TREND MICRO™

# 3.0 TREND MICRO™ Security

## Administrator's Guide

For Enterprise and Medium Business

for MAC®

Endpoint Security

Protected Cloud

TREND MICRO SMART PROTECTION NETWORK™

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

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.: TSEM37299/160114

Release Date: February 2017

The user documentation for Trend Micro Security (for Mac) introduces the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's website.

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.

Please evaluate this documentation on the following site:

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

# Table of Contents

## Preface


Preface ..... vii

Trend Micro Security (for Mac) Documentation ..... viii

Audience ..... viii

Document Conventions ..... ix

Terminology ..... ix


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


About Trend Micro Security (for Mac) ..... 1-2

New in this Release ..... 1-2

Key Features and Benefits ..... 1-5

The Trend Micro Security (for Mac) Server ..... 1-7

The Trend Micro Security (for Mac) Agent ..... 1-8


## Chapter 2: Installing the Server


Server Installation Requirements ..... 2-2

Update Source ..... 2-3

Installing the Trend Micro Security (for Mac) Server ..... 2-5

Activating the Product for the First Time ..... 2-6

Performing Post-installation Tasks on the Server ..... 2-8

Uninstalling the Trend Micro Security (for Mac) Server ..... 2-9


## Chapter 3: Getting Started


The Web Console ..... 3-2

Opening the Web Console ..... 3-2

Security Summary ..... 3-3

The Agent Tree ..... 3-4
Agent Tree General Tasks ..... 3-4
Agent Tree Specific Tasks ..... 3-5

Groups ..... 3-7
Adding a Group ..... 3-7
Deleting a Group or Agent ..... 3-8
Renaming a Group ..... 3-8
Moving Agents ..... 3-8

Widgets ..... 3-10
Agent Connectivity (Mac) Widget ..... 3-10
Agent Updates (Mac) Widget ..... 3-13
Security Risk Detections (Mac) Widget ..... 3-14

Trend Micro Smart Protection ..... 3-14
Smart Feedback ..... 3-17

## Chapter 4: Installing the Agent

Agent Installation Requirements ..... 4-2

Agent Installation Methods and Setup Files ..... 4-2
Installing on a Single Endpoint ..... 4-3
Installing on Several Endpoints Using Apple Remote Desktop ..... 4-9

Agent Post-installation ..... 4-12

Agent Uninstallation ..... 4-14

## Chapter 5: Keeping Protection Up-to-Date

Components ..... 5-2

Update Overview ..... 5-3

Server Update ..... 5-4
Configuring the Server Update Source ..... 5-5
Configuring Proxy Settings for Server Updates ..... 5-6
Server Update Methods ..... 5-7

Agent Updates ..... 5-8
Configuring Agent Automatic Update ..... 5-10
Configuring Agent Update Settings ..... 5-11

Launching Agent Update from the Summary Screen ..... 5-12
Launching Agent Update from the Agent Management Screen .. 5-13

## Chapter 6: Protecting Endpoints from Security Risks

About Security Risks ..... 6-2
Viruses and Malware ..... 6-2
Spyware and Grayware ..... 6-4

Scan Method Types ..... 6-5
Default Scan Method ..... 6-5
Scan Methods Compared ..... 6-5
Changing the Scan Method ..... 6-6
Switching from Smart Scan to Conventional Scan ..... 6-7
Switching from Conventional Scan to Smart Scan ..... 6-8

Scan Types ..... 6-11
Real-time Scan ..... 6-11
Manual Scan ..... 6-12
Scheduled Scan ..... 6-14
Scan Now ..... 6-15

Settings Common to All Scan Types ..... 6-16
Scan Criteria ..... 6-16
Scan Actions ..... 6-19
Scan Exclusions ..... 6-23
Cache Settings for Scans ..... 6-27

Viewing Scan Operation Logs ..... 6-29

Security Risk Notifications and Logs ..... 6-30
Configuring Administrator Notification Settings ..... 6-30
Configuring Security Risk Notifications for Administrators ..... 6-30
Configuring Outbreak Notifications for Administrators ..... 6-31
Viewing Security Risk Logs ..... 6-33
Resetting Security Risk Count ..... 6-36

## Chapter 7: Protecting Endpoints from Web-based Threats

Web Threats ..... 7-2

Web Reputation ..... 7-2

Configuring Web Reputation Settings ..... 7-3
Configuring the Approved and Blocked URL Lists ..... 7-5
Viewing Web Reputation Logs ..... 7-6

## Chapter 8: Managing the Server and Agents

Agent Self-protection ..... 8-2
Configuring Agent Self-protection ..... 8-2
Enabling Certified Safe Software Service ..... 8-3
Upgrading the Server and Agents ..... 8-4
Upgrading the Server ..... 8-4
Upgrading Agents ..... 8-6
Managing Logs ..... 8-7
Managing Licenses ..... 8-7
Backing Up the Server Database ..... 8-9
Restoring the Server Database ..... 8-10
Trend Micro Control Manager ..... 8-10
Control Manager Integration in this Release ..... 8-11
Key Performance Indicators Widget ..... 8-12
Configuring Agent-Server Communication Settings ..... 8-15
Inactive Agents ..... 8-16
Automatically Removing Inactive Agents ..... 8-17
Agent Icons ..... 8-17

## Chapter 9: Getting Help

Troubleshooting ..... 9-2
Web Console Access ..... 9-2
Server Uninstallation ..... 9-4
Agent Installation ..... 9-5
General Agent Error ..... 9-6
The Trend Micro Knowledge Base ..... 9-7

Technical Support ..... 9-7
Troubleshooting Resources ..... 9-8
Contacting Trend Micro ..... 9-9
Sending Suspicious Content to Trend Micro ..... 9-10
Other Resources ..... 9-11

## Appendix A: IPv6 Support in Trend Micro Security (for Mac)

IPv6 Support for Trend Micro Security (for Mac) Server and Agents .. A-2

Trend Micro Security (for Mac) Server IPv6 Requirements ..... A-2

Trend Micro Security (for Mac) Agent IPv6 Requirements ..... A-2

Pure IPv6 Server Limitations ..... A-3

Pure IPv6 Agent Limitations ..... A-3

Configuring IPv6 Addresses ..... A-4

Screens That Display IP Addresses ..... A-5

## Index

Index ..... IN-1

# Preface

## Preface

Welcome to the Trend Micro Security (for Mac) Administrator's Guide. This document discusses Trend Micro Security (for Mac) server and 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 |
|---|---|
| Administrator's Guide | A PDF document that discusses Trend Micro Security (for Mac) server and 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:<br>http://esupport.trendmicro.com |

View and download product documentation at:

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 |
| **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 Trend Micro Security (for Mac) documentation:

| TERMINOLOGY | DESCRIPTION |
|---|---|
| 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<br>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<br>`/Library/Application Support/TrendMicro` |

| TERMINOLOGY | DESCRIPTION |
| --- | --- |
| `Server installation folder` | 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.<br><br>If you accept the default settings during OfficeScan server installation, you will find the server installation folder at any of the following locations:<br><br>• `C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM`<br><br>• `C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\TMSM` |
| Dual-stack | An entity that has both IPv4 and IPv6 addresses. For example:<br><br>• A dual-stack endpoint is an endpoint with both IPv4 and IPv6 addresses.<br><br>• A dual-stack agent refers to an agent installed on a dual-stack endpoint.<br><br>• A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses. |
| Pure IPv4 | An entity that only has an IPv4 address |
| Pure IPv6 | An entity that only has an IPv6 address |

# 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)

Trend Micro™ Security (for Mac)™ provides the latest endpoint protection against security risks, blended threats, and platform independent web-based attacks.

The Trend Micro Security (for Mac) server is a plug-in program integrated with Trend Micro products such as OfficeScan and Worry-free Business Security and installed through the Plug-in Manager framework. The Trend Micro Security (for Mac) server deploys agents to endpoints.

