TREND MICRO™

Trend Micro Apex One™(Mac) as a Service

Administrator's Guide

For Enterprise and Medium Business

for MAC

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/#Enterprise

Trend Micro, the Trend Micro t-ball logo, Apex One, Worry-Free, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: APEM09821/230828

Release Date: September 2023

Protected by U.S. Patent No.: Patents pending.

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

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

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

https://www.trendmicro.com/privacy

Table of Contents

Preface

Chapter 1: Introducing Apex One (Mac)

Chapter 2: Getting Started

Chapter 3: Installing the Security Agent

Chapter 4: Keeping Protection Up-to-Date

Chapter 5: Protecting Endpoints from Security Risks

Chapter 6: Protecting Endpoints from Web-based Threats

Chapter 7: Managing the Server and Security Agents

Chapter 8: Getting Help

Chapter 9: IPv6 Support in Apex One (Mac)

Appendix A: Product Terminology and Concepts

Index

Preface

Welcome to the Apex One (Mac) Administrator's Guide. This document discusses Apex One (Mac) server and agent installation, getting started information, and server and agent management.

Apex One (Mac) Documentation

Apex One (Mac) documentation includes the following:

Documentation	Description
Administrator's Guide	A PDF document that discusses Apex One (Mac) agent installation, getting started information, and server and agent management
Help	HTML files that provide "how to's", usage advice, and field-specific information
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the other documents.
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com

View and download product documentation at:

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

Audience

Apex One (Mac) documentation is intended for the following users:

- Apex One (Mac) administrators: Responsible for Apex One (Mac) management, including server and Security Agent installation and management. These users are expected to have advanced networking and server management knowledge.

- End users: Users who have the Apex One (Mac) Security Agent installed on their endpoints. The computer skill level of these individuals ranges from beginner to power user.

Document Conventions

To help you locate and interpret information easily, the Apex One (Mac) documentation uses the following conventions:

Table 1. Document Conventions

Convention	Description
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation or new technology components
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, `C:\Program Files\<file_name>` can be `C:\Program Files\sample.jpg`.
Note	Provides configuration notes or recommendations
Tip	Provides best practice information and Trend Micro recommendations
WARNING!	Provides warnings about activities that may harm endpoints on your network

Terminology

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

Terminology	Description
Agent or Security Agent	The Apex One (Mac) Security Agent program installed on an endpoint
Endpoint	The computer where the Security Agent is installed
Agent user (or user)	The person managing the Security Agent on the endpoint
Server	The Apex One (Mac) server program
Server computer	The computer where the Apex One (Mac) server is installed
Administrator (or Apex One (Mac) administrator)	The person managing the Apex One (Mac) server
Console	The user interface for configuring and managing Apex One (Mac) server and Security Agent settings The console for the server program is called "web console", while the console for the Security Agent program is called "agent console".
Security risk	The collective term for virus/malware, spyware/grayware, and web threats
Product service	The Apex One (Mac) service, which is managed from the Microsoft Management Console (MMC)
Components	Responsible for scanning, detecting, and taking actions against security risks
`Agent installation folder`	The folder on the endpoint that contains the Security Agent files `/Library/Application Support/TrendMicro`
Dual-stack	An entity that has both IPv4 and IPv6 addresses. For example: • A dual-stack endpoint is an endpoint with both IPv4 and IPv6 addresses. • A dual-stack agent refers to an agent installed on a dual-stack endpoint. • A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses.

Terminology	Description
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address

Chapter 1

Introducing Apex One (Mac)

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

About Apex One™ (Mac)

Apex One (Mac) protects Mac endpoints against security risks, blended threats, and platform independent web-based attacks. An integrated solution, Apex One (Mac) consists of the Security Agent program that resides at endpoints and a server program that manages all Security Agents. The Apex One (Mac) Security Agent guards an endpoint and reports its security status to the server. Administrators can manage and deploy updates to Security Agents through the web-based management console on the Apex One (Mac) server.

New in this Release

Apex One (Mac) includes the following new features and enhancements:

Table 1-1. September 2023

Feature/ Enhancement	Description
Agent notifications	This release of Apex One (Mac) enables administrators to customize the notification message to display on Security Agent endpoints after detecting a device control policy violation.

Table 1-2. January 2023

Feature/ Enhancement	Description
Enhanced policy information display	The Security Agent console has been enhanced to display the policy name and version on the **Component Versions** screen.

Table 1-3. November 2022

Feature/ Enhancement	Description
Platform support	The Apex One (Mac) Security Agent can now be installed on macOS 13 (Ventura) endpoints.
End of support for older macOS versions	The Apex One (Mac) Security Agent no longer supports endpoints running macOS 10.13 (High Sierra).

TABLE 1-4. August 2022

FEATURE/ ENHANCEMENT	DESCRIPTION
Apple® M2 support	The Apex One (Mac) Security Agent can now be installed on endpoints using Apple® M2 processors.

TABLE 1-5. January 2022

FEATURE/ ENHANCEMENT	DESCRIPTION
Platform support	The Apex One (Mac) Security Agent can now be installed on macOS™ 12 (Monterey) endpoints.
End of support for older macOS versions	The Apex One (Mac) Security Agent no longer supports endpoints running macOS 10.11 (El Capitan) and macOS 10.12 (Sierra).

Key Features and Benefits

Apex One (Mac) provides the following features and benefits:

TABLE 1-6. Key Features and Benefits

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

Feature	Benefits
Damage Cleanup Services	Damage Cleanup Services™ cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, viral files) through a fully-automated process. To address the threats and nuisances posed by Trojans, Damage Cleanup Services does the following: • Detects and removes live Trojans • Kills processes that Trojans create • Repairs system files that Trojans modify • Deletes files and applications that Trojans drop Because Damage Cleanup Services runs automatically in the background, it is not necessary to configure it. Users are not even aware when it runs. However, Apex One (Mac) may sometimes notify users to restart their endpoints to complete the process of removing a Trojan.
Security Risk Protection	Apex One (Mac) protects endpoints from security risks by scanning files and then performing a specific action on each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak. Apex One (Mac) notifies you of any outbreak so you can take immediate action, such as cleaning infected endpoints and isolating them until they are completely risk-free.
Web Reputation	Web Reputation technology proactively protects endpoints within or outside the corporate network from malicious and potentially dangerous websites. Web Reputation breaks the infection chain and prevents downloading of malicious code. Verify the credibility of websites and pages by integrating Apex One with the Smart Protection Server or the Trend Micro Smart Protection Network.
Centralized Management	A web-based management console gives administrators transparent access to all Security Agents on the network. The web console coordinates automatic deployment of security policies, pattern files, and software updates on every Security Agent. Administrators can perform remote administration and configure settings for individual agents or agent groups.

The Apex One (Mac) Server

The Apex One (Mac) server is the central repository for all Security Agent configurations, security risk logs, and updates.

The server performs two important functions:

- Monitors and manages Security Agents
- Downloads components needed by Security Agents. By default, the Apex One (Mac) server downloads components from the Trend Micro ActiveUpdate server and then distributes them to Security Agents.

Apex One (Mac) provides real-time, bidirectional communication between the server and Security Agents. Manage the Security Agents from a browser-based web console, which you can access from virtually anywhere on the network. The server communicates with the Security Agents through the ActiveMQ™ protocol.

The Apex One (Mac) Security Agent

Protect endpoints from security risks by installing the Apex One (Mac) Security Agent on each endpoint. The Security Agent provides three scan types:

- Real-time Scan
- Scheduled Scan
- Manual Scan

The Security Agent reports to the parent Apex One (Mac) server from which it was installed. The Security Agent sends events and status information to the server in real time. Security Agents communicate with the server through the ActiveMQ protocol.

Chapter 2

Getting Started

This chapter describes how to get started with Apex One (Mac) and initial configuration settings.

Getting Started Tasks

Getting Started Tasks provides a high-level overview of procedures required to get Apex One (Mac) up and running as quickly as possible.

