



# TREND MICRO™ Security as a Service

## Administrator's Guide

For Enterprise and Medium Business

for MAC®



Endpoint Security



Protected Cloud



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/trend-micro-security-\(for-mac\).aspx](http://docs.trendmicro.com/en-us/enterprise/trend-micro-security-(for-mac).aspx)

Trend Micro, the Trend Micro t-ball logo, OfficeScan, 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.

Copyright © 2017. Trend Micro Incorporated. All rights reserved.

Document Part No.: TSEM08095/171121

Release Date: November 2017

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](mailto:docs@trendmicro.com).

Evaluate this documentation on the following site:

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



# Table of Contents

## Preface

Preface .....	v
Trend Micro Security (for Mac) Documentation .....	v
Audience .....	v
Document Conventions .....	vi
Terminology .....	vii

## Chapter 1: Introducing Trend Micro Security (for Mac)

About .....	1-2
Key Features and Benefits .....	1-2
The Trend Micro Security (for Mac) Server .....	1-4
The Trend Micro Security (for Mac) Agent .....	1-5

## Chapter 2: Getting Started

The Web Console .....	2-2
Security Summary .....	2-2
The Agent Tree .....	2-3
Agent Tree General Tasks .....	2-4
Agent Tree Specific Tasks .....	2-5
Groups .....	2-5
Adding a Group .....	2-6
Deleting a Group or Agent .....	2-6
Renaming a Group .....	2-7
Moving Agents .....	2-7
Widgets .....	2-8
Agent Connectivity (Mac) Widget .....	2-9
Agent Updates (Mac) Widget .....	2-11
Security Risk Detections (Mac) Widget .....	2-12

Trend Micro Smart Protection .....	2-12
Smart Feedback .....	2-13

### **Chapter 3: Installing the Trend Micro Security (for Mac) Agent**

Trend Micro Security (for Mac) Agent System Requirements .....	3-2
Agent Installation Methods and Setup Files .....	3-3
Agent Post-installation .....	3-4
Agent Uninstallation .....	3-5

### **Chapter 4: Keeping Protection Up-to-Date**

Components .....	4-2
Update Overview .....	4-3
Agent Updates .....	4-4
Configuring Agent Automatic Update .....	4-6
Launching Agent Update from the Summary Screen .....	4-7
Launching Agent Update from the Agent Management Screen .....	4-7

### **Chapter 5: Protecting Endpoints from Security Risks**

About Security Risks .....	5-2
Viruses and Malware .....	5-2
Spyware and Grayware .....	5-4
Scan Now .....	5-5
Initiating Scan Now .....	5-5
Viewing Scan Operation Logs .....	5-5
Security Risk Notifications and Logs .....	5-6
Configuring Security Risk Notifications for Administrators .....	5-6
Configuring Outbreak Notifications for Administrators .....	5-7
Viewing Security Risk Logs .....	5-9
Resetting Security Risk Count .....	5-12

## Chapter 6: Protecting Endpoints from Web-based Threats

Web Threats .....	6-2
Web Reputation .....	6-2
Configuring the Approved and Blocked URL Lists .....	6-3
Viewing Web Reputation Logs .....	6-4

## Chapter 7: Managing the Server and Agents

Enabling Certified Safe Software Service .....	7-2
Managing Logs .....	7-2
Trend Micro Control Manager .....	7-3
Control Manager Integration in this Release .....	7-3
Key Performance Indicators Widget .....	7-4
Inactive Agents .....	7-7
Automatically Removing Inactive Agents .....	7-7
Agent Icons .....	7-7

## Chapter 8: Getting Help

Troubleshooting .....	8-2
Web Console Access .....	8-2
Agent Installation .....	8-2
General Agent Error .....	8-3
Technical Support .....	8-4
Troubleshooting Resources .....	8-4
Contacting Trend Micro .....	8-5
Sending Suspicious Content to Trend Micro .....	8-7
Other Resources .....	8-8

## Chapter 9: IPv6 Support in Trend Micro Security (for Mac)

Trend Micro Security (for Mac) Agent IPv6 Requirements .....	9-2
Pure IPv6 Agent Limitations .....	9-2
Configuring IPv6 Addresses .....	9-3

Screens That Display IP Addresses ..... 9-3

## **Appendix A: Product Terminology and Concepts**

IntelliScan ..... A-2  
Uncleanable Files ..... A-2

## **Index**

Index ..... IN-1



## Preface

Welcome to the Trend Micro Security (for Mac) Online Help. This document discusses Trend Micro Security (for Mac) agent installation, getting started information, and server and agent management.

## Trend Micro Security (for Mac) Documentation

Trend Micro Security (for Mac) documentation includes the following:

DOCUMENTATION	DESCRIPTION
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: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a>

View and download product documentation at:

[http://docs.trendmicro.com/en-us/enterprise/trend-micro-security-\(for-mac\).aspx](http://docs.trendmicro.com/en-us/enterprise/trend-micro-security-(for-mac).aspx)

## Audience

Trend Micro Security (for Mac) documentation is intended for the following users:




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

- End users: Users who have the Trend Micro Security (for Mac) 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 Trend Micro Security (for 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
<b>Bold</b>	Menus and menu commands, command buttons, tabs, options, and tasks
<i>Italics</i>	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.
 <b>Note</b>	Provides configuration notes or recommendations
 <b>Tip</b>	Provides best practice information and Trend Micro recommendations
 <b>WARNING!</b>	Provides warnings about activities that may harm endpoints on your network