# New in this Release

Trend Micro Security (for Mac) includes the following new features and enhancements:

| FEATURE/ ENHANCEMENT | DETAILS |
|---|---|
| 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.<br><br>For information about smart scan and how to deploy it to agents, see *Scan Method Types on page 6-5*. |

| Feature/ Enhancement | Details |
|---|---|
| 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:<br>• Detects and removes live Trojans<br>• Kills processes that Trojans create<br>• Repairs system files that Trojans modify<br>• Deletes files and applications that Trojans drop<br>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. |
| Web reputation blocked list | Web reputation enhancements include the URL blocked list. You can add websites that you consider dangerous to the blocked list. When the Trend Micro Security (for Mac) agent detects access to one of these websites on an endpoint, it automatically denies the connection without sending a query to the smart protection sources. |
| Key Performance Indicator dashboard widget | This version of Trend Micro Security (for Mac) integrates with Control Manager that allows you to customize a score card on the Control Manager dashboard regarding the status of your endpoint environment. |
| Agent self-protection | The Trend Micro Security (for Mac) agent implements the following self-protection features:<br>• Prevents the removal or modification of Trend Micro Security (for Mac) agent program files and folders<br>• Prevents the blocking of Trend Micro Security (for Mac) agent processes |

| Feature/ Enhancement | Details |
|---|---|
| Scan monitoring | Trend Micro Security (for Mac) provides more visibility and control over scan features through:<br>• Scan Operation logs: Monitor scan time, scan status, and scan results using the web console and the agent console.<br>• Security risk log filtering by scan actions on the agent console.<br>• Virus/malware count reset for selected agents or agent groups. |
| External drive scanning | Administrators configure agents to scan network drives or Time Machine drives. |
| Certified Safe Software Service | The Certified Safe Software Service queries Trend Micro datacenters to verify the safety of a program detected by antivirus scans and reduce the likelihood of false positive detections. |
| Enhanced agent update and upgrade features | This version of Trend Micro Security (for Mac) includes the following agent update features:<br>• Agent automatic update: Trend Micro Security (for Mac) server can deploy updated components to agents when an agent endpoint restarts or when a new component is available on the server.<br>• Granular agent update: Option to update components without upgrading the agent program. |
| Agent migration | Administrators can migrate Trend Micro Security (for Mac) agents to another Trend Micro Security (for Mac) server without having to reinstall Trend Micro Security (for Mac) agents on endpoints. |
| Agent deployment | This version of Trend Micro Security (for Mac) supports agent deployment using operating system images. When you include the Trend Micro Security (for Mac) agent in an operating system image that is deployed to multiple endpoints, the Trend Micro Security (for Mac) agent automatically registers to the Trend Micro Security (for Mac) server after installation and starts protecting the endpoints without manual configuration. |

| Feature/ Enhancement | Details |
|---|---|
| Trend Micro Security (for Mac) agent interface redesign | The Trend Micro Security (for Mac) agent interface has been redesigned to provide an easier, more streamlined, and more modern experience. All the features available in the previous Trend Micro Security (for Mac) client version are still available in the updated version. |
| Trend Micro Security (for Mac) server interface enhancement | The top-level menu on the Trend Micro Security (for Mac) server web console has been enhanced to align with the web console menu on OfficeScan to provide a more consistent experience. All the features available in the previous Trend Micro Security (for Mac) server are still available in the updated version. |
| Browser support | The Trend Micro Security (for Mac) server web console supports the following browsers on supported OS X™ or macOS™ platforms:<br>• Chrome<br>• Firefox<br>• Safari |

# 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.<br>For information about smart scan and how to deploy it to agents, see *Scan Method Types on page 6-5*. |

| 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:<br>• Detects and removes live Trojans<br>• Kills processes that Trojans create<br>• Repairs system files that Trojans modify<br>• Deletes files and applications that Trojans drop<br>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. |
| Security Risk Protection | 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. |
| 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.<br>Verify the credibility of websites and pages by integrating OfficeScan 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 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. |

# 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

# Installing the Server

This chapter describes system requirements and the installation procedure for Trend Micro Security (for Mac) server.

# Server Installation Requirements

The following are the requirements for installing the Trend Micro Security (for Mac) server:

**TABLE 2-1. Server Installation Requirements**

| RESOURCE | REQUIREMENTS |
|---|---|
| OfficeScan server | 10.6 SP2 or later |
| Plug-in Manager | 2.0 and higher |
| RAM | 1GB minimum, 2GB recommended |
| Available disk space | • 1.5GB minimum if the OfficeScan server is installed on the system drive (usually, C: drive)<br>• If the OfficeScan server is not installed on the system drive:<br>  • 600MB minimum on the drive where the OfficeScan server is installed. The Trend Micro Security (for Mac) server will be installed on this drive.<br>  • 900MB minimum on the system drive. Third-party programs used by the Trend Micro Security (for Mac) server will be installed on this drive. |

| Resource | Requirements |
|---|---|
| Others | • Microsoft™ .NET Framework 3.0 SP2 or 3.5 SP1<br>• Microsoft Windows™ Installer 3.1 and above<br>• Java runtime environment™ (JRE) 1.7 or later, with the latest update<br>**Note**<br>For best performance, install JRE 1.8 or later. Install JRE for Windows x86 or JRE for Windows x64, depending on the operating system of the host machine.<br>• The following third-party programs will be installed automatically, if it does not exist:<br>  • Microsoft SQL Server 2005 or 2008 R2 Express<br>  • Apache™ ActiveMQ 5.14.0<br>  • Microsoft Visual C++ 2005 Redistributable |

# Update Source

Before installing the Trend Micro Security (for Mac) server, check the Plug-in Manager update source by navigating to **Updates** > **Server** > **Update Source** on the OfficeScan web console. The update source can be any of the following:

**TABLE 2-2. Possible Update Sources**

| UPDATE SOURCE SELECTED | DESCRIPTION AND INSTRUCTIONS |
|---|---|
| `ActiveUpdate Server` | The Trend Micro ActiveUpdate server is the default update source for OfficeScan. Internet connection is required to connect to this server.<br><br>If the server computer connects to the Internet through a proxy server, ensure that Internet connection can be established using the proxy settings. |
| `Other Update Source` | If you have specified multiple update sources:<br><br>• Ensure the server computer can connect to the first update source on the list. If the server computer cannot connect to the first update source, it does not attempt to connect to the other update sources.<br><br>• Check if the first update source contains the latest version of the Plug-in Manager component list (`OSCE_AOS_COMP_LIST.xml`) and the Trend Micro Security (for Mac) installation package.<br><br>For assistance in setting up an update source, contact your support provider. |
| `Intranet Location Containing a Copy of the Current File` | If the update source is an intranet location:<br><br>• Check if there is functional connection between the server computer and the update source.<br><br>• Check if the update source contains the latest version of the Plug-in Manager component list (`OSCE_AOS_COMP_LIST.xml`) and the Trend Micro Security (for Mac) installation package.<br><br>For assistance in setting up the intranet source, contact your support provider. |

# Installing the Trend Micro Security (for Mac) Server

**Procedure**

1. Do the following ONLY if you are installing Trend Micro Security (for Mac) on a server with a domain controller role:

   - Install Trend Micro Security (for Mac) on an OfficeScan 10.6 SP2 server:

     a. Open a text file and add the following:

     ```
     [SQLSERVER2005]
     SQLACCOUNT="NT AUTHORITY\SYSTEM"
     [SQLSERVER2008]
     SQLSVCACCOUNT="NT AUTHORITY\SYSTEM"
     ```

     b. Save the file as `InstallCfgFile.ini` under the `...OfficeScan\PCCSRV\Admin\Utility\SQL` folder.

   - Install Trend Micro Security (for Mac) on an OfficeScan 11.0 server:

     a. Go to the `...OfficeScan\PCCSRV\Admin\Utility\SQL` folder.

     b. Open the `InstallCfgFile.ini` file using a text editor.

     c. Change the `SQLSVCACCOUNT` value setting from `NT AUTHORITY\NETWORK SERVICE` to `NT AUTHORITY\SYSTEM`.

     d. Save the file.

2. Open the OfficeScan web console and click **Plug-ins** on the main menu.

3. Go to the **Trend Micro Security (for Mac)** section and click **Download**.

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

   Plug-in Manager downloads the package to `<OfficeScan server installation folder>\PCCSRV\Download`.

   `<OfficeScan server installation folder>` is typically `C:\Program Files\Trend Micro\OfficeScan`.

4. Monitor the download progress.

   You can navigate away from the screen during the download.

   If you encounter problems downloading the package, check the server update logs on the OfficeScan web console. On the main menu, click **Logs** > **Server Updates**.

5. After the download process is complete, click **Install** to install Trend Micro Security (for Mac).

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

   The installation starts.

7. Monitor the installation progress. After the installation, the Plug-in Manager screen reloads.

# Activating the Product for the First Time

**Procedure**

1. Open the OfficeScan web console and click **Plug-ins** on the main menu.

2. Go to the **Trend Micro Security (for Mac)** section and click **Manage Program**.

3. Type the Activation Code for the product and click **Save**. The Activation Code is case-sensitive.

If you do not have the Activation Code, click the **register online** link to access the Trend Micro registration website. After you complete the registration, Trend Micro sends an email with the Activation Code. You can then continue with activation.

If you have activated an evaluation version license, ensure that you upgrade to the full version before the license expires.

4. In the License Details screen that appears, click **Launch** to open the web console.

5. Click **Launch** to open the web console.

# Performing Post-installation Tasks on the Server

**Procedure**

1. Verify that the following services display on the Microsoft Management Console:
   - **ActiveMQ for Trend Micro Security**
   - **SQL Server (TMSM)**
   - **Trend Micro Security for (Mac)**
2. Verify that the following process is running on Windows Task Manager: **TMSMMainService.exe**
3. Verify that the following registry key exists in Registry Editor: `HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_TMSM`
4. Verify that the Trend Micro Security (for Mac) server files are found under the <*Server installation folder*>.