Procedure

1. If a firewall is in use on the computer where you installed the Apex One (Mac) server, verify that the firewall does not block traffic through the listening port for agent-server communication.

   If the Apex One Security Agent firewall has been enabled on the computer, add a policy exception that allows incoming and outgoing traffic through the listening port.

2. Install the Apex One (Mac) Security Agent on endpoints.

   For more information, see *Installing the Security Agent on page 3-1*.

The Web Console

The web console is the central point for monitoring Security Agents and configuring settings to be deployed to Security Agents. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications.

Use the web console to do the following:

- Manage Security Agents installed on endpoints
- Organize Security Agents into logical groups for simultaneous configuration and management
- Initiate scanning on a single or multiple endpoints
- Configure security risk notifications and view logs sent by Security Agents
- Configure outbreak criteria and notifications

Opening the Web Console

You can access the Apex One (Mac) web console from the Apex Central web console.

Procedure

1. On the Apex Central web console, go to **Administration** > **Managed Servers** > **Server Registration**.
2. Click the server address for Apex One (Mac).

Security Summary

The **Summary** screen appears when you open the Apex One (Mac) web console or click **Summary** in the main menu.

Tip

Refresh the screen periodically to get the latest information.

Agents

The **Agents** section displays the following information:

- The connection status of all Security Agents with the Apex One (Mac) server. Clicking a link opens the agent tree where you can configure settings for the Security Agents.
- The number of detected security risks and web threats
- The number of endpoints with detected security risks and web threats. Clicking a number opens the agent tree displaying a list of endpoints with security risks or web threats. In the agent tree, perform the following tasks:
  - Select one or several Security Agents, click **Logs** > **Security Risk Logs**, and then specify the log criteria. In the screen that displays, check the **Results** column to see if the scan actions on the security risks were successfully carried out.

For a list of scan results, see *Scan Results on page 5-11*.

- Select one or several Security Agents, click **Logs** > **Web Reputation Logs**, and then specify the log criteria. In the screen that displays, check the list of blocked websites. You can add websites you do not want blocked to the list of approved URLs.

  For details, see *Configuring the Approved and Blocked URL Lists on page 6-3*.

Detection Status

The **Detection Status** table displays the total number of detections for security risks and web threats, and the number of affected endpoints.

Update Status

The **Update Status** table contains information about Apex One (Mac) components and the Security Agent program that protects endpoints from security risks.

Tasks in this table:

- Update outdated components immediately.

  For details, see *Launching Agent Update from the Summary Screen on page 4-7*.

- Upgrade agents to the latest program version or build if a new version is available.

The Agent Tree

The Apex One (Mac) agent tree displays all the Security Agents that the server currently manages. All Security Agents belong to a certain group. Use the menu items above the agent tree to simultaneously configure, manage, and apply the same configuration to all Security Agents belonging to a group.

Agent Tree General Tasks

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

Procedure

- Click the root icon () to select all groups and agents. When you select the root icon and then choose a task above the agent tree, a screen for configuring settings displays. On the screen, choose from the following general options:
    - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future group. Future groups are groups not yet created at the time you configure the settings.
    - **Apply to Future Groups Only**: Applies settings only to agents added to future groups. This option will not apply settings to new agents added to an existing group.
- To select multiple adjacent groups or agents, click the first group or agent in the range, hold down the SHIFT key, and then click the last group or agent in the range.
- To select a range of non-contiguous groups or agents, hold down the CTRL key and then click the groups or agents that you want to select.
- Search for an agent to manage by specifying a full or partial endpoint name in the **Search for endpoints** text box. A list of matching agent names will appear in the agent tree.
- Sort agents based on column information by clicking the column name.
- View the total number of agents below the agent tree.
- Click the **Export** button (Export) to export the list and status for agents from the agent tree, in a `csv.` format.

Agent Tree Specific Tasks

Above the agent tree are menu items that allow you perform the following tasks:

Menu Button	Task
Tasks	• Update agent components. For details, see *Agent Updates on page 4-4*. • Run Scan Now on endpoints. For details, see *Scan Now on page 5-4*.
Logs	View logs and reset statistics. • *Viewing Security Risk Logs on page 5-10* • *Viewing Web Reputation Logs on page 6-4* • *Viewing Scan Operation Logs on page 5-5* • *Viewing Device Control Logs on page 5-6* • *Resetting Security Risk Count on page 5-13*
Manage Agent Tree	Manage Apex One (Mac) groups. For details, see *Groups on page 2-6*.

Groups

A group in Apex One (Mac) is a set of agents that share the same configuration and run the same tasks. By organizing agents into groups, you can simultaneously configure, manage, and apply the same configuration to all agents belonging to the groups.

For ease of management, group agents based on their departments or the functions they perform. You can also group agents that are at a greater risk of infection to apply a more secure configuration to all of them. You can add or rename groups, move agents to a different group, move agents to another server, or remove agents permanently. An agent removed from the agent tree is not automatically uninstalled from the endpoint. The agent can still perform server-dependent tasks, such as updating components. However, the server is unaware of the existence of the agent and therefore cannot send configurations or notifications to the agent.

If the agent has been uninstalled from the endpoint, it is not automatically removed from the agent tree and its connection status is "Offline". Manually remove the agent from the agent tree.

Adding a Group

Procedure

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

   The new group appears in the agent tree.

Deleting a Group or Security Agent

Before you begin

Before deleting a group, check if there are Security Agents that belong to the group and then move the Security Agents to another group.

For details about moving agents, see *Moving Agents to Another Group on page 2-8*.

Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, select specific groups or Security Agents.
3. Click **Manage Agent Tree** > **Remove Group/Agent**.
4. Click **OK** to confirm the deletion.

Renaming a Group

Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, select the group to rename.
3. Click **Manage Agent Tree** > **Rename Group**.
4. Type a new name for the group.
5. Click **Rename**.

   The new group name appears in the agent tree.

Moving Security Agents

You can move Security Agents to another agent group or Apex One (Mac) server.

Moving Agents to Another Group

Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, select one or several agents.
3. Click **Manage Agent Tree** > **Move Agent**.
4. Select **Move selected agent(s) to another group**.
5. Select the group from the drop-down list.
6. Decide whether to apply the settings of the new group to the agents.

   Tip

   Alternatively, you can drag and drop the agents to another group in the agent tree.

7. Click **Move**.

Moving Security Agents to Another Server

Note

- You can move Security Agents only to another Trend Micro Apex One (Mac) server of the same version or later.
- If you are moving Security Agents from an on-premises Trend Micro Apex One (Mac) server to a Server as a Service (SaaS) server (or vice versa), ensure that Trend Micro Apex One (Mac) Security Agents can communicate with the server through the listening port and that no application is using the same port on the Security Agent endpoints.

  The following table shows the listening ports.

Table 2-1. Agent-server communication ports

Server Type	Listening Port
On-premises	• For Security Agent version 3.5.3xxx or later: 4343 • For Security Agent version 3.5.2xxx or earlier: 61617
SaaS	443

Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, select one or more Security Agents.
3. Click **Manage Agent Tree** > **Move Agent**.
4. Select **Move selected agent(s) to another server**.

5. Type the server name or address, and HTTPS port number.

6. Select **Force move offline agents** to move offline Security Agents to the specified server.

   Note

   If an offline Security Agent is not online after 7 days, the Security Agent remains on the original server and is not moved to the specified server.