# Terminology

The following table provides the official terminology used throughout the Trend Micro Security (for Mac) documentation:

<b>TERMINOLOGY</b>	<b>DESCRIPTION</b>
Agent	The Trend Micro Security (for Mac) agent program installed on an endpoint
Endpoint	The computer where the agent is installed
Agent user (or user)	The person managing the agent on the endpoint
Server	The Trend Micro Security (for Mac) server program
Server computer	The computer where the Trend Micro Security (for Mac) server is installed
Administrator (or Trend Micro Security (for Mac) administrator)	The person managing the Trend Micro Security (for Mac) server
Console	The user interface for configuring and managing Trend Micro Security (for Mac) server and agent settings  The console for the server program is called "web console", while the console for the agent program is called "agent console".
Security risk	The collective term for virus/malware, spyware/grayware, and web threats
Product service	The Trend Micro Security (for 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 Trend Micro Security (for Mac) agent files  <code>/Library/Application Support/TrendMicro</code>

<b>TERMINOLOGY</b>	<b>DESCRIPTION</b>
Server installation folder	<p>The folder on the server computer that contains the Trend Micro Security (for Mac) server files. After installing Trend Micro Security (for Mac) server, the folder is created on the same OfficeScan server directory.</p> <p>If you accept the default settings during OfficeScan server installation, you will find the server installation folder at any of the following locations:</p> <ul style="list-style-type: none"><li>• C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM</li><li>• C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\TMSM</li></ul>
Dual-stack	<p>An entity that has both IPv4 and IPv6 addresses. For example:</p> <ul style="list-style-type: none"><li>• A dual-stack endpoint is an endpoint with both IPv4 and IPv6 addresses.</li><li>• A dual-stack agent refers to an agent installed on a dual-stack endpoint.</li><li>• A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses.</li></ul>
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address

# Chapter 1

## Introducing Trend Micro Security (for Mac)

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

## About

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

## Key Features and Benefits

Trend Micro Security (for Mac) provides the following features and benefits:

**TABLE 1-1. Key Features and Benefits**

FEATURE	BENEFITS
Smart Scan	Trend Micro Security (for 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.

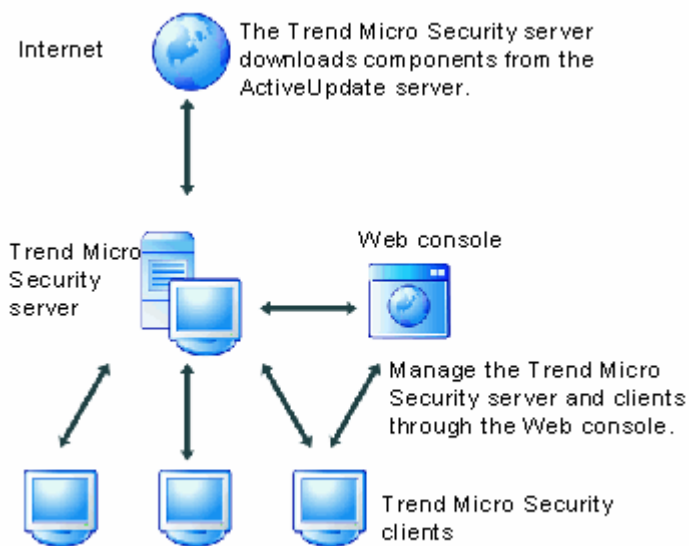
FEATURE	BENEFITS
Damage Cleanup Services	<p>Damage Cleanup Services™ cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, viral files) through a fully-automated process. To address the threats and nuisances posed by Trojans, Damage Cleanup Services does the following:</p> <ul style="list-style-type: none"> <li>• Detects and removes live Trojans</li> <li>• Kills processes that Trojans create</li> <li>• Repairs system files that Trojans modify</li> <li>• Deletes files and applications that Trojans drop</li> </ul> <p>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, Trend Micro Security (for Mac) may sometimes notify users to restart their endpoints to complete the process of removing a Trojan.</p>
Security Risk Protection	<p>Trend Micro Security (for 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. Trend Micro Security (for 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.</p>
Web Reputation	<p>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.</p> <p>Verify the credibility of websites and pages by integrating OfficeScan with the Smart Protection Server or the Trend Micro Smart Protection Network.</p>
Centralized Management	<p>A web-based management console gives administrators transparent access to all agents on the network. The web console coordinates automatic deployment of security policies, pattern files, and software updates on every agent. Administrators can perform remote administration and configure settings for individual agents or agent groups.</p>

## The Trend Micro Security (for Mac) Server

The Trend Micro Security (for Mac) server is the central repository for all agent configurations, security risk logs, and updates.

The server performs two important functions:

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



**FIGURE 1-1. How the Trend Micro Security (for Mac) server works**

Trend Micro Security (for Mac) provides real-time, bidirectional communication between the server and agents. Manage the agents from a browser-based web console,



which you can access from virtually anywhere on the network. The server communicates with the agent through the ActiveMQ™ protocol.

## The Trend Micro Security (for Mac) Agent

Protect endpoints from security risks by installing the Trend Micro Security (for Mac) agent on each endpoint. The agent provides three scan types:

- Real-time Scan
- Scheduled Scan
- Manual Scan

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



# Chapter 2

## Getting Started

This chapter describes how to get started with Trend Micro Security (for Mac) and initial configuration settings.