# Uninstalling the Trend Micro Security (for Mac) Server

**Procedure**

1. Open the OfficeScan web console and click **Plug-ins** on the main menu.
2. Go to the Trend Micro Security (for Mac) section and click **Uninstall**.
3. Monitor the uninstallation progress. You can navigate away from the screen during the uninstallation. After the uninstallation is complete, the Trend Micro Security (for Mac) server is again available for installation.

**Note**

The uninstallation package does not remove Java runtime environment (JRE) used by Trend Micro Security (for Mac). You can remove JRE if no other application is using it.

# Chapter 3

## 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
- Set scan configurations and initiate scanning on a single or multiple endpoints
- Configure security risk notifications and view logs sent by agents
- Configure outbreak criteria and notifications

## Opening the Web Console

### Before you begin

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

- Monitor that supports 1024 x 768 resolution at 256 colors or higher
- Web browser:
    - Microsoft Internet Explorer 8.0, Microsoft Edge, or later versions
    - Firefox
    - Chrome
    - Safari

**Procedure**

1. On a web browser, type the OfficeScan server URL.
2. Type the user name and password to log on to the OfficeScan server.
3. On the main menu, click **Plug-in Manager**.
4. Go to the **Trend Micro Security (for Mac)** section and click **Manage Program**.

# 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 6-34*.
  - 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 7-5*.

### 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 5-12*.

- Upgrade agents to the latest program version or build if you recently upgraded the server.

  For agent upgrade instructions, see *Upgrading the Server and Agents on page 8-4*.

# 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 (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.<br>For details, see *Agent Updates on page 5-8*.<br>• Run Scan Now on endpoints.<br>For details, see *Scan Now on page 6-15*. |

| MENU BUTTON | TASK |
|---|---|
| **Settings** | • Configure the scan method.<br>For details, see *Scan Method Types on page 6-5*.<br>• Configure scan settings.<br>  • *Manual Scan on page 6-12*<br>  • *Real-time Scan on page 6-11*<br>  • *Scheduled Scan on page 6-14*<br>  • *Scan Exclusions on page 6-23*<br>  • *Cache Settings for Scans on page 6-27*<br>• Configure Web Reputation settings.<br>For details, see *Configuring Web Reputation Settings on page 7-3*.<br>• Configure agent self-protection.<br>For details, see *Configuring Agent Self-protection on page 8-2*.<br>• Configure update settings.<br>For details, see *Configuring Agent Update Settings on page 5-11*. |
| **Logs** | View logs and reset statistics.<br>• *Viewing Security Risk Logs on page 6-33*<br>• *Viewing Web Reputation Logs on page 7-6*<br>• *Viewing Scan Operation Logs on page 6-29*<br>• *Resetting Security Risk Count on page 6-36* |
| **Manage Agent Tree** | Manage Trend Micro Security (for Mac) groups.<br>For details, see *Groups on page 3-7*. |

# 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 3-9*.

**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 IPv4/IPv6 address and HTTP 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

**FIGURE 3-1. 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 3-2. 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 3-3. 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.

**FIGURE 3-4. 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™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 7-2*.
- **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 3-17*.

### 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 Protection Source for External Agents

External agents, which are agents that are unable to maintain a functional connection with the Trend Micro Security (for Mac) server, send Web Reputation queries to Smart Protection Network. Internet connection is required to send queries successfully.

Go to the Web Reputation Services screen and enable Web Reputation policy for external agents. For the detailed steps, see *Configuring Web Reputation Settings on page 7-3*.

### Smart Protection Sources for Internal Agents

Internal agents, which are agents that maintain a functional connection with the Trend Micro Security (for Mac) server, can send queries to either Smart Protection Server or Smart Protection Network.

| SOURCE | DETAILS |
|---|---|
| Smart Protection Servers | Configure Smart Protection Servers as source if you have privacy concerns and want to keep Web Reputation queries within the corporate network. |
| Smart Protection Network | Configure Smart Protection Network as source if you do not have the resources required to set up and maintain Smart Protection Servers. |

### Smart Protection Servers as Source for Internal Agents

With this option, Trend Micro Security (for Mac) agents send queries to Smart Protection Servers configured for OfficeScan clients.

**Note**

This option is only available if the OfficeScan version is 10.6 SP3 Patch 1 Critical Patch or later.

If your Trend Micro Security (for Mac) server is installed with an earlier version of OfficeScan, upgrade OfficeScan to version SP3 Patch 1 Critical Patch or later.

If your OfficeScan version is 10.6 SP3 Patch 1 Critical Patch or later, read the following guidelines to allow agents to send queries to Smart Protection Servers successfully:

1. Set up the smart protection environment, if you have not done so. For instructions and guidelines on setting up the environment, refer to the OfficeScan documentation.

2. On the web console for Trend Micro Security (for Mac) server, go to the Web Reputation Settings screen and enable the option **Send queries to Smart Protection Servers**. For the detailed steps, see *Configuring Web Reputation Settings on page 7-3*.

**Important**

This option cannot be enabled if the Trend Micro Security (for Mac) server is installed with OfficeScan 10.6. If this option is enabled from Control Manager Policy Management and then deployed to Trend Micro Security (for Mac) server installed with OfficeScan 10.6, the setting will not take effect and the option will remain disabled.

3. Be sure that Smart Protection Servers are available. If all Smart Protection Servers are unavailable, agents do not send queries to Smart Protection Network, leaving endpoints vulnerable to threats.

4. Be sure to update Smart Protection Servers regularly so that protection remains current.

### Smart Protection Network as Source for Internal Agents

Internet connection is required to send queries to Smart Protection Network successfully.

To configure Smart Protection Network as source for internal agents, go to the Web Reputation Services screen and enable Web Reputation policy for internal agents. Be sure not to select the option **Send queries to Smart Protection Servers**. For the detailed steps, see *Configuring Web Reputation Settings on page 7-3*.

## 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 4

# Installing the Agent

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

For details on upgrading the agent, see *Upgrading the Server and Agents on page 8-4*.

# Agent Installation Requirements

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

**TABLE 4-1. Agent installation requirements**

| RESOURCE | REQUIREMENT |
|---|---|
| Operating system | • macOS™ High Sierra 10.13<br>• macOS™ Sierra 10.12<br>• OS X™ El Capitan 10.11<br>• OS X™ Yosemite 10.10 or later<br>• OS X™ Mavericks 10.9 or later<br>• OS X™ Mountain Lion 10.8.3 or later<br>• OS X™ Lion 10.7.5 or later (64-bit only) |
| Hardware | • **Processor**: Intel® Core™ processor<br>• **RAM**: 512MB minimum<br>• **Available disk space**: 300MB minimum |

**Note**

This product version no longer supports Mac OS X Snow Leopard™ 10.6.8 or earlier. If there are agents installed on Mac OS X Snow Leopard, do not upgrade the agents and be sure that there is a Trend Micro Security (for Mac) 2.0 SP1 server that can manage these agents.

# Agent Installation Methods and Setup Files

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 (`tmsminstall.zip`) on the endpoint

- Install on several endpoints by launching the installation package (`tmsminstall.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.

**Note**

To upgrade agents, see *Upgrading the Server and Agents on page 8-4*.

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

There are two ways to obtain the package:

- 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 4-14*.

- Navigate to <*Server installation folder*>`TMSM_HTML\ActiveUpdate\ClientInstall\`.

## Installing on a Single Endpoint

The process of installing the Trend Micro Security (for Mac) agent on a single endpoint is similar to the installation process for other Mac software.

During the installation, users may be prompted to allow connections to **iCoreService**, which is used to register the agent to the server. Instruct users to allow the connection when prompted.

**Procedure**

1. Check for and uninstall any security software on the endpoint.
2. Obtain the agent installation package `tmsminstall.zip`.

   For information on obtaining the package, see *Agent Installation Methods and Setup Files on page 4-2*.

3. Copy `tmsminstall.zip` on the endpoint and then launch it using a built-in archiving tool, such as Archive Utility.

   **WARNING!**

   The files on `tmsminstall.zip` may become corrupted if users launch it using archiving tools not built-in on the Mac.

   To launch `tmsminstall.zip` from Terminal, use the following command:

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

   For example:

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

   Launching `tmsminstall.zip` creates a new folder `tmsminstall`.

4. Open the `tmsminstall` folder and launch `tmsminstall.pkg`.
5. When a message prompting you to continue with installation displays, click **Continue**.

6. On the Introduction screen, click **Continue** to proceed.

7. Read the reminders and click **Continue**.

8. On the Installation Type screen, click **Install**.

9. Fill in the **Name** and **Password** fields to begin the installation process.

**Note**

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

**10.** If the installation was successful, click **Close** to finish the installation process.

The agent automatically registers to the server where the agent installation package was obtained. The agent also updates for the first time.

