Hosts widget displays a table with host-related information:

Table 23-1. Host-related Information

Column Name	Information
Date	Date and time when Deep Discovery Inspector generated the detection log
Severity	Severity rating descriptions: - High: Known malicious or involved in high-severity connections - Medium: IP address/domain/URL is unknown to reputation service - Low: Reputation service indicates previous compromise or spam involvement - Informational: An object that is most likely benign
Detection	The rule description or malware name

Column Name	Information
Threat Type	Any of the following: • File Pattern • Malicious Behavior • Suspicious Behavior • Exploit • Grayware • Web Reputation • Disruptive Applications
Source IP	The IP address of the source where a suspicious object originates
Destination IP	The IP address of the intended destination of a suspicious object
Protocol	The protocol used when transporting a suspicious object from the source to the destination
File Name	File name extracted from the sample
Logged By	The host name of Deep Discovery Inspector that analyzed the sample
Details	Click **View** to launch another window that provides detailed analysis related to the suspicious object in Deep Discovery Inspector.

Deep Discovery Inspector System Status Widget

Use this widget to display the resource usage and number of queued samples waiting for Virtual Analyzer processing for selected Deep Discovery Inspector appliances.

By default the widget displays data from all the managed products/servers that a user's account privileges allow.

Click the settings icon (⋮ > 🎚) to configure the following:

- **Title**: Specify a new and meaningful title for the widget.

- **Scope: All Products**: Click the **>>** button to specify the products that contribute data for display.

The widget displays the following system resource data to verify that all Deep Discovery Inspector resources are operating within specifications.

Column	Description
Server Name	The server name for each Deep Discovery Inspector appliance • **View detailed status**: Click this option to view product status details. "View detailed status" data can also be viewed through a Product Status log query. This table displays percentage of CPU usage, percentage and actual memory and disk usage, and number of queued samples waiting for Virtual Analyzer processing. To assist with troubleshooting, refer to the Product Host, Product IP, Connection Status, and Product Version fields. Deep Discovery Inspector sends a system status update to Apex Central every five minutes. When ⚠ is displayed, Apex Central is not receiving the latest Deep Discovery Inspector system status logs. Confirm that Deep Discovery Inspector is active and connected. • **Log-on console**: Click this option to access the Deep Discovery Inspector management console. No logon credentials are required.
CPU Usage	The percent of CPU in use by the server • ⚠ is displayed when the server's CPU average exceeds 80%. **Note** CPU, memory, and disk usage and queue sample limits are not configurable. If alerts are persistent, consider upgrading your Deep Discovery Inspector/Virtual Analyzer appliances.

Column	Description
Memory Usage	The percent of available memory on the server • ❗ is displayed when memory usage exceeds 80%. **Note** CPU, memory, and disk usage and queue sample limits are not configurable. If alerts are persistent, consider upgrading your Deep Discovery Inspector/Virtual Analyzer appliances.
Disk Usage	The percent of available disk space on the server • ❗ is displayed when disk usage exceeds 80%. **Note** CPU, memory, and disk usage and queue sample limits are not configurable. If alerts are persistent, consider upgrading your Deep Discovery Inspector/Virtual Analyzer appliances.
Samples Queued	The number of queued samples waiting for Virtual Analyzer processing • ❗ is displayed when the Virtual Analyzer queue exceeds 40 samples. **Note** CPU, memory, and disk usage and queue sample limits are not configurable. If alerts are persistent, consider upgrading your Deep Discovery Inspector/Virtual Analyzer appliances.

Deep Discovery Inspector Policy Settings

This section discusses how to configure Deep Discovery Inspector policy settings on the **Create Policy** screen.

Deny List/Allow List

The Deny List/Allow List screen is separated in to the following tabs: Deny List, Allow List, Import/Export.

Table 23-2. Deny List/Allow List Tabs

Tab	Description
Deny List	Deep Discovery Inspector monitors or monitors and resets the connection to entries in the Deny List.
Allow List	Deep Discovery Inspector allows the connection to entries in the Allow List. **Tip** Use the Allow List to lower the number of false positive detections from the Deny List.
Import/Export	Import or export Deny List or Allow List entries.

Creating a Custom Deny List

Procedure

1. Select the **Deny List** tab.
2. To add an entity to the Deny List, select **Add**.

   The **Add Item to Deny List** window appears.
3. At the **Add Item to Deny List** window, verify information, add any comments, and click **Save**.

Creating a Custom Allow List

Procedure

1. Select the **Allow List** tab.
2. To add an entity to the Allow List, select **Add**.

   The **Add Item to Allow List** window appears.
3. At the **Add Item to Allow List** window, verify information, add any comments, and click **Save**.

Importing/Exporting Custom Deny or Allow Lists

Procedure

1. Select the **Import/Export** tab.
2. To export the current Deny or Allow List, select a list and click **Export**.
3. To overwrite the current Deny or Allow List, select a list, browse to the storage location and click **Import**.

   The current selected list is overwritten.

Adding Monitored Network Groups

Establish groups of monitored networks using IP addresses to allow Deep Discovery Inspector to determine whether attacks originate from within or outside the network.

Procedure

1. Click **Add**.
2. Specify a group name.

Tip

Provide specific groups with descriptive names for easy identification of the network to which the IP address belongs. For example, "Finance network", "IT network", or "Administration".

3. Specify an IP address range in the text box (up to 1,000 IP address ranges).

   Deep Discovery Inspector comes with a monitored network called **Default**, which contains the following IP address blocks reserved by the Internet Assigned Numbers Authority (IANA) for private networks:

   - 10.0.0.0 - 10.255.255.255
   - 172.16.0.0 - 172.31.255.255
   - 192.168.0.0 - 192.168.255.255

Note

- If you did not remove **Default**, you do not need to specify these IP address blocks when adding a new monitored network.
- Use a dash to specify an IP address range.

  Example: 192.168.1.0-192.168.1.255.
- Use a slash to specify the subnet mask for IP addresses.

  Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24.
- Up to three layers of sub-groups can be added.

4. Select the network zone of network group:

   - **Trusted**: This is a secure network
   - **Untrusted**: There is a degree of doubt about the security of the network.

5. Click **Add**.

6. Click **Finish**.

Adding Registered Services

Add different servers for specific services that your organization uses internally or considers trustworthy to establish the network profile. Identifying trusted services in the network ensures detection of unauthorized applications and services.

Add only trusted services (up to 1,000 services) to ensure the accuracy of your network profile.

Procedure

1. Select a service from the drop-down list.

TABLE 23-3. Service Types

SERVICE	DESCRIPTION
DNS	The network server used as a DNS server.
FTP	The network server used as an FTP server.
HTTP Proxy	The network server used as an HTTP Proxy server.
SMTP	The network server used as an SMTP server.
SMTP Open Relay	The network server used as an SMTP Open Relay server.
Software Update Server	The network server responsible for Windows Server Update Services (WSUS) or the server that performs remote deployment.
Security Audit Server	The network server used to detect both vulnerabilities and insecure configurations.

Service	Description
Active Directory	The network server used as the Active Directory server.
Domain Controller	The network server used as the Domain Controller server.
Database Server	The network server used as the database server.
Authentication Servers - Kerberos	The network server used to provide Kerberos authentication.
File Server	The network server used to provide a location for shared file access.
Web Server	The network server used as a web server.
Content Management Server	The network server used for managing content.
Radius Server	The network server used as the Radius authentication server.

Registered service names appear in the **Defined Registered Services** section.

2. Specify a server name.
3. Specify an IP address.
4. Click **Add**.

Configuring Virtual Analyzer Settings

Use this option to enable or disable analysis of threat files.

Procedure

1. Ensure that the management port can access the Internet; the virtual analyzer may need to query data through this port.

2. At the **Virtual Analyzer Configuration** window, check **Submit files to Virtual Analyzer**.

3. Select an analysis module.

    - For **Internal Analyzer** select a network type.

TABLE 23-4. Analyzer Network Types

MODULE OPTION	DESCRIPTION
Management Network	Select this network type to direct virtual analyzer traffic through a management port.
Custom network / Specified Network	Select this network type to configure a specific port for virtual analyzer traffic. Ensure that the port is able to connect to an outside network directly.
No network / Isolated Network	Select this network type to isolate virtual analyzer traffic within the virtual analyzer, and when the environment has no connection to an outside network.

TABLE 23-5. Custom network / Specified network options

OPTION	ACTION
Virtual Analyzer port	Select a Virtual Analyzer port. **Note** Assign a Virtual Analyzer port different from the Deep Discovery Inspector data port.
Configure IPv4	**Automatically (using DHCP)** is selected. This setting cannot be changed.

- For **External Analyzer** specify a Virtual Analyzer IP address and an API Key.

Tip

The external analyzer (Deep Discovery Advisor or Deep Discovery Analyzer) has more analysis capability than the internal analyzer (Virtual Analyzer).

4. (Optional) For the internal Virtual Analyzer, enable and configure a dedicated proxy.

Note

To configure the proxy settings, the management network or custom network must be selected as the network type.

a. In **Proxy Setting** select **Use dedicated proxy settings**.

b. In **Server address**, type the proxy server's IP address, host name, or FQDN.

c. Type the port number.

d. (Optional) Type the proxy server's authentication credentials.

5. (Optional) For the internal Virtual Analyzer, select **Send possible Mac OS threats to the Trend Micro cloud sandboxes for analysis**.

6. Configure **File submission** options:

a. Specify the maximum file size. Changing this setting may affect Deep Discovery Inspector performance.

b. Enable Certified Safe Software Service (CSSS).

Note

Certified Safe Software Service (CSSS) is the Trend Micro cloud database of safe files. Deep Discovery Inspector queries Trend Micro datacenters to check submitted files against the database.

Part IX

Deep Security Manager Widgets

Chapter 24

Deep Security Manager Dashboard Widgets

This section contains help topics for the Deep Security Manager dashboard widgets supported in Apex Central.

Topics include:

- *Deep Security Intrusion Prevention Event History Widget on page 24-13*
- *Deep Security IPS Activity (Detected) Widget on page 24-13*
- *Deep Security IPS Activity (Prevented) Widget on page 24-14*
- *Deep Security Log Inspection Activity Widget on page 24-15*
- *Deep Security Log Inspection Event History Widget on page 24-16*
- *Deep Security Reconnaissance Scan Event History Widget on page 24-17*
- *Deep Security Status Summary Widget on page 24-17*
- *Deep Security Web Reputation Event History Widget on page 24-19*
- *Deep Security Web Reputation URL Activity Widget on page 24-20*

Deep Security Anti-Malware Event History Widget

This widget displays the number of Anti-Malware Events that occurred over the specified time range.

Click a bar to display the Deep Security Manager **Events** page filtered to show the Anti-Malware Events for the specified event type and time period. You can also click the event types in the legend to change the chart view.

Use the **Range** drop-down to select the time period for the data that displays.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

Deep Security Anti-Malware Status (Malware) Widget

This widget displays the five most common malware threats detected on your endpoints.

Click a count in the **Total** column to view additional details in the Deep Security Manager console.

Use the **Range** drop-down to select the time period for the data that displays.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

To make a Deep Security installation available to the Deep Security widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Deep Security server.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

DATA	DESCRIPTION
Malware Name	The name of the malware threat
Number of Uncleanable	The number of occurrences of the threat that Deep Security was unable to clean
Total	Number of events in the time range and the percentage of the total Events of this type that it represents
Previous Total	Number of events in the time period preceding the current time range
Trend	The percentage change from the previous to the current period

Deep Security Application Type Activity (Detected) Widget

This widget displays the top five Application Types associated with IPS (Detected) events.

Click on a value in the **Total** column to display the of Deep Security Manager **Events** screen filtered to show the IPS (Detected) events associated with the specific Application Type.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

Data	Description
Application Type Name	The name of the Application Type
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage of change from the previous to the current time period

Deep Security Application Type Activity (Prevented) Widget

This widget displays the top five Application Types associated with IPS (Prevented) events.

Click on a value in the **Total** column to display the of Deep Security Manager **Events** screen filtered to show the IPS (Prevented) events associated with the specific Application Type.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

Data	Description
Application Type Name	The name of the Application Type
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage of change from the previous to the current time period

Deep Security Component Summary Widget

This widget displays version numbers of available Deep Security component updates and the percentage of endpoints that have been updated to the latest version.

Important

This widget only displays data from Deep Security 7.5 or later.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Data	Description
Components	The name of the Deep Security component.
Current Version	The version that is currently available on Deep Security Manager.
Percent Updated	The percentage of managed computers that have updated to the latest version. **Note** Updates may not be applicable to all managed computers.

The widget displays version numbers for the following components.

Component	Description
Smart Scan Agent Pattern	The smaller malware pattern detection file that is sent to the Deep Security Virtual Appliance. If a comparison to these patterns suggests that a file on a computer may be malicious, the file is compared to the more robust pattern file on the Smart Scan server for confirmation.
Virus Pattern	A file that helps the Deep Security virtual appliance identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.

Component	Description
IntelliTrap Pattern	IntelliTrap searches malware that may be hidden in files that use real-time compression paired with other malware characteristics like packers.
Spyware Active Monitoring Pattern	Spyware detection patterns.
Virus Scan Engine	The engine that applies virus patterns to a file during a virus scan.
Deep Security Rule Update	DPI Rules provide Intrusion Detection and Prevention (IDS/IPS) protection by protecting vulnerabilities from known and as-yet unknown attacks.

Deep Security Feature Summary Widget

This widget shows the recent activity of each of the Deep Security modules.

Use the **Range** drop-down to select the time period for the data that displays.

The widget displays aggregated information from multiple managed servers.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Tip

To view non-aggregated data from multiple managed servers, add a new widget for each managed server.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

DATA	DESCRIPTION
Module	The Deep Security module
Protected Computers	The current number of managed computers being protected by this module and the percentage of all managed computers that this represents
Event Count	The number of events generated by the module during the specified time period
Trend	The percentage of change in the number of events since the previous time period
Total Number of Computers	The total number of computers being managed by Deep Security

Deep Security Firewall Activity (Detected) Widget

This widget displays the top five Firewall Rules that have triggered the greatest number of events and are operating in Detect mode .

Click on a value in the **Total** column to display the of Deep Security Manager **Events** screen filtered to show the firewall events triggered by the specific rule.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

DATA	DESCRIPTION
Reason	The name of the rule

Data	Description
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage of change from the previous to the current time period

Deep Security Firewall Activity (Prevented) Widget

This widget displays the top five Firewall Rules that have triggered the greatest number of events and are operating in Prevent mode.

Click on a value in the **Total** column to display the of Deep Security Manager **Events** screen filtered to show the firewall events triggered by the specific rule.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Data	Description
Reason	The name of the rule
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage of change from the previous to the current time period

Deep Security Firewall Event History Widget

This widget displays the number of Firewall Events detected by Deep Security Manager over the specified time range. The chart displays Events triggered by Firewall Rules in both Detect and Prevent mode.

Click a bar to view additional details in the Deep Security Manager console. You can also click the event types in the legend to change the chart view.

Use the **Range** drop-down to select the time period for the data that displays.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > ⚙). On the screen that appears, select the managed server to use as the source and click **Save**.

To make a Deep Security installation available to the Deep Security widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Deep Security server.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

Deep Security Integrity Monitoring Activity Widget

This widget displays the top five Integrity Monitoring Rules that have triggered the greatest number of events.

Click on a value in the **Total** column to display the of Deep Security Manager **Events** screen filtered to show the integrity monitoring events triggered by the specific rule.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Data	Description
Reason	The name of the rule
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage of change from the previous to the current time period

Deep Security Integrity Monitoring Event History Widget

This widget displays the severity level of events logged by Integrity Monitoring scans for the specified period.

Use the **Range** drop-down to select the time period for the data that displays.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

Deep Security Intrusion Prevention Event History Widget

This widget displays the number of intrusion prevention events detected by Deep Security over the specified time range. The chart displays Events triggered by IPS Rules in both Detect and Prevent mode.

Click a bar to display the Deep Security Manager **Events** page filtered to show the IPS Events for the specified mode and time range. You can also click a mode (**Detect** or **Prevent**) in the legend to change the chart view.

Use the **Range** drop-down to select the time period for the data that displays.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

Deep Security IPS Activity (Detected) Widget

This widget displays the top five IPS Rules that have triggered the greatest number of events and are operating in Detect mode .

Click on a value in the **Total** column to display the of Deep Security Manager **Events** screen filtered to show the IPS (Detected) events triggered by the specific rule.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Data	Description
Reason	The name of the rule
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage of change from the previous to the current time period

Deep Security IPS Activity (Prevented) Widget

This widget displays the top five IPS Rules that have triggered the greatest number of events and are operating in Prevent mode.

Click on a value in the **Total** column to display the of Deep Security Manager **Events** screen filtered to show the IPS (Prevented) events triggered by the specific rule.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Data	Description
Reason	The name of the rule
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage of change from the previous to the current time period

Deep Security Log Inspection Activity Widget

This widget displays the top five Log Inspection Rules that have triggered the greatest number of events.

Click on a value in the **Total** column to display the of Deep Security Manager **Events** screen filtered to show the log inspection events triggered by the specific rule.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Data	Description
Reason	The name of the rule

Data	Description
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage of change from the previous to the current time period

Deep Security Log Inspection Event History Widget

This widget displays the number of Events triggered by Log Inspection Rules that occurred over the specified time range.

Click a bar (Detect or Prevent) to display the Deep Security Manager **Events** page filtered to show the Log Inspection Events for the specified event type and time period. You can also click the event types in the legend to change the chart view.

Use the **Range** drop-down to select the time period for the data that displays.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > ⚙). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

Deep Security Reconnaissance Scan Event History Widget

This widget displays the number of Events triggered by Reconnaissance Scan detection settings that occurred over the specified time range.

Click a bar to display the Deep Security Manager **Events** page filtered to show the Reconnaissance Scan detections for the specified event type and time period. You can also click the event types in the legend to change the chart view.

Use the **Range** drop-down to select the time period for the data that displays.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Tip

This widget can only display data from a single Deep Security server. To monitor multiple Deep Security servers, create a new widget for each server.

Deep Security Status Summary Widget

This widget displays the number of critical and warning alerts, as well as the state of endpoints across the network.

The widget displays aggregated information from multiple managed servers.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Tip

To view non-aggregated data from multiple managed servers, add a new widget for each managed server.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

TABLE 24-1. Alerts

DATA	DESCRIPTION
Critical Alerts	The number of critical alerts **Note** Whether an alert is classified as critical or warning is user-configurable in the Deep Security Manager web console.
Warning Alerts	The number of warning alerts **Note** Whether an alert is classified as critical or warning is user-configurable in the Deep Security Manager web console.

TABLE 24-2. Computer Status

DATA	DESCRIPTION
Managed (green)	Protected and without errors or warnings.
Unmanaged (blue)	Not protected.
Lock (grey)	Locked. When a computer is in a locked state, Deep Security Manager will not communicate with the Agent/Appliance or generate any computer-related alerts.
Critical (red)	In an error state.

Data	Description
Warning (yellow)	In a warning state.

Deep Security Web Reputation Event History Widget

This widget displays the number of events triggered by Web Reputation Services that occurred over the specified time range.

Use the **Range** drop-down to select the time period for the data that displays.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Data	Description
Dangerous	The URL is verified to be fraudulent or known sources of threats
Highly Suspicious	The URL is suspected to be fraudulent or possible sources of threats
Suspicious	The URL is associated with spam or possibly compromised
Blocked	The URL was blocked by an administrator
Untested	The URL has not been tested by Trend Micro yet While Trend Micro actively tests web pages for safety, users may encounter untested pages when visiting new or less popular websites.

Deep Security Web Reputation URL Activity Widget

This widget displays the top five Web Reputation Services URLs that have the greatest number of events.

Change the managed server that the widget uses as its source by clicking the settings icon (⋮ > 🎚). On the screen that appears, select the managed server to use as the source and click **Save**.

Note

The data displayed in the widget is restricted to what is permitted by the user account privileges.

Data	Description
URL	The URL
Total	Number of events in the time period and the percentage of the total events of this type that it represents
Previous Total	Number of events in the time period preceding the current time period
Trend	The percentage change from the previous to the current period

Part X

Endpoint Application Control Widgets and Policies

Chapter 25

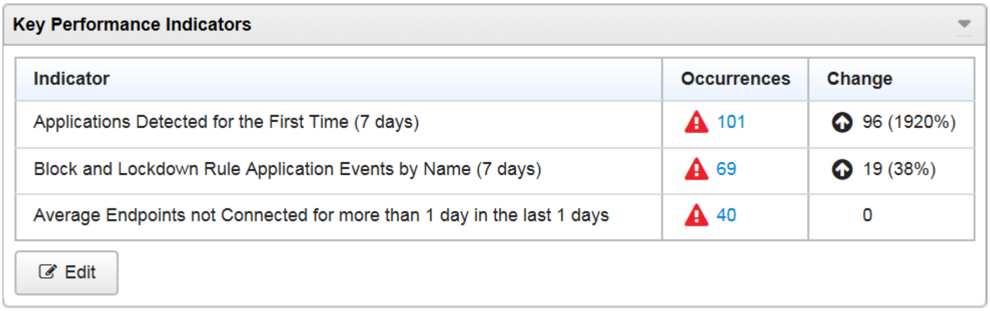
Endpoint Application Control Dashboard Widgets

This section contains help topics for all the Endpoint Application Control dashboard widgets supported in Apex Central.

Topics include:

Endpoint Application Control Key Performance Indicators Widget

This widget displays Endpoint Application Control key performance indicators based on selected criteria, and includes customizable templates for applications detected for the first time, applications not in the Certified Safe Software list, average agents stopped, average endpoints not connected, block and lockdown rule.



Key Performance Indicators

Indicator	Occurrences	Change
Applications Detected for the First Time (7 days)	⚠ 101	⬆ 96 (1920%)
Block and Lockdown Rule Application Events by Name (7 days)	⚠ 69	⬆ 19 (38%)
Average Endpoints not Connected for more than 1 day in the last 1 days	⚠ 40	0

FIGURE 25-1. KPI Widget Example

By default, the widget marks events as “Important” (❗) at 5 occurrences and “Critical” (⚠) at 10 occurrences. Optionally, mark events as Important or Critical by customizing event thresholds.

See table *Add or Edit Indicator Tasks*.

Go to **Dashboard** and then select **Widget Settings** from the menu on the top-right of the widget to do the following tasks:

Table 25-1. KPI Widget Configuration Tasks

Task	Steps
Edit indicator trend calculation used by the widget.	The widget displays trends in the **Change** column. The widget calculates indicator trends by comparing the current period with an average of previous periods. Under **Trend Calculations**, type a number of previous periods to average. The default setting is **1**.

Go to **Dashboard**, locate this widget, and then click **Edit** to do the following indicator-related tasks. After completing tasks, click **Done**.

Table 25-2. KPI Widget Indicator Tasks

Task	Steps
Add new indicator.	1. Click **Add Indicator**. The **Add Indicator** screen appears. 2. Select a template, optionally customize settings, and then click **Save**. See table *Add or Edit Indicator Tasks*.
Edit indicator.	1. Click the indicator in the list. The **Edit Indicator** screen appears. 2. Customize settings, and then click **Save**. See table *Add or Edit Indicator Tasks*.
Delete indicator.	Click ⛔ to the left of the indicator and then click **Delete**.

TABLE 25-3. Add or Edit Indicator Tasks

TASK	STEPS
Name indicator.	Under **Title**, type a name. **Tip** Leave this field blank to allow Apex Central to name the indicator based on your configuration.
Select template.	Under **Template**, select a template. See *About Templates*.
Edit period.	Under **Period**, select a period for indicator data.
Display threshold icons.	Select **Enable thresholds**.
Hide threshold icons.	Clear **Enable thresholds**.
Set "Important" (❗) threshold.	Under **Mark events as Important**, type the minimum number of event occurrences. The icon displays in the **Occurrences** column if the following are true: • The number of event occurrences that match this indicator is equal to or more than the threshold. • **Enable thresholds** is selected.
Set "Critical" (⚠) threshold.	Under **Mark events as Critical**, type the minimum number of event occurrences. The icon displays in the **Occurrences** column if the following are true: • The number of event occurrences that match this indicator is equal to or more than the threshold. • **Enable thresholds** is selected.