## The Web Console

The web console is the central point for monitoring Trend Micro Security (for Mac) agents and configuring settings to be deployed to 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 agents installed on endpoints
- Organize 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 agents
- Configure outbreak criteria and notifications

## Security Summary

The **Summary** screen appears when you open the Trend Micro Security (for 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 agents with the Trend Micro Security (for Mac) server. Clicking a link opens the agent tree where you can configure settings for the 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 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 5-10*.

- Select one or several 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 Trend Micro Security (for Mac) components and the 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 Trend Micro Security (for Mac) agent tree displays all the agents that the server currently manages. All 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 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 () 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
<b>Tasks</b>	<ul style="list-style-type: none"> <li>• Update agent components. For details, see <a href="#">Agent Updates on page 4-4</a>.</li> <li>• Run Scan Now on endpoints. For details, see <a href="#">Scan Now on page 5-5</a>.</li> </ul>
<b>Logs</b>	View logs and reset statistics. <ul style="list-style-type: none"> <li>• <a href="#">Viewing Security Risk Logs on page 5-9</a></li> <li>• <a href="#">Viewing Web Reputation Logs on page 6-4</a></li> <li>• <a href="#">Viewing Scan Operation Logs on page 5-5</a></li> <li>• <a href="#">Resetting Security Risk Count on page 5-12</a></li> </ul>
<b>Manage Agent Tree</b>	Manage Trend Micro Security (for Mac) groups. For details, see <a href="#">Groups on page 2-5</a> .

## Groups

A group in Trend Micro Security (for 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 Agent

### Before you begin

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

For details about moving agents, see [Moving Agents to Another Group on page 2-7](#).

---

### Procedure

1. Navigate to **Agent Management**.
  2. In the agent tree, select specific groups or 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 Agents

You can move agents to another group or Trend Micro Security (for 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 an Agent to Another Server

---



### Note

You can move agents only to another Trend Micro Security (for Mac) server of the same version or later.

---

### Procedure

1. Navigate to **Agent Management**.
  2. In the agent tree, select one or more 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 agents to the specified server.
- 



### Note

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

---

7. Click **Move**.
- 

## Widgets

Manage Trend Micro Security (for Mac) widgets on the OfficeScan dashboard. The widgets are available after activating Trend Micro Security (for Mac).

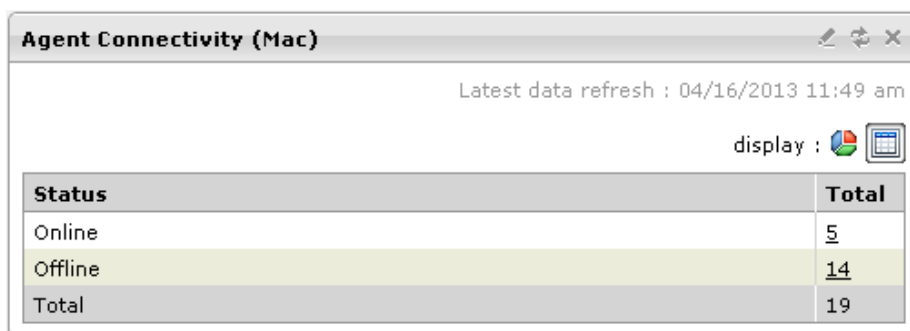
To view widgets, be sure that the OfficeScan version is 10.6 SP2 or later and the Plug-in Manager version is 1.5 or later.

For details on working with widgets, see the OfficeScan documentation.

## Agent Connectivity (Mac) Widget

The Agent Connectivity (Mac) widget shows the connection status of agents with the Trend Micro Security (for 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



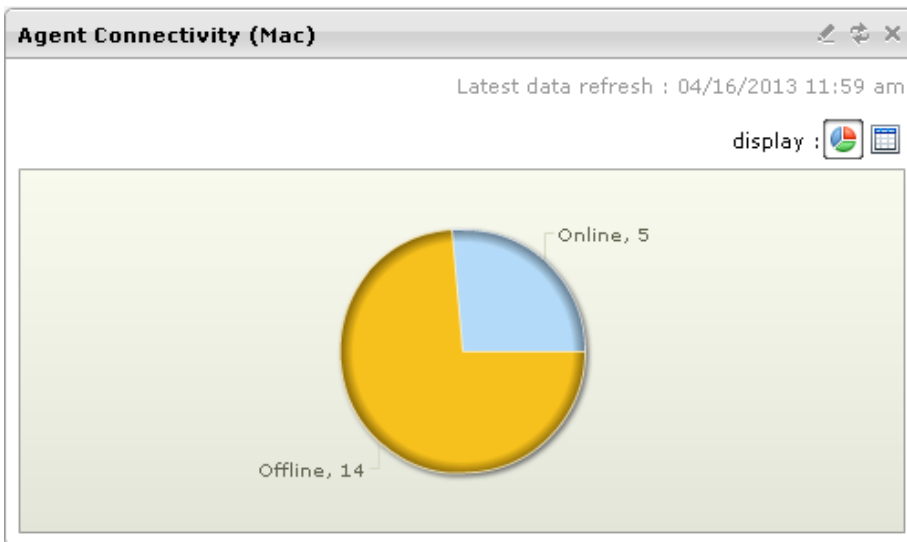
The screenshot shows a window titled "Agent Connectivity (Mac)" with standard window controls. Below the title bar, it displays "Latest data refresh : 04/16/2013 11:49 am" and "display : 📊📄". The main content is a table with two columns: "Status" and "Total". The "Offline" row is highlighted in yellow. The numbers in the "Total" column are underlined.