7. Click **Move**.

Widgets

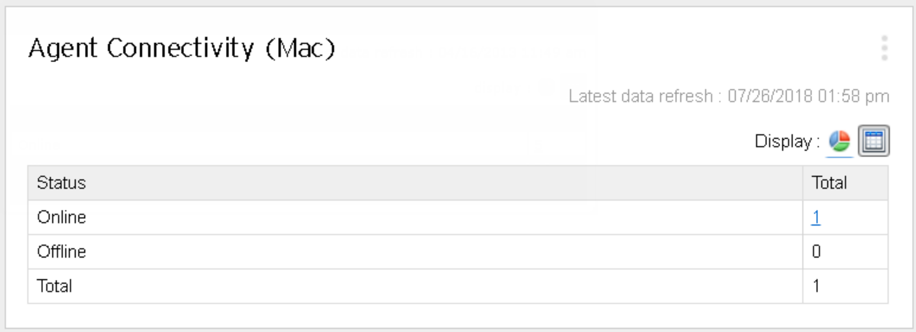
Manage Apex One (Mac) widgets on the Apex One dashboard. The widgets are available after activating Apex One (Mac).

For details on working with widgets, see the Apex One documentation.

Agent Connectivity (Mac) Widget

The Agent Connectivity (Mac) widget shows the connection status of agents with the Apex One (Mac) server. Data displays in a table and pie chart. You can switch between the table and pie chart by clicking the display icons (◕▦).

Agent Connectivity (Mac) Widget Presented as a Table



Agent Connectivity (Mac)

Latest data refresh : 07/26/2018 01:58 pm

Status	Total
Online	1
Offline	0
Total	1

FIGURE 2-1. Agent Connectivity (Mac) widget displaying a table

If the number of agents for a particular status is 1 or more, you can click the number to view the agents in the Apex One (Mac) agent tree. You can initiate tasks on these agents or change their settings.

Agent Connectivity (Mac) Widget Presented as a Pie Chart

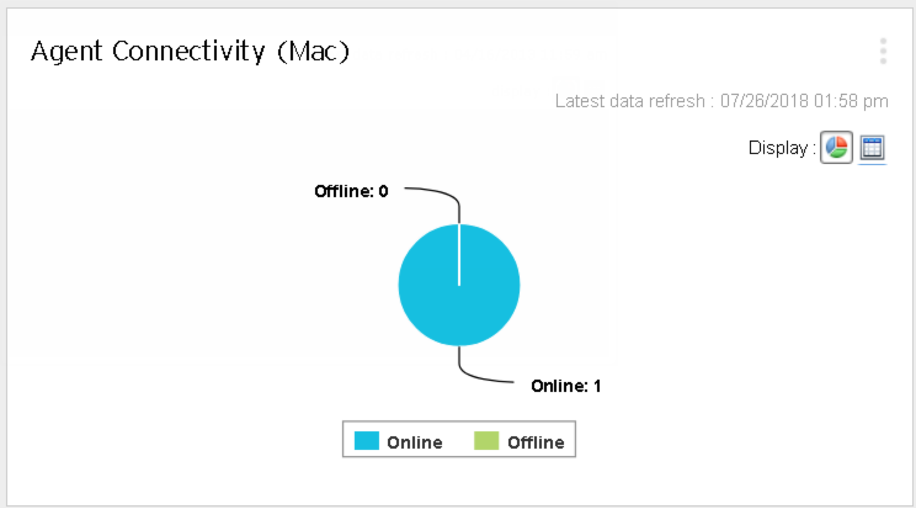
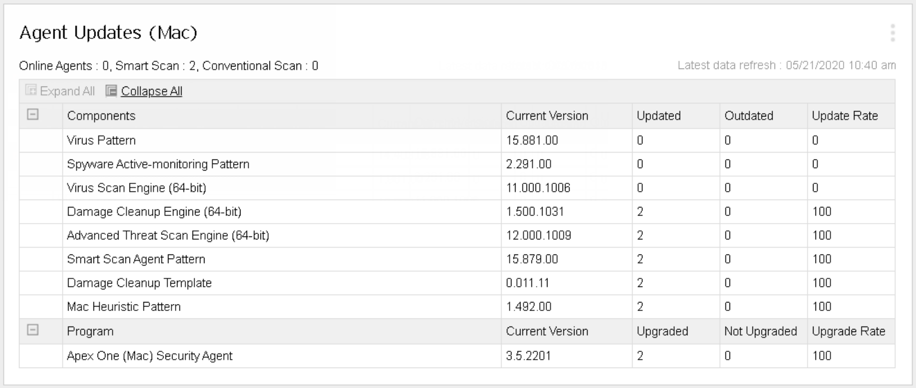


FIGURE 2-2. Agent Connectivity (Mac) widget displaying a pie chart

The pie chart shows the number of agents for each status but does not provide links to the Apex One (Mac) agent tree. Clicking a status separates it from, or re-connects it to, the rest of the pie.

Agent Updates (Mac) Widget

The Agent Updates (Mac) widget shows components and programs that protect endpoints from security risks.



Agent Updates (Mac)

Online Agents : 0, Smart Scan : 2, Conventional Scan : 0

Latest data refresh : 05/21/2020 10:40 am

	Components	Current Version	Updated	Outdated	Update Rate
	Virus Pattern	15.881.00	0	0	0
	Spyware Active-monitoring Pattern	2.291.00	0	0	0
	Virus Scan Engine (64-bit)	11.000.1006	0	0	0
	Damage Cleanup Engine (64-bit)	1.500.1031	2	0	100
	Advanced Threat Scan Engine (64-bit)	12.000.1009	2	0	100
	Smart Scan Agent Pattern	15.879.00	2	0	100
	Damage Cleanup Template	0.011.11	2	0	100
	Mac Heuristic Pattern	1.492.00	2	0	100
⊟	Program	Current Version	Upgraded	Not Upgraded	Upgrade Rate
	Apex One (Mac) Security Agent	3.5.2201	2	0	100

FIGURE 2-3. Agent Updates (Mac) widget

In this widget, you can:

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

Note

The links open the Apex One (Mac) server console, where you can perform additional tasks.

Security Risk Detections (Mac) Widget

The Security Risk Detections (Mac) widget shows the number of security risks and web threats.

If the number of infected endpoints is 1 or more, you can click the number to view the agents in the Apex One (Mac) agent tree. You can initiate tasks on these agents or change their settings.

Trend Micro Smart Protection

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

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

Smart Protection Services

Smart protection services include:

- **File Reputation Services**: File Reputation Services off-loads a large number of anti-malware signatures that were previously stored on agent endpoints to smart protection sources.
- **Web Reputation Services**: Web Reputation Services allows local smart protection sources to host URL reputation data that were previously hosted solely by Trend Micro. Both technologies ensure smaller bandwidth consumption when updating patterns or checking a URL's validity.

  For details, see *Web Reputation on page 6-2*.
- **Smart Feedback**: Trend Micro continues to harvest information sent from Trend Micro products worldwide to proactively determine each new threat.

For details, see *Smart Feedback on page 2-15*.

Smart Protection Sources

File Reputation Services and Web Reputation Services are delivered through **smart protection sources**, namely, **Trend Micro Smart Protection Network** and **Smart Protection Servers**.

Trend Micro Smart Protection Network is a globally scaled, Internet-based, infrastructure and is intended for users who do not have immediate access to their corporate network.

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

Smart Feedback

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

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

Samples of information sent to Trend Micro:

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

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

Tip

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

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Chapter 3

Installing the Security Agent

This chapter describes Security Agent installation requirements and methods.

Mac Platforms

The following are the requirements for installing the Security Agent on a Mac endpoint.

TABLE 3-1. Security Agent installation requirements

RESOURCE	REQUIREMENT
Operating system	• macOS™ Ventura 13 • macOS™ Monterey 12 • macOS™ Big Sur 11 • macOS™ Catalina 10.15 • macOS™ Mojave 10.14
Hardware	• **Processor**: Apple® M1, Apple® M2, or Intel® Core™ processor • **RAM**: 2GB minimum • **Available disk space**: 512MB minimum
Server-agent communication	Listening port: 443
Others	• Access to *.trendmicro.com • If required, proxy server settings for Internet connection

Agent Installation Methods and Setup Files

Note

Before installing Security Agents:

- Ensure that agent endpoints can communicate with the server through port 443
- Ensure that endpoints can access *.trendmicro.com
- If required, configure agent proxy server settings

You can install the Security Agent using one of the following ways:

- Install on a single endpoint by launching the installation package (`tmsminstall.zip`) on the endpoint
- Install on several endpoints by deploying an operating system image that includes the Security Agent. After installation, the Security Agent automatically registers to the Apex One (Mac) server.