This widget includes customizable templates for the following indicators:

"Template"	"Log type"	"By" Occurrences Aggregated by Data Column	"Period" (Default)
Applications Detected for the First Time	Trusted Applications **Important** This data matches the log type "Known applications".		7 days
Applications not in the Certified Safe Software List	Policy Actions		7 days
Average Agents Stopped	Clients Samplings **Important** This data matches the data source "Users and Endpoints".		1 day
Average Endpoints not Connected	Clients Samplings **Important** This data matches the data source "Users and Endpoints".		More than 1 day in the last 1 day

"Template"	"Log type"	"By" Occurrences Aggregated by Data Column	"Period" (Default)
Block and Lockdown Rule Application Events	Policy Actions	• Endpoint Name • Name (default) • User Name	7 days
Block Rule Application Events	Policy Actions	• Endpoint Name • Name (default) • User Name	7 days
Lockdown Rule Application Events	Policy Actions	• Endpoint Name • Name (default) • User Name	7 days
Uncategorized Applications Detected	Policy Actions		7 days

Endpoint Application Control Rule Management

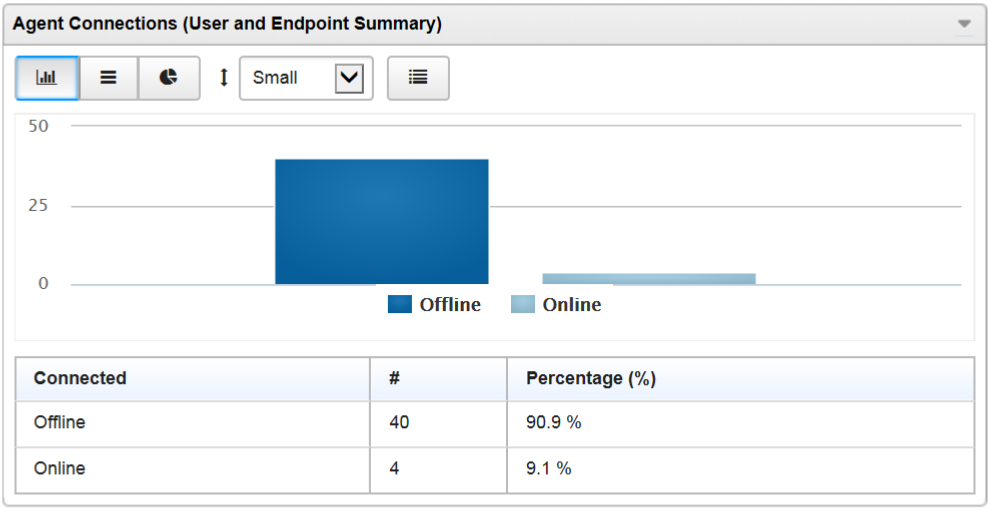
This widget provides a list of rules types and rule names in Endpoint Application Control rules.

To add new rules to Endpoint Application Control, click **Add Rule** to select specific types of rules to be added.

Rule	Description
Allow	Use the **Allow** rule to extend the Allow rights of trusted applications.
Block	Use the **Block** rule to block applications before or after execution.
Lockdown	Use the **Lockdown** rule to allow all currently-installed applications. Therefore, a complete and up-to-date endpoint inventory is required.

Endpoint Application Control User and Endpoint Summary Widget

This widget displays a distribution summary of Endpoint Application Control users and endpoints based on selected criteria, and includes customizable templates for agent connections, agent versions, endpoint Windows versions, policies, policy updates, and rules. Modify the templates by using custom settings.



Agent Connections (User and Endpoint Summary)

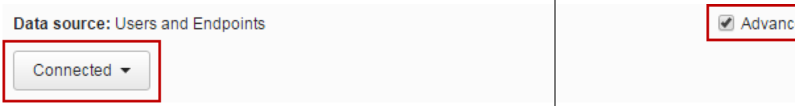
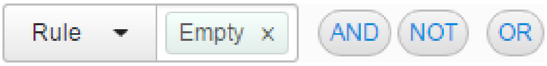
Small

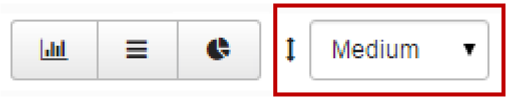
Connected	#	Percentage (%)
Offline	40	90.9 %
Online	4	9.1 %

Figure 25-2. User and Endpoint Summary Widget Example

Go to **Dashboard** and then select **Widget Settings** from the menu on the top-right of the widget to do the following tasks:

TABLE 25-4. User and Endpoint Summary Widget Configuration Tasks

TASK	STEPS
Name widget.	Under **Title**, type a name. **Tip** Leave this field blank to allow Apex Central to name the widget based on your configuration.
Select template.	Under **Template**, select a template.
Edit data source.	Select **Advanced**. Under **Data source**, select a data source for data displayed by the widget.  **Data source:** Users and Endpoints Connected ▾ ☑ Advanc **FIGURE 25-3. Data Source**
Limit displayed results.	Select **Advanced**. Under **Limit results to the following**, use dynamic search. 

Task	Steps
Change chart type.	Under **Display**, select one of the following types of chart: - Select ▲ for a line chart with data points. - Select ☰ for a horizontal histogram. - Select ◕ for a pie chart. (default) - Select ▦ for a data table. **Note** This control is not available if ☷ (display data table under chart) is selected.
Change chart size.	To the right of the chart types, select one of the following a chart sizes: - Select **Small** for a chart that is about 1 unit tall. - Select **Medium** for a chart that is about 2 units tall. (default) - Select **Large** for a chart that is about 4 units tall.  Medium ▼ **Figure 25-4. Chart Size**

Task	Steps
Change legend location.	Under **Legend**, select one of the following locations: - **None** - **Bottom** (default) - **Right** - **Top** - **Left** **Note** This control is not available if ◕ (display data as pie chart) is selected.
Display chart controls on widget.	Select the **Toolbar** check box. (default)
Hide chart controls on widget.	Clear the **Toolbar** check box.
Display data summary table below chart.	Select **Data summary table below chart**.
Hide data summary table below chart.	Clear **Data summary table below chart**. (default)
Save configuration as new template.	Under **Template**, select ✚ **Save current settings as template**.
Delete widget.	Select **Close Widget** from the menu on the top-right of the widget. The widget and any customizations you have made to the widget's settings are deleted.

This widget includes the following customizable templates:

Note

Only one template can be displayed at a time.

"Template"	"Data source"	Scope	"Advanced" Data Column (Default)
Agent Connections	Users and Endpoints	All (not user configurable)	Connected
Agent Versions	Users and Endpoints	Top 3	Agent Version
Endpoint Windows Versions	Users and Endpoints	Top 3	Windows Version
Policies	Users and Endpoints	Top 3	Policy
Policy Updates	Users and Endpoints	All (not user configurable)	Policy Updates
Rules	Users and Endpoints	Top 3	Rules

Endpoint Application Control Application, Rule, and Policy Events Widget

Use this widget to display a distribution summary of Endpoint Application Control application events based on selected criteria.

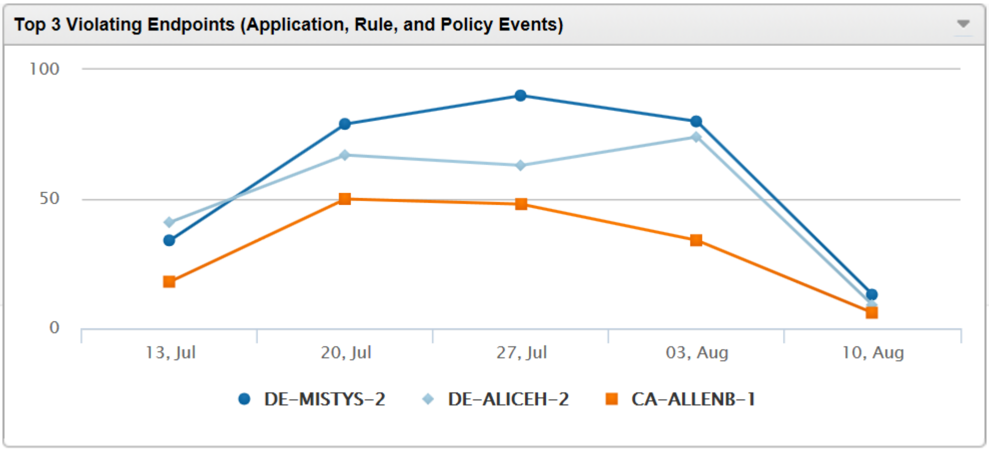
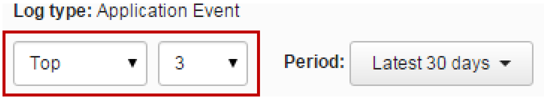
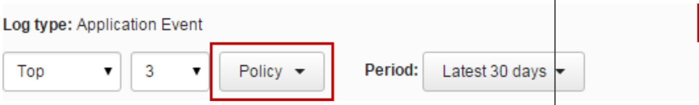
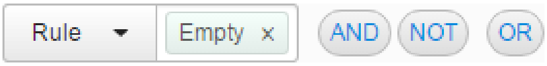


FIGURE 25-5. Application, Rule, and Policy Events Widget Example

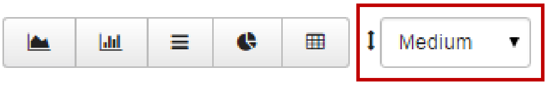
Go to **Dashboard** and then select **Widget Settings** from the menu on the top-right of the widget to do the following tasks:

TABLE 25-5. Application, Rule, and Policy Events Widget Configuration Tasks

TASK	STEPS
Name widget.	Under **Title**, type a name. **Tip** Leave this field blank to allow Apex Central to name the widget based on your configuration.

TASK	STEPS
Select template.	Under **Template**, select a template. See **About Templates**.
Edit data scope.	Under **Log type**, select a scope for data displayed by the widget. Log type: Application Event Top 3 Period: Latest 30 days **FIGURE 25-6. Data Scope**
Edit period.	Under **Period**, select a period for widget data.
Edit data source.	1. Select **Advanced**. The widget displays additional settings. 2. Under **Log type**, select a data source for data displayed by the widget. Log type: Application Event Top 3 Policy Period: Latest 30 days **FIGURE 25-7. Data Source**
Limit displayed results.	Select **Advanced**. Under **Limit results to the following**, use dynamic search. 

Task	Steps
Change chart type.	Under **Display**, select one of the following types of chart: - Select 📈 for a line chart with data points. (default) - Select 📊 for a vertical histogram. - Select ≡ for a horizontal histogram. - Select ◔ for a pie chart. - Select ▦ for a data table. **Note** This control is not available if ☰ (display data table under chart) is selected.

TASK	STEPS
Change chart size.	To the right of the chart types, select one of the following a chart sizes: • Select **Small** for a chart that is about 1 unit tall. • Select **Medium** for a chart that is about 2 units tall. (default) • Select **Large** for a chart that is about 4 units tall.  **FIGURE 25-8. Chart Size** **Note** This control is not available if ▦ (display data as table) is selected.
Change legend location.	Under **Legend**, select one of the following locations: • **None** • **Bottom** (default) • **Right** • **Top** • **Left** **Note** This control is not available if ◔ (display data as pie chart) or ▦ (display data as table) is selected.
Display chart controls on widget.	Select the **Toolbar** check box.

Task	Steps
Hide chart controls on widget.	Clear the **Toolbar** check box. (default)
Display data summary table below chart.	Select **Data summary table below chart**.
Hide data summary table below chart.	Clear **Data summary table below chart**. (default)
Save configuration as new template.	Under **Template**, select ✚ **Save current settings as template**.

This widget includes the following customizable templates:

Note

Only one template can be displayed at a time.

"Template"	"Log type"	Scope (Default)	"Period" (Default)	"Advanced" Data Column (Default)	"Advanced" Dynamic Search (Default)
Applications without Rules	Application Event **Important** This data matches the log type "Policy actions".	Top 3	Last 14 days	Name	Rule is Empty

"Template"	"Log type"	Scope (Default)	"Period" (Default)	"Advanced" Data Column (Default)	"Advanced" Dynamic Search (Default)
Applied Policies	Application Event **Important** This data matches the log type "Policy actions".	Top 3	Last 14 days	Policy	Policy is Not Empty
Blocked Applications	Application Event **Important** This data matches the log type "Policy actions".	Top 3	Last 14 days	Name	Action Taken is Blocked
Used Applications	Application Event **Important** This data matches the log type "Policy actions".	Top 3	Last 14 days	Name	Action Taken is Allowed

"Template"	"Log type"	Scope (Default)	"Period" (Default)	"Advanced" Data Column (Default)	"Advanced" Dynamic Search (Default)
Violated Policies	Application Event **Important** This data matches the log type "Policy actions".	Top 3	Last 14 days	Policy	Policy is Not Empty AND Action Taken is Blocked
Violated Rules	Application Event **Important** This data matches the log type "Policy actions".	Top 3	Last 14 days	Name	Rule is Not Empty AND Action Taken is Blocked
Violating Endpoints	Application Event **Important** This data matches the log type "Policy actions".	Top 3	Last 14 days	Endpoint Name	Action Taken is Blocked

"TEMPLATE"	"LOG TYPE"	SCOPE (DEFAULT)	"PERIOD" (DEFAULT)	"ADVANCED" DATA COLUMN (DEFAULT)	"ADVANCED" DYNAMIC SEARCH (DEFAULT)
Violating Users	Application Event **Important** This data matches the log type "Policy actions".	Top 3	Last 14 days	User Name	Action Taken is Blocked

Chapter 26

Endpoint Application Control Policy Settings

Use the following Endpoint Application Control policy settings to manage your Endpoint Application Control agents from Apex Central.

Policy Rules

Expand **Rules** to do the following tasks:

Task	Steps
View list of rules assigned to this policy.	Rules assigned to the policy appear in the table below the **Assign Rule** button. **Tip** Operating system applications considered safe by Certified Safe Software are allowed unless specifically blocked by a rule.
Assign rule to this policy.	Click **Assign Rule**, and then do one of the following: • To select existing rules to assign to the policy, select **Existing**. The **Assign Existing Rules to Policy** screen appears. Select the rule or rules to assign and then click **Assign Rules**.
Remove selected rules from this policy.	Select the rule or rules in the list, click **Remove Selected**, and then click **Remove Selected** again.

The following table outlines additional configuration options.

Policy Setting	Details
Always allow all applications in the Windows directory (overrides block and lockdown rules)	By default, Endpoint Application Control allows all applications located in the Windows directory. This functions like an **Allow** rule for the Windows default path, overriding any **Block** or **Lockdown** rules.
Automatically apply Lockdown rules to endpoints while they are disconnected	Disconnected endpoints are unable to receive or apply new policies. By default, that means a disconnected endpoint continues applying its current policy.
Enable protection against suspicious objects (requires subscription to Apex Central)	Endpoint Application Control protects matched endpoints against suspicious objects.

Policy Setting	Details
Use the more compatible, less feature-rich, user-level blocking method	Kernel-level blocking prevents applications from starting by blocking file access. This provides greater security, but may unexpectedly block or momentarily delay access to certain files needed by allowed applications. This feature is only supported on policies set to first match “User and Group” criteria (excluding the “SYSTEM” account). User-level blocking allows applications to start and then stops them at the task level. This may be unable to stop certain applications after they start and does not support the Trusted Source feature and blocking of link libraries (DLLs) and Java interpreter applications.

Policy Logging

Expand **Logging** to configure the following policy settings for matched users and endpoints:

POLICY SETTING	DETAILS
Log the following actions	Select one of the following logging limitations: - Select **None** to log no actions. - Select **Block** to log any blocked application start or access that does not originate from an excluded directory. This is the default setting for a new policy. - Select **Selected** to log any selected application start or access that does not originate from an excluded directory. Use the list that appears to select the rules to match. - Select **Any** to log any application start or access that does not originate from an excluded directory. **Note** Selecting this option may generate large log files and substantially increase network data transfers.
Exclude the following directories from logs	Select **Exclude the following directories from logs** and then type the application paths to exclude. Separate each path with a carriage return. The default paths are `%SYSTEMROOT%` and `%WINDIR%`.
Collect aggregated logs every	Select the interval for collecting the logs aggregated by endpoints. The default setting is **2 hours**. The suggested setting depends on the number of deployed agents.

Policy Deployment

Expand **Deployment** to configure the following policy settings for matched users and endpoints:

Policy Setting	Details
Send policy updates every	Select the policy update time interval. The default setting is **15 minutes**. The suggested interval depends on the number of deployed agents. By default, to reduce network data transfers and local storage needs, deployed policies only include matched applications already detected in an endpoint's inventory. At each policy deployment interval, Endpoint Application Control includes any newly added applications on the endpoint that match rules in the deployed policy.
Deploy the full policy in the following conditions **Note** Selecting these options may substantially increase network data transfers.	You can optionally deploy the “full policy”, which includes all matched applications and disregards endpoint inventory matching. • Select **Endpoint connects for fewer than** and specify a number of hours per week if matched endpoints do not regularly connect to the server. • Select **Endpoint starts applying lockdown rules** if matched endpoints should be allowed to install and run any applications specified in **Allow** rules after applying lockdown rules.

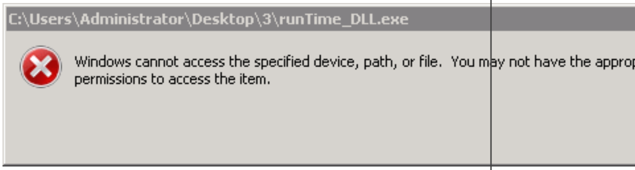
Policy Server Connection

Expand **Server connection** to configure the following policy settings for matched users and endpoints:

Policy Setting	Details
Connect to the following server	Your network may include more than one Endpoint Application Control server or a server may have moved to a new IP address. Specify the server that the endpoint should connect to after this policy is applied. • Select **Default** to use the same server as the one hosting the web console. This is the default setting for a new policy. • Select **Specified** and then type the server address and port to specify a server.
Use HTTPS	By default, Endpoint Application Control uses the HTTP or HTTPS configuration selected during server installation. Select **Use HTTPS** to permanently set all matched users or endpoints to use HTTPS. **Tip** Using this option requires you to import the server CA to agent endpoints. For detailed steps, go to https://success.trendmicro.com/solution/1115573

Policy User Experience

Expand **User experience** to configure the following policy settings for matched users and endpoints:

Policy Setting	Details
Display the system tray icon	The Endpoint Application Control system tray icon () can display notifications, allow the user to request access to applications, and allow the user to manually update Endpoint Application Control settings and logs. • Select **Yes** to display the icon in matched users' Windows system trays. • Select **No** to hide the icon.
Display notification popups	Displaying notifications to some users may be inappropriate. For example, users of special-purpose endpoints such as ATMs, medical devices, kiosks, and gas pumps may be confused by notifications and related requests for interaction. • Select **Yes** to display Endpoint Application Control notifications to matched users. • Select **No** to prevent the display of notifications and disable related user-interactions. **Important** After Endpoint Application Control blocks or delays an application start using the kernel-level method, Windows may display the following notification to end-users:  C:\Users\Administrator\Desktop\3\runTime_DLL.exe Windows cannot access the specified device, path, or file. You may not have the approp permissions to access the item. **FIGURE 26-1. Windows Block Notification** Endpoint Application Control is unable to hide this notification. You can avoid this notification by applying user-level blocking instead.

Policy Setting	Details
Generate a new inventory	Endpoints generate inventories to track new and deleted applications. Endpoint Application Control periodically collects application inventories from endpoints. Select a time interval, such as daily or a weekly.
Start time	Select a start time for the inventory scan.

Part XI

Endpoint Encryption Widgets and Policies

Chapter 27

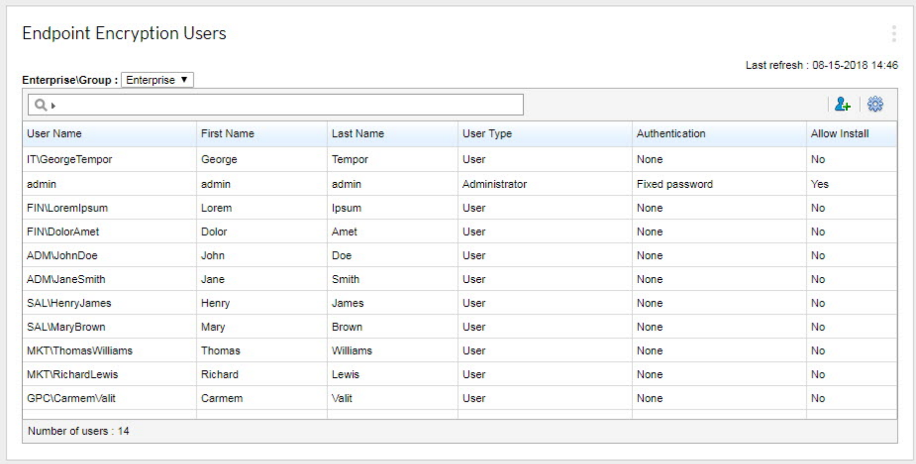
Endpoint Encryption Dashboard Widgets

This section contains help topics for Endpoint Encryption widgets supported on the Apex Central dashboard.

Topics include:

Endpoint Encryption Users

The **Endpoint Encryption Users** widget provides user management capability directly from the Apex Central dashboard. Use the **Endpoint Encryption Users** widget to add or remove Apex Central user accounts, reset passwords, change permissions, configure policy group priority, import from Active Directory, and search for specific user accounts.



Endpoint Encryption Users

Last refresh : 08-15-2018 14:46

Enterprise\Group : Enterprise ▼

User Name	First Name	Last Name	User Type	Authentication	Allow Install
IT\GeorgeTempor	George	Tempor	User	None	No
admin	admin	admin	Administrator	Fixed password	Yes
FIN\LoremIpsum	Lorem	Ipsum	User	None	No
FIN\DolorAmet	Dolor	Amet	User	None	No
ADM\JohnDoe	John	Doe	User	None	No
ADM\JaneSmith	Jane	Smith	User	None	No
SAL\HenryJames	Henry	James	User	None	No
SAL\MaryBrown	Mary	Brown	User	None	No
MKT\ThomasWilliams	Thomas	Williams	User	None	No
MKT\RichardLewis	Richard	Lewis	User	None	No
GPC\CarmemValit	Carmem	Valit	User	None	No

Number of users : 14

Item	Description
Show	Select which users to display: all users in the Enterprise, or users in a specific policy.
Search (🔍 ▾)	Click the 🔍 ▾ icon to filter which Apex Central users appear in the table. Use the search field to specify parameters to search against.
Settings (⚙) Right-click a user	Click the ⚙ icon to view user attributes or to perform actions on any selected user.
Add users (👤+)	Click the 👤+ icon to add individual users, import users from a CSV file, or import users from Active Directory LDAP.

Item	Description
Number of users	View the total number of users in the entire Enterprise, selected policy, or specified search.

User Settings Options

The following table explains the options available under the settings icon.

Table 27-1. User Settings Options

Option	Description
Change password	Specify a new password for users using the Fixed password authentication type. The widget does not support changing passwords for the Domain authentication type.
Delete user	Removes the selected user.
Modify user	Update the properties of the selected user. The following properties can be modified: • User name • First name • Last name • Employee ID • Email address • Freeze • User type • One policy • Authentication method

Option	Description
List policies	Displays the policies where the selected user is a member. If the **Allow Install** column for the selected user is **Yes**, then the option to allow or disallow the installation of selected policies, as well as selecting which policies should be given first priority is enabled.

Add New User Options

The following table explains the options available when adding a new Apex Central user.

Table 27-2. Add New User Options

Option	Description
User name	Specify the account user name that the user uses to authenticate.
First name	Specify the user's first name.
Last name	Specify the user's last name.
Employee ID	Specify the user's employee ID (optional).
Email address	Specify user's email address (optional).
Freeze	Select **Yes** to temporarily lock the account. A locked account cannot log on to Apex Central devices.
User type	Select **User**, **Authenticator**, or **Administrator**.
One group	Select **Yes** to only allow the user to belong to one policy at a time. The user may not be added to any other policy groups. If you set this option to **Yes** and set the **User type** to **Authenticator** or **Administrator**, the user will be a group authenticator or group administrator respectively.
Authentication method	Select the authentication method available to the user.

Policy Membership

The following table explains how to understand Apex Central user policy membership.

Note

Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Security Agent software only affects the Full Disk Encryption and File Encryption agents.

Header	Example	Description
Priority	1, 2. 3	Shows the order that Apex Central applies policies. When a policy is triggered that affects a user, Apex Central performs the action, and then no other policies affect the user for that event.
Policy Name	GP1	Shows the name of all policies that the user is currently assigned.
Description	Temporary employees policy.	Shows the description of the policy.
Allow Install	Yes, No	Shows whether the user can install new devices.

Importing Users from a CSV File

Note

Importing users from a CSV file is supported only for users using fixed password authentication.

Format each line in the CSV file as follows:

```
<User ID (required)>, <first name>, <last name>, <employee ID>,
<email address>
```

For fields with no data, use a comma as a placeholder. The following is an example CSV entry:

```
example_id, name,,, name@example.com
```

Procedure

1. From the **Endpoint Encryption Users** widget, click **Add User** and then select **Import Users from a File**.

   The **Import Users from a File** screen appears.

2. Click **Choose File** to select the CSV file.

   The **Open CSV File** window appears.

3. Select the file and then click **Open**.

4. Click **Add**.

   The users in the CSV file are imported.

Importing Active Directory Users

PolicyServer maintains a user directory separate from the Active Directory database. This allows PolicyServer absolute security over access to all Apex Central devices, user rights, and authentication methods.

Use the **Endpoint Encryption Users** widget in Apex Central to import Active Directory users.