Status	Total
Online	<u>5</u>
Offline	<u>14</u>
Total	19

**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 Trend Micro Security (for 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 Trend Micro Security (for 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 : 1		Latest data refresh : 04/12/2016 02:40 pm		
Expand All Collapse All				
Components	Current Version	Updated	Outdated	Update Rate
Virus Pattern	12.459.00	0	0	0.00
Spyware Active-monitoring Pattern	1.721.00	0	0	0.00
Virus Scan Engine	9.850.1008	1	0	100.00
Damage Cleanup Engine	1.000.1025	1	0	100.00
Smart Scan Agent Pattern	12.231.00	1	0	100.00
Damage Cleanup Template	0.010.21	1	0	100.00
Program	Current Version	Upgraded	Not Upgraded	Upgrade Rate
Trend Micro Security (for Mac) Agent	3.0.1043	1	0	100.00

**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.

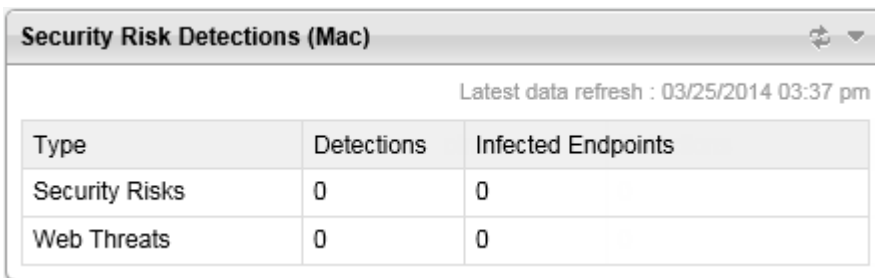


### Note

The links open the Trend Micro Security (for 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.



The screenshot shows a widget titled "Security Risk Detections (Mac)" with a refresh icon and a dropdown arrow. Below the title, it indicates "Latest data refresh : 03/25/2014 03:37 pm". The main content is a table with three columns: "Type", "Detections", and "Infected Endpoints". There are two rows of data: "Security Risks" and "Web Threats", both showing 0 in both the "Detections" and "Infected Endpoints" columns.

Type	Detections	Infected Endpoints
Security Risks	0	0
Web Threats	0	0

**FIGURE 2-4.** Security Risk Detections (Mac) widget

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

## Trend Micro Smart Protection

Trend Micro<sup>TM</sup> 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 anonymously sent from Trend Micro products worldwide to proactively determine each new threat.

For details, see *Smart Feedback on page 2-13*.

## 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 Trend Micro Security (for Mac) Agent

This chapter describes Trend Micro Security (for Mac) agent installation requirements and methods.

# Trend Micro Security (for Mac) Agent System Requirements

The following are the requirements for installing the Trend Micro Security (for Mac) agent on an endpoint.

**TABLE 3-1. Agent installation requirements**

RESOURCE	REQUIREMENT
Operating system	<ul style="list-style-type: none"><li>• macOS™ Mojave 10.14</li><li>• macOS™ High Sierra 10.13</li><li>• macOS™ Sierra 10.12</li><li>• OS X™ El Capitan 10.11</li><li>• OS X™ Yosemite 10.10 or later</li><li>• OS X™ Mavericks 10.9.5 or later</li><li>• OS X™ Mountain Lion 10.8.3 or later</li><li>• OS X™ Lion 10.7.5 or later (64-bit only)</li></ul>
Hardware	<ul style="list-style-type: none"><li>• <b>Processor:</b> Intel® Core™ processor</li><li>• <b>RAM:</b> 512MB minimum</li><li>• <b>Available disk space:</b> 300MB minimum</li></ul>
Communication port	8443
Others	<ul style="list-style-type: none"><li>• Access to *.trendmicro.com</li><li>• If required, proxy server settings for Internet connection</li></ul>

## Agent Installation Methods and Setup Files



### Note

Before installing Trend Micro Security (for Mac) agents:

- Ensure that agent endpoints can communicate with the server through port 8443
  - Ensure that endpoints can access \*.trendmicro.com
  - If required, configure agent proxy server settings
- 

You can install the Trend Micro Security (for Mac) agent using one of the following ways:

- Install on a single endpoint by launching the installation package (tmsinstall.zip) on the endpoint
- Install on several endpoints by launching the installation package (tmsinstall.mpkg.zip) from Apple Remote Desktop
- Install on several endpoints by deploying an operating system image that includes the Trend Micro Security (for Mac) agent. After installation, the Trend Micro Security (for Mac) agent automatically registers to the Trend Micro Security (for Mac) server.

Obtain the necessary agent installation package from the Trend Micro Security (for Mac) server and copy it to the endpoint.