Obtain the necessary agent installation package from the Apex One (Mac) server and copy it to the endpoint.

On the Apex One (Mac) web console, navigate to **Agents** > **Agent Setup Files** and click a link under **Agent Installation File**.

Note

The links to the Security Agent uninstallation packages are also available on this screen. Use these packages to remove the Security Agent program from endpoints. Choose the package according to the version of the Security Agent program that you wish to remove.

For information on uninstalling the Apex One (Mac) Security Agent, see *Security Agent Uninstallation on page 3-8*.

Agent Post-installation

Procedure

1. If this is the first time you install the Security Agent on an endpoint running a supported macOS™ version, the system displays the setup wizard that prompts you to allow the required permissions for the Security Agent to function. Follow the on-screen instruction to complete the settings.

   The setup wizard automatically skips the permission settings that are not required for your macOS version. Complete the installation procedure for your macOS version.

   For macOS 13:

a. Click **Open Privacy & Security** or access the Apple menu and go to **System Settings** > **Privacy & Security**.

b. Scroll to the **Security** section and click **Details**.

c. Provide your macOS administrator password and click **Unlock** to make changes.

d. Click the toggle switch to turn on all iCore Service entries and click **OK**.

e. Click **Allow** to allow the Security Agent to filter network content.

f. Click **Continue**.

g. Click **Open Full Disk Access** or access the Apple menu and go to **System Settings** > **Privacy & Security** > **Full Disk Access**.

h. Click **Open File Location** and locate the `com.trendmicro.icore.es.systemextension` file; then, drag and drop the file into the Full Disk Access table.

i. Click **Open File Location** and drag and drop `Apex One (Mac) Security Agent` from the Applications folder into the Full Disk Access table, click **Later** on the screen that appears.

j. Click **Open File Location** and locate the `iCore Service` file; then, drag and drop the file into the Full Disk Access table.

k. Click the toggle switch to turn on the following apps:

   - iCore Service
   - Apex One (Mac) Security Agent
   - Trend Micro Extension (if available)

l. Click **Continue**.

m. Restart the computer to make the changes take effect.

For macOS 10.14, 10.15, 11, and 12:

a. Click **Open Security & Privacy** or access the Apple menu and go to **System Preferences** > **Security & Privacy** > **General**.

b. Click the lock icon in the bottom left corner and provide your macOS administrator password to make changes.

c. Click **Allow** to install the Trend Micro certificate.

d. Click **Continue**.

e. On the **Security & Privacy** screen, click **Allow**.

f. Select all **Trend Micro Inc.** options and click **OK**.

g. Click **Allow** to allow the Security Agent to filter network content.

h. Click **Continue**.

i. On the **Security & Privacy** screen, select **Full Disk Access** from the list of services.

j. Click **Open File Location** and locate the `iCore Service` file; then, drag and drop the file into the Full Disk Access table.

k. Click **Open File Location** and drag and drop `Apex One (Mac) Security Agent` from the Applications folder into the Full Disk Access table.

l. Make sure the following apps are selected:

   - iCore Service
   - Apex One (Mac) Security Agent
   - Trend Micro Extension (if available)

m. Click **Continue**.

n. Restart the computer to make the changes take effect.

2. The system displays an alert notification prompting you to install and enable the Trend Micro Toolbar for Mac extension. Complete the following steps for your web browser:

   - Safari:

     a. On the alert notification window, click **Enable Extension**.

        The configuration overview screen appears.

    b. Click **Open Safari Extensions**.

    c. Select the **Trend Micro Toolbar for Mac** option to enable the extension.

- Firefox:

    a. On the alert notification window, click **Enable Extension**.

    The configuration overview screen appears.

    b. Click **Open File Location** to locate `Trend Micro Toolbar for Mac extension.xpi` file; then, drag and drop the file into the Firefox window to install the file.

    c. Click **Add** to install the Trend Micro Toolbar for Mac extension.

- (Required for macOS 11.0) Google Chrome:

    a. On the alert notification window, click **Enable Extension**.

    The configuration overview screen appears.

    b. Click **Open File Location** to locate and double-click `Trend Micro Toolbar For Mac (Chrome).mobileconfig` file.

    c. Click **Open Profiles**.

    d. On the Profiles screen, select `Trend Micro Toolbar for Mac (Chrome)` and click **Install ...**.

    e. Click **Install**.

    f. When prompted, type the macOS administrator password and click **OK**.

    g. Restart Google Chrome to make the changes take effect.

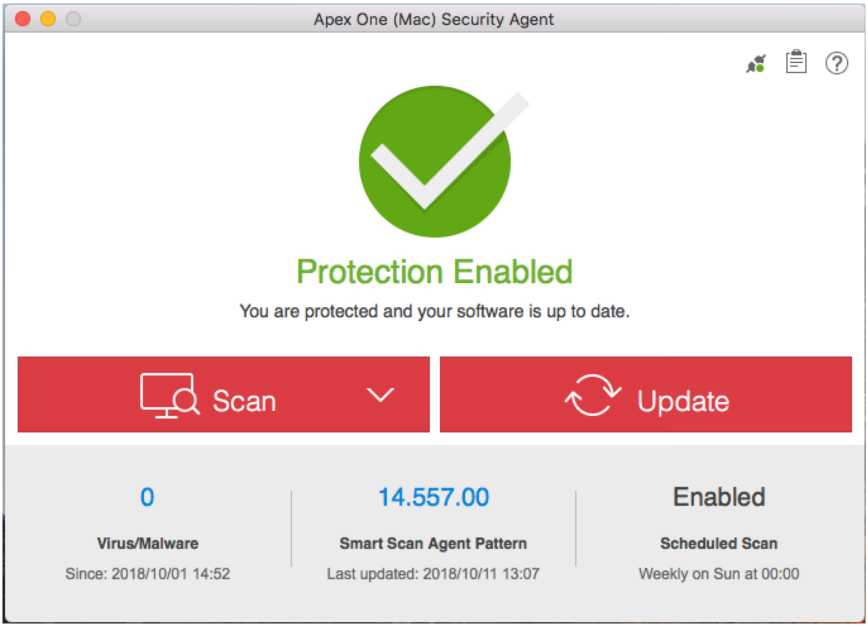
3. Verify the following:

- The Security Agent icon (●) displays on the menu bar of the endpoint.

- The Security Agent files are found under the `<Agent installation folder>`.

- The Security Agent appears on the web console's agent tree. To access the agent tree, click **Agent Management** on the main menu.

4. Update Apex One (Mac) components by clicking **Update** on the Security Agent console. The agent downloads components from the Apex One (Mac) server. For more information, see *Agent Updates on page 4-4*.



Protection Enabled

You are protected and your software is up to date.

0	14.557.00	Enabled
Virus/Malware	Smart Scan Agent Pattern	Scheduled Scan
Since: 2018/10/01 14:52	Last updated: 2018/10/11 13:07	Weekly on Sun at 00:00

If the Security Agent cannot connect to the Apex One (Mac) server, it downloads directly from the Trend Micro ActiveUpdate server. Internet connection is required to connect to the Apex One (Mac) and ActiveUpdate servers.

5. To start a manual scan on the endpoint, click **Scan** and choose one of the following scan options:

    - **Quick Scan**: Scans areas of the endpoint typically targeted by security risks. The pattern files on the Security Agent contain information on the endpoint areas to scan.

- **Custom Scan**: Scans the files or folders of your choice. Run custom scan on files or folders that you suspect to be infected.
- **Full Scan**: Scans all files, except encrypted and password-protected files.

What to do next

If there are problems with the Security Agent after installation, try uninstalling and then reinstalling the Security Agent.