Procedure

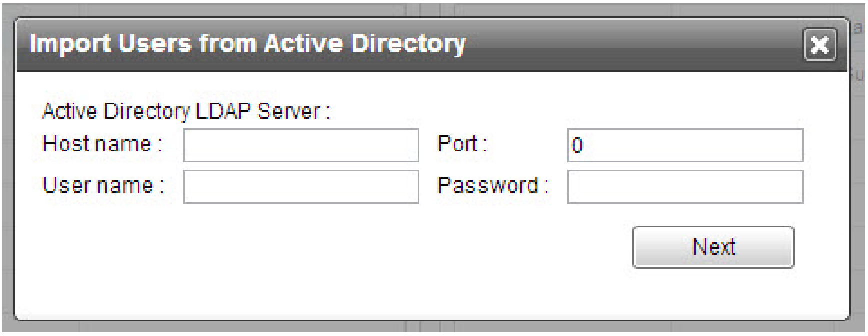
1. Log on to Apex Central.

2. Go to the **Endpoint Encryption Users** widget.

3. Click the 👤 icon.

4. Select **Import Users from Active Directory**.

   The **Import Users from Active Directory** screen appears.



Import Users from Active Directory

Active Directory LDAP Server :

Host name :

Port : 0

User name :

Password :

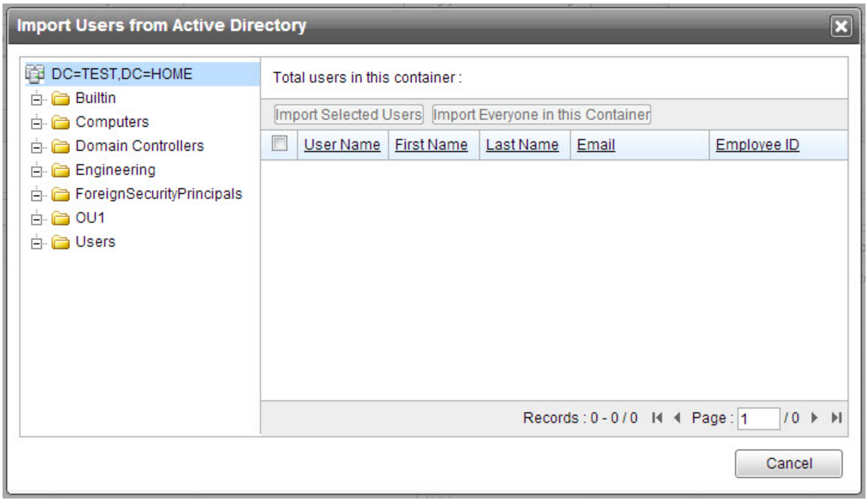
5. Specify your credentials for the Active Directory LDAP server.

> **Note**
>
> For **Port**, the value “0” specifies the default port. The default port is 389.

6. Click **Next**.

7. Wait for the specified Active Directory domain to populate.

The Active Directory tree for the specified domain appears in the left pane.



8. From the left pane, use the navigation tree to select the container from which to add users.

   The available users populate in the right pane.

9. Do one of the following:

   - Select individual users, then click **Import Selected Users**.
   - Click **Import Everyone in this Container**.

10. Click **OK** to add the users to the specified location.

    A confirmation window appears.

11. Click **OK** to confirm.

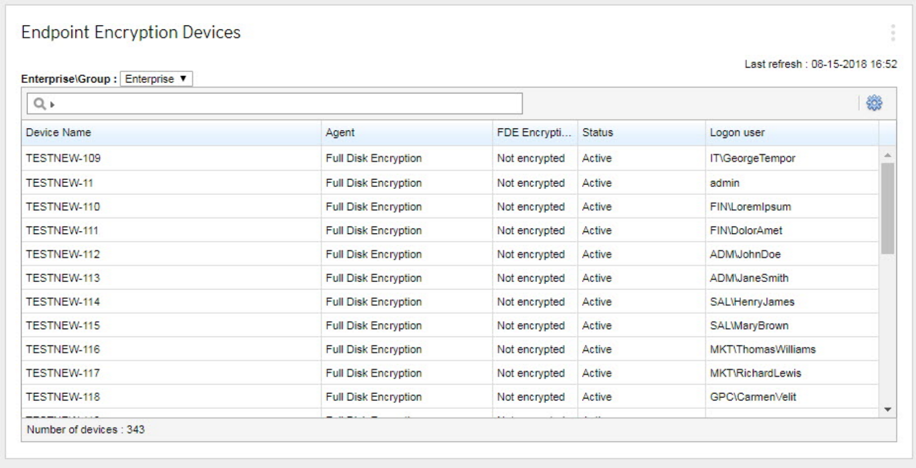
    An import status message displays.

12. Click **Close** to finish, or repeat the procedure to select more users to import.

Endpoint Encryption Devices

Endpoint Encryption devices are Endpoint Encryption agents that have registered with PolicyServer. Installing any Endpoint Encryption agent automatically registers the endpoint with PolicyServer as a new Endpoint Encryption device. Since multiple Endpoint Encryption agents may protect a given endpoint, a single endpoint may appear as more than one Endpoint Encryption device on PolicyServer.

The **Endpoint Encryption Devices** widget provides Endpoint Encryption device management capability directly from the Apex Central dashboard. Use the **Endpoint Encryption Devices** widget to monitor activity, search for Endpoint Encryption devices, or secure endpoint data by initiating lock or kill commands when an endpoint is lost or stolen.



Endpoint Encryption Devices

Last refresh : 08-15-2018 16:52

Enterprise\Group : Enterprise ▼

Device Name	Agent	FDE Encrypti...	Status	Logon user
TESTNEW-109	Full Disk Encryption	Not encrypted	Active	IT\GeorgeTempor
TESTNEW-11	Full Disk Encryption	Not encrypted	Active	admin
TESTNEW-110	Full Disk Encryption	Not encrypted	Active	FIN\LoremIpsum
TESTNEW-111	Full Disk Encryption	Not encrypted	Active	FIN\DolorAmet
TESTNEW-112	Full Disk Encryption	Not encrypted	Active	ADM\JohnDoe
TESTNEW-113	Full Disk Encryption	Not encrypted	Active	ADM\JaneSmith
TESTNEW-114	Full Disk Encryption	Not encrypted	Active	SAL\HenryJames
TESTNEW-115	Full Disk Encryption	Not encrypted	Active	SAL\MaryBrown
TESTNEW-116	Full Disk Encryption	Not encrypted	Active	MKT\ThomasWilliams
TESTNEW-117	Full Disk Encryption	Not encrypted	Active	MKT\RichardLewis
TESTNEW-118	Full Disk Encryption	Not encrypted	Active	GPC\CarmenVelit

Number of devices : 343

Options	Description
Show	Select which devices to display: all devices in the Enterprise, or devices in a specific policy.

Options	Description
Search (🔍▼)	Click the 🔍▼ icon to select the Security Agent and filter the devices shown in the table. Use the search field to specify parameters to search against. Any attributes listed in devices attributes can be searched.
Settings (⚙) Right-click a device	Select a device and click the ⚙ icon or right-click a device to view device attributes or to perform actions on the selected device.
Number of devices	View the total number of devices in the entire Enterprise, selected policy, or specified search.

Device Actions

Select a device and click the ⚙ icon or right-click a device to perform the following actions:

Action	Description
Delete device	Deleting any Apex Central device from the Enterprise also removes the device from all policy groups. The deleted Apex Central device continues functioning as long as connectivity and password policies are current on the device. The agent will be unable to synchronize its policy with PolicyServer. ⚠ **WARNING!** Before deleting a Full Disk Encryption device, decrypt your disk, and uninstall the Full Disk Encryption agent. If you delete a Full Disk Encryption device without deleting the agent, the Full Disk Encryption preboot may be unable to authenticate with PolicyServer and the data may become inaccessible.
Soft token	Generating a "software token" creates a unique string that you can use to unlock Apex Central devices and to remotely help Apex Central users reset forgotten passwords. The software token is only available in the full version of Full Disk Encryption, not Encryption Management for Apple FileVault or Encryption Management for Microsoft BitLocker.

Action	Description
Recovery key	Generating a “recovery key” allows the user to decrypt a hard disk when the user has forgotten the original password or key. The recovery key is only available to Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker agents because they do not use the other recovery methods available in Full Disk Encryption.
Device attributes	View a current snapshot of the selected device.
Kill device	Initiating a “kill” command deletes all Apex Central device data. The deleted data is different depending on the scope of data that the associated Security Agent manages. For example, initiating a “kill” command to a Full Disk Encryption device deletes all data from the endpoint, while initiating a “kill” command to a File Encryption device deletes all files and folders in local or removable storage protected by the File Encryption agent. The “kill” command is issued when the Security Agent communicates with PolicyServer. ⚠ **WARNING!** Killing a device cannot be undone. Back up all the data before initiating a kill command.
Lock device	Initiating a “lock” command to the Apex Central device prevents Apex Central user access until after performing a successful Remote Help authentication. Locking a device reboots the endpoint and forces it into a state that requires Remote Help. The lock command is issued when the Security Agent communicates with PolicyServer.
Soft reset	Initiating a “soft reset” command reboots the endpoint. The command issues the next time that the agent communicates with PolicyServer.

Device Attributes

The following table describes the Apex Central device attributes.

Attribute Name	Example	Description
AD NetBIOS Name	Enterprise	The name assigned to the AD NetBIOS.

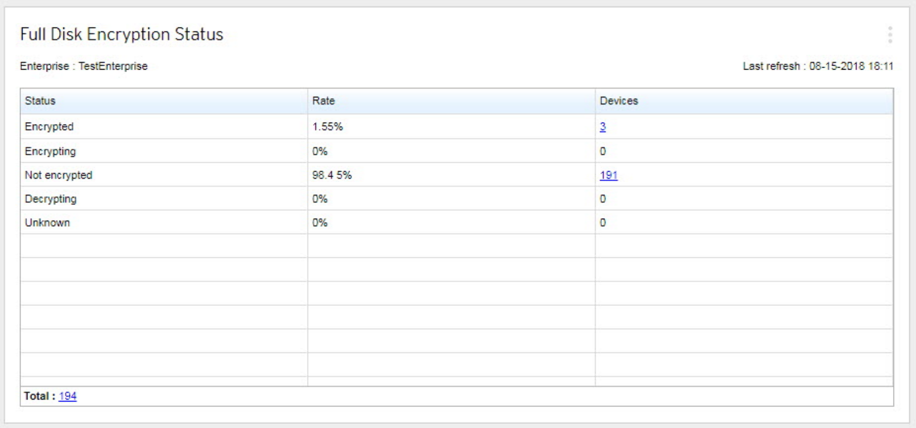
Attribute Name	Example	Description
AD Object GUID	6629bdeb-99a8-456b -b7c5-dbbc50ad13d0	The GUID assigned to the AD object.
Battery Count	2	The number of batteries installed.
.NET Version	2.0.50727.3620	The version and build number for the installed .NET framework.
Common Framework Build Number	5.0.0.84	The Security Agent uses a common framework for encryption. The build number is used to tell whether the agent is up-to-date.
Disk Model	VMware Virtual IDE	The hard disk model.
Disk Name	`\\.\PHYSICALDRIVE0`	The name of the hard disk.
Disk Serial Number		The serial number of the hard disk.
Disk Partitions	1	The number of partitions on the disk with the agent installed.
Disk Size	10733990400	The total capacity of the hard disk (in bytes).
Domain Name	WORKGROUP	The domain that the endpoint is a member.
Endpoint ID	85b1e3e2a3c25d882540ef6e4818c3e4	The unique ID of the endpoint used for Apex Central integration.
File Encryption Version	6.0.0.1039	The version of File Encryption installed on the endpoint.
Hostname	TREND-4136D2DB3	The endpoint's host name.
IP Address	`10.1.152.219`	The endpoint's IP address.
Language	English (United States)	The language used by the endpoint.
Locale	en-US	The regional settings used by the endpoint.
MAC Address	00-50-56-01-xx-xx	The endpoint's MAC address.

Attribute Name	Example	Description
Machine Name	TREND-4136D2DB3	The computer name that the endpoint used.
Manufacturer	VMware, Inc.	The manufacturer of the hard disk.
Model	VMware Virtual Platform	The model of the hard disk.
Operating System	Microsoft Windows NT 5.1.2600 Service Pack 3	The operating system installed on the same hard disk as the agent.
Operating System Name	Microsoft Windows XP Professional	The common name of the operating system installed on the same hard disk as the agent.
Operating System Service Pack	Service Pack 3	The service pack number of the operating system installed on the same hard disk as the agent.
Operating System Version	5.1.2600.196608	The version number of the operating system installed on the same hard disk as the agent.
Partition Scheme	Classical MBR	The partition scheme for the hard disk.
Processor	x86 Family 6 Model 30 Stepping 5, Genuine Intel	The processor make and model of the endpoint.
Processor Count	2	The number of processors in the endpoint.
Processor Revision	1e05	The processor revision number.
Time Zone	Taipei Standard Time	The time zone that the endpoint resides.
Total Physical Memory	2047MB	The total RAM installed in or allocated to the endpoint.
Type	X86-based PC	The endpoint processor type.
Windows User Name	TREND-4136D2DB3\admin	The user name of the Windows account that last logged on the endpoint.
<Agent> User	john_smith	The user name for the last logged on used.

Attribute Name	Example	Description
<Agent> Version	5.0.0.260	The version and build number for the agent installation.

Full Disk Encryption Status

The **Full Disk Encryption Status** widget shows the current encryption status of any device on your network.



Full Disk Encryption Status

Enterprise : TestEnterprise

Last refresh : 08-15-2018 18:11

Status	Rate	Devices
Encrypted	1.55%	3
Encrypting	0%	0
Not encrypted	98.4 5%	191
Decrypting	0%	0
Unknown	0%	0

Total : 194

COLUMN	DESCRIPTION
Status	The status of the endpoint. Statuses include: • **Encrypted**: The endpoint is 100% encrypted. • **Encrypting**: The endpoint is currently encrypting the hard disk. The status changes to “Fully Encrypted” once encryption completes and the endpoint restarts. • **Not encrypted**: The endpoint is 0% encrypted. • **Decrypting**: The endpoint is currently decrypting the hard disk. The status changes to Not Encrypted once the decryption completes and the endpoint restarts. • **Unknown**: The endpoint is synchronized, but PolicyServer cannot determine the encryption status.
Rate	The percentage that the endpoint is encrypted.
Devices	The number of endpoints with that current status. Click the number to view the Endpoint Encryption Devices report.

Note

At the bottom of the widget, click the number next to **Total** to view the Full Disk Encryption Status report.

Full Disk Encryption Status Report

The following table describes the **Full Disk Encryption Status** report. Use it to understand how to read the report details.

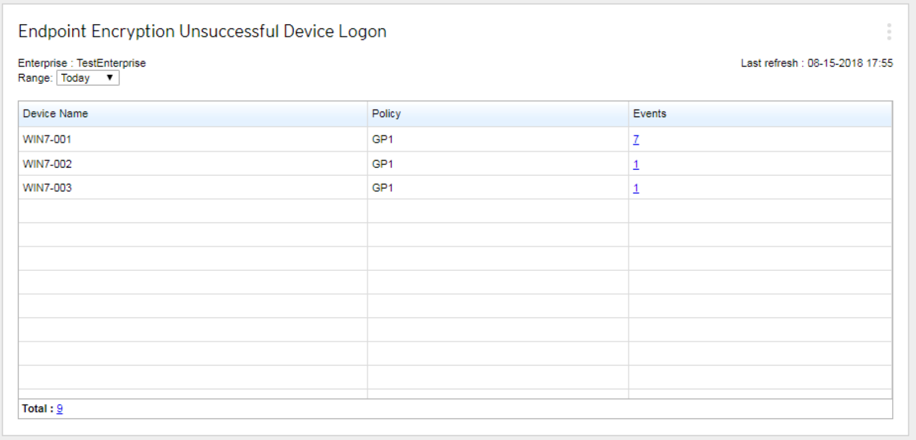
TABLE 27-3. Full Disk Encryption Status Report Example

HEADER	EXAMPLE	DESCRIPTION
Policy	GP1	The title of the policy controlling the endpoint.
Device Name	TREND-4136D2DB3	The computer name used by the endpoint.

Header	Example	Description
Device ID	1fabfbff-0001-06e5-000c-297085710000	The unique ID established after the Security Agent was installed on the endpoint and a new endpoint was registered with PolicyServer.
Agent	Full Disk Encryption	The currently installed Security Agent.
Status	Not Encrypted	The current state of the endpoint.
Last Synchronized Date	10/07/2013 11:05 am	The timestamp when the endpoint last updated policies from PolicyServer.
Last Policy Enforcement	10/07/2013 11:05 am	The timestamp when the Apex Central last enforced policy changes on PolicyServer.

Endpoint Encryption Unsuccessful Device Logon

The **Endpoint Encryption Unsuccessful Device Logon** widget shows all devices (managed endpoints) that had unsuccessful logon attempts by any user. Unsuccessful device logon events may represent a security breach or the user may have forgotten their logon credentials.



Endpoint Encryption Unsuccessful Device Logon

Enterprise : TestEnterprise
Range: Today ▼

Last refresh : 08-15-2018 17:55

Device Name	Policy	Events
WIN7-001	GP1	7
WIN7-002	GP1	1
WIN7-003	GP1	1

Total : 9

Column	Description
Device Name	The computer name of the endpoint.
Policy	The policy managing the endpoint.
Events	The number of unsuccessful logon attempts. Click the number to view the **Endpoint Encryption Unsuccessful Device Logon** report.

Unsuccessful Device Logon Report

The following table explains the **Endpoint Encryption Unsuccessful Device Logon** report. Use it to understand how to read the report details.

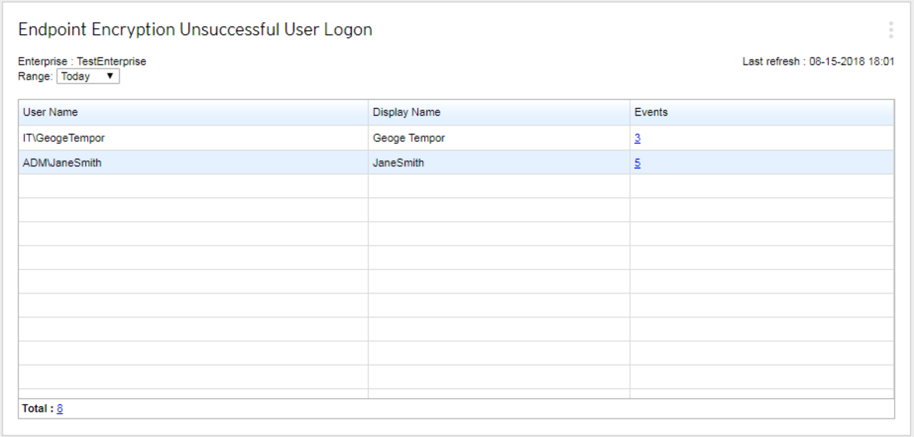
Table 27-4. Endpoint Encryption Unsuccessful Device Logon Example

Header	Example	Description
Event Timestamp	07/02/2012 01:56 pm	When the event occurred.

Header	Example	Description
Policy	GP1	The title of the policy controlling the endpoint.
Device Name	TREND-4136D2DB3	The computer name used by the endpoint.
Device ID	1fabfbff-0001-06e5-000c-297085710000	The unique ID established after the Security Agent was installed on the endpoint and a new endpoint was registered with PolicyServer.
IP Address	`10.1.152.219`	The endpoint IP address.
Agent	Full Disk Encryption	The currently installed Security Agent.
User Name	user325	The user name used to attempt to log on to the endpoint.
Display Name	Mary Jones	The first and last name of the Apex Central user account. If the specified user name is not a valid Apex Central user name, the column shows “Not Recorded”.
Event	Unsuccessful Fixed Password Login	The logged event including the authentication method.

Endpoint Encryption Unsuccessful User Logon

The **Endpoint Encryption Unsuccessful User Logon** widget shows all unsuccessful logon attempts by any user to any managed endpoint on the Apex Central network.



Endpoint Encryption Unsuccessful User Logon

Enterprise : TestEnterprise

Range: Today ▼

Last refresh : 08-15-2018 18:01

User Name	Display Name	Events
IT\GeogeTempor	Geoge Tempor	3
ADM\JaneSmith	JaneSmith	5

Total : 8

Column	Description
User Name	The user name used to attempt to log on to the endpoint.
Display Name	The display name of the user account that attempted to log on to the endpoint.
Events	The number of authentication attempts. Click the number to view the **Endpoint Encryption Unsuccessful User Logon** report.

Unsuccessful User Logon Report

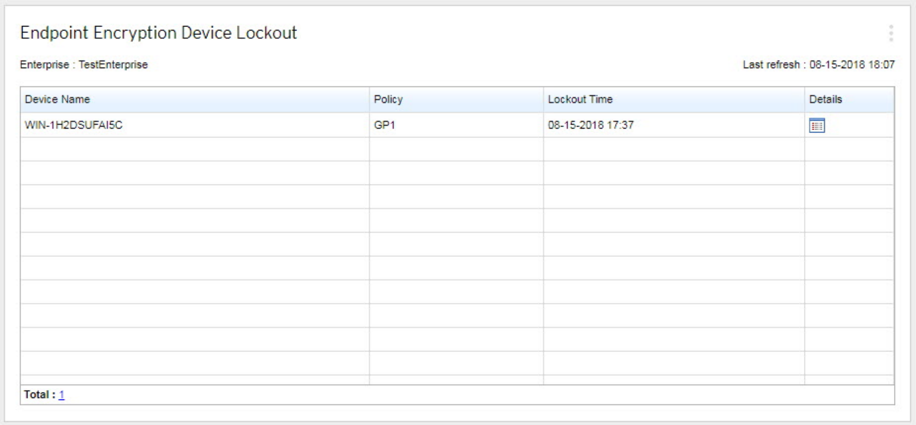
The following table explains the **Endpoint Encryption Unsuccessful User Logon** report. Use it to understand how to read the report details.

Table 27-5. Endpoint Encryption Unsuccessful User Logon Report Example

Header	Example	Description
Event Timestamp	07/02/2012 01:56 pm	When the event occurred.
Policy	GP1	The title of the policy controlling the endpoint.
Device Name	TREND-4136D2DB3	The computer name used by the endpoint.
Device ID	1fabfbff-0001-06e5-000c-297085710000	The unique ID established after the Security Agent was installed on the endpoint and a new endpoint was registered with PolicyServer.
IP Address	`10.1.152.219`	The endpoint IP address.
Agent	Full Disk Encryption	The currently installed Security Agent.
User Name	user325	The user name used to attempt to log on to the endpoint.
Display Name	Mary Jones	The first and last name of the Apex Central user account. If the specified user name is not a valid Apex Central user name, the column shows “Not Recorded”.
Event	Unsuccessful Fixed Password Login	The logged event including the authentication method.

Endpoint Encryption Device Lockout

The **Endpoint Encryption Device Lockout** widget shows Apex Central devices that are locked out due to policy restrictions.



Endpoint Encryption Device Lockout

Enterprise : TestEnterprise

Last refresh : 08-15-2018 18:07

Device Name	Policy	Lockout Time	Details
WIN-1H2DSUFAI5C	GP1	08-15-2018 17:37	▤

Total : 1

Header	Description
Device Name	The computer name used by the endpoint.
Policy	The title of the policy controlling the endpoint.
Lockout Time	The timestamp when PolicyServer issued the device lock command. The endpoint does not actually lock out until after the Endpoint Encryption agent synchronizes policies with PolicyServer.
Details	Click the details icon to view the **Endpoint Encryption Device Lockout** report.

At the bottom of the widget, click the number next to **Total** to view the report.

Device Lockout Report

The following table explains the **Endpoint Encryption Device Lockout** report. Use it to understand how to read the report details.

TABLE 27-6. Endpoint Encryption Device Lockout Report Example

HEADER	EXAMPLE	DESCRIPTION
Event Timestamp	07/02/2012 01:56 pm	When the event occurred.
Policy	GP1	The title of the policy controlling the Endpoint Encryption device.
Device Name	TREND-4136D2DB3	The computer name used by the Endpoint Encryption device.
Device ID	1fabfbff-0001-06e5-000c-297085710000	The unique ID established after the Endpoint Encryption agent was installed on the endpoint and a new Endpoint Encryption device was registered with PolicyServer.
IP Address	`10.1.152.219`	The Endpoint Encryption device IP address.
Agent	Full Disk Encryption	The currently installed Endpoint Encryption agent.
User Name	user325	The user name used to attempt to log on to the Endpoint Encryption device.
Display Name	Mary Jones	The first and last name of the Endpoint Encryption user account. If the specified user name is not a valid Endpoint Encryption user name, the column shows “Not Recorded”.