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



### Note


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

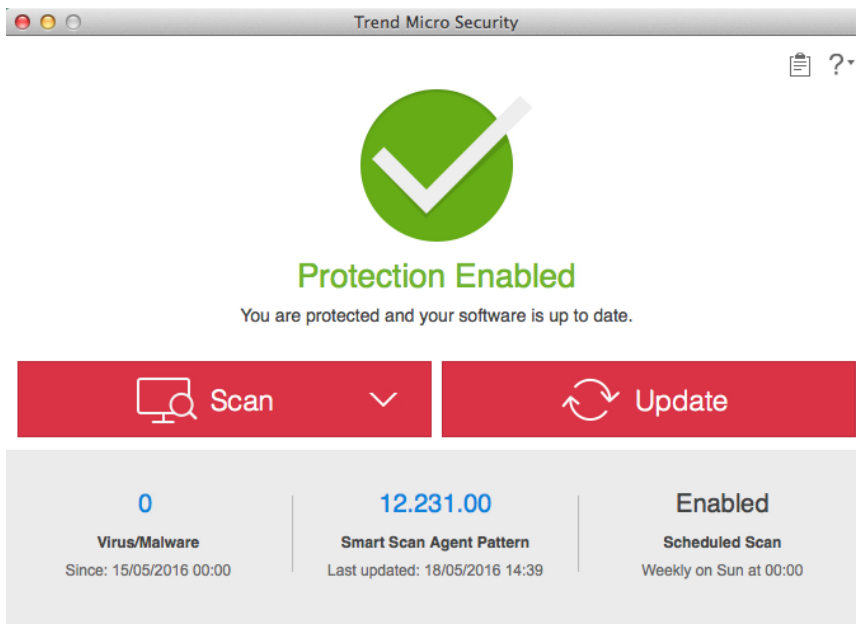
For information on uninstalling the Trend Micro Security (for Mac) agent, see [Agent Uninstallation on page 3-5](#).

---

## Agent Post-installation

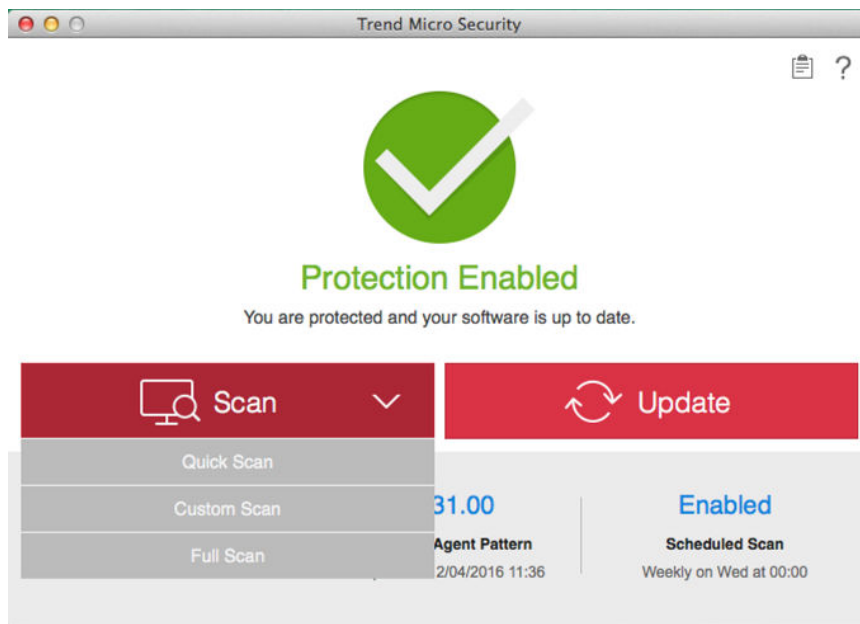
### Procedure

1. Verify the following:
  - The Trend Micro Security (for Mac) agent icon () displays on the menu bar of the endpoint.
  - The Trend Micro Security (for Mac) agent files are found under the *<Agent installation folder>*.
  - The agent appears on the web console's agent tree. To access the agent tree, click **Agent Management** on the main menu.
2. Update Trend Micro Security (for Mac) components by clicking **Update** on the agent console. The agent downloads components from the Trend Micro Security (for Mac) server. For more information, see *Agent Updates on page 4-4*.



If the agent cannot connect to the server, it downloads directly from the Trend Micro ActiveUpdate server. Internet connection is required to connect to the ActiveUpdate server.

3. Start a manual scan on the endpoint.



### What to do next

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

## Agent Uninstallation

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

---

### Procedure

1. Obtain the agent uninstallation package (`tmsmuninstall.zip`) from the Trend Micro Security (for Mac) server. On the Trend Micro Security (for Mac) web console, navigate to **Agents > Agent Setup Files** and click the link under **Agent Uninstallation File**.
2. Copy and then launch the package on the endpoint.
3. Fill in the **Name** and **Password** fields to begin the uninstallation process.



#### Note

Specify the name and password for an account with administrative rights on the endpoint.

---

4. If the uninstallation was successful, click **Close** to finish the uninstallation process.
- 

### What to do next

Unregister the agent from the server.

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

# Chapter 4

## Keeping Protection Up-to-Date

This chapter describes Trend Micro Security (for Mac) components and update procedures.

## Components

Trend Micro Security (for 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, Trend Micro Security (for Mac) agents also receive updated configuration files from the Trend Micro Security (for Mac) server. Agents need the configuration files to apply new settings. Each time you modify Trend Micro Security (for Mac) settings through the web console, the configuration files change.

COMPONENT	DESCRIPTION
Agent Program	The Trend Micro Security (for Mac) agent program provides the actual protection from security risks.
Damage Cleanup Engine (64-bit)	The Damage Cleanup Engine scans for and removes Trojans and Trojan processes.
Damage Cleanup Template	The Damage Cleanup Template is used by the Damage Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.
Smart Scan Agent Pattern	The pattern file that the 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 Trend Micro Security (for Mac) identify spyware and grayware.