### What to do next

Perform agent post-installation tasks. For details, see *Agent Post-installation on page 4-12*.

## Installing on Several Endpoints Using Apple Remote Desktop

The process of installing Trend Micro Security (for Mac) agent on several endpoints can be simplified by using Apple Remote Desktop.

**Note**

If endpoints only have an IPv6 address, read the IPv6 limitations for Apple Remote Desktop agent deployment in *Pure IPv6 Agent Limitations on page A-3*.

**Procedure**

1. Check for and uninstall any security software on the endpoint.
2. Obtain the agent installation package `tmsminstall.mpkg.zip`.

   For information on obtaining the package, see *Agent Installation Methods and Setup Files on page 4-2*.
3. Copy `tmsminstall.mpkg.zip` on the endpoint with Apple Remote Desktop and then launch it using a built-in archiving tool, such as Archive Utility.

**WARNING!**

The files on `tmsminstall.mpkg.zip` may become corrupted if users launch it using archiving tools not built-in on the Mac.

To launch `tmsminstall.mpkg.zip` from Terminal, use the following command:

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

For example:

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

Launching `tmsminstall.mpkg.zip` extracts the file `tmsminstall.mpkg`.

4. Open Apple Remote Desktop on the endpoint.
5. Select the endpoints to which to install the Trend Micro Security (for Mac) agent and then click **Install**.

6. On the Install Packages screen, drag the installation package or click "+" to locate the installation package.

7. (Optional) Click **Save** to automatically run the installation task on new endpoints that connect to the network.

8. Click **Install**.

   The Apple Remote Desktop starts installing the agent to the selected endpoints. If the installation was successful on all endpoints, the message `Install`

`Packages: Succeeded on all` appears. Otherwise, `Successful` appears under **Task Status** for each endpoint on which the installation was successful.

Agents automatically register to the server where the agent installation package was obtained. Agents also update for the first time.

### What to do next

Perform agent post-installation tasks. For details, see *Agent Post-installation on page 4-12*.

## 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. See *Agent Updates on page 5-8* for details.

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 5

# 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) | 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.<br><br>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:<br><br>• Incorporation of new scanning and detection technologies into the software<br>• Discovery of a new, potentially harmful security risk that the scan engine cannot handle<br>• Enhancement of the scanning performance<br>• Addition of file formats, scripting languages, encoding, and/or compression formats |
| Virus Pattern | 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. |

# 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.

You can configure the Trend Micro Security (for Mac) server to update from a source other than the Trend Micro ActiveUpdate server. To do this, you need to set up a custom update source. For assistance in setting up this update source, contact your support provider.

The following table describes the different component update options for the Trend Micro Security (for Mac) server and agents:

**TABLE 5-1. Server-Agent Update Options**

| UPDATE OPTION | DESCRIPTION |
|---|---|
| ActiveUpdate server<br>↓<br>Trend Micro Security (for Mac) server<br>↓<br>Agents | The Trend Micro Security (for Mac) server receives updated components from the Trend Micro ActiveUpdate server (or another update source if a custom source has been set up) and then deploys the components to agents. |
| ActiveUpdate server<br>↓<br>Agents | 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. |

# Server Update

The Trend Micro Security (for Mac) server downloads the following components and deploys them to agents:

- Virus Pattern

- Spyware Active-monitoring Pattern
- Virus Scan Engine (32-bit/64-bit)
- Damage Cleanup Engine (64-bit)
- Damage Cleanup Template
- Smart Scan Agent Pattern

View the current versions of components on the web console's Summary screen, and determine the number of agents with updated and outdated components.

If you use a proxy server to connect to the Internet, use the correct proxy settings to download updates successfully.

## Configuring the Server Update Source

Configure the Trend Micro Security (for Mac) server to download components from the Trend Micro ActiveUpdate server or from another source.

**Note**

If the server only has an IPv6 address, read the IPv6 limitations for server updates in *Pure IPv6 Server Limitations on page A-3*.

After the server downloads any available updates, it automatically notifies agents to update their components. If the component update is critical, let the server notify the agents at once by navigating to **Agents** > **Agent Management** > **Tasks** > **Update**.

**Procedure**

1. Navigate to **Updates** > **Server** > **Update Source**.
2. Select the location from where you want to download component updates.
   - If you choose ActiveUpdate server:
     - Ensure that the Trend Micro Security (for Mac) server has Internet connection.

- If you are using a proxy server, test if Internet connection can be established using the proxy settings.

  For details, see *Configuring Proxy Settings for Server Updates on page 5-6*.

- If you choose a custom update source:
  - Set up the appropriate environment and update resources for this update source.
  - Ensure that there is functional connection between the server computer and this update source. For assistance in setting up an update source, contact your support provider.
  - You can obtain updates from Control Manager by typing the Control Manager HTTP address.

3. Click **Save**.

## Configuring Proxy Settings for Server Updates

Configure the Trend Micro Security (for Mac) server to use proxy settings when downloading updates from the Trend Micro ActiveUpdate server.

**Note**

If the server only has an IPv6 address, read the IPv6 limitations for proxy settings in *Pure IPv6 Server Limitations on page A-3*.

**Procedure**

1. Navigate to **Administration** > **External Proxy Settings**.
2. Select the check box to enable the use of a proxy server.
3. Specify the proxy server name or IPv4/IPv6 address and port number.
4. If the proxy server requires authentication, type the user name and password in the fields provided.

5. Click **Save**.

## Server Update Methods

Update Trend Micro Security (for Mac) server components manually or by configuring an update schedule.

- **Manual update**: When an update is critical, perform manual update so the server can obtain the updates immediately. See *Manually Updating the Server on page 5-8* for details.
- **Scheduled update**: The Trend Micro Security (for Mac) server connects to the update source during the scheduled day and time to obtain the latest components. See *Scheduling Updates for the Server on page 5-7* for details.

After the server finishes an update, it immediately notifies agents to update.

### Scheduling Updates for the Server

Configure the Trend Micro Security (for Mac) server to regularly check its update source and automatically download any available updates. Using scheduled update is an easy and effective way of ensuring that protection against security risks is always current.

After the server finishes an update, it notifies agents to update.

**Procedure**

1. Navigate to **Updates** > **Server** > **Scheduled Update**.
2. Select the components to update.
3. Specify the update schedule.

   For daily, weekly, and monthly updates, the period of time is the number of hours during which Trend Micro Security (for Mac) will perform the update. Trend Micro Security (for Mac) updates at any given time during this time period.

For monthly updates, if you selected the 29th, 30th, or 31st day and a month does not have this day, Trend Micro Security (for Mac) runs the update on the last day of the month.

4. Click **Save**.

---

### Manually Updating the Server

Manually update the components on the Trend Micro Security (for Mac) server after installing or upgrading the server and whenever there is an outbreak.

---

**Procedure**

1. Navigate to **Updates** > **Server** > **Manual Update**.
2. Select the components to update.
3. Click **Update**.

   The server downloads the updated components.

   After the server finishes an update, it immediately notifies agents to update.

---

## 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:<br>• Agent Management screen.<br>For details, see *Launching Agent Update from the Agent Management Screen on page 5-13*.<br>• Summary screen.<br>For details, see *Launching Agent Update from the Summary Screen on page 5-12*. |
| Automatic update | • After the server finishes an update, it immediately notifies agents to update.<br>For details, see *Configuring Agent Automatic Update on page 5-10*.<br>• Updates can run according to the schedule that you configured. You can configure a schedule that applies to one or several agents and domains, or to all the agents that the server manages.<br>For details, see *Configuring Agent Update Settings on page 5-11*. |
| 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.

Before updating the agents, check if the Trend Micro Security (for Mac) server has the latest components.

For information on how to update the Trend Micro Security (for Mac) server, see *Server Update on page 5-4*.

Configure one, several, or all agents to download from the Trend Micro ActiveUpdate server if the Trend Micro Security (for Mac) server is unavailable.

For details, see *Configuring Agent Update Settings on page 5-11*.

**Note**

If an agent only has an IPv6 address, read the IPv6 limitations for agent updates in *Pure IPv6 Agent Limitations on page A-3*.

### 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 5-2. 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**.

## Configuring Agent Update Settings

For a detailed explanation of agent updates, see *Agent Updates on page 5-8*.

**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 **Settings** > **Update Settings**.
4. Select **Agents download updates from the Trend Micro ActiveUpdate server when unable to connect to the Trend Micro Security (for Mac) server** to allow external agents to download updates from the Trend Micro ActiveUpdate server.

**Note**

If an agent only has an IPv6 address, read the IPv6 limitations for agent updates in *Pure IPv6 Agent Limitations on page A-3*.

5. Select **Agents can update the components but not upgrade the agent program or install hot fixes** to allow component updates to proceed but prevents Trend Micro Security (for Mac) agent upgrade.