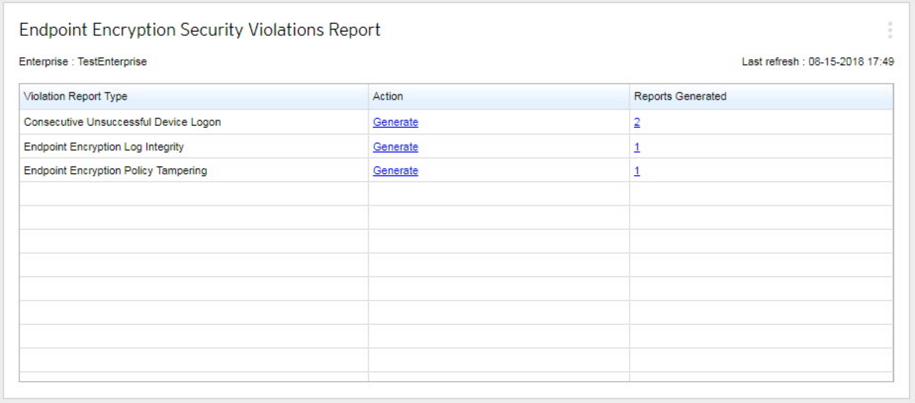
Header	Example	Description
Event	Locked device due to invalid login attempt violation.	The logged event including the authentication method.

Endpoint Encryption Security Violations Report

The **Endpoint Encryption Security Violations Report** widget shows the security violations assessed by the following reports:

- **Endpoint Encryption Consecutive Unsuccessful Device Logon**
- **Endpoint Encryption Policy Tampering**
- **Endpoint Encryption Log Integrity**

Generating a report gathers all security violations currently logged by PolicyServer. Once generated, click the number on the **Reports** column to view generated reports for that violation.



Endpoint Encryption Security Violations Report

Enterprise : TestEnterprise

Last refresh : 08-15-2018 17:49

Violation Report Type	Action	Reports Generated
Consecutive Unsuccessful Device Logon	Generate	2
Endpoint Encryption Log Integrity	Generate	1
Endpoint Encryption Policy Tampering	Generate	1

HEADER	DESCRIPTION
Violation report type	The available report types for various violations.
Action	Click **Generate** to create a new report.
Reports	The total number of generated reports for that violation. Click the number to view available reports.

Note

To specify the number of unsuccessful logons attempts before it is considered a security violation, click ▾ to open the **Widget Settings** window, type a value in the **Consecutive unsuccessful logons** textbox, and then click **Save**.

Consecutive Unsuccessful Device Logon Report

The following table explains the **Endpoint Encryption Consecutive Unsuccessful Device Logon** report. Use it to understand when the logon attempt occurred, the affected Endpoint Encryption device, and how many times the user attempted to log on to the Endpoint Encryption device.

TABLE 27-7. Endpoint Encryption Consecutive Unsuccessful Device Logon Report Example

ENTRY	EXAMPLE	DESCRIPTION
Event Timestamp	07/02/2012 01:56 pm	When the event occurred.
Device Name	TREND-4136D2DB3	The computer name used by the Endpoint Encryption device.
Attempts	5	The number of times that a user attempted to log on to the Endpoint Encryption device.

Policy Tampering Report

The following table explains the **Endpoint Encryption Policy Tampering** report. Use it to understand how to read the report details.

TABLE 27-8. Endpoint Encryption Policy Tampering Report Example

HEADER	EXAMPLE	DESCRIPTION
Event Timestamp	07/02/2012 01:56 pm	When the event occurred.
Event	Policy Value Integrity Check Failed	The logged event including the authentication method.

Log Integrity Report

The following table explains the **Endpoint Encryption Log Integrity** report. Use it to understand how to read the report details.

TABLE 27-9. Endpoint Encryption Log Integrity Report Example

HEADER	EXAMPLE	DESCRIPTION
Event Timestamp	07/02/2012 01:56 pm	When the event occurred.
Event	Audit Log Record Missing	The logged event including the authentication method.

Chapter 28

Endpoint Encryption Policy Settings

This section discusses how to configure Endpoint Encryption policies on the Apex Central console.

Topics include:

- *Authentication Overview on page 28-2*
- *Configuring Endpoint Encryption Users Rules on page 28-5*
- *Configuring Full Disk Encryption Rules on page 28-8*
- *Configuring File Encryption Rules on page 28-11*
- *Configuring Common Policy Rules on page 28-14*
- *Migrating Groups to Apex Central on page 28-18*

Authentication Overview

The primary form of protection that Endpoint Encryption delivers is prevention of unauthorized user access to encrypted endpoints and devices. Correctly configuring Endpoint Encryption devices, users, and policy groups prevents data loss risk from accidental information release or deliberate sabotage.

Devices on page 28-2	Endpoint Encryption counts the amount of consecutive logon attempts on a given device and the amount of time since the last communication with PolicyServer for a given length of time. If a device violates the policy criteria, Endpoint Encryption can reset, lock, or erase the disk.
Users on page 28-3	In addition to checking authentication attempts on a device, Endpoint Encryption also counts the amount of consecutive logon attempts by a particular user account. If that user violates the policy criteria, Endpoint Encryption can reset, lock, or erase the disk.
Groups on page 28-4	Groups act as a container for users for policy management. Administrators and authenticators within a group have those special privileges only within that group, but unassigned administrators and authenticators have that role throughout the Enterprise.

Devices

Endpoint Encryption devices are Endpoint Encryption agents that have registered with PolicyServer. Installing any Endpoint Encryption agent automatically registers the endpoint with PolicyServer as a new Endpoint Encryption device. Since multiple Endpoint Encryption agents may protect a given endpoint, a single endpoint may appear as more than one Endpoint Encryption device on PolicyServer.

Depending on the policy settings, Endpoint Encryption takes one of the following actions when users attempt to consecutively log on that device unsuccessfully:

- Delay the next authentication attempt

- Lock the device
- Erase all data on the device

Note

To configure Endpoint Encryption devices, use the **Endpoint Encryption Devices** widget. See *Endpoint Encryption Devices on page 27-9*.

Users

Endpoint Encryption users are any user account manually added to PolicyServer or synchronized with Active Directory.

Endpoint Encryption has several types of account roles and authentication methods for comprehensive identity-based authentication and management. Using Endpoint Encryption or PolicyServer MMC, you can add or import user accounts, control authentication, synchronize with the Active Directory, and manage policy group membership, as needed.

The following table describes the Endpoint Encryption user roles:

Role	Description
Administrator	Administrators may access the management consoles and perform any configurations within their domain. This role has different rights depending on the level that the administrator role is added: • Enterprise administrator: These administrators have control over all policies, groups, users, and devices in the enterprise. • Group administrator: These administrators have control over users and devices that authenticate within a specific group. Endpoint Encryption makes a group for each policy, so these administrators may also be known as “policy administrators”.

Role	Description
Authenticator	Authenticators provide remote assistance when users forget their Endpoint Encryption passwords or have technical problems. This role has different rights depending on the level that the authenticator role is added: • Enterprise authenticator: These authenticators can assist any users in the enterprise. • Group authenticator: These authenticators can assist any users within a specific group. Endpoint Encryption makes a group for each policy, so these authenticators may also be known as “policy authenticators”.
User	Basic end users have no special privileges. The user role may not log on the Endpoint Encryption management consoles. Unless allowed by PolicyServer, the user role also may not use recovery tools.

Note

To configure Endpoint Encryption users, use the **Endpoint Encryption Users** widget. See *Endpoint Encryption Users on page 27-2*.

Groups

Apex Central manages policies by user groups. Groups management differs between PolicyServer MMC and Apex Central. After modifying policies and groups, PolicyServer synchronizes groups across both consoles.

Important

Apex Central always takes precedence over PolicyServer MMC for policy and group assignment. Any modifications to the group assignment in PolicyServer MMC are automatically overwritten the next time that Apex Central synchronizes with PolicyServer.

Console	Group Management
Apex Central	Apex Central automatically creates a group each time a policy with specific targets is deployed. After deployment, modify the groups a user is in from the **Endpoint Encryption Users** widget, and modify the users in the policy from the **Policy Management** screen.
PolicyServer MMC	Add and modify groups directly from the left pane of PolicyServer MMC. Groups in PolicyServer MMC can be assigned as follows: • **Top Group**: Top Groups are the highest level of groups under the Enterprise. Each Top Group has a unique node underneath the Enterprise. • **Subgroup**: Subgroups are created within Top Groups. Subgroups inherit the policies of the Top Group on creation, but do not inherit changes made to the Top Group. Subgroups may not be more permissive than the Top Group. **Note** You must manually assign devices and users to each subgroup. Adding Apex Central users to a subgroup does not automatically add the users to the Top Group. However, you can add users to both the Top Group and subgroup.

Note

To configure the users within a policy group on Apex Central, use the **Endpoint Encryption Users** widget.

To configure users within a policy group on PolicyServer MMC, see the *Endpoint Encryption PolicyServer MMC Guide*.

Configuring Endpoint Encryption Users Rules

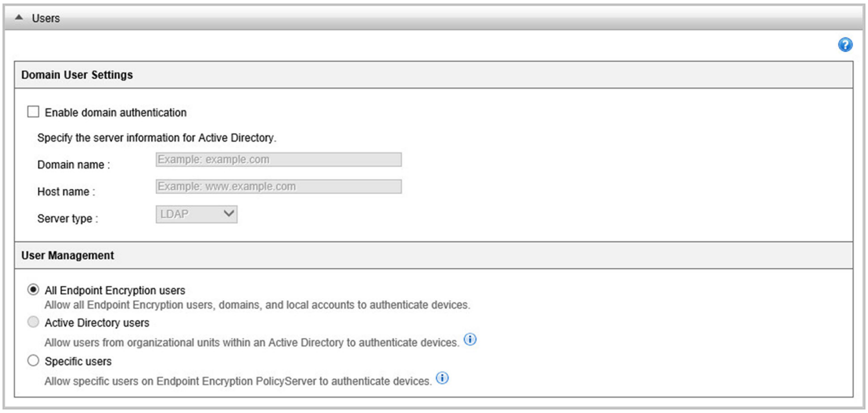
The following procedure explains the configurable options for policy rules that affect authentication and Endpoint Encryption user accounts.

Procedure

1. Create a new Endpoint Encryption policy.

2. Click **Users**.

   The **Users** policy rules settings appear.



Users

Domain User Settings

□ Enable domain authentication

Specify the server information for Active Directory.

Domain name :	Example: example.com
Host name :	Example: www.example.com
Server type :	LDAP

User Management

● All Endpoint Encryption users
Allow all Endpoint Encryption users, domains, and local accounts to authenticate devices.

○ Active Directory users
Allow users from organizational units within an Active Directory to authenticate devices.

○ Specific users
Allow specific users on Endpoint Encryption PolicyServer to authenticate devices.

FIGURE 28-1. Endpoint Encryption Users Policy Rules

3. If users require domain authentication, select **Enable domain authentication** under **Domain User Settings**.

   If you selected **Enable domain authentication**, specify the server information for your Active Directory (AD) account.

   a. Configure the AD domain name.

   b. Configure the host name of the AD server.

   c. Select the server type:

      - **LDAP**

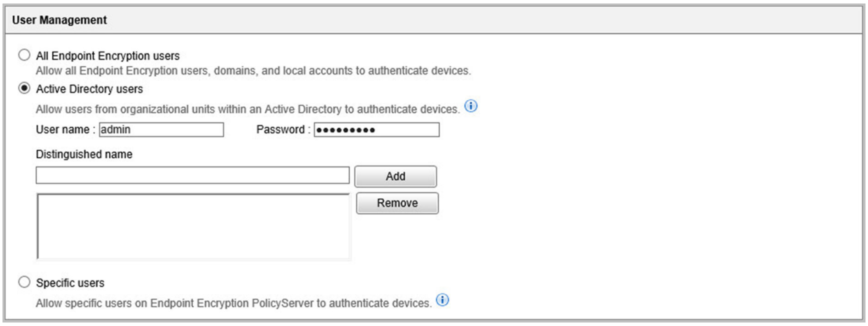
      - **LDAP proxy**

4. Under **User Management**, configure user access.

Option	Description
All Endpoint Encryption users	Allow all users, domain and local accounts, to authenticate devices.
Active Directory users	Allow users from organizational units (OUs) within an AD to authenticate devices. **Note** Select **Enable domain authentication** to enable the **Active Directory users** option.
Select specific users	Specify which already added users can authenticate to managed endpoints. **Note** In order to select specific users with this option, you must populate the user list. Add OUs with the **Active Directory users** option or add users with the Endpoint Encryption Users widget.

5. If you selected **Active Directory users**, add OUs to the policy by their distinguished name.

   After selecting **Active Directory users**, the following additional options appear:



User Management

○ All Endpoint Encryption users

Allow all Endpoint Encryption users, domains, and local accounts to authenticate devices.

● Active Directory users

Allow users from organizational units within an Active Directory to authenticate devices. ⓘ

User name : admin Password : ●●●●●●●●●

Distinguished name

○ Specific users

Allow specific users on Endpoint Encryption PolicyServer to authenticate devices. ⓘ

Option	Description
User name	Specify your Active Directory user name.
Password	Specify your Active Directory password.
Distinguished name	Specify each OU by its sequence of relative distinguished names (RDN) separated by commas. Example: OU=TW, DC=mycompany, DC=com After specifying the OU distinguished name, click **OK**. **Important** Apex Central supports up to 12 OUs per policy.

Configuring Full Disk Encryption Rules

The following procedure explains the configurable options for policy rules affecting Full Disk Encryption devices.

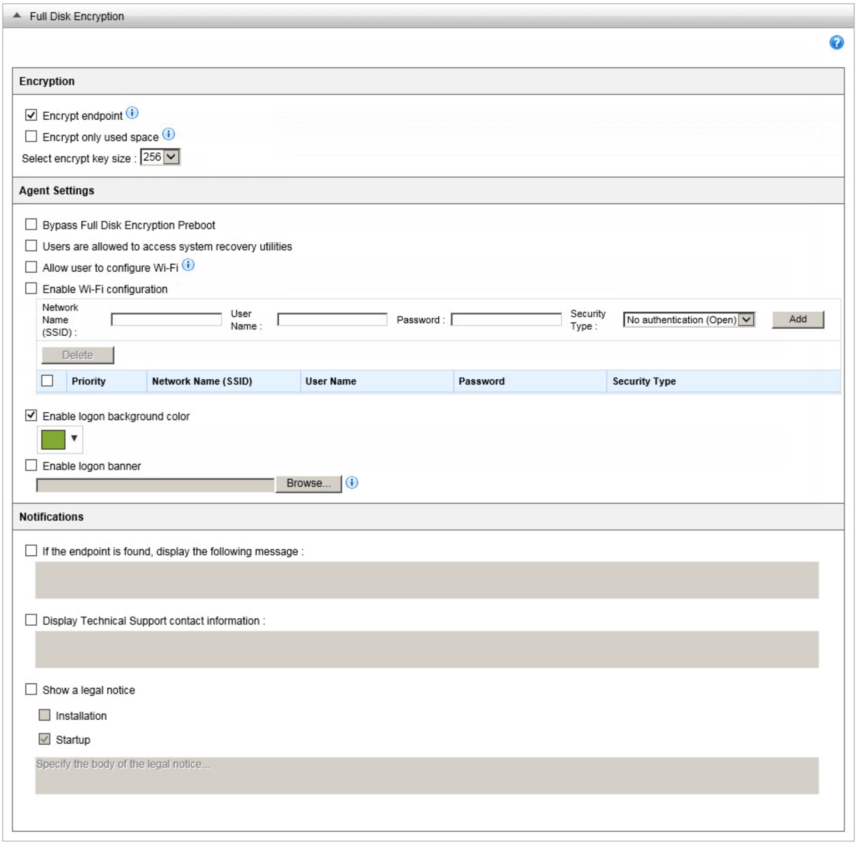
Note

Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

Procedure

1. Create a new Endpoint Encryption policy.
2. Click **Full Disk Encryption**.

The **Full Disk Encryption** policy rules settings appear.



Encryption

☑ Encrypt endpoint ⓘ

□ Encrypt only used space ⓘ

Select encrypt key size : 256

Agent Settings

□ Bypass Full Disk Encryption Preboot

□ Users are allowed to access system recovery utilities

□ Allow user to configure Wi-Fi ⓘ

□ Enable Wi-Fi configuration

Network Name (SSID) : User Name : Password : Security Type : No authentication (Open)

□	Priority	Network Name (SSID)	User Name	Password	Security Type

☑ Enable logon background color

🟩 ▼

□ Enable logon banner

Notifications

□ If the endpoint is found, display the following message :

□ Display Technical Support contact information :

□ Show a legal notice

□ Installation

☑ Startup

Specify the body of the legal notice...

FIGURE 28-2. Full Disk Encryption Policy Rules

3. Under **Encryption**, select the following options:

    - Select **Encrypt device** to start full disk encryption when the Endpoint Encryption agent synchronizes policies with PolicyServer.

WARNING!

Do not deploy encryption to Full Disk Encryption agents without first preparing the endpoint's hard drive.

For information about preparing the hard drive, see *Full Disk Encryption Deployment Outline* in the *Endpoint Encryption Installation Guide*.

- Select **Encrypt only used space** to encrypt only the used space.
- Select **Select encrypt key size** to specify a device encryption key size in bits.

4. Under **Agent Settings**, select the following options:
    - Select **Bypass Full Disk Encryption Preboot** to allow the user to authenticate directly into Windows without protection from preboot authentication.
    - Select **Users are allowed to access system recovery utilities on the device** to allow the user to access the Recovery Console.
    - Select **Allow user to configure Wi-Fi** to allow users to configure Wi-Fi policies on the device during preboot.
    - Select **Enable Wi-Fi configuration** to use a predetermined Wi-Fi configuration during preboot. Specify the following details:
        - Network name (SSID)
        - User name
        - Password
        - Security type
    - Select **Enable logon background color** to specify the background color during logon.
    - Select **Enable logon banner** to specify a logon banner image.

Image should not exceed 128 KB in size and should measure 512 x 64 pixels. Accepted file formats are PNG with transparency (recommended), JPG and GIF

5. Under **Notifications**, configure the following options:

   - Select **If found, display the following message on the device** to show a message when the **If Found** policy is active.
   - Select **Display Technical Support contact information** to show a message after the user logs on to the Full Disk Encryption agent.
   - Select **Show a legal notice** to show the specific legal message at start up or only after installing the Full Disk Encryption agent.

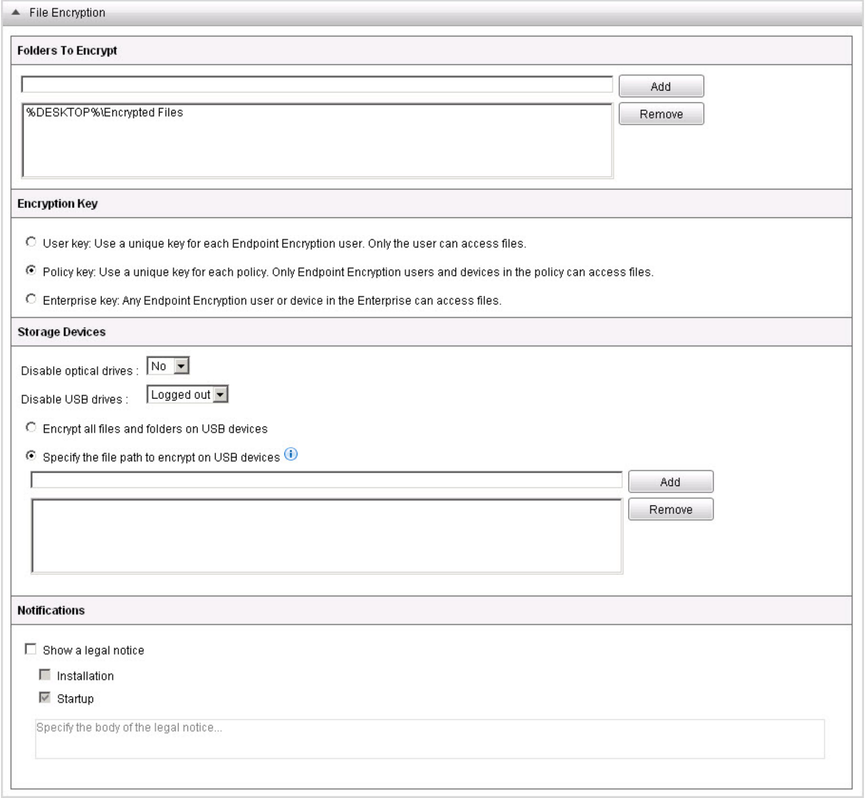
Configuring File Encryption Rules

The following procedure explains the configurable options for policy rules affecting File Encryption devices.

Procedure

1. Create a new Endpoint Encryption policy.
2. Click File Encryption.

The **File Encryption** policy rules settings appear.



Folders To Encrypt

%DESKTOP%\Encrypted Files

Encryption Key

○ User key: Use a unique key for each Endpoint Encryption user. Only the user can access files.

● Policy key: Use a unique key for each policy. Only Endpoint Encryption users and devices in the policy can access files.

○ Enterprise key: Any Endpoint Encryption user or device in the Enterprise can access files.

Storage Devices

Disable optical drives : No

Disable USB drives : Logged out

○ Encrypt all files and folders on USB devices

● Specify the file path to encrypt on USB devices

Notifications

□ Show a legal notice

□ Installation

☑ Startup

Specify the body of the legal notice...

FIGURE 28-3. File Encryption Policy Rules

3. Under **Folder to Encrypt**, specify folders that are automatically created and encrypted on the endpoint when the File Encryption agent synchronized policies.

4. Under **Encryption Key**, select the encryption for the File Encryption encrypted folder.

   - **User key**: Use a unique key for each Endpoint Encryption user. Only the Endpoint Encryption user can decrypt files that he or she encrypted.

- **Policy key**: Use a unique key for each policy. Only Endpoint Encryption users and devices in the policy can decrypt files.
- **Enterprise key**: Any Endpoint Encryption user or device in the Enterprise can decrypt the files.

Note

Selecting **Policy key** or **Enterprise key** controls the sharing for the File Encryption shared key.

5. Under **Storage Devices**, configure the following options:
   - Select **Disable optical drives** to control whether removable media is accessible from the endpoint.
   - Select **Disable USB drives** to control when the USB ports are disabled. Options are:
     - **Always**
     - **Logged out**
     - **Never**
   - Select **Encrypt all files and folders on USB devices** to automatically encrypt all the files and folders on removable drives when plugged into the endpoint.
   - Select **Specify the file path to encrypt on USB devices** to add or remove encrypted folders to USB drives. If a folder does not exist, it is created. If no drive letter is specified, all USB devices are affected.
6. Under **Notifications**, select **Show a legal notice** to show the specific legal message at start up or only after installing the File Encryption agent.

Note

Notifications are only supported by Trend Micro File Encryption agents versions 3.1.3 and earlier.

Configuring Common Policy Rules

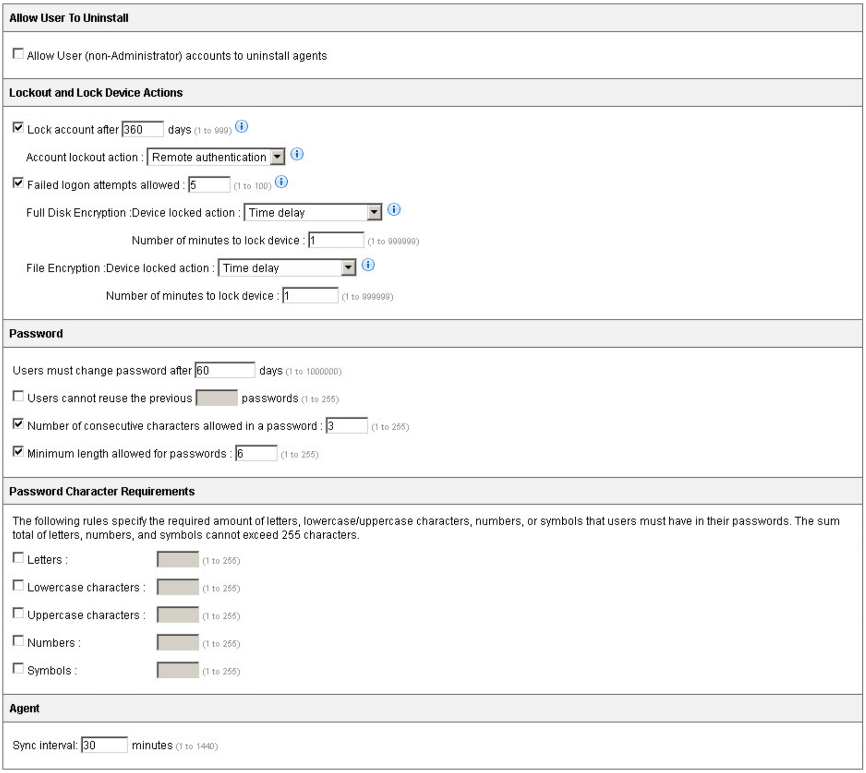
This section explains the configurable options for policy rules affecting all Endpoint Encryption devices.