COMPONENT	DESCRIPTION
Virus Scan Engine (32-bit/64-bit)	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Incorporation of new scanning and detection technologies into the software</li> <li>• Discovery of a new, potentially harmful security risk that the scan engine cannot handle</li> <li>• Enhancement of the scanning performance</li> <li>• Addition of file formats, scripting languages, encoding, and/or compression formats</li> </ul>
Virus Pattern	<p>The Virus Pattern contains information that helps Trend Micro Security (for 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.</p>




## Update Overview

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

The Trend Micro Security (for 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 Trend Micro Security (for Mac) server and agents:

**TABLE 4-1. Server-Agent Update Options**

UPDATE OPTION	DESCRIPTION
<p data-bbox="266 467 475 492">ActiveUpdate server</p>  <p data-bbox="216 594 525 643">Trend Micro Security (for Mac) server</p>  <p data-bbox="333 745 408 769">Agents</p>	<p data-bbox="561 467 1076 574">The Trend Micro Security (for Mac) server receives updated components from the Trend Micro ActiveUpdate server and then deploys the components to agents.</p>
<p data-bbox="266 795 475 820">ActiveUpdate server</p>  <p data-bbox="333 919 408 943">Agents</p>	<p data-bbox="561 795 1085 902">Trend Micro Security (for Mac) agents receive updated components directly from the ActiveUpdate server if they cannot connect to the Trend Micro Security (for Mac) server.</p>

## Agent Updates

To ensure that agents stay protected from the latest security risks, update agent components regularly. Also update agents with severely out-of-date components and whenever there is an outbreak. Components become severely out-of-date when the agent is unable to update from the Trend Micro Security (for Mac) server or the ActiveUpdate server for an extended period of time.

### Agent Update Methods

There are several ways to update agents.

UPDATE METHOD	DESCRIPTION
Administrator-initiated manual update	Initiate an update from the following web console screens: <ul style="list-style-type: none"> <li>• Agent Management screen. For details, see <a href="#">Launching Agent Update from the Agent Management Screen on page 4-7</a>.</li> <li>• Summary screen. For details, see <a href="#">Launching Agent Update from the Summary Screen on page 4-7</a>.</li> </ul>
Automatic update	After the server finishes an update, it immediately notifies agents to update.  For details, see <a href="#">Configuring Agent Automatic Update on page 4-6</a> .
User-initiated manual update	Users launch the update from their endpoints.

### Agent Update Source

By default, agents download components from the Trend Micro Security (for Mac) server. In addition to components, Trend Micro Security (for Mac) agents also receive updated configuration files when updating from the Trend Micro Security (for Mac) server. Agents need the configuration files to apply new settings. Each time you modify Trend Micro Security (for 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

- Trend Micro Security (for Mac) agents can use proxy settings during an update. Proxy settings are configured on the agent console.
- During an update, the Trend Micro Security (for Mac) icon on the menu bar of the endpoint indicates that the product is updating. If an upgrade to the agent program

is available, 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 agents have been updated.

## Configuring Agent Automatic Update

Automatic update relieves you of the burden of notifying all agents to update and eliminates the risk of agent computers not having up-to-date components.

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

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

1. Click **Updates > Agents > 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 server notifies agents to update as soon as it completes an update.
Let agents initiate component update after restarting and connecting to the server	Any agent that missed an update immediately downloads components when it establishes connection with the server. The agent may miss an update if it is offline or if the endpoint where it is installed is not up and running.

**Note**

By default, update notifications are retained on the Trend Micro Security (for Mac) server for up to seven days. Offline agents will receive update notifications if the 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 agents that require an update.

3. Select the agents that you want to update.
4. Click **Tasks > Update**.

Agents that receive the notification start to update. On endpoints, the Trend Micro Security (for 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 agents or select specific groups or agents.
3. Click **Tasks > Update**.

Agents that receive the notification start to update. On endpoints, the Trend Micro Security (for 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. Trend Micro Security (for 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 Trend Micro Security (for 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.

Trend Micro Security (for Mac) protects endpoints from the following virus/malware types:

<b>VIRUS/MALWARE TYPES</b>	<b>DESCRIPTION</b>
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	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>Boot sector virus:</b> A virus that infects the boot sector of a partition or a disk</li> <li>• <b>Java malicious code:</b> Operating system-independent virus code written or embedded in Java</li> <li>• <b>Macro virus:</b> A virus encoded as an application macro and often included in a document</li> <li>• <b>VBScript, JavaScript, or HTML virus:</b> A virus that resides on web pages and downloads through a browser</li> <li>• <b>Worm:</b> A self-contained program or set of programs able to spread functional copies of itself or its segments to other endpoints, often through email</li> </ul>
Test virus	<p>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.</p>
Packer	<p>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.</p>
Probable virus/malware	<p>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:</p> <p><a href="http://www.trendmicro.com/vinfo/virusencyclo/">http://www.trendmicro.com/vinfo/virusencyclo/</a></p>
Others	<p>"Others" include viruses/malware not categorized under any of the virus/malware types.</p>

## 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.

Trend Micro Security (for Mac) protects endpoints from the following spyware/grayware types:

<b>SPYWARE/ GRAYWARE TYPES</b>	<b>DESCRIPTION</b>
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 Trend Micro Security (for 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 Control Manager documentation.

---

#### Procedure

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

## Viewing Scan Operation Logs

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

---

#### Procedure

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

2. In the agent tree, click the root icon (🌐) to include all agents or select specific groups or 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](#).

## Security Risk Notifications and Logs

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

Trend Micro Security (for Mac) generates logs when it detects security risks.