Security Agent Uninstallation

Run the Security Agent uninstallation program to remove the Security Agent program from endpoints. Depending on your configuration, uninstallation may or may not require a password. If a password is required, ensure that you share the password only to users that will run the uninstallation program and then change the password immediately if it has been divulged to other users.

Note

Uninstall the Security Agent program only if you encounter problems with the program. Reinstall it immediately to keep the endpoint protected from security risks.

Uninstalling the Security Agent

Procedure

1. Obtain the Security Agent uninstallation package (`tmsmuninstall.zip`) from the Apex One (Mac) server.

   On the Apex One (Mac) web console, navigate to **Agents** > **Agent Setup** and click the link under **Agent Uninstallation File**.

2. Do one of the following:

- To uninstall the Security Agent from an endpoint, copy and then launch the uninstallation package on the endpoint.

  Note

  - If prompted, type the uninstallation password.
  - (For macOS 11.0 only) Click **Continue** to remove the system extensions.

- To silently uninstall the Security Agent from more than one endpoint and an uninstallation password is required, perform the following tasks:

  a. Click **Show Instruction**.

  b. Type the uninstallation password.

  c. Click **Generate Token**.

     The system generates and displays the password token on the screen.

  d. Click the icon to copy the generated token.

  e. Type the following command with the generated token to deploy the unintallation package.

     ```
     sudo ./TMUninstallLauncher.app/Contents/MacOS/
     TMUninstallLauncher --uninstall -token [password
     token]
     ```

What to do next

Unregister the Security Agent from the server.

1. On the web console, click **Agent Management** and select the Security Agent that was uninstalled.
2. Click **Manage Agent Tree** > **Remove Group/Agent**.

Chapter 4

Keeping Protection Up-to-Date

This chapter describes Apex One (Mac) components and update procedures.

Components

Apex One (Mac) makes use of components to keep endpoints protected from the latest security risks. Keep these components up-to-date by running manual or scheduled updates.

In addition to the components, Security Agents also receive updated configuration files from the Apex One (Mac) server. Security Agents need the configuration files to apply new settings. Each time you modify Apex One (Mac) settings through the web console, the configuration files change.

Component	Description
Agent Program	The Security Agent program provides the actual protection from security risks.
Advanced Threat Scan Engine (Universal)	The Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature-based, behavior-based, and aggressive heuristic detection.
Damage Cleanup Engine (Universal)	The Damage Cleanup Engine scans for and removes Trojans and Trojan processes.
Damage Cleanup Template	The Damage Cleanup Template is used by the Damage Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.
Mac Heuristic Pattern	The Mac Heuristic Pattern is used by Smart Scan to identify malware targeting Mac platforms.
Smart Scan Agent Pattern	The pattern file that the Security Agent uses to identify threats. This pattern file is stored on the agent endpoint.
Spyware Active-monitoring Pattern	The Spyware Active-monitoring Pattern contains information that helps Apex One (Mac) identify spyware and grayware.

Component	Description
Virus Scan Engine (Universal)	At the heart of all Trend Micro products lies the scan engine, which was originally developed in response to early file-based computer viruses. The scan engine today is exceptionally sophisticated and capable of detecting different types of security risks, including spyware. The scan engine also detects controlled viruses that are developed and used for research. By storing the most time-sensitive information about security risks in the pattern files, Trend Micro minimizes the number of scan engine updates while keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. Trend Micro releases new engines under the following circumstances: • Incorporation of new scanning and detection technologies into the software • Discovery of a new, potentially harmful security risk that the scan engine cannot handle • Enhancement of the scanning performance • Addition of file formats, scripting languages, encoding, and/or compression formats
Virus Pattern	The Virus Pattern contains information that helps Apex One (Mac) identify the latest virus/malware and mixed threat attack. Trend Micro creates and releases new versions of the Virus Pattern several times a week, and any time after the discovery of a particularly damaging virus/malware.

Update Overview

All component updates originate from the Trend Micro ActiveUpdate server. When updates are available, the Apex One (Mac) server downloads the updated components.

The Apex One (Mac) server automatically checks for and downloads updates from the Trend Micro ActiveUpdate server.

The following table describes the different component update options for the Apex One (Mac) server and Security Agents:

TABLE 4-1. Server-Agent Update Options

UPDATE OPTION	DESCRIPTION
ActiveUpdate server ↓ Apex One (Mac) server ↓ Security Agents	The Apex One (Mac) server receives updated components from the Trend Micro ActiveUpdate server and then deploys the components to agents.
ActiveUpdate server ↓ Security Agents	Security Agents receive updated components directly from the ActiveUpdate server if they cannot connect to the Apex One (Mac) server.

Agent Updates

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. For details, see *Launching Agent Update from the Agent Management Screen on page 4-7*. • Summary screen. For details, see *Launching Agent Update from the Summary Screen on page 4-7*.
Automatic update	After the server finishes an update, it immediately notifies Security Agents to update. For details, see *Configuring Agent Automatic Update on page 4-6*.
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.

Note

If an agent only has an IPv6 address, read the IPv6 limitations for agent updates in *Pure IPv6 Agent Limitations on page 9-2*.

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.

Configuring Agent Automatic Update

Automatic update relieves you of the burden of notifying all Security Agents to update and eliminates the risk of endpoints not having up-to-date components.

In addition to components, Apex One (Mac) Security Agents also receive updated configuration files during automatic update. Security Agents need the configuration files to apply new settings. Each time you modify Apex One (Mac) settings through the web console, the configuration files change.

The Apex One (Mac) server can notify online Security Agents to update components after it downloads the latest components, and offline Security Agents when they restart and then connect to the server. Optionally initiate **Scan Now** (manual scan) on Trend Micro Apex One (Mac) Security Agent endpoints after the update.

1. Click **Updates** > **Agent Automatic Update**.

2. Select the options.

TABLE 4-2. Event-triggered Update

OPTION	DESCRIPTION
Initiate component update on agents immediately after the server downloads a new component	The Apex One (Mac) server notifies Security Agents to update as soon as it completes an update.
Let agents initiate component update after restarting and connecting to the server	Any Security Agent that missed an update immediately downloads components when it establishes connection with the server. The Security Agent may miss an update if it is offline or if the endpoint where it is installed is not up and running.

Note

By default, update notifications are retained on the Trend Micro Apex One (Mac) server for up to seven days. Offline Security Agents will receive update notifications if the Security Agents are online within the seven-day period.

3. Click **Save**.

Launching Agent Update from the Summary Screen

For other agent update methods, see *Agent Updates on page 4-4*.

Procedure

1. Click **Summary** in the main menu.
2. Go to the **Update Status** section and click the link under the **Outdated** column.

   The agent tree opens, showing all the Security Agents that require an update.
3. Select the Security Agents that you want to update.
4. Click **Tasks** > **Update**.

   Security Agents that receive the notification start to update. On endpoints, the Apex One (Mac) icon on the menu bar indicates that the product is updating. Users cannot run any task from the console until the update is complete.

Launching Agent Update from the Agent Management Screen

For other agent update methods, see *Agent Updates on page 4-4*.

Procedure

1. Navigate to **Agent Management**.

2. In the agent tree, click the root domain icon () to include all Security Agents or select specific groups or Security Agents.

3. Click **Tasks** > **Update**.

   Security Agents that receive the notification start to update. On endpoints, the Apex One (Mac) icon on the menu bar indicates that the product is updating. Users cannot run any task from the console until the update is complete.

Chapter 5

Protecting Endpoints from Security Risks

This chapter describes how to protect endpoints from security risks using file-based scanning.

About Security Risks

Security risk includes viruses, malware, spyware, and grayware. Apex One (Mac) protects endpoints from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak, which Apex One (Mac) can help contain by enforcing outbreak prevention policies and isolating infected endpoints until they are completely risk-free. Notifications and logs help you keep track of security risks and alert you if you need to take immediate action.