Procedure

1. Create a new Endpoint Encryption policy.

2. Click **Common**.

   The **Common** policy rules settings appear.



Allow User To Uninstall

☐ Allow User (non-Administrator) accounts to uninstall agents

Lockout and Lock Device Actions

☑ Lock account after 360 days (1 to 999)

Account lockout action : Remote authentication

☑ Failed logon attempts allowed : 5 (1 to 100)

Full Disk Encryption :Device locked action : Time delay

Number of minutes to lock device : 1 (1 to 999999)

File Encryption :Device locked action : Time delay

Number of minutes to lock device : 1 (1 to 999999)

Password

Users must change password after 60 days (1 to 1000000)

☐ Users cannot reuse the previous passwords (1 to 255)

☑ Number of consecutive characters allowed in a password : 3 (1 to 255)

☑ Minimum length allowed for passwords : 6 (1 to 255)

Password Character Requirements

The following rules specify the required amount of letters, lowercase/uppercase characters, numbers, or symbols that users must have in their passwords. The sum total of letters, numbers, and symbols cannot exceed 255 characters.

☐ Letters : (1 to 255)

☐ Lowercase characters : (1 to 255)

☐ Uppercase characters : (1 to 255)

☐ Numbers : (1 to 255)

☐ Symbols : (1 to 255)

Agent

Sync interval: 30 minutes (1 to 1440)

FIGURE 28-4. Common Policy Rules

3. Under **Allow User to Uninstall**, select **Allow User (non-administrator) accounts to uninstall agent software** to allow any Endpoint Encryption user to uninstall the agent.

   Note

   By default, only Administrator accounts can uninstall Endpoint Encryption agents.

4. Under **Lockout and Lock Device Actions**, configure the following options:

   - Select **Lock account after <number> days** to specify the number of days that the Endpoint Encryption device locks if it does not synchronize policies.

     - Use **Account lockout action** to specify whether the remote authentication or erase action occurs at lockout.

       Note

       For information about lock options, see *Lockout Actions on page 28-17*

   - Select **Failed log on attempts allowed** to specify how many times that a user can attempt to authenticate before the Endpoint Encryption device locks.

   - For Full Disk Encryption or File Encryption devices, separately configure the following:

     - Use **Device locked action** to specify whether the “Remote Authentication” or the “Erase” action occurs at lockout.

       Note

       For information about lock options, see *Lockout Actions on page 28-17*

    - Use **Number of minutes to lock device** to specify the duration that time delay locks the Endpoint Encryption device from authentication

5. Under **Password**, configure the following options:

    - Select **Users must change password after <number> days** to control when a user is prompted to update password.

    - Select **Users cannot reuse the previous <number> passwords** to specify how many previous passwords the user may reuse.

    - Select **Number of consecutive characters allowed in a password** to specify how many repeated characters a user may specify in the password.

    - Select **Minimum length allowed for passwords** to specify how many characters the user is required to use in the password.

6. Under **Password Requirements**, specify the password character limitations.

    - **Letters**

    - **Lowercase characters**

    - **Uppercase characters**

    - **Numbers**

    - **Symbols**

    Important

    The sum total of letters, numbers, and symbols cannot exceed 255 characters.

7. Under **Agent**, specify the **Sync internal** in minutes.

Lockout Actions

Some policies have settings to lock out a user account or to lock a device based on certain criteria. Account lockout and device lockout actions affect the Endpoint Encryption device whether or not the agent synchronizes policies with PolicyServer. For example, if the Endpoint Encryption agent does not communicate with PolicyServer for a certain period of time, the Endpoint Encryption agent automatically locks the Endpoint Encryption device. Use the tables below to understand the actions available for the account lockout and device lock actions.

The following table describes when the lockout actions occur:

Type	Description
Account lockout	Account lockout actions take effect when the Endpoint Encryption agent does not communicate with PolicyServer for a certain period of time as set by the policy.
Full Disk Encryption device lockout	Full Disk Encryption device lockout actions take effect when the Endpoint Encryption user exceeds the number of unsuccessful logon attempts to that Full Disk Encryption device as set by the policy.
File Encryption device lockout	File Encryption device lockout actions take effect when the Endpoint Encryption user exceeds the number of unsuccessful logon attempts to that File Encryption device as set by the policy.

The options for lockout actions are as follows:

Action	Description
Erase	PolicyServer erases all data controlled by the associated Endpoint Encryption agent. **WARNING!** The Endpoint Encryption user cannot recover the erased data.
Remote authentication	PolicyServer locks the Endpoint Encryption device until the Endpoint Encryption user contacts receives Remote Help authentication from an authenticator or from Support.

Action	Description
Time delay	PolicyServer temporarily locks the Endpoint Encryption device and notifies the Endpoint Encryption user that the device is locked. The ability to authenticate or reset the password is disabled during the time delay. The duration of the time delay is determined by policy. Once the time delay has expired, the user is permitted to authenticate.

Migrating Groups to Apex Central

Use the following procedure to add existing groups from PolicyServer MMC to Apex Central.

Procedure

1. Log on to PolicyServer MMC.
2. Gather the following information:
   - Total number of groups, their names, and the subgroups
   - All users assigned to each group
   - The policy configuration of each group
3. Log on to Apex Central.
4. For each group in PolicyServer MMC, configure a new policy that matches the corresponding group policy configuration.

   Note

   Subgroups are not supported in Apex Central. To replicate the subgroup policy settings, create a separate policy for each subgroup.
5. Add users to each corresponding new policy.
6. Deploy each policy.

Part XII

Endpoint Sensor Widgets and Policies

Chapter 29

Trend Micro Endpoint Sensor Dashboard Widgets

This section contains help topics for the Trend Micro Endpoint Sensor dashboard widgets supported in Apex Central.

Topics include:

Endpoint Sensor Investigation

The **Endpoint Sensor Investigation** widget connects with a remote Trend Micro Endpoint Sensor server to start an investigation and display the results from this investigation directly from the Apex Central dashboard.

Click **Start a New Investigation** to initiate a new investigation, and then select an investigation method:

- **Historical Records** to Investigate historical events based on user-defined criteria
- **System Snapshot** to investigate the current state of the selected endpoints

Once the **New Investigation** page appears, fill in the required criteria. The following investigation types are available:

INVESTIGATION TYPE	DESCRIPTION
Historical Records - Retro Scan	Investigate historical events based on user-defined criteria
Historical Records - IOC rule	Investigate historical events using an IOC rule
System Snapshot - Registry search	Investigate the Windows registry
System Snapshot - YARA rule	Investigate for memory-resident threats using a YARA rule
System Snapshot - IOC rule	Investigate for events using an IOC rule
System Snapshot - Disks IOC rule	Investigate for files using an IOC rule
System Snapshot - System audit	Investigate all currently running processes, services, and modules

Click **Investigate** to start the investigation. To stop an ongoing investigation, click **Cancel**.

The widget refreshes periodically to display the progress of the investigation. The widget displays a doughnut chart which gives a visual representation of the total endpoints classified as:

- **Matched**: indicates the number of endpoints where a matched object was found.
- **Safe**: indicates the number of endpoints where a matched object was not found.
- **Pending**: indicates the number of endpoints not yet investigated.
- **Canceled**: indicates the number of endpoints that meet any of the following criteria:
    - The investigation performed on the endpoint encountered an error
    - The endpoint is offline, or all commands sent to the endpoint result in a timeout
    - The investigation for the endpoint was manually interrupted by the user

A breakdown of the totals is given on the right of the doughnut chart. Click the count for each classification to view the **Investigation Results** screen. This screen gives more details regarding the latest investigation results started from Apex Central.

Note

- Once a server is added, refresh the widget to start retrieving data from the new server.
- If multiple servers are added, the widget displays the aggregate result of all the servers' data.

Intelligent Monitoring Summary by Host

This widget displays a summary of the most recent endpoints where a monitoring rule was triggered. The data is pulled from the **Intelligent**

Monitoring Summary by Host widget in the Trend Micro Endpoint Sensor server dashboard.

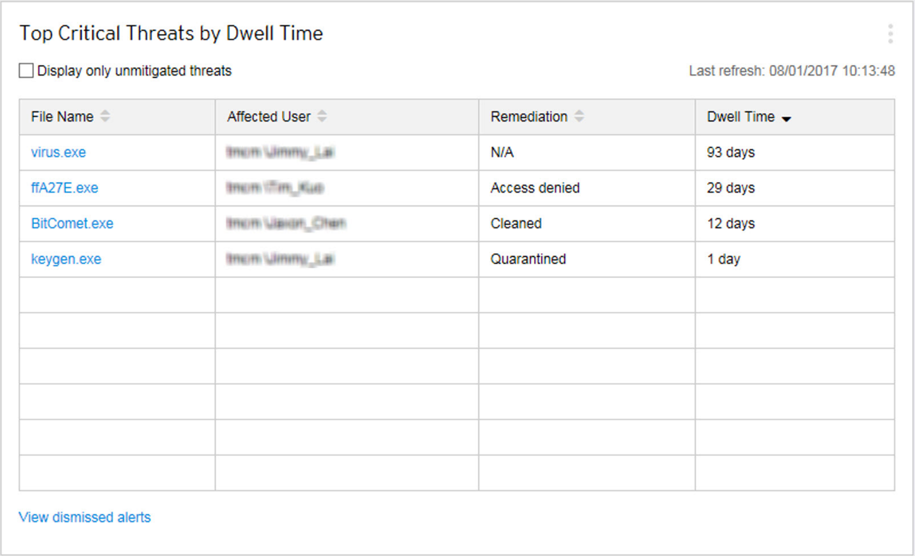
Column Name	Description
Host Name	Host name of the endpoint
Hit Counts	Number of matching rules triggered on the endpoint Click to view details about the rules triggered on the endpoint.
Rule Category	Classification based on the six stages of a targeted attack
Detection time	Date and time when the rule was last triggered in the endpoint

The default time period is **Last 24 hours**. Change the time period according to your preference.

Note

- The widget requires an existing connection to a Trend Micro Endpoint Sensor server. After adding a server, refresh the widget to start retrieving data from the new server.
- If multiple servers are added, the widget displays the aggregate result of all the servers' data.

Top Critical Threats by Dwell Time Widget



Top Critical Threats by Dwell Time

□ Display only unmitigated threats

Last refresh: 08/01/2017 10:13:48

File Name	Affected User	Remediation	Dwell Time
virus.exe	[redacted]	N/A	93 days
ffA27E.exe	[redacted]	Access denied	29 days
BitComet.exe	[redacted]	Cleaned	12 days
keygen.exe	[redacted]	Quarantined	1 day

View dismissed alerts

This widget provides an overview of the top critical threats based on the length of time the threat has been present on the endpoint of the affected user.

Important

This widget requires a registered Trend Micro Endpoint Sensor server. The widgets displays the results of the impact assessment performed by the Trend Micro Endpoint Sensor server, based on the SHA-1 values of files considered as critical threats.

You can select **Display only unmitigated threats** to view only the critical threats that require remediation.

Click the column headings to sort the data in the table.

Column	Description
File Name	Displays the file name of the critical threat detected Click the **File Name** to view additional threat information or perform further investigation.
Affected User	Displays the name of the affected user
Remediation	Displays the remediation action taken by a Trend Micro product
Dwell Time	Displays the length of time that the threat has persisted on the endpoint of the affected user

Click **View dismissed alerts** to open the **Dismissed Alerts** screen and view information for only critical threat alerts that have been manually dismissed by an Apex Central user account.

Column	Description
Dismissed	Displays the time when the critical threat alert was dismissed
File Name	Displays the file name of the critical threat detected Click the **File Name** to view additional threat information or perform further investigation.
Affected User	Displays the name of the affected user
Dwell Time	Displays the length of time that the threat has persisted on the endpoint of the affected user
Dismissed By	Displays the Apex Central user account that dismissed the critical threat alert

Chapter 30

Trend Micro Endpoint Sensor Integration and Policy Settings

The following content explains how to integrate Trend Micro Endpoint Sensor with Apex Central and manage policies from the Apex Central console.

Topics include:

Endpoint Sensor Integration

Apex Central integration with standalone Endpoint Sensor servers enables the following features and capabilities:

- Use uploaded IOC files in Apex Central to initiate investigations directly to Endpoint Sensor from the Apex Central console.
- Register multiple Endpoint Sensor servers. Apex Central can start simultaneous investigations on multiple Endpoint Sensor servers.
- Pull data from Endpoint Sensor investigation results. The data is then displayed in a Apex Central widget.
- Create and deploy policies to Endpoint Sensor servers registered with Apex Central.
- Manage monitoring rules in Apex Central.
- Configure and deploy **Submission settings** to Endpoint Sensor servers registered with Apex Central.

Registering with Apex Central

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/index.html`

   Where `<Apex Central server name>` is the IP address or host name of the Apex Central server

2. Go to **Administration** > **Managed Servers** > **Server Registration**.

3. On the screen that appears, select **Trend Micro Endpoint Sensor** as the **Server Type**, and then click **Add**.

4. On the **Add Server** screen, provide the following details:

   - Server
   - Display name
   - User name
   - Password

5. Click **Save** to add the server to the list. Repeat these steps to add another server.

Adding the Endpoint Sensor Widgets

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/index.html`

   Where `<Apex Central server name>` is the IP address or host name of the Apex Central server

2. Go to **Administration** > **Managed Servers** > **Server Registration**.

3. On the screen that appears, select **Trend Micro Endpoint Sensor** as the **Server Type**, and then click **Add**.

4. Specify the details of the server to be added, and click **Save**.

5. Go to the **Dashboard**.

6. Select an existing tab or create a new tab.

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

8. Click **Add Widgets**.

9. On the screen that appears, select the **Endpoint Sensor** category from the drop-down list.

   The following widgets are available:

   TABLE 30-1. Endpoint Sensor Widgets

WIDGET NAME	DESCRIPTION
Intelligent Monitoring Summary by Host	Displays the endpoints which triggered a monitoring rule. Manually refresh the widget to view the most recent data. To configure the widget settings, click ▼.
Endpoint Sensor Investigation	Run an investigation and view a quick summary of the latest Trend Micro Endpoint Sensor investigation started from Apex Central. By default, the widget automatically refreshes every 2 minutes. To configure the widget settings, click ▼. For details, see the *Trend Micro Endpoint Sensor Administrator's Guide*.

10. Select one or both widgets, and click **Add**.

    Added widgets appear on the **Dashboard**. These widgets display a summary of the most recent investigations and monitoring results of all the registered servers.

    Note

    After registering a new Endpoint Sensor server, refresh the **Endpoint Sensor Investigation** and **Intelligent Monitoring Summary by Host** widgets to update the contents of the widgets with data from the new server.

Using Apex Central to Check Status

Use the **Product Connection Status** and **Agent Connection Status** widgets to check the status of registered Endpoint Sensor servers or agents. These widgets display information from Endpoint Sensor servers added via the **Administration** > **Managed Servers** > **Server Registration** screen.

Procedure

1. Go to the **Dashboard**.

2. Click the **Compliance** tab to view the following widgets:

   Note

   The **Product Connection Status** is also available on the **Summary** tab.

   - **Product Connection Status**: Displays the server status in the **Status** column

     Click **View details** to view detailed information about the servers.

   - **Agent Connection Status**: Displays the total number of agents, online agents, and offline agents for each server

     Click the count in the **Online**, **Offline**, or **Total** column to view detailed information about the agents.

3. To add the widgets to a tab:

   a. Go to an existing tab or create a new tab.

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

   c. Click **Add Widgets**.

   d. On the **Add Widgets** screen, select the **Compliance** category.

   e. Select **Agent Connection Status** or **Product Connection Status**.

   f. Click **Add**.

   The added widget appears on the current tab.

Using the Endpoint Sensor Investigation Widget

Procedure

1. Open the Apex Central management console.

2. Go to the tab where the Endpoint Sensor Investigation widget has been added.

3. In the Endpoint Sensor Investigation widget, click **Start a New Investigation** , and then click **Historical Records** or **System Snapshot**, depending on the type of investigation you plan to run.

4. In the screen that appears, specify the required information.

   The Endpoint Sensor Investigation widget also supports importing C&C callback events as investigation criteria.

   a. On the Endpoint Sensor Investigation widget, click **Start a New Investigation** > **Historical Records**.

   b. Select **Retro Scan** as the investigation method.

   c. Click **Import from C&C Callback Events**.

   d. On the screen that appears, select the C&C callback events that need to be investigated, and click **OK**. The events will be added as investigation criteria.

5. Click **Investigate**.

   The screen refreshes and displays the progress of the investigation.

   Note

   To stop an ongoing investigation, click **Cancel**.

6. Once the investigation is finished, the widget shows the number of endpoints classified as **Matched**, **Safe**, **Pending** or **Cancelled** during the investigation. Click the result of each classification to view more details.

Using Automatic Updates

To use Apex Central as a local update server for Endpoint Sensor, perform the following steps:

Procedure

1. Set up automatic updates in Apex Central.

    a. Open the Apex Central management console.

    b. Go to **Administration** > **Updates** > **Scheduled Update**.

    c. Locate the following patterns:

    - Endpoint Sensor Exception Pattern
    - Endpoint Sensor Trusted Pattern
    - Attack Discovery Pattern

    d. For each pattern, click the pattern name, and select **Enable scheduled downloads**. Leave everything else at the default values.

    Note

    For Endpoint Sensor integration, **Automatic Deployment Settings** is not supported.

    e. Click **Save**.

2. Configure Endpoint Sensor to use Apex Central as its update source.

    a. Open the Endpoint Sensor server management console.

    b. Click **Administration** > **Updates**.

    c. Enable **Download monitoring rules from the following source**.

    d. Select **Other update source**, and type the following in the textbox below:

```
http://<Apex Central server Name>/TVCSDownload/
Activeupdate
```

e. Click **Save**.

Apex Central includes the Endpoint Sensor patterns during the next scheduled update. Afterwards, Endpoint Sensor then downloads these patterns from Apex Central during the next Endpoint Sensor scheduled update.

Trend Micro Endpoint Sensor Policy

Apex Central includes a Policy Management feature which allows administrators to remotely update monitoring rules and deploy submission settings on registered servers.

Note

Multiple Endpoint Sensor policies can be created, but each server can issue only one policy at a time.

For details, see the Apex Central documentation at:

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

Preparing the Server for Policy Deployment

By default, recently added Endpoint Sensor servers are placed in the **New Entity** folder. The servers have to be moved to another folder to be visible for policy deployment.

Procedure

1. Open the Apex Central management console.

2. Go to **Directories** > **Products**, and click **Directory Management**.

3. In the directory tree, expand the **New Entity** folder and locate the server you wish to manage.

4. Perform any of the following:

   - Drag and drop the server to another folder
   - Click **Add Folder** to create a new folder, and then drag and drop the server to the new folder.

Creating and Deploying Policies

Procedure

1. Open the Apex Central management console.

2. Go to **Policies** > **Policy Management**.

3. On the **Product** drop down, select **Trend Micro Endpoint Sensor**.

4. Click **Create**.

5. Click **Specify Target(s)** and select which Endpoint Sensor servers you wish to deploy to.

6. On the **Monitoring Settings** section, configure monitoring rules and submission settings for the new policy.

7. Click **Deploy** to immediately start the policy deployment.

   Afterwards, Apex Central enforces any subsequent updates to the policy on the target Endpoint Sensor servers every 24 hours.

   For details, see the Apex Central documentation at:

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

Managing Monitoring Rules

Take note of the following considerations:

- Managing monitoring rules:

  The **Monitoring Rules** tab displays user-defined rules only. While monitoring rules are shared across policies, the status of a monitoring rule (Enabled/Disabled/remove) is independent for each policy. Administrators can customize policies by selecting which monitoring rules are enabled, disabled, or remove for each policy. New monitoring rules are disabled by default.

  Apex Central is limited to remotely controlling monitoring rules in Endpoint Sensor servers where the rules are part of a Endpoint Sensor policy.

  If a new Endpoint Sensor server is registered, Apex Central automatically includes the new Endpoint Sensor server in its rule deployment schedule. Once the next deployment schedule is due, Apex Central uploads all active monitoring rules to the newly registered server.

- Uploading monitoring rules:

  To upload a monitoring rule, Click **Policies** > **Policies Management** , and select **Trend Micro Endpoint Sensor** as the **Product** . Click **Create** to ceate a new policy, or click an existing policy to open the **Create / Edit Policy** screen. Expand **Monitoring Settings**, click **Upload IOC Rule** > **Choose File**, and navigate to the location of the monitoring rule. Click **Open** to automatically upload the monitoring rule. After the upload is complete, click **Save** or **Deploy**.

  Note

  - It is recommended to specify the target Endpoint Sensor servers before uploading the rule.
  - The **Upload IOC Rule** feature is enabled only when there is at least one Endpoint Sensor server registered to Apex Central.

  Uploading the same monitoring rule in both Apex Central and in a Endpoint Sensor server registered with Apex Central may cause conflicts. Regularly keep track of the uploaded monitoring rules through the **Monitoring Settings** screen to avoid duplication.

If a duplicate monitoring rule is encountered, the following message appears: "Unable to upload file. The file already exists in the Endpoint Sensor server. Use the Endpoint Sensor management console to remove the file first, and try again."

- Changing the status of a monitoring rule:

  To change the status of a monitoring rule, click **Toggle Status**, and select **Enable** or **Disable**. Afterwards, update the remote rule of the Endpoint Sensor servers specified as targets in this policy.

  The status of a monitoring rule is independent for each policy.

- Removing monitoring rules:

  To remove a rule, select the rule and click **Remove**. The status of the removed rule changes to **remove**. Click **Save** or **Deploy** to complete the process.

WARNING!

- Removal of a monitoring rule also removes the monitoring rule from all other Endpoint Sensor policies.
- If the same rule is re-uploaded in a new policy, the old policy will remove the rule again during its scheduled run.

If problems persist, contact Trend Micro support for assistance.

Managing Submission Settings

Use the **Submission Settings** tab to specify if the collected files are sent to a local file server, or sent to Deep Discovery Analyzer for further analysis.

Apex Central is unable to configure a proxy connection between Endpoint Sensor endpoints and Deep Discovery Analyzer. To configure a proxy connection between Endpoint Sensor endpoints and Deep Discovery Analyzer, use the **Proxy** screen of the Endpoint Sensor server computer.

Part XIII

InterScan Security Policies

Chapter 31

InterScan Messaging Security Suite Policy Settings

This section discusses how to configure InterScan Messaging Security Suite policy settings in Apex Central.

Topics include:

IMSS Rules

InterScan Messaging Security Suite (IMSS) evaluates *data in an email message* against a set of defined rules. Rules determine data that must be protected from unauthorized transmission and the action that IMSS performs when it detects transmission.

IMSS rules have the following components:

- Mail Route: A set of sender and recipient email addresses or groups, or an LDAP user or group to which the policy is applied. You can use the asterisk (*) to create wildcard expressions and simplify route configuration.
- Filter: A rule or set of rules that apply to a specific route. In Apex Central, you can set rules for protecting against data loss using templates.
- Action: The action that IMSS performs if the filter conditions are met.

Adding IMSS Rules

Creating a rule involves the following steps:

- Step 1: Set Rule Name
- Step 2: Select Recipients and Senders
- Step 3: Select Templates
- Step 4: Select Actions

Procedure

1. Under **Settings**, click **Add**.

   The **Add Rule** screen appears.

Step 1: Set Rule Name

Procedure

1. Type a name for the rule. The name must not exceed 122 bytes in length.
2. Assign an order number that represents its position within the hierarchy of rules.
3. Click **Next**.

   The **Select Recipients and Senders** screen appears.

Step 2: Select Recipients and Senders

Set the sender and recipient email addresses or groups, or an LDAP user or group to which the rule is applied. You can also configure exceptions to a mail route.

Procedure

1. Click the link next to **To:** or **From:**.

   The **Set Recipients** or **Set Senders** screen appears.

2. Select one of the following:

   - **Anyone**: Select this option to remove any restriction on the recipients or senders.
   - **Any of the selected addresses**

3. If you selected **Any of selected addresses**, choose one of the following from the list box:

   - **Enter email address**: Type the email address to add.
   - **Search for LDAP users or groups**: Type the LDAP user or group name and click **Search**. The results display in the list box.

- **Select address groups**: All existing address groups appear in the list.

When selecting an LDAP group as the recipients or senders, you can use wildcards at the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server.

For more information, see *Using the Asterisk Wildcard on page 31-5*.

4. If you are adding an email address, click **Add >**. If you are adding an LDAP user or group, or an address group, click it in the list box, and then click **Add >**.

5. Click **Save**.

6. Click **Next**.

   The **Step 3: Select Template** screen appears.

Configuring Exceptions

You can configure a route that applies to a large group of senders or recipients, with the exception of specific users, to whom the rule does not apply.

Procedure

1. Click **Senders and Recipients** next to **Exceptions**.

   The **Set Exceptions** screen appears.

2. Under **Select addresses**, select one of the following for both the **From (sender)** and **To (recipient)** addresses:

   - **Enter email address**: Type the email address to add.