6. To set up scheduled updates, complete the following steps:

   a. Select **Enable scheduled update**.

   b. Configure the schedule.

   c. If you select **Daily** or **Weekly**, specify the time of the update and the time period the Trend Micro Security (for Mac) server will notify agents to update components. For example, if the start time is 12pm and the time period is 2 hours, the server randomly notifies all online agents to update components from 12pm until 2pm. This setting prevents all online agents from simultaneously connecting to the server at the specified start time, significantly reducing the amount of traffic directed to the server.

7. If you selected group(s) or agent(s) on the agent tree, click **Save** to apply settings to the group(s) or agent(s). If you selected the root icon ( ), choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future 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.

## Launching Agent Update from the Summary Screen

For other agent update methods, see *Agent Updates on page 5-8*.

**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 5-8*.

**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 6

# 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:

| 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.<br>• **Boot sector virus**: A virus that infects the boot sector of a partition or a disk<br>• **Java malicious code**: Operating system-independent virus code written or embedded in Java<br>• **Macro virus**: A virus encoded as an application macro and often included in a document<br>• **VBScript, JavaScript, or HTML virus**: A virus that resides on web pages and downloads through a browser<br>• **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:<br>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.

Trend Micro Security (for 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 Method Types

Trend Micro Security (for Mac) agents can use one of two scan methods when scanning for security risks. The scan methods are smart scan and conventional scan.

- **Smart Scan**

  Agents that use smart scan are referred to as "smart scan agents" in this document. Smart scan agents benefit from local scans and in-the-cloud queries provided by File Reputation Services.

- **Conventional Scan**

  Agents that do not use smart scan are called "conventional scan agents". A conventional scan agent stores all Trend Micro Security (for Mac) components on the agent endpoint and scans all files locally.

## Default Scan Method

If Trend Micro Security (for Mac) is installed on a server with OfficeScan 10.6 SP3 P1 Critical Patch or later, the default scan method for fresh installations is smart scan.

If Trend Micro Security (for Mac) is installed on a server with an OfficeScan version earlier than version 10.6 SP3 P1 Critical Patch, the default scan method for fresh installations is conventional scan.

## Scan Methods Compared

The following table provides a comparison between the two scan methods:

**TABLE 6-1. Conventional Scan and Smart Scan Compared**

| BASIS OF COMPARISON | CONVENTIONAL SCAN | SMART SCAN |
|---|---|---|
| Availability | Available in this Trend Micro Security (for Mac) version and all earlier versions. | Available starting in Trend Micro Security (for Mac) 3.0. |

| Basis of Comparison | Conventional Scan | Smart Scan |
|---|---|---|
| Scanning behavior | The conventional scan agent performs scanning on the local endpoint. | • The smart scan agent performs scanning on the local endpoint.<br>• If the agent cannot determine the risk of the file during the scan, the agent verifies the risk by sending a scan query to a smart protection source.<br>• The agent "caches" the scan query result to improve the scan performance. |
| Components in use and updated | All components available on the update source, except the Smart Scan Agent Pattern. | All components available on the update source, except the Virus Pattern and Spyware Active-monitoring Pattern. |
| Typical update source | Trend Micro Security (for Mac) server | Trend Micro Security (for Mac) server |

## Changing the Scan Method

**Procedure**

1. Go 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 **Settings** > **Scan Methods**.
4. Select **Conventional scan** or **Smart scan**.
5. If you selected group(s) or agent(s) in the agent tree, click **Save**. If you clicked the root icon, choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future group. Future groups are groups not yet created at the time you configured the settings.

- **Apply to Future Groups Only**: Applies settings only to agents added to future groups. This option will not apply settings to new agent added to an existing group.

## Switching from Smart Scan to Conventional Scan

The following table provides other considerations when switching agents to conventional scan.

**TABLE 6-2. Considerations When Switching to Conventional Scan**

| CONSIDERATION | DETAILS |
|---|---|
| Number of agents to switch | Switching a relatively small number of agents at a time allows efficient use of the Trend Micro Security (for Mac) server and Smart Protection Server resources. These servers can perform other critical tasks while agents change their scan methods. |
| Timing | When switching back to conventional scan, agents will likely download the full version of the Virus Pattern and Spyware-active Monitoring Pattern from the Trend Micro Security (for Mac) server. These pattern files are only used by conventional scan agents.<br><br>Consider switching during off-peak hours to ensure the download process finishes within a short amount of time. Also consider switching when no agent is scheduled to update from the server. |

| CONSIDERATION | DETAILS |
| --- | --- |
| Agent tree settings | Scan method is a granular setting that can be set on the root, domain, or individual agent level. When switching to conventional scan, you can:<br>• Create a new group and assign conventional scan as its scan method. Any agent you move to this group will use conventional scan. When you move the agent, enable the setting **Apply settings of new group to selected agent(s)**.<br>• Select a group and configure it to use conventional scan. Smart scan agents belonging to the group will switch to conventional scan.<br>• Select one or several smart scan agents from a group and then switch them to conventional scan.<br>**Note**<br>Any changes to the group's scan method overrides the scan method you have configured for individual agents. |

## Switching from Conventional Scan to Smart Scan

If you are switching agents from conventional scan to smart scan, ensure that you have set up Smart Protection Services on the OfficeScan server. For details, see the OfficeScan documentation.

The following table provides other considerations when switching agents to smart scan.

**TABLE 6-3. Considerations When Switching to Smart Scan**

| CONSIDERATION | DETAILS |
|---|---|
| Product license | To use smart scan, ensure that you have activated the licenses for the following services on the OfficeScan server and that the licenses are not expired:<br>• Antivirus<br>• Web Reputation and Anti-spyware |
| Trend Micro Security (for Mac) server | Ensure that agents can connect to the Trend Micro Security (for Mac) server. Only online agents will be notified to switch to smart scan. Offline agents get notified when they become online. Roaming agents are notified when they become online or, if the agent has scheduled update privileges, when scheduled update runs.<br>Also verify that the Trend Micro Security (for Mac) server has the latest components because smart scan agents need to download the Smart Scan Agent Pattern from the server. To update components, see *Server Update on page 5-4*. |
| Number of agents to switch | Switching a relatively small number of agents at a time allows efficient use of Trend Micro Security (for Mac) server resources. The Trend Micro Security (for Mac) server can perform other critical tasks while agents change their scan methods. |
| Timing | When switching to smart scan for the first time, agents need to download the full version of the Smart Scan Agent Pattern from the Trend Micro Security (for Mac) server. The Smart Scan Pattern is only used by smart scan agents.<br>Consider switching during off-peak hours to ensure the download process finishes within a short amount of time. Also consider switching when no agent is scheduled to update from the server. |

| CONSIDERATION | DETAILS |
|---|---|
| Agent tree settings | Scan method is a granular setting that can be set on the root, group, or individual agent level. When switching to smart scan, you can:<br>• Create a new group and assign smart scan as its scan method. Any agent you move to this group will use smart scan. When you move the agent, enable the setting **Apply settings of new group to selected agent(s)**.<br>• Select a group and configure it to use smart scan. Conventional scan agents belonging to the group will switch to smart scan.<br>• Select one or several conventional scan agents from a group and then switch them to smart scan.<br>**Note**<br>Any changes to the group's scan method overrides the scan method you have configured for individual agents. |
| IPv6 support | Smart scan agents send scan queries to smart protection sources.<br>A pure IPv6 smart scan agent cannot send queries directly to pure IPv4 sources, such as:<br>• Smart Protection Server 3.0 (integrated or standalone)<br>**Note**<br>IPv6 support for Smart Protection Server starts in version 2.5.<br>• Trend Micro Smart Protection Network<br>Similarly, a pure IPv4 smart scan agent cannot send queries to pure IPv6 Smart Protection Servers.<br>A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow smart scan agents to connect to the sources. |

# Scan Types

Trend Micro Security (for Mac) provides the following scan types to protect endpoints from security risks:

| Scan Type | Description |
|---|---|
| Real-time Scan | Automatically scans a file on the endpoint as it is received, opened, downloaded, copied, or modified<br><br>See *Real-time Scan on page 6-11*. |
| Manual Scan | A user-initiated scan that scans a file or a set of files requested by the user<br><br>See *Manual Scan on page 6-12*. |
| Scheduled Scan | Automatically scans files on the endpoint based on the schedule configured by the administrator<br><br>See *Scheduled Scan on page 6-14*. |
| Scan Now | An administrator-initiated scan that scans files on one or several target endpoints<br><br>See *Scan Now on page 6-15*. |

## Real-time Scan

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If Trend Micro Security (for Mac) does not detect a security risk, the file remains in its location and users can proceed to access the file. If Trend Micro Security (for Mac) detects a security risk, it displays a notification message, showing the name of the infected file and the specific security risk.