Viruses and Malware

Tens of thousands of virus/malware exist, with more being created each day. Endpoint viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and websites.

Apex One (Mac) protects endpoints from the following virus/malware types:

Virus/Malware Types	Description
Joke program	A joke program is a virus-like program that often manipulates the appearance of things on an endpoint monitor.
Trojan horse program	A Trojan horse is an executable program that does not replicate but instead resides on endpoints to perform malicious acts, such as opening ports for hackers to enter. This program often uses Trojan ports to gain access to endpoints. An application that claims to rid an endpoint of viruses when it actually introduces viruses to the endpoint is an example of a Trojan program.

Virus/Malware Types	Description
Virus	A virus is a program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes. • **Boot sector virus**: A virus that infects the boot sector of a partition or a disk • **Java malicious code**: Operating system-independent virus code written or embedded in Java • **Macro virus**: A virus encoded as an application macro and often included in a document • **VBScript, JavaScript, or HTML virus**: A virus that resides on web pages and downloads through a browser • **Worm**: A self-contained program or set of programs able to spread functional copies of itself or its segments to other endpoints, often through email
Test virus	A test virus is an inert file that is detectable by virus scanning software. Use test viruses, such as the EICAR test script, to verify that the antivirus installation scans properly.
Packer	Packers are compressed and/or encrypted Windows or Linux™ executable programs, often a Trojan horse program. Compressing executables makes packers more difficult for antivirus products to detect.
Probable virus/ malware	Suspicious files that have some of the characteristics of virus/malware are categorized under this virus/malware type. For details about probable virus/malware, see the following page on the Trend Micro online Virus Encyclopedia: http://www.trendmicro.com/vinfo/virusencyclo/
Others	"Others" include viruses/malware not categorized under any of the virus/malware types.

Spyware and Grayware

Spyware and grayware refer to applications or files not classified as viruses or malware, but can still negatively affect the performance of the endpoints on the network. Spyware and grayware introduce significant security, confidentiality, and legal risks to an organization. Spyware/Grayware often performs a variety of undesired and threatening actions such as irritating users with pop-up windows, logging user keystrokes, and exposing endpoint vulnerabilities to attack.

Apex One (Mac) protects endpoints from the following spyware/grayware types:

Spyware/ Grayware Types	Description
Spyware	Spyware gathers data, such as account user names, passwords, credit card numbers, and other confidential information, and transmits it to third parties.
Adware	Adware displays advertisements and gathers data, such as web surfing preferences, used for targeting future advertising at the user.
Dialer	A dialer changes client Internet settings and can force an endpoint to dial pre-configured phone numbers through a modem. These are often pay-per-call or international numbers that can result in a significant expense for an organization.
Hacking tool	A hacking tool helps hackers enter an endpoint.
Remote access tool	A remote access tool helps hackers remotely access and control an endpoint.
Password cracking application	This type of application helps decipher account user names and passwords.
Others	"Others" include potentially malicious programs not categorized under any of the spyware/grayware types.

Scan Now

Scan Now is initiated remotely by a Apex One (Mac) administrator through the web console and can be run on one or several endpoints.

Initiate Scan Now on endpoints that you suspect to be infected.

Initiating Scan Now

Before you begin

All the Scheduled Scan settings in policies, except the actual schedule, are used during Scan Now. For more information about configuring policies, see the Apex Central documentation.

Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, click the root icon (●) to include all Security Agents or select specific groups or Security Agents.
3. Click **Tasks** > **Scan Now**.

Viewing Scan Operation Logs

When a Manual Scan or Scheduled Scan runs, the Apex One (Mac) Security Agent creates a scan log that contains information about the scan. You can view the scan log by accessing the Apex One (Mac) server or agent consoles.

Procedure

1. Navigate to **Agents** > **Agent Management**.
2. In the agent tree, click the root icon (●) to include all Security Agents or select specific groups or Security Agents.
3. Click **Logs** > **Scan Operation Logs**.
4. Specify the log criteria and click **Display Logs**.

   The **Scan Operation Logs** screen appears.
5. To save logs to a comma-separated value (CSV) file, click **Export**. Open the file or save it to a specific location.

What to do next

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Managing Logs on page 7-2*.

Viewing Device Control Logs

When a new storage device is connected to an endpoint, the Apex One (Mac) Security Agent creates a log entry for the event with the access permission based on the device control settings.

Procedure

1. Navigate to **Agents** > **Agent Management**.
2. In the agent tree, click the root icon ( ) to include all Security Agents or select specific groups or Security Agents.
3. Click **Logs** > **Device Control Logs**.
4. Specify the log criteria and then click **Display Logs**.

   The **Device Control Logs** screen appears.
5. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Security Risk Notifications and Logs

Apex One (Mac) comes with a set of default notification messages to inform you and other Apex One (Mac) administrators of detected security risks or any outbreak that has occurred.

Apex One (Mac) generates logs when it detects security risks.

Configuring Security Risk Notifications for Administrators

Configure Apex One (Mac) to send a notification when it detects a security risk, or only when the action on the security risk is unsuccessful and therefore requires your intervention.

You can receive notifications through email. Configure administrator notification settings to allow Apex One (Mac) to successfully send notifications through email.

Procedure

1. Navigate to **Notifications** > **Standard Notifications**.
2. In the **Criteria** tab, specify whether to send notifications each time Apex One (Mac) detects a security risk, or only when the action on the security risks is unsuccessful.
3. Click **Save**.
4. In the **Email** tab:
   a. Enable notifications to be sent through email.
   b. Specify the email recipients and accept or modify the default subject.

      Token variables are used to represent data in the **Message** field.

VARIABLE	DESCRIPTION
%v	Security risk name
%s	The endpoint where the security risk was detected
%m	Agent group name
%ii	Endpoint IP address
%nm	Endpoint MAC address
%p	Location of the security risk
%y	Date and time of detection
%a	Scan action performed

5. Click **Save**.

Configuring Outbreak Notifications for Administrators

Define an outbreak by the number of security risk detections and the detection period. After defining the outbreak criteria, configure Apex One (Mac) to notify you and other Apex One (Mac) administrators of an outbreak so you can respond immediately.

Procedure

1. Navigate to **Notifications** > **Outbreak Notifications**.

2. In the **Criteria** tab, specify the following:

   - Number of unique sources of security risks
   - Number of detections
   - Detection period

   Tip

   Trend Micro recommends accepting the default values in this screen.

   Apex One (Mac) declares an outbreak and sends a notification message when the number of detections is exceeded. For example, if you specify 10 unique sources, 100 detections, and a time period of 5 hours, Apex One (Mac) sends the notification when 10 different Security Agents have reported a total of 101 security risks within a 5-hour period. If all instances are detected on only one Security Agent within a 5- hour period, Apex One (Mac) does not send the notification.

3. Click **Save**.

4. In the **Email** tab:

   a. Enable notifications to be sent through email.

   b. Specify the email recipients and accept or modify the default subject.

      Token variables are used to represent data in the **Message** field.

Variable	Description
%CV	Total number of security risks detected
%CC	Total number of endpoints with security risks

5. Select additional information to include in the email. You can include the Security Agent or group name, security risk name, path and infected file, date and time of detection, and scan result.

6. Click **Save**.

Configuring Device Control Notifications for Security Agents

You can configure Apex One (Mac) to display notification messages on Security Agent endpoints to notify end users when device control violations occur.

Procedure

1. Navigate to **Notifications** > **Agent Notifications**.

2. Under **Device Control Violations**, accept or modify the default message.

   The following table describes the token variables you can use to represent data for notification message display.