   - **Search for LDAP users or groups**: Type the LDAP user or group name and click Search. The results display in the list box.

- **Select address groups**: All existing address groups appear in the list.

3. If you are adding an email address, click **Add >**. If you are adding an LDAP user or group, or an address group, click it in the list box, and then click **Add >**.

4. Click **Save**.

Using the Asterisk Wildcard

You can use the asterisk (*) as a wildcard in email addresses when defining routes.

Wildcards can appear in the name or domain sections of an email address. The following are valid examples:

- *@*: Valid representation of all email addresses.
- *@domain.tld, name@*.tld: Valid representation of the whole name or the domain (not the top level domain (TLD)).
- *@*.tld: Valid representation of both the name and the domain (not the TLD).

Wildcards cannot appear in a subdomain or the top-level domain. Wildcards also cannot appear with other letters; they must appear alone. The following are invalid examples:

- name@domain.*.tld: Invalid representation of a subdomain.
- name@domain.*: Invalid representation of a TLD.
- *name@domain.tld: Invalid use in conjunction with a name.

Step 3: Select Templates

Templates prevent your digital assets (for example, social security numbers and credit card numbers) from leaving your company network. They also provide compliance for government regulations regarding privacy.

Procedure

1. Select templates from the **Available** templates list, and then click **>>**.

   Tip

   Select multiple templates by pressing and holding the CTRL key and then selecting the templates.

2. Click **Next**.

   The **Step 4: Select Actions** screen appears.

Step 4: Select Actions

IMSS performs one or more actions when it detects an attempt to transmit digital assets.

Procedure

1. Select one of the following actions:

   - **Quarantine to**: Instructs IMSS to intercept the messages and prevent them from reaching the recipients.

   - **Send notifications**: Instructs IMSS to send an email notification to one or more recipients.

2. If you selected **Send notifications**, select the type of notification message that you want to use from the dropdown list. The notification messages that are available for use will depend on the targets that you selected.

3. Click **Finish**.

Modifying Existing IMSS Rules

Procedure

1. Click the name of the rule to edit.

   The **Summary** screen for the rule appears.

2. In the **Rule** tab, click **Edit** for **If recipients and senders are**.

3. Configure the route settings.

   For more information, see *Step 2: Select Recipients and Senders on page 31-3*.

4. Click **Edit** for **And scanning conditions match**.

5. Configure the template settings.

6. Click **Edit** for **Then action is**.

7. Configure the action settings.

   Note

   If Apex Central is unable to connect to the selected targets, some action options may become unavailable.

8. Click **Save**.

Deleting IMSS Rules

Procedure

1. Select the check box next to the rule to be deleted.

2. Click **Delete**.

Chapter 32

InterScan Messaging Security Virtual Appliance Policy Settings

This section discusses how to configure InterScan Messaging Security Virtual Appliance policy settings in Apex Central.

Topics include:

IMSVA Rules

InterScan Messaging Security Virtual Appliance (IMSVA) evaluates data in an email message against a set of defined rules. Rules determine data that must be protected from unauthorized transmission and the action that IMSVA performs when it detects transmission.

IMSVA rules have the following components:

- Mail Route: A set of sender and recipient email addresses or groups, or an LDAP user or group to which the policy is applied. You can use the asterisk (*) to create wildcard expressions and simplify route configuration.
- Filter: A rule or set of rules that apply to a specific route. In Apex Central, you can set rules for protecting against data loss using templates.
- Action: The action that IMSVA performs if the filter conditions are met.

Adding IMSVA Rules

Creating a rule involves the following steps:

- Step 1: Set Rule Name
- Step 2: Select Recipients and Senders
- Step 3: Select Templates
- Step 4: Select Actions

Procedure

1. Under **Settings**, click **Add**.

   The **Add Rule** screen appears.

Step 1: Set Rule Name

Procedure

1. Type a name for the rule. The name must not exceed 122 bytes in length.
2. Assign an order number that represents its position within the hierarchy of rules.
3. Click **Next**.

   The **Select Recipients and Senders** screen appears.

Step 2: Select Recipients and Senders

Set the sender and recipient email addresses or groups, or an LDAP user or group to which the rule is applied. You can also configure exceptions to a mail route.

Procedure

1. Click the link next to **To:** or **From:**.

   The **Set Recipients** or **Set Senders** screen appears.
2. Select one of the following:
   - **Anyone**: Select this option to remove any restriction on the recipients or senders.
   - **Any of the selected addresses**
3. If you selected **Any of selected addresses**, choose one of the following from the list box:
   - **Enter email address**: Type the email address to add.
   - **Search for LDAP users or groups**: Type the LDAP user or group name and click **Search**. The results display in the list box.

- **Select address groups**: All existing address groups appear in the list.

When selecting an LDAP group as the recipients or senders, you can use wildcards at the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server. For more information, see Using the Asterisk Wildcard.

4. If you are adding an email address, click **Add >**. If you are adding an LDAP user or group, or an address group, click it in the list box, and then click **Add >**.

5. Click **Save**.

6. Click **Next**.

   The **Step 3: Select Template** screen appears.

Configuring Exceptions

You can configure a route that applies to a large group of senders or recipients, with the exception of specific users, to whom the rule does not apply.

Procedure

1. Click the link next to **Exceptions**.

   The **Set Exceptions** screen appears.

2. Under **Select addresses**, select one of the following for both the From and To addresses:

   - **Enter email address**: Type the email address to add.
   - **Search for LDAP users or groups**: Type the LDAP user or group name and click Search. The results display in the list box.
   - **Select address groups**: All existing address groups appear in the list.

3. If you are adding an email address, click **Add >**. If you are adding an LDAP or address group, click it in the list box, and then click **Add >**.
4. Click **Save**.

Using the Asterisk Wildcard

You can use the asterisk (*) as a wildcard in email addresses when defining routes.

Wildcards can appear in the name or domain sections of an email address. The following are valid examples:

- *@*: Valid representation of all email addresses.
- *@domain.tld, name@*.tld: Valid representation of the whole name or the domain (not the top level domain (TLD)).
- *@*.tld: Valid representation of both the name and the domain (not the TLD).

Wildcards cannot appear in a subdomain or the top-level domain. Wildcards also cannot appear with other letters; they must appear alone. The following are invalid examples:

- name@domain.*.tld: Invalid representation of a subdomain.
- name@domain.*: Invalid representation of a TLD.
- *name@domain.tld: Invalid use in conjunction with a name.

Step 3: Select Templates

Templates prevent your digital assets (for example, social security numbers and credit card numbers) from leaving your company network. They also provide compliance for government regulations regarding privacy.

Procedure

1. Select templates from the Available templates list, and then click **>>**.

   Select multiple templates by pressing and holding the Ctrl key and then selecting the templates.

2. Click **Next**.

   The **Step 4: Select Actions** screen appears.

Step 4: Select Actions

IMSVA performs one or more actions when it detects an attempt to transmit digital assets.

Procedure

1. Select one of the following actions:

   - **Quarantine to**: Instructs IMSVA to intercept the messages and prevent them from reaching the recipients.
   - **Send notifications**: Instructs IMSVA to send an email notification to one or more recipients.

2. If you selected **Send notifications**, select the type of notification message that you want to use from the drop-down list.

   The notification messages that are available for use will depend on the targets that you selected.

3. Click **Finish**.

Modifying Existing IMSVA Rules

Procedure

1. Click the name of the rule to edit.

   The **Summary** screen for the rule appears.

2. In the **Rule** tab, click **Edit** for **If recipients and senders are**.

3. Configure the route settings.

   For more information, see *Step 2: Select Recipients and Senders on page 32-3*.

4. Click **Edit** for **And scanning conditions match**.

5. Configure the template settings.

6. Click **Edit** for **Then action is**.

7. Configure the action settings.

   Note

   If Trend Micro Apex Central is unable to connect to the selected targets, some action options may become unavailable.

8. Click **Save**.

Deleting IMSVA Rules

Procedure

1. Select the check box next to the rule to be deleted.

2. Click **Delete**.

Chapter 33

InterScan Web Security Suite Policy Settings

This section discusses how to configure InterScan Web Security Suite policy settings in Apex Central.

Topics include:

Data Loss Prevention Rule List

When you enable the Data Loss Prevention option, you can also enable or disable individual Data Loss Prevention rules. The green check icon indicates the rule is enabled. The red "x" icon indicates the rule is disabled. You can click the icon to toggle between enabled and disabled states.

The following options are available on this screen:

Rule: Click to edit the rule.

Add: Opens the **Add Rule** screen that allows you to configure a new rule.

Copy: Allows you to copy a selected rule from the list.

Delete: Allows you to delete a rule from the list.

Priority: Click the arrow to change the rule priority.

Status: Click the icon to enable or disable the rule.

Save: Click to save the rule.

Step 1: Set Rule Name

The following is a brief description of the options available on this screen.

- **Enable**: Select to enable the rule.
- **Rule name**: Type a name for this rule to display.
- **Next >**: Click to continue.

Step 2: Select Accounts

The following is a brief description of the options available on this screen.

Note

Not all options are available when creating draft rules. Specify a server to enable all options.

- Specify IP addresses of the accounts that apply to the rule.
    - Type an IP range in **From** and **To**, a specific account IP address or host name in **IP/Hostname**, or an IP subnet in **Address** and **Prefix Length**.
    - Click **Add** to create one or multiple accounts in the right table.
    - Click **Delete** to remove one or multiple accounts from the right table.
- **< Back**: Click to return to the previous page.
- **Next >**: Click to continue.

Step 3: Select Compliance Templates to Block

The following is a brief description of the options available on this screen.

- **Specify the compliance templates you would like to block using this rule.**
    - **Available Template(s)**: The templates listed are available to use with the rule.
    - **Selected Template(s) to Block**: The rule to block is applied to the templates in the list.

    Tip

    Select multiple templates by holding the Shift or Ctrl key and clicking account names.

    - **>>**: Click to add available templates to the selected template list.
    - **<<**: Click to remove templates from the selected template list.
- **< Back**: Click to return to the previous page.
- **Next >**: Click to continue.

Step 4: Select Compliance Templates to Monitor

The following is a brief description of the options available on this screen.

- **Specify the compliance templates you would like to monitor using this rule.**
  - **Available Template(s)**: The templates listed are available to use with the rule.
  - **Selected Template(s) to Monitor**: The rule to monitor is applied to the templates in the list.

    Tip

    Select multiple templates by holding the Shift or Ctrl key and clicking account names.

  - **>>**: Click to add available templates to the selected template list.
  - **<<**: Click to remove templates from the selected template list.
- **< Back**: Click to return to the previous page.
- **Finish**: Click to return to the list of rules.

Chapter 34

InterScan Web Security Virtual Appliance Policy Settings

This section discusses how to configure InterScan Web Security Virtual Appliance policy settings in Apex Central.

Topics include:

Data Loss Prevention Rule List

When you enable the Data Loss Prevention option, you can also enable or disable individual Data Loss Prevention rules. The green check icon indicates the rule is enabled. The red "x" icon indicates the rule is disabled. You can click the icon to toggle between enabled and disabled states.

The following options are available on this screen:

Rule: Click to edit the rule.

Add: Opens the **Add Rule** screen that allows you to configure a new rule.

Copy: Allows you to copy a selected rule from the list.

Delete: Allows you to delete a rule from the list.

Priority: Click the arrow to change the rule priority.

Status: Click the icon to enable or disable the rule.

Save: Click to save the rule.

Step 1: Set Rule Name

The following is a brief description of the options available on this screen.

- **Enable**: Select to enable the rule.
- **Rule name**: Type a name for this rule to display.
- **Next >**: Click to continue.

Step 2: Select Accounts

The following is a brief description of the options available on this screen.

Note

Not all options are available when creating draft rules. Specify a server to enable all options.

- Specify IP addresses of the accounts that apply to the rule.
    - Type an IP range in **From** and **To**, a specific account IP address or host name in **IP/Hostname**, or an IP subnet in **Address** and **Prefix Length**.
    - Click **Add** to create one or multiple accounts in the right table.
    - Click **Delete** to remove one or multiple accounts from the right table.
- **< Back**: Click to return to the previous page.
- **Next >**: Click to continue.

Step 3: Select Compliance Templates to Block

The following is a brief description of the options available on this screen.

- **Specify the compliance templates you would like to block using this rule.**
    - **Available Template(s)**: The templates listed are available to use with the rule.
    - **Selected Template(s) to Block**: The rule to block is applied to the templates in the list.

    > **Tip**
    >
    > Select multiple templates by holding the Shift or Ctrl key and clicking account names.

    - **>>**: Click to add available templates to the selected template list.
    - **<<**: Click to remove templates from the selected template list.
- **< Back**: Click to return to the previous page.
- **Next >**: Click to continue.

Step 4: Select Compliance Templates to Monitor

The following is a brief description of the options available on this screen.

- **Specify the compliance templates you would like to monitor using this rule.**
  - **Available Template(s)**: The templates listed are available to use with the rule.
  - **Selected Template(s) to Monitor**: The rule to monitor is applied to the templates in the list.

    Tip

    Select multiple templates by holding the Shift or Ctrl key and clicking account names.

  - **>>**: Click to add available templates to the selected template list.
  - **<<**: Click to remove templates from the selected template list.
- **< Back**: Click to return to the previous page.
- **Finish**: Click to return to the list of rules.

Part XIV

ScanMail for Microsoft Exchange Policies

Chapter 35

ScanMail for Microsoft Exchange Policy Settings

This section explains how to configure ScanMail for Microsoft Exchange policy settings on the Apex Central console.

Topics include:

Configuring a Data Loss Prevention Policy

Data Loss Prevention policies govern the actions Apex Central takes when it discovers sensitive information in email messages.

Create a new policy by clicking **Data Loss Prevention** > **DLP Policies** > **Add**.

Modify an existing policy by clicking **Data Loss Prevention** > **DLP Policies** > **[DLP Policy Name]**.

Configure Data Loss Prevention policies through the following five step process:

1. *Selecting Accounts on page 35-2*
2. *Configuring DLP Targets on page 35-3*
3. *Configuring DLP Actions on page 35-4*
4. *Configuring DLP Notifications on page 35-5*
5. *Enabling a DLP Policy on page 35-6*

Selecting Accounts

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to **Data Loss Prevention** > **DLP Policies**.

2. Add or edit a policy or exception:

- For new policies or exceptions:

  Click **Add**.

- For preexisting policies or exceptions:

  a. Click the policy or exception name.

  b. Click the **Accounts** tab.

3. Select one of the following:
    - **Anyone**: Apply this policy or exception to all users.
    - **Specific accounts**: Select from Active Directory groups or Apex Central special groups.
4. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list.
5. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list on the **Exclude Accounts** screen.

Configuring DLP Targets

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to the following:
    - For Real-time scans: **Data Loss Prevention** > **DLP Policies**
    - For Manual scans: **Manual Scan** > **Data Loss Prevention**
    - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Data Loss Prevention**
2. Add or edit a policy or exception:
    - For new policies or exceptions:
        a. Click **Add**.
        b. Go to the **Specify Rule** screen.
    - For preexisting policies or exceptions:
        a. Click the policy or exception name.
        b. Click the **Target** tab.

3. Select the check box(es) for the target area(s) of the email message to scan.

   Available targets are:

   - **Header** (**From**, **To**, and **Cc**)
   - **Subject**
   - **Body**
   - **Attachment**

4. Select templates from the list of available templates and click **Add >>** to apply the templates to the policy.

   Note

   A Data Loss Prevention policy requires selecting at least one template before activation.

5. In the Available DLP Template(s) toolbar, click **Add** to create a new template or click **Import** to import a template file.

Configuring DLP Actions

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to the following:

   - For Real-time scans: **Data Loss Prevention** > **DLP Policies**
   - For Manual scans: **Manual Scan** > **Data Loss Prevention**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Data Loss Prevention**

2. Add or edit a policy or exception:

- For new policies or exceptions:

    a. Click **Add**.

    b. Go to the **Specify Action** screen.

- For preexisting policies or exceptions:

    a. Click the policy or exception name.

    b. Click the **Action** tab.

3. Select an action for Apex Central to take when it detects undesirable content.

4. To notify specific individuals:

    - Select the check box **Forward to sender's manager**.

    - Select the check box **Forward to specific email address(es)** and type the email address of the recipients.

5. Specify whether to send notifications when an action is taken by selecting **Notify** or **Do not notify**.

6. Configure **Advanced Options** as necessary.

Configuring DLP Notifications

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to the following:

    - For Real-time scans: **Data Loss Prevention** > **DLP Policies**

    - For Manual scans: **Manual Scan** > **Data Loss Prevention**

    - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Data Loss Prevention**

2. Add or edit a policy or exception:
   - For new policies or exceptions:
     a. Click **Add**.
     b. Go to the **Specify Notification** screen.
   - For preexisting policies or exceptions:
     a. Click the policy or exception name.
     b. Click the **Notification** tab.
3. Click the check boxes corresponding to the people Apex Central will notify.
4. Click **Show details** to customize the notification for that recipient.
5. Select from the notification options.
6. Click **Write to Windows event log** to have Apex Central write the notification to a Windows event log.

Enabling a DLP Policy

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to the following:
   - For Real-time scans: **Data Loss Prevention** > **DLP Policies**
   - For Manual scans: **Manual Scan** > **Data Loss Prevention**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Data Loss Prevention**
2. Add or edit a policy before enabling:
   - For new policies:

    a. Click **Add**.

    b. Go to the **Name and Priority** screen.

- For pre-existing policies:

  Click the policy name.

3. Select to enable this policy or exception.

4. Type the name of your policy in the **Policy name** space.

5. Specify the priority.

   - For new policies:

     Type the priority of your policy in the **Priority** space.

   - For preexisting policies:

     a. Select the check box next to the policy or exception name in the list.

     b. Click **Reorder**.

     c. Type the priority number in the **Priority** field.

     d. Click **Save Reorder**.

6. Click **Save**.

Part XV

Smart Protection Server Widgets

Chapter 36

Smart Protection Server Dashboard Widgets

This section contains help topics for the Smart Protection Server dashboard widgets supported in Apex Central.

Topics include:

Active Users for File Reputation

The Active Users widget displays the number of users that have made file reputation queries to the Smart Protection Server. Each unique client computer is considered an active user.

Note

This widget displays information in a 2-D graph and is updated every hour or click the refresh icon (⟳) at any time to update the data.

Table 36-1. Widget Data

Data	Description
Users	The number of users that sent queries to Smart Protection Serverr computers.
Date	The date of the query.

Active Users for Web Reputation

The Active Users widget displays the number of users that have made web reputation queries to the Smart Protection Server. Each unique client computer is considered an active user.

Note

This widget displays information in a 2-D graph and is updated every 5 minutes or click the refresh icon (⟳) at any time to update the data.

Table 36-2. Widget Data

Data	Description
Users	The number of users that sent queries to Smart Protection Server computers.

Data	Description
Date	The date of the query.

HTTP Traffic Report for File Reputation

The HTTP Traffic Report widget displays the total amount of network traffic in kilobytes (KB) that has been sent to the Smart Protection Server from file reputation queries generated by clients. The information in this widget is updated hourly. You can also click the refresh icon (⟳) at any time to update the data.

Table 36-3. Widget Data

Data	Description
Traffic (KB)	The network traffic generated by queries.
Date	The date of the queries.

HTTP Traffic Report for Web Reputation

The HTTP Traffic Report widget displays the total amount of network traffic in kilobytes (KB) that has been sent to the Smart Protection Server from web reputation queries generated by clients. The information in this widget is updated hourly. You can also click the refresh icon (⟳) at any time to update the data.

Table 36-4. Widget Data

Data	Description
Traffic (KB)	The network traffic generated by queries.
Date	The date of the queries.

Real Time Status

Use the real time status widget to monitor the Smart Protection Server status.

Note

When this widget displays on the Summary screen, the product console session will not expire. The Computer Status is updated every minute which means the session will not expire due to the requests sent to the server. However, the session will still expire if the tab that is currently displayed does not contain this widget.

TABLE 36-5. Widget Data

DATA	DESCRIPTION
Service	Services provided by the Smart Protection Server.
Protocol	This displays the protocols supported by services. File reputation supports both HTTP and HTTPS protocols. Web reputation supports HTTP. HTTPS provides a more secure connection while HTTP uses less bandwidth.
Host	File reputation and Web reputation service addresses. These addresses are used with Trend Micro products that support Smart Protection Server computers. The addresses are used for configuring connections to Smart Protection Server computers.

DATA	DESCRIPTION
Computer Status	The following items are displayed under Health Status: • **File Reputation Query**: displays whether File reputation is functioning as expected. • **Web Reputation Query**: displays whether Web reputation is functioning as expected. • **ActiveUpdate**: displays whether ActiveUpdate is functioning as expected. • **Average CPU load**: displays the computer load average for the past 1, 5, and 15 minutes generated by the kernel. • **Free memory**: displays the available physical memory on the computer. • **Swap disk usage**: displays the swap disk usage. • **Free space**: displays the available free disk space on the computer.

Top 10 Infected Computers for File Reputation

This widget displays the top 10 computer IP addresses which have been classified as infected computers after Smart Protection Server receives a known virus from file reputation query. Information in this widget is displayed in a table, which includes the computer IP address and the total number of detections on each computer. The information in this widget is updated hourly or you can click the refresh icon (⟳) at any time to update the data.

Use this widget to track computers with the most number of infections on your network.

Note

If you enable more than one Smart Protection Server in this widget, this widget will calculate the total number of detections on the selected Smart Protection Server and display the top 10 infected computers from the selected Smart Protection Server computers in the list.

TABLE 36-6. Widget Data

DATA	DESCRIPTION
IP	The IP address of the computer.
Detections	The number of security threats detected by this computer.

Top 10 Blocked Computers for Web Reputation

This widget displays the top 10 computer IP addresses which have been classified as blocked computers after the Smart Protection Server receives a URL for web reputation query. Information in this widget is displayed in a table, which includes the computer IP address and the total number of blocked URLs on each computer. The information in this widget is updated daily or you can click the refresh icon (⟳) at any time to update the data.

Use this widget to track computers who access the most number of blocked sites on your network.

Note

If you enable more than one Smart Protection Server in this widget, this widget will calculate the total number of detections on the selected Smart Protection Server and display the top 10 blocked computers from the selected Smart Protection Server computers in the list.

TABLE 36-7. Widget Data

DATA	DESCRIPTION
IP	The IP address of the computer.
Detections	The number of blocked URLs from this computer.

Part XVI

Trend Micro Mobile Security Widgets and Policies

Chapter 37

Trend Micro Mobile Security Dashboard Widgets

This section contains help topics for the Trend Micro Mobile Security dashboard widgets supported in Apex Central.

Topics include:

- *Windows Phone Device Health Status Widget on page 37-17*
- *Windows Phone Device Operating System Version Summary Widget on page 37-17*

Android Device Health Status

This widget displays a summary of the health status of registered Android mobile devices.

A status of **Healthy** indicates that the Android mobile device is enrolled to the Mobile Security Management Server, and all components and policies on the Android mobile device are up-to-date.

Status	Description
Healthy	Number of Android mobile devices that are healthy
Unhealthy	Number of Android mobile devices that are unhealthy

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Android Device Encryption Status Summary Widget

This widget displays a summary of the encryption status of registered Android mobile devices.

Status	Description
Encrypted	Number of Android mobile devices that are encrypted
Not Encrypted	Number of Android mobile devices that are not encrypted

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Android Device Operating System Version Summary Widget

This widget displays a summary of the operating system versions installed on registered Android mobile devices.

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Android Device Rooted Status Summary Widget

This widget displays a summary of the rooted status of registered Android mobile devices.

Status	Description
Rooted	Number of mobile devices that are rooted
Not Rooted	Number of mobile devices that are not rooted

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Android Device Security Status Widget

This widget displays a summary of the security status of registered Android mobile devices.

- Not scanned
- Risky
- Protected
- Dangerous

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Android Malware Scan Summary Widget

This widget displays a summary of the Malware Scan results for all installed Android apps.

The widget groups the results into the following categories:

- Unknown
- Potentially Unwanted Objects
- Normal
- Malware

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Android Modified App Scan Summary Widget

This widget displays a summary of the Modified App scan results for all installed Android apps.

The widget groups the results into the following categories:

- Unknown
- Modified
- Not Modified

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Android Privacy Data Leak Scan Summary Widget

This widget displays a summary of the Privacy Scan results for all installed Android apps.

The widget groups the results into the following categories:

- Unknown
- Potentially Unwanted Objects
- Normal
- Malware

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Android Vulnerability Scan Summary Widget

This widget displays a summary of the Vulnerability Scan results for all installed Android apps.

The widget groups the results into the following categories:

- Unknown
- Normal
- High
- Medium

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Components Update Status Widget

This widget displays a summary of the device update status of registered mobile devices.