Configure and apply Real-time Scan settings to one or several agents and groups, or to all agents that the server manages.

## Configuring Real-time Scan Settings

**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 **Settings** > **Real-time Scan Settings**.
4. Configure the following scan criteria:
   - *User Activity on Files on page 6-16*
   - *Scan Settings on page 6-17*
5. Click the **Action** tab to configure the scan actions Trend Micro Security (for Mac) performs on detected security risks.

   For details about scan actions, see *Scan Action Options and Additional Settings on page 6-20*.
6. If you selected group(s) or agent(s) on the agent tree, click **Save** to apply settings to the group(s) or agent(s). If you selected the root icon ( ), choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future 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.

# Manual Scan

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the agent console. The time it takes to complete scanning depends on the number of files to scan and the endpoint's hardware resources.

Configure and apply Manual Scan settings to one or several agents and groups, or to all agents that the server manages.

## Configuring Manual Scan Settings

**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 **Settings** > **Manual Scan Settings**.
4. Configure the following scan criteria:
   - *Scan Settings on page 6-17*
   - *CPU Usage on page 6-18*
5. Click the **Action** tab to configure the scan actions Trend Micro Security (for Mac) performs on detected security risks.

   For details about scan actions, see *Scan Action Options and Additional Settings on page 6-20*.
6. If you selected group(s) or agent(s) on the agent tree, click **Save** to apply settings to the group(s) or agent(s). If you selected the root icon ( ), choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future 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.

# Scheduled Scan

Scheduled Scan runs automatically on the appointed date and time. Use Scheduled Scan to automate routine scans on the agent and improve scan management efficiency.

Configure and apply Scheduled Scan settings to one or several agents and groups, or to all agents that the server manages.

## Configuring Scheduled Scan Settings

**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 **Settings** > **Scheduled Scan Settings**.
4. Select the check box to enable Scheduled Scan.
5. Configure the following scan criteria:
   - *Schedule on page 6-19*
   - *Scan Target on page 6-16*
   - *Scan Settings on page 6-17*
   - *CPU Usage on page 6-18*
6. Click the **Action** tab to configure the scan actions Trend Micro Security (for Mac) performs on detected security risks.

   For details about scan actions, see *Scan Action Options and Additional Settings on page 6-20*.
7. If you selected group(s) or agent(s) on the agent tree, click **Save** to apply settings to the group(s) or agent(s). If you selected the root icon ( ), choose from the following options:

- **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future 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.

## 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, except the actual schedule, are used during Scan Now. To configure settings before initiating Scan Now, follow the steps in *Configuring Scheduled Scan Settings on page 6-14*.

**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**.

# Settings Common to All Scan Types

For each scan type, configure three sets of settings: scan criteria, scan exclusions, and scan actions. Deploy these settings to one or several agents and groups, or to all agents that the server manages.

## Scan Criteria

Specify which files a particular scan type should scan using file attributes such as file type and extension. Also specify conditions that will trigger scanning. For example, configure Real-time Scan to scan each file after it is downloaded to the endpoint.

### User Activity on Files

Choose activities on files that will trigger Real-time Scan. Select from the following options:

- **Scan files being created/modified**: Scans new files introduced into the endpoint (for example, after downloading a file) or files being modified
- **Scan files being retrieved/executed**: Scans files as they are opened
- **Scan files being created/modified and retrieved/executed**

For example, if the third option is selected, a new file downloaded to the endpoint will be scanned and stays in its current location if no security risk is detected. The same file will be scanned when a user opens the file and, if the user modified the file, before the modifications are saved.

### Scan Target

Select from the following options:

- **All scannable files**: Scan all files
- **File types scanned by IntelliScan**: Only scan files known to potentially harbor malicious code, including files disguised by a harmless extension name.

- **File or folder name with full path**: Only scan the specified file or files found in a specific folder.

  1. Type a full file path or directory path and then click **Add**.

     - Full file path example: `/Users/username/temp.zip`
     - Directory path example: `/Users/username`

  2. To delete a directory path or full file path, select it and then click **Remove**.

## Scan Settings

Select one or more of the following options:

- **Scan compressed files**: Allows Trend Micro Security (for Mac) can scan individual files within compressed files. Trend Micro Security (for Mac) supports the following compression types:

| EXTENSION | TYPE |
|---|---|
| .zip | Archive created by Pkzip |
| .rar | Archive created by RAR |
| .tar | Archive created by Tar |
| .arj | ARJ Compressed archive |
| .hqx | BINHEX |
| .gz; .gzip | Gnu ZIP |
| .Z | LZW/Compressed 16bits |
| .bin | MacBinary |
| .cab | Microsoft Cabinet file |
| Microsoft Compressed/ MSCOMP | |
| .eml; .mht | MIME |

| EXTENSION | TYPE |
|---|---|
| .td0 | Teledisk format |
| .bz2 | Unix BZ2 Bzip compressed file |
| .uu | UUEncode |
| .ace | WinAce |

- **Scan Time Machine**: Allows Trend Micro Security (for Mac) to detect and scan Time Machine drives.

**Note**

After enabling the **Scan Time Machine** option for Manual and Scheduled Scan, Trend Micro Security (for Mac) can only detect malware threats but not take any action (clean, quarantine, or delete) due to a permission limitation in the Mac OS. Any configured actions display as unsuccessful in the product logs.

- **Scan network drives**: Scans network drives or folders mapped to the endpoint.
- **Skip Scheduled Scan When a Wireless Endpoint's Battery Life is Less Than __ % and its AC Adapter is Unplugged**: Trend Micro Security (for Mac) skips a Scheduled Scan if it detects that a wireless endpoint's battery life is running low and its AC adapter is not connected to any power source. If battery life is low but the AC adapter is connected to a power source, scanning proceeds. If a scan is in progress when the battery life is low, the scan is not terminated.

## CPU Usage

Trend Micro Security (for Mac) can pause after scanning one file and before scanning the next file. This setting is used during Manual Scan, Scheduled Scan, and Scan Now.

Select from the following options:

- **High**: No pausing between scans
- **Low**: Pause between file scans

### Schedule

Configure how often (daily, weekly, or monthly) and what time Scheduled Scan will run.

For monthly Scheduled Scans, if you selected the 29th, 30th, or 31st day and a month does not have this day, Trend Micro Security (for Mac) runs Scheduled Scan on the last day of the month.

## Scan Actions

Specify the action Trend Micro Security (for Mac) performs when a particular scan type detects a security risk.

The action Trend Micro Security (for Mac) performs depends on the scan type that detected the security risk. For example, when Trend Micro Security (for Mac) detects a security risk during Manual Scan (scan type), it cleans (action) the infected file.

The following are the actions Trend Micro Security (for Mac) can perform against security risks:

| Scan Action | Details |
|---|---|
| Delete | Trend Micro Security (for Mac) removes the infected file from the endpoint. |
| Quarantine | Trend Micro Security (for Mac) renames and then moves the infected file to the quarantine directory on the endpoint located in <*Agent installation folder*>`/common/lib/vsapi/quarantine`.<br><br>Once in the quarantine directory, Trend Micro Security (for Mac) can perform another action on the quarantined file, depending on the action specified by the user. Trend Micro Security (for Mac) can delete, clean, or restore the file. Restoring a file means moving it back to its original location without performing any action. Users may restore the file if it is actually harmless. Cleaning a file means removing the security risk from the quarantined file and then moving it to its original location if cleaning is successful. |

| SCAN ACTION | DETAILS |
|---|---|
| Clean | Trend Micro Security (for Mac) removes the security risk from an infected file before allowing users to access it.<br><br>If the file is uncleanable, Trend Micro Security (for Mac) performs a second action, which can be one of the following actions: Quarantine, Delete, and Pass. To configure the second action, navigate to **Agent Management** > **Settings** > **{Scan Type}** and click the **Action** tab. |
| Pass | Trend Micro Security (for Mac) performs no action on the infected file but records the detected security risk in the logs. The file stays where it is located.<br><br>Trend Micro Security (for Mac) always performs "Pass" on files infected with the Probable Virus/Malware type to mitigate a False Positive. If further analysis confirms that probable virus/malware is indeed a security risk, a new pattern will be released to allow Trend Micro Security (for Mac) to perform the appropriate scan action. If actually harmless, probable virus/malware will no longer be detected.<br><br>For example: Trend Micro Security (for Mac) detects "x_probable_virus" on a file named "123.pdf" and performs no action at the time of detection. Trend Micro then confirms that "x_probable_virus" is a Trojan horse program and releases a new Virus Pattern version. After loading the new pattern, Trend Micro Security (for Mac) will detect "x_probable_virus" as a Trojan program and, if the action against such programs is "Delete", will delete "123.pdf". |