Token	Description
%DeviceType%	Device type (for example, "USB storage device") for a Security Agent endpoint
%Permission%	Device Control policy setting (for example, "Block")

3. Click **Save**.

Viewing Security Risk Logs

Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, click the root icon () to include all Security Agents or select specific groups or Security Agents.
3. Click **Logs** > **Security Risk Logs**.
4. Specify the log criteria and click **Display Logs**.
5. View logs. Logs contain the following information:
    - Date and time of security risk detection
    - Endpoint with security risk
    - Security risk name
    - Security risk source
    - Scan type that detected the security risk
    - Scan results, which indicate whether scan actions were performed successfully. For details about scan results, see *Scan Results on page 5-11*.
    - Platform
6. To save logs to a comma-separated value (CSV) file, click **Export**. Open the file or save it to a specific location.

> **Note**
>
> If you are exporting a large number of logs, wait for the export task to finish. If you close the page before the export task is finished, the .csv file will not be generated.

What to do next

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Managing Logs on page 7-2*.

Scan Results

The following scan results display in the virus/malware logs:

- **Deleted**
  - First action is Delete and the infected file was deleted.
  - First action is Clean but cleaning was unsuccessful. Second action is Delete and the infected file was deleted.
- **Quarantined**
  - First action is Quarantine and the infected file was quarantined.
  - First action is Clean but cleaning was unsuccessful. Second action is Quarantine and the infected file was quarantined.
- **Cleaned**

  An infected file was cleaned.
- **Passed**
  - First action is Pass. Apex One (Mac) did not perform any action on the infected file.
  - First action is Clean but cleaning was unsuccessful. Second action is Pass so Apex One (Mac) did not perform any action on the infected file.
- **Unable to clean or quarantine the file**

  Clean is the first action. Quarantine is the second action, and both actions were unsuccessful.

  Solution: See “Unable to quarantine the file” below.
- **Unable to clean or delete the file**

Clean is the first action. Delete is the second action, and both actions were unsuccessful.

Solution: See “Unable to delete the file” below.

- **Unable to quarantine the file**

  The infected file may be locked by another application, is executing, or is on a CD. Apex One (Mac) will quarantine the file after the application releases the file or after it has been executed.

  Solution

  For infected files on a CD, consider not using the CD as the virus may infect other endpoints on the network.

- **Unable to delete the file**

  The infected file may be locked by another application, is executing, or is on a CD. Apex One (Mac) will delete the file after the application releases the file or after it has been executed.

  Solution

  For infected files on a CD, consider not using the CD as the virus may infect other endpoints on the network.

- **Unable to clean the file**

  The file may be uncleanable. For details and solutions, see *Uncleanable Files on page 5-12*.

Uncleanable Files

The Virus Scan Engine is unable to clean the following files:

Uncleanable File	Explanation and Solution
Files infected with worms	A computer worm is a self-contained program (or set of programs) able to spread functional copies of itself or its segments to other 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 files or compressed files. **Solution**: Remove the password protection for 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.

Resetting Security Risk Count

You can go to the **Reset Statistics** screen to reset the detection count for security risks back to zero.

Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, click the root icon () to include all Security Agents or select specific groups or Security Agents.
3. Click **Logs** > **Reset Statistics**.

Note

The **Security Risk** field displays the total detection count for the selected Security Agents, all Security Agents in the selected groups, or all Security Agents.

4. Click **Reset**.
5. Click **OK**.

Chapter 6

Protecting Endpoints from Web-based Threats

This chapter describes web-based threats and using Apex One (Mac) to protect your network and endpoints from web-based threats.

Web Threats

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, web threat creators constantly change the version or variant used. Because the web threat is in a fixed location of a website rather than on an infected endpoint, the web threat creator constantly modifies its code to avoid detection.

In recent years, individuals once characterized as hackers, virus writers, spammers, and spyware makers have become known as cyber criminals. Web threats help these individuals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is leakage of confidential information in the form of identity loss. The infected endpoint may also become a vector to deliver phish attacks or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in web commerce, corrupting the trust needed for Internet transactions. The second goal is to hijack a user's CPU power to use it as an instrument to conduct profitable activities. Activities include sending spam or conducting extortion in the form of distributed denial-of-service attacks or pay-per-click activities.

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™, and Google Chrome™ browsers.

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. Navigate to **Agents** > **Web Reputation Approved/Blocked URL List**.
2. 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.
3. Click **Add to Approved List** or **Add to Blocked List**.
4. To delete an entry, select an option from the **View** drop-down list and click the icon next to a URL.
5. Click **Save**.

Viewing Web Reputation Logs

Before you begin

Configure internal Security Agents to send Web Reputation logs to the server. Do this if you want to analyze URLs that Apex One (Mac) blocks and take appropriate actions on URLs you think are safe to access.

Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, click the root icon (●) to include all Security Agents or select specific groups or Security Agents.
3. Click **Logs** > **Web Reputation Logs**.
4. Specify the log criteria and click **Display Logs**.
5. View logs. Logs contain the following information:
   - Date/Time Apex One (Mac) blocked the URL
   - Endpoint where the user accessed the URL
   - Blocked URL
   - URL's risk level
   - Link to the Trend Micro Web Reputation Query system that provides more information about the blocked URL
6. To save logs to a comma-separated value (CSV) file, click **Export**. Open the file or save it to a specific location.

   Note

   If you are exporting a large number of logs, wait for the export task to finish. If you close the page before the export task is finished, the .csv file will not be generated.

What to do next

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule.

For more information about managing logs, see *Managing Logs on page 7-2*.

Chapter 7

Managing the Server and Security Agents

This chapter describes Apex One (Mac) server and agent management and additional configurations.

Enabling Certified Safe Software Service

The Certified Safe Software Service queries Trend Micro datacenters to verify the safety of a program detected by antivirus scans. Enable Certified Safe Software Service to reduce the likelihood of false positive detections.

Procedure

1. Navigate to **Agents** > **Global Agent Settings** > **Certified Safe Software Service**.
2. Select **Enable Certified Safe Software Service for antivirus scan**.
3. Click **Save**.

Managing Logs

Apex One (Mac) keeps comprehensive logs about security risk detections, blocked URLs, scan operations, and device control events. Use these logs to assess your organization's protection policies and to identify Security Agents that are at a higher risk of infection or attack.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule from the web console.

Procedure

1. Navigate to **Administration** > **Log Maintenance**.
2. Select **Enable scheduled deletion of logs**.
3. Select whether to delete all logs or only logs older than a certain number of days.
4. Specify the log deletion frequency and time.
5. Click **Save**.

Trend Micro Apex Central and Control Manager

Trend Micro Apex Central and Control Manager are central management consoles that manage Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The web-based management console provides a single monitoring point for managed products and services throughout the network.

Apex Central and Control Manager allow system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Apex Central and Control Manager allow both manual and pre-scheduled updates, and the configuration and administration of products as groups or as individuals for added flexibility.

Apex Central Policies

You can create, manage, and deploy Apex One (Mac) policies and monitor endpoints from Apex Central.

The following are the policy configurations available:

- Manual Scan Settings
- Real-time Scan Settings
- Scan Exclusion Settings
- Cache Settings for Scans
- Scheduled Scan Settings
- Update Settings
- Web Reputation Settings
- Agent Self-protection Settings
- Scan Method Settings
- Endpoint Sensor Settings (Apex Central only)

- Device Control Settings (Apex Central only)
- Trusted Program List Settings (Apex Central only)
- Predictive Machine Learning Settings (Apex Central only)

You can monitor endpoints using the **Apex One (Mac) Key Performance Indicators** widget in Apex Central.

For details, see *Key Performance Indicators Widget on page 7-4*.

See the Apex Central documentation for details.

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 Server Connection Settings

Specify the Apex Central server to obtain data for widget display.

1. Go to the **Dashboard** screen on Apex Central.
2. Click the tab on which the **Apex One (Mac) Key Performance Indicators** widget is added.
3. Select the **Server Settings** icon (▤) from the top-right menu (⋮) of the widget.
4. Select one or more Apex One (Mac) servers.
5. Click **Save**.

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 7-1. 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**.
Delete an indicator	1. Click the indicator in the list. The **Edit Indicator** screen appears. 2. Click **Delete**. 3. Click **OK**.