Column	Description
Current Version	Current version number of the Mobile Device Agent or components on the Mobile Security Management Server
Up-to-date	Number of mobile device with updated Mobile Device Agent versions or components
Out-of-date	Number of mobile devices that are using out-of-date components
Update Rate	Percentage of mobile devices using the latest component versions
Upgraded	Number of mobile devices using the latest Mobile Device Agent versions
Not Upgraded	Number of mobile devices that have not upgraded to use the latest Mobile Device Agent versions
Upgrade Rate	Percentage of mobile devices using the latest Mobile Device Agents

Cyber Security News for Mobile Widget

This widget displays cyber security news related to mobile devices, published by Trend Micro. .

iOS Device Encryption Status Summary Widget

This widget displays a summary of the encryption status of registered iOS mobile devices.

Status	Description
Encrypted	Number of iOS mobile devices that are encrypted
Not Encrypted	Number of iOS mobile devices that are not encrypted

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

iOS Device Health Status Widget

This widget displays a summary of the health status of registered iOS mobile devices.

A status of **Healthy** indicates that the iOS mobile device is enrolled to the Mobile Security Management Server, and all components and policies on the iOS mobile device are up-to-date.

Status	Description
Healthy	Number of iOS mobile devices that are healthy
Unhealthy	Number of iOS mobile devices that are unhealthy

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

iOS Device Security Status Widget

This widget displays a summary of the security status of registered iOS mobile devices.

- Not scanned
- Risky
- Protected

- Dangerous

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

iOS Device Jailbreak Status Summary Widget

This widget displays a summary of the jailbreak status of registered iOS mobile devices.

Status	Description
Jailbroken	Number of mobile devices that are jailbroken
Not Jailbroken	Number of mobile devices that are not jailbroken

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

iOS Device Operating System Version Summary Widget

This widget displays a summary of the operating system versions installed on registered iOS mobile devices.

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

iOS Malware Scan Summary Widget

This widget displays a summary of the Malware Scan results for all installed iOS apps.

The widget groups the results into the following categories:

- Unknown
- Malware
- Normal

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Mobile Device App Control Status Summary Widget

This widget displays a summary of the application control status of registered mobile devices.

STATUS	DESCRIPTION
Compliant	Number of mobile devices that comply with the Mobile Security's compliance and application control policy
Not Compliant	Number of mobile devices that do not comply with the Mobile Security's compliance and application control policy

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Mobile Device Encryption Status Summary Widget

This widget displays a summary of the encryption status of registered mobile devices.

STATUS	DESCRIPTION
Encrypted	Number of mobile devices that are encrypted
Not Encrypted	Number of mobile devices that are not encrypted

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Mobile Device Health Status Widget

This widget displays a summary of the health status of registered mobile devices.

Status	Description
Healthy	Device is enrolled to the Mobile Security Management Server, and the components and policies on the mobile device are up-to-date
Non-Compliant	Device is enrolled to the Mobile Security Management Server, but does not comply with the server policies
Out of Sync	Device is enrolled to the Mobile Security Management Server, but either the components or the polices are out-of-date
Inactive	Device is not yet enrolled to the Mobile Security Management Server

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Mobile Device Jailbreak Status Summary Widget

This widget displays a summary of the jailbreak status of registered mobile devices.

Status	Description
Jailbroken	Number of mobile devices that are jailbroken
Not Jailbroken	Number of mobile devices that are not jailbroken

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Mobile Device Operating System Version Summary Widget

This widget displays a summary of the operating system versions installed on registered mobile devices.

Operating System	Description
Android	Number of registered Android mobile devices
iOS	Number of registered iOS mobile devices
Windows Phone	Number of registered Windows Phone mobile devices

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Mobile Device Ransomware Scan Summary Widget

This widget displays a summary of the ransomware scan results for all installed apps.

The widget groups the results by mobile operating system.

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Mobile Device Security Status Widget

This widget displays a summary of the security status of registered mobile devices.

- Not scanned
- Risky

- Protected
- Dangerous

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Mobile Device Vendors Summary Widget

This widget displays a summary of the mobile device vendors for registered mobile devices.

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Policy Update Status Summary Widget

This widget displays a summary of the policy update status of registered mobile devices.

Status	Description
Up-to-date	Number of mobile devices running with an updated Mobile Device Agent version or components
Out-of-date	Number of mobile devices that are running with out-of-date components

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Server Component Health Status Summary Widget

This widget displays the server components update status and their version numbers.

Column	Description
Server	Name of the module
Address	Domain name or IP address of the machine hosting the module
Current Version	Version number of the Mobile Security Management Server modules installed
Last Updated	Time and date of the last update

Telephone Carriers Summary Widget

This widget displays a summary of telephone carriers used by registered Android mobile devices.

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Top 10 Applications Installed Widget

This widget displays the list of top ten applications installed on registered mobile devices. Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Top Five Android Ransomware Detected Widget

This widget displays the list of top five Android ransomware detected by Mobile Security, based on the number of times the specified ransomware was detected. Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Top Five Blocked Web Sites Widget

This widget displays the list of top five web sites blocked by Mobile Security, based on the number of times each site was accessed. Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Top Five iOS Ransomware Detected

This widget displays the list of top five iOS ransomware detected by Mobile Security, based on the number of times the specified ransomware was detected. Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Top Five Malware Detected Widget

This widget displays the list of the top five malware detected by Mobile Security, based on the number of times the specified malware was detected. Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Windows Phone Device Encryption Status Summary Widget

This widget displays a summary of the encryption status of registered Windows Phone mobile devices.

Status	Description
Encrypted	Number of Windows Phone mobile devices that are encrypted
Not Encrypted	Number of Windows Phone mobile devices that are not encrypted

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Windows Phone Device Health Status Widget

This widget displays a summary of the health status of registered Windows Phone mobile devices.

A status of **Healthy** indicates that the Windows Phone mobile device is enrolled to the Mobile Security Management Server, and all components and policies on the Windows Phone mobile device are up-to-date.

Status	Description
Healthy	Number of Windows Phone mobile devices that are healthy
Unhealthy	Number of Windows Phone mobile devices that are unhealthy

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Windows Phone Device Operating System Version Summary Widget

This widget displays a summary of the operating system versions installed on registered Windows Phone mobile devices.

Select **All** or the group name from the drop-down list to display the information of the relevant devices.

Chapter 38

Trend Micro Mobile Security Policy Settings

This section discusses how to configure security policies for Mobile Security from the Apex Central management console.

Protecting Devices with Policies

You can configure security policies for a Mobile Security group on the Management Server. These policies apply to all mobile devices in the group. You can apply security policies to all Mobile Security groups by selecting the **Mobile Devices** group (the root group). The following table lists the security policies available in Mobile Security.

TABLE 38-1. Security Policies in Mobile Security

POLICY GROUP	POLICY	REFERENCE
General	Common Policy	For Full Version Deployment Mode, see *Common Policy in Full Version Deployment Mode on page 38-4*. For Security Scan Deployment Mode, see *Common Policy in Security Scan Deployment Mode on page 38-5*.

Policy Group	Policy	Reference
Provisioning	Wi-Fi Policy	See *Wi-Fi Policy on page 38-6*.
	Exchange ActiveSync Policy	See *Exchange ActiveSync Policy on page 38-6*.
	Certificate Policy	See *Certificate Policy on page 38-6*.
	VPN Policy	See *VPN Policy on page 38-7*.
	Global HTTP Proxy Policy	See *Global HTTP Proxy Policy on page 38-7*.
	Single Sign-On Policy	See *Single Sign-On Policy on page 38-7*.
	Cellular Network Policy	See *Cellular Network Policy on page 38-8*.
	AirPlay/AirPrint Policy	See *AirPlay/AirPrint Policy on page 38-8*.
	Theme Policy	See *Theme Policy on page 38-9*.
	Managed Domains Policy	See *Managed Domains Policy on page 38-9*.

POLICY GROUP	POLICY	REFERENCE
Device Security	Security Policy	For Security Policy in Full Version Deployment Mode, see *Security Policy in Full Version Deployment Mode on page 38-10*. For Security Policy in Security Scan Deployment Mode, see *Security Policy in Security Scan Deployment Mode on page 38-12*.
	Spam Prevention Policy	See *Spam Prevention Policy on page 38-13*.
	Call Filtering Policy	See *Call Filtering Policy on page 38-16*.
	Web Threat Protection Policy	See *Web Threat Protection Policy on page 38-18*.
Devices	Password Policy	See *Password Policy on page 38-21*.
	Feature Lock Policy	See *Feature Lock Policy on page 38-21*.
	Compliance Policy	See *Compliance Policy on page 38-31*.
Application Management	Application Monitor & Control Policy	See *Application Monitor and Control Policy on page 38-31*.
	Volume Purchasing Program Policy	See *Volume Purchasing Program Policy on page 38-34*.
Samsung KNOX	Container Policy	See *Container Policy on page 38-37*.

Common Policy in Full Version Deployment Mode

Common Policy provides the common security policies for mobile devices. To configure common security policy settings, click **Policies**, then click the policy name, and then click **Common Policy**.

- **User Privileges**: You can enable or disable the feature that allows users to uninstall the Mobile Device Agent. Additionally, you can select whether to allow users to configure Mobile Security device agent settings.

  The following is a list of features associated with uninstall protection:

  - turn On/Off uninstall protection from the administration console
  - password length must have a minimum of six (6) and a maximum of twelve (12) characters; password may contain numbers, characters or symbols.
  - password can be set for each group from the administration console.

  If you do not select the **Allow users to configure Mobile Security client settings** check box, users cannot change Mobile Device Agent settings. However, the filtering lists for **Spam Prevention Policy**, **Call Filtering Policy** and **Web Threat Protection Policy** are not affected when this option is selected. For more information, see *Spam Prevention Policy on page 38-13*, *Call Filtering Policy on page 38-16* and *Web Threat Protection Policy on page 38-18*.

- **Update Settings**: You can select to have the Mobile Security Management Server notify Mobile Device Agents when a new component is available for update. Or you can select the auto-check option to have Mobile Device Agents periodically check for any component or configuration updates on the Mobile Security Management Server.

- **Log Settings**: When Mobile Device Agents detect a security risk, such as a malware on Android operating system, a log is generated on the mobile device.

Common Policy in Security Scan Deployment Mode

Common Policy provides the common security policies for mobile devices. To configure common security policy settings, click **Policies**, then click the policy name, and then click **Common Policy**.

- **User Privileges**:
    - You can select whether to allow users to configure Mobile Security device agent settings.

      If you do not select the **Allow users to configure Mobile Security client settings** check box, users cannot change Mobile Device Agent settings. However, the filtering lists for **Web Threat Protection Policy** are not affected when this option is selected. For more information, see *Web Threat Protection Policy on page 38-18*.
    - You can select the auto-check option to have Mobile Device Agents periodically check for any component or configuration updates on the Mobile Security Management Server.

Wi-Fi Policy

Wi-Fi Policy enables you to deliver your organization's Wi-Fi network information to Android and iOS mobile devices; including the network name, security type and password.

To configure Wi-Fi policy settings, click **Policies**, then click the policy name, and then click **Wi-Fi Policy**.

Exchange ActiveSync Policy

Exchange ActiveSync Policy enables you to create an Exchange ActiveSync policy for your organization and deliver it to iOS mobile devices.

To configure Exchange ActiveSync policy settings, click **Policies**, then click the policy name, and then click **Exchange ActiveSync Policy**.

Certificate Policy

Certificate Policy enables you to import certificates that you need to deploy on iOS mobile devices.

To configure certificate policy settings, click **Policies**, then click the policy name, and then click **Certificate Policy**.

VPN Policy

VPN policy settings enable you to create a VPN Policy for your organization and deliver it to iOS mobile devices.

To configure VPN policy settings, click **Policies**, then click the policy name, and then click **VPN Policy**

Global HTTP Proxy Policy

Global HTTP Proxy Policy enables you to deliver your organization's proxy information to mobile devices. This policy only applies to iOS mobile devices that are in supervised mode.

To configure global HTTP proxy policy settings, click **Policies**, then click the policy name, and then click **Global HTTP Proxy Policy**

Single Sign-On Policy

Single sign-on (SSO) policy enables the users to use the same credentials across applications, including Mobile Securityand applications from the App Store. Each new application configured with SSO certification verifies user permissions for enterprise resources, and logs users in without requiring them to reenter their passwords.

The single sign-on policy includes the following information:

- **Name**: the Kerberos principal name.
- **Realm**: The Kerberos realm name.

  The Kerberos ream name should be properly capitalized.
- **URL Prefixes** (Optional): List of URLs that must be matched in order to use an account for Kerberos authentication over HTTP. If this field is

blank, the account is eligible to match all http and https URLs. The URL matching patterns must begin with either http or https.

Each entry of this list must contain a URL prefix. Only the URLs that begin with one of the strings in an account are allowed to access the Kerberos ticket. URL matching patterns must include the scheme. For example, http://www.example.com/. If a matching pattern does not end in /, it will automatically add a / to the URL.

- **Application Identifiers** (Optional): List of application identifiers that are allowed to use the account. I f this field is blank, this account matches all application identifiers.

  The **Application Identifiers** array must contain strings that match application bundle IDs. These strings may be exact matches (such as com.mycompany.myapp) or may specify a prefix match on the bundle ID by using the * wildcard character. The wildcard character must appear after a period character (.), and may appear only at the end of the string (such as com.mycompany.*). When a wildcard is used, any application whose bundle ID begins with the prefix is granted access to the account.

To configure Single Sign-On Policy for iOS settings, click **Policies**, then click the policy name, and then click **Single Sign-On Policy**.

Cellular Network Policy

Celluar network policy settings enables you to configure cellular network settings for your organization and deliver it to iOS mobile devices.

To configure the celluar network policy settings, click **Policies**, then click the policy name, and then click **Celluar Network Policy**.

AirPlay/AirPrint Policy

AirPlay/AirPrint policy settings enable you to create AirPlay and AirPrint policies for your organization and deliver it to iOS mobile devices.

To configure AirPlay and/or AirPrint policy settings, click **Policies**, then click the policy name, and then click **AirPlay/AirPrint Policy**.

Theme Policy

Theme policy settings enable you to push a font and set a wallpaper for home screen and lock screen for the iOS mobile devices. This policy applies to iOS mobile devices that are in the supervised mode only.

To configure theme policy settings, click **Policies**, then click the policy name, and then click **Theme Policy**.

Managed Domains Policy

Managed domains policy enables you to configure the email and/or web domains that your organization manages.

- Unmarked Email Domains: When a user is composing an email using the system email client, any email address entered which does not match the configured domains will be highlighted (marked) in red. Administrators should consider using this functionality, to warn users who may be inadvertently attempting to send sensitive information to untrusted email addresses.

- Managed Safari Web Domains: You can specify that files downloaded from specific domains using Safari may only be opened with managed apps. For example, a PDF downloaded from internal.example.com may be opened with Adobe Reader (a managed app) but not Dropbox (an unmanaged app). This provides improved containerization of Safari and wider the use as an enterprise browser.

Important

You must disable the following iOS features in the Feature Lock Policy. Otherwise, the managed Safari Web domains settings will not have any effect, since the downloaded files can be opened with other (unmanaged) apps:

- Open documents from managed apps in other apps (7.0 or above)
- Open documents from other apps in managed apps (7.0 or above)

To configure managed domain policy settings, click **Policies**, then click the policy name, and then click **Managed Domain Policy**.

Security Policy in Full Version Deployment Mode

You can configure the **Security Settings** from the **Security Policy** screen.

To configure the security protection policy settings, click **Policies**, click the policy name, and then click **Security Policy**.

The following table describes the available settings for this policy.

Table 38-2. Security Policy Settings

Section	Item	Description	Supported Mobile Device OS
Security Settings	**Scan installed applications only**	Select this option if you want to scan installed applications only	🤖
	Scan installed applications and files	Select this option if you want to scan installed applications and other files stored on the mobile device. If you select this option, specify whether you want to	

Section	Item	Description	Supported Mobile Device OS
		scan only APK files or all files.	
	Scan after pattern update	Enable this option if you want to run the malware scan after every pattern update. Mobile Security runs a scan automatically after successful pattern update on Android mobile devices.	
	Enable Facebook scan	Enable this option to scan the Facebook privacy settings. **Note** Enabling **Facebook scan** allows users to protect their information and make sure that they only share data with people they trust.	🍎 🤖
Scan Schedule	**Daily**	The scan runs every day on the specified day at the **Start time**.	🍎 🤖
	Weekly	The scan runs once a week on the specified day at the **Start time**.	

Section	Item	Description	Supported Mobile Device OS
	Monthly	The scan runs once a month on the specified day at the **Start time**.	

Security Policy in Security Scan Deployment Mode

You can configure the **Security Settings** from the **Security Policy** screen.

To configure the security protection policy settings, click **Policies**, click the policy name, and then click **Security Policy**.

The following table describes the available settings for this policy.

Table 38-3. Security Policy Settings

Section	Item	Description	Supported Mobile Device OS
Security Settings	**Scan installed applications only**	Select this option if you want to scan installed applications only	🤖
	Scan installed applications and files	Select this option if you want to scan installed applications and other files stored on the mobile device. If you select this option, specify whether you want to scan only APK files or all files.	
	Scan after pattern update	Enable this option if you want to run the malware scan after every pattern update.	

Section	Item	Description	Supported Mobile Device OS
		Mobile Security runs a scan automatically after successful pattern update on Android mobile devices.	
Scan Schedule	**Daily**	The scan runs every day on the specified day at the **Start time**.	🤖
	Weekly	The scan runs once a week on the specified day at the **Start time**.	
	Monthly	The scan runs once a month on the specified day at the **Start time**.	

Spam Prevention Policy

The spam prevention policy in Mobile Security provides protection against spam WAP push and SMS text messages.

To configure spam prevention policy settings, click **Policies**, then click the policy name, and then click **Spam Prevention Policy**.

Spam SMS Prevention Policies

This feature provides you server-side control of SMS spam prevention policies. The following features are available when configuring the SMS Spam Prevention Policies:

- enable or disable spam SMS prevention for mobile device
- configure the mobile device to use a blocked list, approved list or disable the SMS anti-spam feature for mobile device.

- configure an approved list from the administration console
- configure a blocked list from the administration console

Refer to the following table for approved or blocked filtering list configuration details.

TABLE 38-4. Filtering list configuration for Spam SMS Prevention Policy

CENTRAL CONTROL	USER CONTROL	DESCRIPTION
Disabled	Enabled	The user can edit the approved/blocked list on the mobile device agent. Mobile Security allows or blocks the messages based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent
Enabled	Disabled	The user is only allowed to edit the approve/blocked list on the mobile device agent. Mobile Security allows or blocks the messages based on the following priority: 1. Approved List or Blocked List on server 2. Approved List on Mobile Device Agent 3. Blocked List on Mobile Device Agent

Central Control	User Control	Description
Enabled	Enabled	The user can view or edit the approved/blocked list defined by the administrator and can also use the approved/blocked list on the mobile device agent. When the security policies sync with the mobile device agent, it does not sync the filtering lists, and updates all other settings according to the policies. Mobile Security allows or blocks the messages based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent 3. Approved List or Blocked List on server

Note

The SMS approved and blocked list must use the format: "[name1:]number1;[name2:]number2;...".

The 'name' length should not exceed 30 characters, while phone number should be between 4 and 20 characters long and can contain the following: 0-9, +, -, #, (,) and spaces. The maximum number of entries should not exceed 200.

Spam WAP Push Prevention Policies

This feature provides you server-side control of WAP Push Prevention. If enabled, you can select whether to use a WAP approved list.

Note

The WAP approved list must use the format: "[name1:]number1;[name2:]number2;...".

The 'name' length should not exceed 30 characters, while phone number should be between 4 and 20 characters long and can contain the following: 0-9, +, -, #, (,) and spaces. The maximum number of entries should not exceed 200.

The following is a list of features available when configuring WAP Push Prevention policies:

- enable or disable WAP Push Prevention for mobile device
- configure the mobile device to use an approved list or disable WAP Push Prevention on the mobile device
- configure an approved list from the administration console
- if the administrator has enabled server-side control, the user will be unable to change the WAP Push Prevention type defined by the administrator
- if the administrator has disable server-side control, and allowed users to configure Mobile Security settings on mobile device, the user will be unable to view or edit the WAP Push Prevention list configured by the administrator, and may edit the personal WAP Push Prevention list on the mobile device side

Note

The users' personal settings for spam messages will be cleared after the Spam Prevention Policy is applied on the Mobile Device Agents.

Call Filtering Policy

This feature provides you server-side control of call filtering policies. To configure call filtering policy settings, click **Policies**, then click the policy name, and then click **Filtering Policy**.

The following features are available when configuring the Call Filtering Policies:

- enable or disable call filtering for mobile device
- configure the mobile device to use a blocked list or an approved list
- configure an approved list from the administration console

- configure a blocked list from the administration console

Refer to the following table for approved or blocked filtering list configuration details.

TABLE 38-5. Filtering list configuration for Call Filtering Policy

CENTRAL CONTROL	USER CONTROL	DESCRIPTION
Disabled	Enabled	The user can edit the approved/blocked list on the mobile device agent. Mobile Security allows or blocks the URLs based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent
Enabled	Disabled	The user is only allowed to edit the approved/blocked list on the mobile device agent. Mobile Security allows or blocks the incoming calls based on the following priority: 1. Blocked List on server 2. Approved List on Mobile Device Agent 3. Blocked List on Mobile Device Agent You can also configure server-side control for outgoing calls on Android mobile devices.

Central Control	User Control	Description
Enabled	Enabled	The user can view or edit the approved/blocked list defined by the administrator and can also use the approved/blocked list on the mobile device agent. When the security policies sync with the mobile device agent, it does not sync the filtering lists, and updates all other settings according to the policies. Mobile Security allows or blocks the incoming calls based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent 3. Blocked List on server You can also configure server-side control for outgoing calls on Android mobile devices.

Note

The call filtering approved and blocked list must use the format: "[name1:]number1;[name2:]number2;...".

The 'name' length should not exceed 30 characters, while phone number should be between 4 and 20 characters long and can contain the following: 0-9, +, -, #, (,) and spaces. The maximum number of entries should not exceed 200.

Web Threat Protection Policy

Enables you to manage Web threat protection policy from the Mobile Security Management Server and deploys it on Android mobile devices. It also enables Android mobile devices to send the Web threat protection log back to the server.

Note

Mobile Security Web Threat Protection only supports the default Android browser and Google Chrome.

To configure Web Threat Protection Policy settings, click **Policies**, then click the policy name, and then click **Web Threat Protection Policy**.

Web Threat Protection for Android Mobile Devices

Web Threat Protection feature provides you the server-side control of Web threat protection policies on Android mobile devices and provides three pre-defined security levels: **Low**, **Normal**, and **High**. It also provides blocked and approved lists to block or allow certain URLs. Mobile Security will block all the URLs that you add in the Blocked List, and allow all URLs that are in the Approved List.

Note

The Web threat protection policy only supports Google Chrome and Android's default Web browser on mobile devices.

Refer to the following table for approved or blocked filtering list configuration details.

TABLE 38-6. Filtering list configuration for Web Threat Protection policy

SERVER CONTROL	USER CONTROL	DESCRIPTION
Disabled	Enabled	The user can edit the approved/blocked list on the mobile device agent. Mobile Security allows or blocks the URLs based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent

Server Control	User Control	Description
Enabled	Disabled	The user is only allowed to edit the approved/blocked list on the mobile device agent. Mobile Security allows or blocks the URLs based on the following priority: 1. Approved List on server 2. Blocked List on server 3. Approved List on Mobile Device Agent 4. Blocked List on Mobile Device Agent
Enabled	Enabled	The user can view or edit the approved/blocked list defined by the administrator and can also use the approved/blocked list on the mobile device agent. When the security policies sync with the mobile device agent, it does not sync the filtering lists, and updates all other settings according to the policies. Mobile Security allows or blocks the URLs based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent 3. Approved List on server 4. Blocked List on server

Note

The Web threat filtering approved and blocked lists must use the following format: [URL1] [URL2] [URL3], with a blank space or a line break between two URLs.

Web Threat Protection for iOS Mobile Devices

Web Threat Protection provides you the server-side control on supervised iOS mobile devices by providing access to the following:

- Specific websites only
- Limited adult content

Refer to the following table for the feature details:

TABLE 38-7. Filtering list configuration for Web Threat Protection policy

FEATURE	DESCRIPTION
Specific websites only	Using this option will restrict the access to only the websites that you have configured on the server. You can add the URLs that you want to allow, on the iOS tab of the Web Threat Protection Policy. These URLs will be added to the Safari Web browser on the users' iOS mobile devices.
Limited adult content	This option uses filtering lists to provide server control of the websites that you want to allow or block on iOS mobile devices. These filters block or allow the access of the websites irrespective of the default filter settings on iOS mobile devices.

Note

The Web threat filtering approved and blocked lists must use the following format: [URL1] [URL2] [URL3], with a blank space or a line break between two URLs.

Password Policy

The password policy prevents unauthorized access to data on mobile devices.

To configure password policy settings, click **Policies**, then click the policy name, and then click **Password Policy** from the left-menu.