## Scan Action Options and Additional Settings

When configuring the scan action, select from the following options:

| OPTION | DETAILS |
|---|---|
| Use ActiveAction | ActiveAction is a set of pre-configured scan actions for different types of security risks. If you are unsure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction.<br><br>ActiveAction settings are constantly updated in the pattern files to protect endpoints against the latest security risks and the latest methods of attacks. |
| Use the same action for all security risk types | Select this option if you want the same action performed on all types of security risks, except probable virus/malware. For Probable Virus/Malware, the action is always "Pass".<br><br>If you choose "Clean" as the first action, select a second action that Trend Micro Security (for Mac) performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable.<br><br>For details about scan actions, see *Scan Actions on page 6-19*. |

### Additional Real-time Scan Settings

| SETTING | DETAILS |
|---|---|
| Display a notification message when a security risk is detected | When Trend Micro Security (for Mac) detects a security risk during Real-time Scan, it can display a notification message to inform the user about the detection. |

### Scheduled Scan Privileges

If Scheduled Scan is enabled on the endpoint, users can postpone and skip/stop Scheduled Scan.

| PRIVILEGE | DETAILS |
|---|---|
| Postpone Scheduled Scan | Users with the "Postpone Scheduled Scan" privilege can perform the following actions:<br>• Postpone Scheduled Scan before it runs and then specify the postpone duration. Scheduled Scan can only be postponed once.<br>• If Scheduled Scan is in progress, users can stop scanning and restart it later. Users then specify the amount of time that should elapse before scanning restarts. When scanning restarts, all previously scanned files are scanned again. Scheduled Scan can be stopped and then restarted only once.<br>Configure the number of hours and minutes, which corresponds to:<br>• The maximum postpone duration<br>• The maximum amount of time that should elapse before scanning restarts |
| Skip and Stop Scheduled Scan | This privilege allows users to perform the following actions:<br>• Skip Scheduled Scan before it runs<br>• Stop Scheduled Scan when it is in progress |

## Additional Scheduled Scan Settings

| SETTING | DETAILS |
|---|---|
| Display a notification before Scheduled Scan runs | When you enable this option, a notification message displays on the endpoint several minutes before Scheduled Scan runs. Users are notified of the scan schedule (date and time) and their Scheduled Scan privileges, such as postponing, skipping, or stopping Scheduled Scan.<br>Configure the timing for displaying the notification message, in number of minutes. |

| SETTING | DETAILS |
|---|---|
| Automatically stop Scheduled Scan when scanning lasts more than __ hours and __ minutes | The agent stops scanning when the specified amount of time is exceeded and scanning is not yet complete. The agent immediately notifies users of any security risk detected during scanning. |

## Scan Exclusions

Configure scan exclusions to increase the scanning performance and skip scanning files that are known to be harmless. When a particular scan type runs, Trend Micro Security (for Mac) checks the scan exclusion list to determine which files on the endpoint will be excluded from scanning.

| SCAN EXCLUSION LIST | DETAILS |
|---|---|
| Files | Trend Micro Security (for Mac) will not scan a file if:<br>• The file is located under the directory path specified in the scan exclusion list<br>• The file matches the full file path (directory path and file name) specified in the scan exclusion list |
| File extensions | Trend Micro Security (for Mac) will not scan a file if its file extension matches any of the extensions included in this exclusion list. |

### Configuring Scan Exclusion Lists

For details about Scan Exclusion Lists, see *Scan Exclusions on page 6-23*.

**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 **Settings** > **Scan Exclusion Settings**.
4. Select the check box to enable scan exclusion.
5. To configure the **Scan Exclusion List (Files)**:
   a. Type a full file path or directory path and click **Add**.

      Reminders:

      - It is not possible to type only a file name.
      - You can specify a maximum of 64 paths. See the following table for examples.

| PATH | DETAILS | EXAMPLES |
|---|---|---|
| Full file path | Excludes a specific file on the endpoint | • Example 1: `/file.log`<br>• Example 2: `/System/file.log` |

| PATH | DETAILS | EXAMPLES |
|---|---|---|
| Directory path | Excludes all files located on a specific folder and all its subfolders | • Example 1:<br>`/System/`<br>Examples of files excluded from scans:<br>• `/System/file.log`<br>• `/System/Library/file.log`<br>Examples of files that will be scanned:<br>• `/Applications/file.log`<br>• Example 2:<br>`/System/Library`<br>Examples of files excluded from scans:<br>• `/System/Library/file.log`<br>• `/System/Library/Filters/file.log`<br>Examples of files that will be scanned:<br>• `/System/file.log` |

- Use the asterisk wildcard (*) in place of folder names.

  See the following table for examples.

| PATH | WILDCARD USAGE EXAMPLES |
|---|---|
| Full file path | `/Users/Mac/*/file.log`<br>Examples of files excluded from scans:<br>• `/Users/Mac/Desktop/file.log`<br>• `/Users/Mac/Movies/file.log`<br>Examples of files that will be scanned:<br>• `/Users/file.log`<br>• `/Users/Mac/file.log` |
| Directory path | • Example 1:<br>`/Users/Mac/*`<br>Examples of files excluded from scans:<br>• `/Users/Mac/doc.html`<br>• `/Users/Mac/Documents/doc.html`<br>• `/Users/Mac/Documents/Pics/pic.jpg`<br>Examples of files that will be scanned:<br>• `/Users/doc.html`<br>• Example 2:<br>`/*/Components`<br>Examples of files excluded from scans:<br>• `/Users/Components/file.log`<br>• `/System/Components/file.log`<br>Examples of files that will be scanned:<br>• `/file.log`<br>• `/Users/file.log`<br>• `/System/Files/file.log` |

- Partial matching of folder names is not supported. For example, it is not possible to type `/Users/*user/temp` to exclude files on folder names ending in "user", such as "end_user" or "new_user".

b. To delete a path, select it and click **Remove**.

6. To configure the **Scan Exclusion List (File Extensions)**:

   a. Type a file extension without a period (.) and click **Add**. For example, type `pdf`. You can specify a maximum of 64 file extensions.

   b. To delete a file extension, select it and click **Remove**.

7. If you selected group(s) or agent(s) on the agent tree, click **Save** to apply settings to the group(s) or agent(s). If you selected the root icon ( ), choose from the following options:

   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future 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.

---

## Cache Settings for Scans

Each time scanning runs, the agent checks the modified files cache to see if a file has been modified since the last agent startup.

- If a file has been modified, the agent scans the file and adds it to the scanned files cache.
- If a file has not been modified, the agent checks if the file is in the scanned files cache.
  - If the file is in the scanned files cache, the agent skips scanning the file.
  - If the file is not in the scanned files cache, the agent checks the approved files cache.

**Note**

The approved files cache contains files that Trend Micro Security (for Mac) deems trustworthy. Trustworthy files have been scanned by successive versions of the pattern and declared threat-free each time, or threat-free files that have remained unmodified for an extended period of time.

- If the file is in the approved files cache, the agent skips scanning the file.
- If the file is not in the approved files cache, the agent scans the file and adds it to the scanned files cache.

All or some of the caches are cleared whenever the scan engine or pattern is updated.

If scans are run frequently and many files hit the caches, the scanning time reduces significantly.

If scans are seldom run, disable the caches so that files can be checked for threats with each scan.

## Configuring Cache Settings for Scans

For details about the on-demand scan cache, see *Cache Settings for Scans on page 6-27*.

**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 **Settings** > **Cache Settings for Scans**.
4. Select **Enable the on-demand scan cache**.
5. If you selected group(s) or agent(s) on the agent tree, click **Save** to apply settings to the group(s) or agent(s). If you selected the root icon ( ), choose from the following options:

- **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future 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.

# 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 8-7*.

# 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 Administrator Notification Settings

When security risks are detected or when an outbreak occurs, Trend Micro Security (for Mac) administrators can receive notifications through email.

---

**Procedure**

1. Navigate to **Notifications** > **General Settings**.
2. In the **SMTP server** field, type either an IPv4/IPv6 address or endpoint name.
3. Type a port number between 1 and 65535.
4. Type the sender's email address in the **From** field.
5. Click **Save**.

---

## 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. For details, see *Configuring Administrator Notification Settings on page 6-30*.

**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.

You can receive notifications through email. Configure administrator notification settings to allow Trend Micro Security (for Mac) to successfully send notifications through email. For details, see *Configuring Administrator Notification Settings on page 6-30*.

---

**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 |
| %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 6-34*.
   - 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 8-7*.

## 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 6-36*.

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

# 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 7

# 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 Web Reputation Settings

Web Reputation settings include policies that dictate whether Trend Micro Security (for Mac) will block or allow access to a website. To determine the appropriate policy to use, Trend Micro Security (for Mac) checks the agent's location. An agent's location is "internal" if it can connect to the Trend Micro Security (for Mac) server. Otherwise, an agent's location is "external".

**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 **Settings** > **Web Reputation Settings**.
4. To configure a policy for external agents:
   a. Click the **External Agents** tab.
   b. Select **Enable Web Reputation policy**.