Task	Steps
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 7-2. 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.

Inactive Security Agents

Apex One (Mac) displays Security Agents as inactive:

- If you use the agent uninstallation program to remove the agent program from the endpoints but do not unregister the Security Agent from the server.
- If you reformatted the endoint hard drive without unregistering the Security Agent from the server.
- If you manually removed the agent files.
- If a user unloads or disables the Security Agent for an extended period of time.

To have the agent tree display active Security Agents only, configure Apex One (Mac) to automatically remove inactive Security Agents from the agent tree.

Automatically Removing Inactive Security Agents

Procedure

1. Go to **Administration** > **Inactive Agents**.
2. Select **Enable automatic removal of inactive agents**.
3. Select how many days should pass before Apex One (Mac) considers the Security Agent inactive.

4. Click **Save**.

Agent Icons

Icons on the endpoint's system tray and main console indicate the agent's status and the task it is currently running.

Tray Icon	Menu Icon	Description
●	✓	The Security Agent is up and running and is connected to its parent server.
	✓	The product license has been activated.
	!	The Security Agent is up and running but is disconnected from its parent server.
	!	A new component version is available. Update the Security Agent immediately.
	✕	The Security Agent has detected a security threat that requires a computer restart to fix.
🔍	ℹ	The Security Agent is scanning for security risks and is connected to its parent server.
🔄	ℹ	The Security Agent is updating components from its parent server.
● ⚠	ℹ	A component update requires you to restart the Security Agent to finish installation.
	!	Smart Scan or Web Reputation service is not available on the Security Agent. Check your network connection.
	✕	The Security Agent has been registered to its parent server but the product license has not been activated. Some Security Agent features will not be available if the license has not been activated.

Tray Icon	Menu Icon	Description
	⊗	The Security Agent has not been registered to its parent server. The product license may or may not have been activated. If the Security Agent is not registered to its parent server, all functions (including Real-Time Scan, Manual Scan, Scheduled Scan, Web Reputation, and pattern updates) are disabled.
	⊗	The product license (full or evaluation version) has been activated but has expired. Some Security Agent features will not be available if the license has expired.
	⊗	The Security Agent has been installed on an unsupported platform.
	⊗	The Security Agent is not functioning properly. Upgrade the Security Agent to the latest release or contact technical support.
	⊗	The Security Agent has completed a scan or has detected a security threat.

Chapter 8

Getting Help

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

Troubleshooting

Web Console Access

Problem:

The web console cannot be accessed.

Procedure

1. Verify that you have typed the correct user name and password.
2. Contact your service providor if the problem persists.

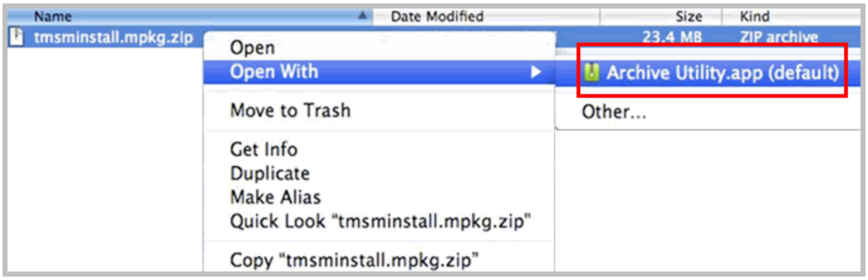
Agent Installation

Problem:

The installation was unsuccessful. The installation package (`tmsminstall.zip` or `tmsminstall.mpkg.zip`) was launched using an archiving tool not built-in on the Mac or through an unsupported command (such as `unzip`) issued from a command-line tool, causing the extracted folder (`tmsminstall`) or file (`tmsminstall.mpkg`) to become corrupted.

Procedure

1. Remove the extracted folder (`tmsminstall`) or file (`tmsminstall.mpkg`).
2. Launch the installation package again using a built-in archiving tool such as Archive Utility.



You can also launch the package from the command line by using the following command:

- If the package is `tmsminstall.zip`:

  ```
  ditto -xk <tmsminstall.zip file path> <destination
  folder>
  ```

  For example:

  ```
  ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/
  Desktop
  ```

- If the package is `tmsminstall.mpkg.zip`:

  ```
  ditto -xk <tmsminstall.mpkg.zip file path> <destination
  folder>
  ```

  For example:

  ```
  ditto -xk users/mac/Desktop/tmsminstall.mpkg.zip
  users/mac/Desktop
  ```

General Agent Error

Problem:

An error or problem was encountered on the Security Agent.

Procedure

1. Open `<agent installation folder>/Tools` and launch Trend Micro Debug Manager.
2. Follow the on-screen instructions in the tool to successfully collect data.

WARNING!

The tool will not work if a user moves it to a different location on the endpoint. If the tool has been moved, uninstall and then install the Security Agent.

If the tool was copied to another location, remove the copied version and then run the tool from its original location.

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 8-4*
- *Contacting Trend Micro on page 8-5*
- *Sending Suspicious Content to Trend Micro on page 8-6*
- *Other Resources on page 8-7*

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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

Tip

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

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

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

Threat Encyclopedia

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

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

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

Contacting Trend Micro

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

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.

Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

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

- Trend Micro product documentation:

  https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

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

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

Chapter 9

IPv6 Support in Apex One (Mac)

This appendix is required reading for users who plan to deploy Apex One (Mac) in an environment that supports IPv6 addressing. This appendix contains information on the extent of IPv6 support in Apex One (Mac).

Trend Micro assumes that the reader is familiar with IPv6 concepts and the tasks involved in setting up a network that supports IPv6 addressing.

Apex One (Mac) Security Agent IPv6 Requirements

All Mac OS X versions supported by the Apex One (Mac) Security Agent also support IPv6.

It is preferable for the Security Agent to have both IPv4 and IPv6 addresses as some of the entities to which it connects only support IPv4 addressing.

Pure IPv6 Agent Limitations

The following table lists the limitations when Security Agents only have an IPv6 address.

Table 9-1. 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 IPv6 Addresses

The web console allows you to configure an IPv6 address or an IPv6 address range. The following are some configuration guidelines.

- Apex One (Mac) accepts standard IPv6 address presentations.

  For example:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- Apex One (Mac) also accepts link-local IPv6 addresses, such as:

  `fe80::210:5aff:feaa:20a2`

WARNING!

Exercise caution when specifying a link-local IPv6 address because even though Apex One (Mac) can accept the address, it might not work as expected under certain circumstances. For example, agents cannot update from an update source if the source is on another network segment and is identified by its link-local IPv6 address.

- When the IPv6 address is part of a URL, enclose the address in square brackets.
- For IPv6 address ranges, a prefix and prefix length are usually required.

Screens That Display IP Addresses

The agent tree displays the IPv6 addresses of agents under the **IPv6 Address** column.

Appendix A

Product Terminology and Concepts

The items contained in this appendix provide further information about Trend Micro products and technologies.

IntelliScan

IntelliScan is a method of identifying files to scan. For executable files (for example, `.exe`), the true file type is determined based on the file content. For non-executable files (for example, `.txt`), the true file type is determined based on the file header.

Using IntelliScan provides the following benefits:

- Performance optimization: IntelliScan does not affect applications on the endpoint because it uses minimal system resources.
- Shorter scanning period: Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

Uncleanable Files

The Virus Scan Engine is unable to clean the following files:

Uncleanable File	Explanation and Solution
Files infected with worms	A computer worm is a self-contained program (or set of programs) able to spread functional copies of itself or its segments to other 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 files or compressed files. **Solution**: Remove the password protection for the Security Agent to clean these files.

Uncleanable File	Explanation and Solution
Backup files	Files with the RB0~RB9 extensions are backup copies of infected files. The Security Agent creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process. **Solution**: If the Security Agent successfully cleans the infected file, you do not need to keep the backup copy. If the endpoint functions normally, you can delete the backup file.

Index

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: APEM09821/230828