Feature Lock Policy

With this feature, you can restrict (disable) or allow (enable) the use of certain mobile device features/components. For example, you can disable the camera for all mobile devices in a particular group.

To configure Feature Lock Policy settings, click **Policies**, then click the policy name, and then click **Feature Lock Policy** from the left-menu.

See *Supported Mobile Device OS Features on page 38-22* for the list of supported features/components.

WARNING!

Use caution while disabling WLAN/WIFI and/or Microsoft ActiveSync. The mobile device may not be able to communicate with the server if both these options are unavailable.

For Android mobile devices, you can also add access point(s) to control the availability of the device components within the range of those access point(s).

Supported Mobile Device OS Features

The following table shows the list of features that Mobile Security supports on each platform.

TABLE 38-8. Trend Micro Mobile Security 9.7 Feature Matrix

POLICY	FEATURES	SETTINGS	🍎	🤖	⊞
Provisioning	Wi-Fi	Standard Wi-Fi configuration	●	●	
		Legacy hotspot configuration	●		
		Hotspot 2.0 configuration	●		
	Exchange ActiveSync	Exchange ActiveSync configuration	●		
	VPN	VPN configuration	●		
	Global HTTP Proxy	Global HTTP Proxy configuration	●		
	Single Sign-on	Single sign-on configuration	●		

Policy	Features	Settings			
	Certificate	Certificate configuration	●		
	Cellular network	Cellular network configuration	●		
	AirPlay/AirPrint	AirPlay/AirPrint configuration	●		
	Themes (Supervised only)	Wallpaper configuration	●		
		Font configuration	●		
	Managed Domains	Unmarked Email Domains	●		
		Managed Safari Web Domains	●		
Device Security	Security Settings	Real-time scan		●	
		Scan after pattern update		●	
		Manual scan	●	●	
		Facebook scan	●	●	
Data Protection	Spam SMS Prevention	Server-side control		●	
		Use blocked list		●	
		Use approved list		●	
	Spam WAP Push Prevention	Server-side control		●	
		Use approved list		●	
	Call Filtering	Server-side control		●	
		Use blocked list		●	
		Use approved list		●	
	Web Threat Protection	Server-side control		●	
		Use blocked list		●	

Policy	Features	Settings	🍎	🤖	⊞
		Use approved list		●	
		Allow specific websites only	●		
		Allow limited adult content	●		
Data Protection	Password Settings	Use password for login	●	●	●
		Allow simple password	●	●	●
		Require alphanumeric password	●	●	●
		Minimum password length	●	●	●
		Password expiration	●	●	●
		Password history	●	●	●
		Auto-lock	●	●	●
		Password failure action	●	●	●
	Feature Lock	Camera	●	●	
		FaceTime	●		
		Screen capture	●		
		Apps installation	●		
		Sync while roaming	●		
		Voice dialing	●		
		In-app purchase	●		
		Multiplayer gaming	●		
		Adding game center friends	●		
		Game Center (Supervised Only)	●		

Policy	Features	Settings		🤖	⊞
		Force encrypted backups	●		
		Explicit music, podcast and iTunes U	●		
		Passbook while device is locked	●		
		Bluetooth and Bluetooth discovery		●	
		WLAN/Wi-Fi		●	
		3G data network		●	
		Tethering		●	
		Developer mode		●	
		Speaker/speakerphone/ microphone			
		Restrict memory cards		●	
		Siri	●		
		Siri while device is locked	●		
		Enable profnity filter	●		
		Enable access to iCloud services	●		
		Cloud backup	●		
		Cloud document sync	●		
		Photo Stream	●		
		Shared Photo Streams	●		
		Diagnostic data	●		

Policy	Features	Settings	🍎	🤖	⊞
		Accept untrusted Transport Layer Security (TLS)	●		
		Force iTunes to store password	●		
		YouTube	●		
		Open documents from managed apps in other apps	●		
		Open documents from other apps in managed apps	●		
		iTunes	●		
		Safari Web browser	●		
		AutoFill	●		
		JavaScript	●		
		Popups	●		
		Force fraud warning	●		
		Accept cookies	●		
		Removing apps (Supervised only)	●		
		Bookstore (Supervised only)	●		
		Erotica (Supervised only)	●		
		Configuration Profile Installation (Supervised only)	●		
		iMessage (Supervised only)	●		
		Ratings region	●		
		Movies	●		

POLICY	FEATURES	SETTINGS	🍎	🤖	⊞
		TV Shows	●		
		Apps	●		
		Account modification (Supervised only)	●		
		AirDrop (Supervised only)	●		
		Applications cellular data modification (Supervised only)	●		
		Assistant (Siri) user-generated content (Supervised only)	●		
		Cloud keychain synchronization	●		
		Find My Friends modification (Supervised only)	●		
		Fingerprint for unlocking a device	●		
		Host pairing (Supervised only)	●		
		Lock screen control center	●		
		Lock screen notifications view	●		
		Lockscreen today view	●		
		Over the Air Public Key Infrastructure (OTAPKI) updates	●		
		Force limit ad tracking	●		
		Force AirPlay outgoing requests pairing password	●		
		Allow managed apps to store data in iCloud	●		

Policy	Features	Settings		🤖	⊞
		Allow backup of enterprise books	●		
		Allow configuration restrictions	●		
		Allow Erase All Content and Settings	●		
		Allow Handoff	●		
		Allow Internet results in spotlight	●		
		Allow notes and highlights sync for enterprise books	●		
		Allow sharing of managed documents using AirDrop	●		
		Allow iCloud Photo Library	●		
		Allow installing apps from device	●		
		Allow keyboard shortcuts	●		
		Allow paired Apple Watch	●		
		Allow passcode modification	●		
		Allow device name modification	●		
		Allow wallpaper modification	●		
		Allow automatic downloading of apps	●		
		Allow trusting of enterprise apps	●		
	Compliance Settings	Rooted/Jailbroken	●	●	
		Unencrypted	●	●	

Policy	Features	Settings	🍏	🤖	⊞
		OS version check	●	●	
Application Management	Application Monitor & Control	Required Applications	●	●	
		Permitted Applications	●	●	
		Lock to App (Supervised only)	●		
	Volume Purchasing Program	Volume Purchasing Program	●		
Remote Control	Register		●	●	
	Update		●	●	
	Anti-theft	Remote locate		●	
		Remote lock	●	●	
		Remote wipe	●	●	●
		Reset password	●	●	
	Samsung KNOX Workspace	Create container		●	
		Remove container		●	
		Lock container		●	
		Unlock container		●	
		Reset container password		●	
Samsung KNOX Workspace Policy	Container account setting	Blocked list		●	
		Approved list		●	
	Restriction settings	Allow users to use camera		●	
		Allow display the share via list of applications		●	

Policy	Features	Settings		🤖	⊞
	Browser settings	Enable auto fill setting		●	
		Enable cookies setting		●	
		Enable popups setting		●	
		Enable force fraud warning setting		●	
		Enable JavaScript setting		●	
		Enable Web Proxy		●	
Samsung KNOX Workspace Policy	Container password settings	Enable password visibility		●	
		Minimum password change length		●	
		Minimum password length		●	
		Maximum inactivity timeout		●	
		Maximum number of failed attempts		●	
		Password history		●	
		Maximum password age		●	
		Minimum number of special characters required in a password		●	
		Password complexity		●	
	Application settings	Installation approved list		●	
		Installation blocked list		●	
		Required applications		●	
		Disabled applications		●	

Policy	Features	Settings		🤖	⊞
Device Enrollment Program			●		

Compliance Policy

Compliance policy enables you to set the compliance criteria for the mobile devices. If any mobile device does not match the criteria, Mobile Security displays its non-compliant status on the server UI. Mobile Security also sends an email to the non-compliant iOS mobile device, while it displays a notification on non-compliant Android mobile devices. The compliance check list includes:

- **Rooted/Jailbroken**—checks whether the mobile device is rooted/jailbroken or not.
- **Unencrypted**—checks whether the encryption is enabled on the mobile device or not
- **OS version check**—checks whether the OS version matches the defined criteria or not.

To configure compliance policy settings, click **Policies**, then click the policy name, and then click **Compliance Policy**.

Application Monitor and Control Policy

Application monitor and control policies provide you server-side control of the applications installed on mobile devices and push the required applications to the mobile devices.

To configure application monitor and control policy settings, click **Policies**, then click the policy name, and then click **Application Monitor and Control Policy**.

- **Required Applications**—using this option will push all the applications that you add in the list, to the mobile devices. You can also link a VPN to applications, so that the applications always use this VPN to connect to the network.

- **Permitted Applications**—control the applications installed on mobile devices by using approved and blocked lists.

  For iOS mobile devices, Mobile Security sends notification to administrator and the user for any application that does not comply with the policy.

  For Android mobile devices, Mobile Security blocks the application that does not comply with the policy and will allow all others.

  - **Enable system apps blocking** (Android only):

    if selected, Mobile Security will block all the system apps on Android mobile devices.

  - **Enable Application Category**: select the application category that you want to enable or disable on mobile devices. You can also make the exception by adding the applications that belong to these categories to the approved or blocked list. For example, if you have disabled a category type Games, Mobile Security will block all the applications that belong to this category, unless any such application exists in the approved list.

    Mobile Security allows or blocks the applications according to the following priority:

    1. **Approved List**—Mobile Security allows applications that are in the approved list even if they belong to the category that you have disabled.

    2. **Blocked List**—Mobile Security blocks applications that are in the blocked list even if they belong to the category that you have enabled.

    3. **Application permissions**—Mobile Security allows or blocks applications according to your selected permission status for the category that they belong to.

  - **Enable Application Permissions** (for Android only): select the application services that you want to enable or disable on Android mobile devices. You can also make the exception by adding the applications that use these services to the approved or blocked list.

For example, if you have disabled service type **Read Data**, Mobile Security will block all the applications that use the Read Data service, unless any such application exists in the approved list.

Mobile Security allows or blocks the applications according to the following priority:

1. **Approved List**—Mobile Security allows applications that are in the approved list even if they use the services that you have disabled.
2. **Blocked List**—Mobile Security blocks applications that are in the blocked list even if they use the services that you have enabled.
3. **Application permissions**—Mobile Security allows or blocks applications according to your selected permission status for the services that they use.

- **Only allow the following applications**: add the applications to the approved list that you want to allow users to use on their mobile devices. If enabled:
  - Mobile Security displays a pop-up warning message on Android mobile devices if it detects applications that are not in the approved list.
  - On iOS mobile devices, if Mobile Security detects any application that is not in the approved list, Mobile Security sends an email notification to the user.
- **Only block the following applications**: add the applications to the blocked list that you do not want users to use on their mobile devices. If enabled:
  - Mobile Security displays a pop-up warning message on Android mobile devices if it detects applications that are in the blocked list.
  - On iOS mobile devices, if Mobile Security detects any application that is in the blocked list, Mobile Security sends an email notification to the user.

- **Lock to App (for Supervised Mode Only)**—restrict the iOS mobile device to the specified application.

Mobile Security checks for restricted applications and sends email alert to the users:

- automatically according to the **Information Collection Frequency** settings in **Administration** > **Communication Server Settings** > **Common Settings (tab)**, or
- when you update the **Information Collection Frequency** settings in **Administration** > **Communication Server Settings** > **Common Settings (tab)**.

Volume Purchasing Program Policy

This policy enables the administrator to import the iOS applications to the Mobile Security administration web console that are purchased through the Apple's Volume Purchase Program. Mobile Security will push all the applications in the Volume Purchasing Program List to mobile devices in a group.

To configure Volume Purchasing Program policy:

1. Add applications to the Enterprise App Store. See *Adding an Application on page 38-35* for the procedure.
2. Click **Policies**, then click the policy name, and then click **Volume Purchasing Program Policy**.
3. Click **Import** and then select applications to import from the Enterprise App Store.
4. Click **Save** to push all the applications to the iOS mobile devices.

Adding an Application

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store**.

   The **Enterprise App Store** screen displays.

2. Click the **Android** or **iOS** tab.

3. Click **Add**.

   The **Add Application** window displays.

4. You can now add an application to the list using one of the following options:

   - **Add from local computer**—select an installation file for Android or iOS mobile devices.

   - **Add a Webclip**—type the application's URL and the application's icon will appear on the home screen of user's mobile device, and the link will open in the default web browser on the mobile device.

   - (Android) **Add from external application store**—type the link to the application in an external app store. The application's icon will appear on the home screen of user's mobile device, and the link will open in the default web browser on the mobile device.

   - (iOS) **Please input search keyword**—type the name of the VPP application you want to search and select a country to search the application in its Apple app store, and then select the application you want to add from the search results. Once added, the VPP application is only available in the **App Store** on Mobile Security administration web console. To push the application to mobile devices, you will need to add the application to the **Volume Purchasing Program Policy**. See *Volume Purchasing Program Policy on page 38-34* for the procedure.

5. Click **Continue**.

The **Edit Application** screen displays.

6. Configure the following:

    - **Application name**: type a name for the application.
    - **Application icon**: if the application icon does not appear, click Upload app icon to select and upload the application icon.
    - **Application ID**: if the application ID does not appear, type the application ID.
    - **VPP codes file**: For iOS VPP application, upload the Volume Purchase Code files that you have received from Apple.
    - **Category**: select a category for the application.

      > **Note**
      >
      > You must select a category from the drop-down list. To add or delete a category, click the **Category** button.

    - **Description**: type the description for the application.
    - **Publish**: select one of the following:
        - **Do not publish**—to upload the application on the server, but keep hidden from the mobile devices.
        - **Publish as production version**—to upload the application on the server, and publish it for mobile devices to download.
        - **Publish as beta version**—to upload the application on the server, and publish it as a beta version for mobile devices to download.
    - **Screenshots**: select and upload application screenshots.

7. Click **Continue**.

    The application appears in the applications list.

Container Policy

This policy enables you to manage Samsung KNOX container security settings. You can configure approved list or blocked list for accounts, apply restrictions, and configure browser, password, and application settings.

Note

You must configure KNOX license in Mobile Security before enabling this policy. To configure the KNOX license, navigate to **Administration** > **Product License** on the administration web console.

- **Account Settings**: Specify accounts that can be added or restricted on Samsung KNOX containers by using approved and/or blocked lists.
- **Restriction Settings**: Disable camera or file sharing on Samsung KNOX containers.
- **Browser Settings**: Configure security settings for the native Android web browser on Samsung KNOX containers.
- **Password Settings**: Configure password security settings for Samsung KNOX container.
- **Application Settings**: Configure the following lists:
  - **Filter Applications List**: Configure approved list or blocked list to restrict applications installation on Samsung KNOX container.
  - **Required Applications**: Configure the required applications list to specify applications that must be installed on Samsung KNOX.
  - **Disable Applications**: Configure the disable applications list to disable certain applications on the mobile device. If the applications on this list are installed on the mobile device, they will not be removed, but the user will not be able to use these applications.

To configure container policy settings, click **Policies**, then click the policy name, and then click **Container Policy**.

Part XVII

Virtual Mobile Infrastructure Widgets

Chapter 39

Virtual Mobile Infrastructure Dashboard Widgets

This section contains help topics for the Virtual Mobile Infrastructure widgets supported in Apex Central.

Topics include:

Top 5 Trend Micro Virtual Mobile Infrastructure Launched Applications Widget

This widget displays the top five most launched applications reported by Trend Micro Virtual Mobile Infrastructure servers.

The data is shown in a bar chat. The y-axis displays the application name and the x-axis displays the amount of times the application was launched.

Change the managed server that the widget uses as its source by clicking the drop-down menu. In the drop-down menu options, select the IP address of the managed server to use as the source.

Top 5 Trend Micro Virtual Mobile Infrastructure Launched Web Applications Widget

This widget displays the top five launched web applications reported by Trend Micro Virtual Mobile Infrastructure servers.

The data is shown in a bar chat. The y-axis displays the application name and the x-axis displays the amount of times the application was launched.

Change the managed server that the widget uses as its source by clicking the drop-down menu. In the drop-down menu options, select the IP address of the managed server to use as the source.

Top 5 Trend Micro Virtual Mobile Infrastructure Online Users Widget

This widget displays the top five most active users who have accessed their workspace for the longest period of time reported by Trend Micro Virtual Mobile Infrastructure servers.

The data is shown in a bar chat. The y-axis displays the user name and the x-axis displays the time in minutes that the user accessed their workspace.

Change the managed server that the widget uses as its source by clicking the drop-down menu. In the drop-down menu options, select the IP address of the managed server to use as the source.

Trend Micro Virtual Mobile Infrastructure Server CPU Usage Status Widget

This widget displays the CPU usage of Trend MicroVirtual Mobile Infrastructure servers.

The data is shown in a graph. The y-axis represents the CPU usage as a percentage and the x-axis represents the time that the CPU usage was recorded.

Change the managed server that the widget uses as its source by clicking the drop-down menu. In the drop-down menu options, select the IP address of the managed server to use as the source.

Trend Micro Virtual Mobile Infrastructure Server Disk Usage Status Widget

This widget displays the disk usage of Trend Micro Virtual Mobile Infrastructure servers.

The following data is shown in a pie chart:

- **Free**: The amount of available disk storage on the managed server.
- **Used**: The amount of used disk storage on the managed server.
- **Total**: The amount of total disk storage on the managed server.

Change the managed server that the widget uses as its source by clicking the drop-down menu. In the drop-down menu options, select the IP address of the managed server to use as the source.

Trend Micro Virtual Mobile Infrastructure Server Memory Usage Status

This widget displays the memory usage of Trend Micro Virtual Mobile Infrastructure servers.

The following data is shown in a pie chart:

- **Free**: The amount of available memory on the managed server.
- **Used**: The amount of used memory on the managed server.
- **Total**: The amount of total memory on the managed server.

Change the managed server that the widget uses as its source by clicking the drop-down menu. In the drop-down menu options, select the IP address of the managed server to use as the source.

Trend Micro Virtual Mobile Infrastructure User Status Widget

This widget displays the current users' statuses reported by Trend Micro Virtual Mobile Infrastructure servers.

The following user statuses are shown in a pie chart:

- **Active**: The user is currently connected to the server and is accessing the workspace.
- **Idle**: The user is connected to the server and is not currently accessing the workspace.
- **Offline**: The user is disconnected from the server.
- **Disabled**: The user account has been disabled and the user cannot access the server.

Change the managed server that the widget uses as its source by clicking the drop-down menu. In the drop-down menu options, select the IP address of the managed server to use as the source.

Part XVIII

Vulnerability Protection Widgets

Chapter 40

Vulnerability Protection Dashboard Widgets

This section contains help topics for the Vulnerability Protection dashboard widgets supported in Apex Central.

Topics include:

Vulnerability Protection Application Type Activity (Detected) Widget

This widget tracks the Application Types associated with IPS (Detected) Events on the endpoint.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > ⚙) and select the source from the provided list.

Tip

This widget can only display data from a single Vulnerability Protection server. To monitor multiple Vulnerability Protection servers, create a new widget for each server.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's **Events** page, filtered to show the IPS (Detected) Events associated with the specific Application Type, click on a value in the **Totals** column.

Data	Description
Application Type Name	The name of the Application Type
Total	Number of Events in the time range and the percentage of the total Events of this type that it represents
Previous Total	Number of Events in the time period preceding the current time range

Data	Description
Trend	The percentage change from the previous to the current period

Vulnerability Protection Application Type Activity (Prevented) Widget

This widget tracks the Application Types associated with IPS (Prevented) Events on the endpoint.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > 🎚) and select the source from the provided list.

Tip

This widget can only display data from a single Vulnerability Protection server. To monitor multiple Vulnerability Protection servers, create a new widget for each server.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's **Events** page, filtered to show the IPS (Prevented) Events associated with the specific Application Type, click on a value in the **Totals** column.

Data	Description
Application Type Name	The name of the Application Type
Total	Number of Events in the time range and the percentage of the total Events of this type that it represents
Previous Total	Number of Events in the time period preceding the current time range
Trend	The percentage change from the previous to the current period

Vulnerability Protection Feature Summary Widget

This widget shows the recent activity of each of the Vulnerability Protection modules.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > 🎚) and select the source from the provided list.

Tip

This widget can display aggregated data from multiple Vulnerability Protection installations. The Vulnerability Protection installations represented in this widget are defined on the **Server Registration** screen. To monitor multiple Vulnerability Protection installations individually, create a new widget for each installation.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

Use the **Range** drop-down to select the time period for the data that displays.

Data	Description
Module	The name of the Vulnerability Protection module
Protected Computers	The current number of managed computers being protected by the module and the percentage of all managed computers that the number represents
Event Count	The number of Events generated by the module during the specified time period
Trend	The percentage change from the previous to the current period

Vulnerability Protection Firewall Event History Widget

This widget displays the number of Firewall Events that occur during a specified time range. The chart shows events triggered by Firewall Rules in both Detect and Prevent mode.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > 🎚) and select the source from the provided list.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's **Events** page, filtered to show the Firewall Events (Detect or Prevent) in the selected time range, click on a section of the bar chart.

Vulnerability Protection Intrusion Prevention Event History Widget

This widget displays the number of IPS Events that occurred over the specified time range. The chart displays Events triggered by IPS Rules in both Detect and Prevent mode.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > 🎚) and select the source from the provided list.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's **Events** page, filtered to show the IPS Events (Detect or Prevent) during a specific time range, click on a section of the bar chart.

Vulnerability Protection IPS Activity (Detected) Widget

This widget displays the five IPS Rules operating Detect mode that have triggered the greatest number of Events.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ >) and select the source from the provided list.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's **Events** page, filtered to show the IPS (Detected) Events triggered by the specific rule, click on a value in the **Totals** column.

Data	Description
Reason	The name of the Rule
Total	Number of Events in the time range and the percentage of the total Events of this type that it represents
Previous Total	Number of Events in the time period preceding the current time range
Trend	The percentage change from the previous to the current period

Vulnerability Protection IPS Activity (Prevented) Widget

This widget displays the five IPS Rules operating Prevent mode that have triggered the greatest number of events.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ >) and select the source from the provided list.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's **Events** page, filtered to show the IPS (Prevented) Events triggered by the specific rule, click on a value in the **Totals** column.

Data	Description
Reason	The name of the Rule
Total	Number of Events in the time range and the percentage of the total Events of this type that it represents
Previous Total	Number of Events in the time period preceding the current time range
Trend	The percentage change from the previous to the current period

Vulnerability Protection Key Performance Indicator Widget

This widget displays the number of Events triggered by Reconnaissance Scan detection settings that occurred over the specified time range.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > 🎚) and select the source from the provided list.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's **Events** page, filtered to show the Reconnaissance Scan detection Events during a specific time range, click on a section of the bar chart.

Vulnerability Protection Reconnaissance Scan Event History Widget

This widget displays the number of Events triggered by Reconnaissance Scan detection settings that occurred over the specified time range.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > 🎚) and select the source from the provided list.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's **Events** page, filtered to show the Reconnaissance Scan detection Events during a specific time range, click on a section of the bar chart.

Vulnerability Protection Status Summary Widget

This widget displays the number of Critical and Warning Alerts, as well as a pie chart indicating what percentage of endpoints are in a particular state.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > 🎛) and select the source from the provided list.

Tip

This widget can display aggregated data from multiple Vulnerability Protection installations. The Vulnerability Protection installations represented in this widget are defined on the **Server Registration** screen. To monitor multiple Vulnerability Protection installations individually, create a new widget for each installation.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

COMPUTER STATUS	DESCRIPTION
Managed (Green)	Protected and without errors or warnings
Unmanaged (Blue)	Not protected
Locked (Gray)	Locked. When a computer is in a locked state, the Vulnerability Protection Manager will not communicate with the Agent/Appliance or generate any computer-related alerts.
Critical (Red)	In an error state
Warning (Yellow)	In a warning state

Vulnerability Protection Vulnerable Endpoints Widget

Use this widget to track vulnerable endpoints.

You can choose which Vulnerability Protection installation to use as the data source for this widget. To select the data source, click the settings icon (⋮ > 🎚) and select the source from the provided list.

Tip

This widget can only display data from a single Vulnerability Protection server. To monitor multiple Vulnerability Protection servers, create a new widget for each server.

To make a Vulnerability Protection installation available to the Vulnerability Protection widgets, go to **Administration** > **Managed Servers** > **Server Registration** and add a new Vulnerability Protection server.

Note

The data displayed in the widgets are restricted to what is permitted by the user account privileges.

To display the Vulnerability Protection Manager's rule properties page, showing virtual patched/unprotected endpoints, click on a value in the **Virtual Patched/Unprotected** column.

Data	Description
Name	The name of the Intrusion Prevention rule
Severity	The severity level of the Intrusion Prevention rule
CVE	Common Vulnerabilities and Exposure (CVE) number
CVSS Score	A measure of the severity of the vulnerability according to the National Vulnerability Database

Data	Description
MS ID	Microsoft Security Patch ID
Virtual Patched	Number of endpoints that are assigned the rule after a scan for recommendations
Unprotected	Number of endpoints that are not assigned the rule after a scan for recommendations

Index

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: APEM09004/200609