### Configuring Security Risk Notifications for Administrators

Configure Trend Micro Security (for 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 Trend Micro Security (for 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 Trend Micro Security (for 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 Trend Micro Security (for Mac) to notify

you and other Trend Micro Security (for 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.

---

Trend Micro Security (for 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, Trend Micro Security (for Mac) sends the notification when 10 different agents have reported a total of 101 security risks within a 5-hour period. If all instances are detected on only one agent within a 5-hour period, Trend Micro Security (for 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

VARIABLE	DESCRIPTION
%CC	Total number of endpoints with security risks

5. Select additional information to include in the email. You can include the agent/group name, security risk name, path and infected file, date and time of detection, and scan result.
6. Click **Save**.

---

## Viewing Security Risk Logs

### Procedure

1. Navigate to **Agent Management**.
2. In the agent tree, click the root icon (🌐) to include all agents or select specific groups or 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 5-10](#).
  - 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. Trend Micro Security (for Mac) did not perform any action on the infected file.
- First action is Clean but cleaning was unsuccessful. Second action is Pass so Trend Micro Security (for 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. Trend Micro Security (for 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. Trend Micro Security (for 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	<p>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.</p> <p><b>Solution:</b> Trend Micro recommends deleting worms.</p>
Write-protected infected files	<p><b>Solution:</b> Remove the write-protection to allow the Trend Micro Security (for Mac) agent to clean the file.</p>
Password-protected files	<p>Includes password-protected files or compressed files.</p> <p><b>Solution:</b> Remove the password protection for the Trend Micro Security (for Mac) agent to clean these files.</p>
Backup files	<p>Files with the RB0~RB9 extensions are backup copies of infected files. The Trend Micro Security (for Mac) agent creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.</p> <p><b>Solution:</b> If the Trend Micro Security (for Mac) 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.</p>

## 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 agents or select specific groups or agents.

3. Click **Logs** > **Reset Statistics**.



**Note**

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

---

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



## Chapter 6

# Protecting Endpoints from Web-based Threats

This chapter describes web-based threats and using Trend Micro Security (for 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.

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 agent will either block or allow access to the website.

**Note**

This feature supports the latest Safari™, Mozilla™ Firefox™, and Google Chrome™ browsers released as of April 2014.

---

## Configuring the Approved and Blocked URL Lists

Add websites that you consider safe or dangerous to the approved or blocked list. When Trend Micro Security (for 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 > Global Agent Settings > 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 agents to send Web Reputation logs to the server. Do this if you want to analyze URLs that Trend Micro Security (for 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 agents or select specific groups or 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 Trend Micro Security (for 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.



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 Agents

This chapter describes Trend Micro Security (for 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 **Certified Safe Software Service**.
  3. Select **Enable Certified Safe Software Service for antivirus scan**.
  4. Click **Save**.
- 

## Managing Logs

Trend Micro Security (for Mac) keeps comprehensive logs about security risk detections, blocked URLs, and scan operations. Use these logs to assess your organization's protection policies and to identify 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 Control Manager

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

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

### Control Manager Integration in this Release

This Trend Micro Security (for Mac) release supports Control Manager 6.0 SP3 and later. In this release, you can create, manage, and deploy Trend Micro Security (for Mac) policies and monitor endpoints from Control Manager.

The following are the policy configurations available in Control Manager:

- 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

You can monitor endpoints using the **Security (for Mac) Key Performance Indicators** widget in Control Manager.

For details, see [Key Performance Indicators Widget on page 7-4](#).

See the Control Manager documentation for details.

## Key Performance Indicators Widget

Use this widget on the Control Manager **Dashboard** screen to display Trend Micro Security (for Mac) key performance indicators (KPIs) based on selected criteria.

For information on how to add a widget to the **Dashboard** screen, see the 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 Control Manager server to obtain data for widget display.


1. Go to the **Dashboard** screen on Control Manager.
2. Click the tab on which the **Security (for 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 Trend Micro Security (for Mac) servers.
5. Click **Save**.

## Configuring Key Performance Indicators

In Control Manager, access the **Security (for 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	<ol style="list-style-type: none"><li data-bbox="646 440 1171 490">1. Click <b>Add Indicator</b>. The <b>Add Indicator</b> screen appears.</li><li data-bbox="646 509 1159 560">2. Select an option from the <b>Name</b> drop-down list and optionally customize settings.</li><li data-bbox="646 579 803 605">3. Click <b>Save</b>.</li></ol>
Edit an indicator	<ol style="list-style-type: none"><li data-bbox="646 631 1171 682">1. Click the indicator in the list. The <b>Edit Indicator</b> screen appears.</li><li data-bbox="646 701 888 727">2. Customize settings.</li><li data-bbox="646 747 803 773">3. Click <b>Save</b>.</li></ol>
Delete an indicator	<ol style="list-style-type: none"><li data-bbox="646 794 1171 844">1. Click the indicator in the list. The <b>Edit Indicator</b> screen appears.</li><li data-bbox="646 863 821 889">2. Click <b>Delete</b>.</li><li data-bbox="646 909 790 935">3. Click <b>OK</b>.</li></ol>

TASK	STEPS
Configure event threshold settings	<ol style="list-style-type: none"> <li>1. On the <b>Add Indicator</b> or <b>Edit Indicator</b> screen, select <b>Enable alerts at the following thresholds</b>.</li> <li>2. Type the minimum number of event occurrences for each event type.</li> <li>3. Click <b>Save</b>.</li> </ol> <hr/> <p> <b>Note</b> The important or critical icon displays in the <b>Occurrences</b> column if both of the following are true:</p> <ul style="list-style-type: none"> <li>• The number of event occurrences that match this indicator is equal to or more than the threshold.</li> <li>• <b>Enable alerts at the following threshold</b> is selected.</li> </ul>

## Configuring Widget Settings

On the 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.
Configure daily update time	<p>From the drop-down list, select the hour to generate the widget data every day.</p> <hr/> <p> <b>Tip</b> To manually refresh the widget data, click the refresh () icon.</p>



## Inactive Agents

Trend Micro Security (for Mac) displays agents as inactive:

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

To have the agent tree display active agents only, configure Trend Micro Security (for Mac) to automatically remove inactive agents from the agent tree.

## Automatically Removing Inactive Agents











---










### Procedure

1. Go to **Administration > Inactive Agents**.
  2. Select **Enable automatic removal of inactive agents**.
  3. Select how many days should pass before Trend Micro Security (for Mac) considers the 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 agent is up and running and is connected to its parent server.
		The product license has been activated.
		The agent is up and running but is disconnected from its parent server.
		A new component version is available. Update the agent immediately.
		The agent has detected a security threat that requires a computer restart to fix.
		The agent is scanning for security risks and is connected to its parent server.
		The agent is updating components from its parent server.

TRAY ICON	MENU ICON	DESCRIPTION
		A component update requires you to restart the agent to finish installation.
		Smart Scan or Web Reputation service is not available on the agent. Check your network connection.
		The agent has been registered to its parent server but the product license has not been activated. Some agent features will not be available if the license has not been activated.
		The agent has not been registered to its parent server. The product license may or may not have been activated.  If an 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 agent features will not be available if the license has expired.
		The agent has been installed on an unsupported platform.
		The agent is not functioning properly. Upgrade the agent to the latest release or contact technical support.
		The 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 provider if the problem persists.

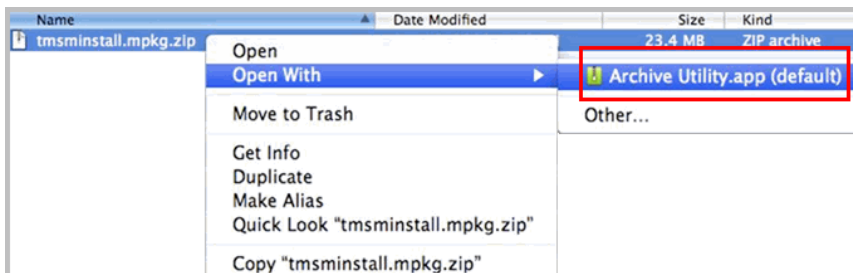
## Agent Installation

**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 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 Trend Micro Security (for Mac) 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 8-7](#)*
- *[Other Resources on page 8-8](#)*

## 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 <http://esupport.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:

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

---

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 <http://about-threats.trendmicro.com/us/threatencyclopedia#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	<a href="http://www.trendmicro.com">http://www.trendmicro.com</a>
Email address	<a href="mailto:support@trendmicro.com">support@trendmicro.com</a>

- Worldwide support offices:  
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:  
<http://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://ers.trendmicro.com/>

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

<http://esupport.trendmicro.com/solution/en-US/1112106.aspx>

### File Reputation Services

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

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

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):

<http://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:

<http://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:

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

## Chapter 9

# IPv6 Support in Trend Micro Security (for Mac)

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

## Trend Micro Security (for Mac) Agent IPv6 Requirements

All Mac OS X versions supported by the Trend Micro Security (for Mac) agent also support IPv6.

It is preferable for the 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 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: <ul style="list-style-type: none"> <li>• Trend Micro ActiveUpdate Server</li> <li>• A pure IPv4 Trend Micro Security (for Mac) server</li> </ul>
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.

- Trend Micro Security (for 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
```

- Trend Micro Security (for 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 Trend Micro Security (for 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	<p>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.</p> <p><b>Solution:</b> Trend Micro recommends deleting worms.</p>
Write-protected infected files	<p><b>Solution:</b> Remove the write-protection to allow the Trend Micro Security (for Mac) agent to clean the file.</p>
Password-protected files	<p>Includes password-protected files or compressed files.</p> <p><b>Solution:</b> Remove the password protection for the Trend Micro Security (for Mac) agent to clean these files.</p>

<b>UNCLEANABLE FILE</b>	<b>EXPLANATION AND SOLUTION</b>
Backup files	<p>Files with the RB0~RB9 extensions are backup copies of infected files. The Trend Micro Security (for Mac) agent creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.</p> <p><b>Solution:</b> If the Trend Micro Security (for Mac) 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.</p>



# Index

## A

agent tree, 2-4  
    general tasks, 2-4

## C

components, 2-11  
Control Manager integration, 7-3

## D

Damage Cleanup Services, 1-3  
documentation feedback, 8-8

## F

File Reputation Services, 2-13

## I

IPv6 support  
    limitations, 9-2

## P

programs, 2-11

## S

Smart Feedback, 2-13  
Smart Protection  
    File Reputation Services, 2-13  
    Web Reputation Services, 2-13  
support  
    resolve issues faster, 8-6

## T

Trojan horse program, 1-3

## V

virus/malware scan  
    results, 5-10

## W

web console, 2-2  
    about, 2-2  
web reputation, 6-2  
Web Reputation Services, 2-13  
web threats, 6-2  
widgets, 2-9, 2-11, 2-12



**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](http://www.trendmicro.com)

Item Code: TSEM08095/171120