      When the policy is enabled, external agents send web reputation queries to the Smart Protection Network.

      **Note**

      If an agent only has an IPv6 address, read the IPv6 limitations for Web Reputation queries in *Pure IPv6 Agent Limitations on page A-3*.

   c. Select from the available web reputation security levels: **High**, **Medium** or **Low**

      **Note**

      The security levels determine whether Trend Micro Security (for Mac) will allow or block access to a URL. For example, if you set the security level to Low, Trend Micro Security (for Mac) only blocks URLs that are known to be web threats. As you set the security level higher, the web threat detection rate improves but the possibility of false positives also increases.

d. To submit web reputation feedback, click the URL provided. The Trend Micro Web Reputation Query system opens in a browser window.

**5.** To configure a policy for internal agents:

a. Click the **Internal Agents** tab.

b. Select **Enable Web Reputation policy**.

When the policy is enabled, internal agents send web reputation queries to:

- Smart Protection Servers if the **Send queries to Smart Protection Servers** option is enabled.
- Smart Protection Network if the **Send queries to Smart Protection Servers** option is disabled.

**Note**

If an agent only has an IPv6 address, read the IPv6 limitations for Web Reputation queries in *Pure IPv6 Agent Limitations on page A-3*.

c. Select **Send queries to Smart Protection Servers** if you want internal agents to send web reputation queries to Smart Protection Servers.

- If you enable this option, agents refer to the same smart protection source list used by OfficeScan agents to determine the Smart Protection Servers to which they send queries.

**Important**

Before enabling this option, read the guidelines in *Trend Micro Smart Protection on page 3-14*.

- If you disable this option, agents send web reputation queries to Smart Protection Network. Endpoints must have Internet connection to send queries successfully.

d. Select from the available web reputation security levels: **High**, **Medium** or **Low**

**Note**

The security levels determine whether Trend Micro Security (for Mac) will allow or block access to a URL. For example, if you set the security level to Low, Trend Micro Security (for Mac) only blocks URLs that are known to be web threats. As you set the security level higher, the web threat detection rate improves but the possibility of false positives also increases.

Agents do not block untested websites, regardless of the security level.

e. To submit web reputation feedback, click the URL provided. The Trend Micro Web Reputation Query system opens in a browser window.

f. Select whether to allow the agents to send web reputation logs to the server. Allow agents to send logs if you want to analyze URLs being blocked by Trend Micro Security (for Mac) and take the appropriate action on URLs you think are safe to access.

**6.** If you selected group(s) or agent(s) on the agent tree, click **Save** to apply settings to the group(s) or agent(s). If you selected the root icon ( ), choose from the following options:

- **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future 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.

# 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.

**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 8-7*.

# Chapter 8

# Managing the Server and Agents

This chapter describes Trend Micro Security (for Mac) server and agent management and additional configurations.

# Agent Self-protection

The Trend Micro Security (for Mac) agent self-protection feature prevents other programs and even the user from modifying or deleting files that Trend Micro Security (for Mac) agent uses.

When you enable **Protect files used by the agent** and the Trend Micro Security (for Mac) agent is running on an endpoint, Trend Micro Security (for Mac) locks the following files and folders:

- /Library/Application Support/TrendMicro/common
- /Library/Application Support/TrendMicro/Kext
- /Library/Application Support/TrendMicro/TmccMac
- /Library/Application Support/TrendMicro/TmccUpdate
- /Library/Application Support/TrendMicro/Plug-in
- /Library/Application Support/TrendMicro/Tools
- /Library/LaunchDaemons/com.trendmicro.icore.*
- /Library/LaunchDaemons/com.trendmicro.tmsm.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.launcher.plist
- /Application/TrendMicroSecurity.app

**Note**

Trend Micro Security (for Mac) allows files to be added in the `/Library/Application Support/TrendMicro/Tools` folder, files cannot be deleted from the folder.

## Configuring Agent Self-protection

**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 **Settings** > **Agent Self-protection**.
4. Select **Protect files used by the agent**.
5. If you selected group(s) or agent(s) on the agent tree, click **Save** to apply settings to the group(s) or agent(s). If you selected the root icon ( ), choose from the following options:
   - **Apply to All Agents**: Applies settings to all existing agents and to any new agent added to an existing/future 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.

---

# 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**.

---

# Upgrading the Server and Agents

The Plug-in Manager console displays any new Trend Micro Security (for Mac) build or version.

Upgrade the server and agents immediately when the new build or version becomes available.

Before upgrading, be sure that the server and agents have the resources outlined in *Server Installation Requirements on page 2-2* and *Agent Installation Requirements on page 4-2*.

## Upgrading the Server

### Before you begin

Trend Micro recommends backing up the server's program files and database, which can be restored if there are problems with the upgrade.

- Program files
  - Default path:

    `C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM`

    Or

    `C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\TMSM`
  - Files to back up:
    - `..\apache-activemq\conf\.*`
    - `..\apache-activemq\bin\wrapper.conf`
    - `.\ServerInfo.plist`
- Database files. See *Backing Up the Server Database on page 8-9*.

---

**Procedure**

1. Open the OfficeScan web console and click **Plug-ins** on the main menu.

2. Go to the **Trend Micro Security (for Mac)** section and click **Download**.

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

Plug-in Manager downloads the package to `<OfficeScan server installation folder>\PCCSRV\Download`.

`<OfficeScan server installation folder>` is typically `C:\Program Files\Trend Micro\OfficeScan`.

3. Monitor the download progress.

You can navigate away from the screen during the download.

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

4. To upgrade Trend Micro Security (for Mac) immediately, click **Upgrade Now**, or to install at a later time, perform the following:

   a. Click **Upgrade Later**.

   b. Open the Plug-in Manager screen.

   c. Go to the **Trend Micro Security (for Mac)** section and click **Upgrade**.

5. Monitor the upgrade progress. After the upgrade, the Plug-in Manager screen reloads.

## Upgrading Agents

**Attention**

To allow agent upgrade, make sure that the **Agents can update the components but not upgrade the agent program** check box is not select in the **Agent Management** > **Settings** > **Update Settings** screen.

**Procedure**

1. Perform any of the following steps:

   - Perform a manual update. Ensure that you select **Trend Micro Security (for Mac) Agent** from the list of components.
   - On the agent tree, select the agents to upgrade and then click **Tasks** > **Update**.
   - If scheduled update has been enabled, ensure that **Trend Micro Security (for Mac) Agent** is selected.
   - Instruct users to click **Update** from the agent console.

   Agents that receive the notification start to upgrade. On the endpoint, 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 upgrade is complete.

2. Check the upgrade status.

   a. Click Summary on the main menu and go to the **Program** section under **Update Status**.

   b. Click the link under the **Not Upgraded** column. The agent tree opens, showing all the agents that have not been upgraded.

   c. To upgrade the agents that have not been upgrade, click **Tasks** > **Update**.

# 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**.

# Managing Licenses

View, activate, and renew the Trend Micro Security (for Mac) license on the web console.

The status of the product license determines the features available to users. Refer to the table below for details.

| License Type and Status | Features | | | |
|---|---|---|---|---|
| | Real-time Scan | Scheduled Scan | Web Reputation | Pattern Update |
| Full version and Activated | Enabled | Enabled | Enabled | Enabled |
| Evaluation (trial) version and Activated | Enabled | Enabled | Enabled | Enabled |
| Full version and Expired | Enabled | Enabled | Disabled | Disabled |
| Evaluation version and Expired | Disabled | Disabled | Disabled | Disabled |
| Not activated | Disabled | Disabled | Disabled | Disabled |

**Note**

If the server only has an IPv6 address, read the IPv6 limitations for license updates in *Pure IPv6 Server Limitations on page A-3*.

**Procedure**

1. Navigate to **Administration** > **Product License**.
2. View license information. To get the latest license information, click **Update Information**.

   The **License Information** section provides you the following details:

   - **Status**: Displays either "Activated" or "Expired"
   - **Version**: Displays either "Full" or "Evaluation" version. If you are using an evaluation version, you can upgrade to the full version anytime. For upgrade instructions, click **View license upgrade instructions**.

- **Seats**: The maximum number of agents installations the license supports
- **License expires on**: The expiration date of the license
- **Activation Code**: The code used to activate the license

3. To specify a new Activation Code, click **New Activation Code**.
4. In the screen that opens, type the Activation Code and click **Save**.

   This screen also provides a link to the Trend Micro website where you can view detailed information about your license.

# Backing Up the Server Database

**Procedure**

1. Stop the following services from Microsoft Management Console:
   - **ActiveMQ for Trend Micro Security**
   - **Trend Micro Security for (Mac)**
2. Open SQL Server Management Studio (for example, from **Windows Start menu** > **Programs** > **Microsoft SQL Server {version}** > **SQL Server Management Studio**.
3. Search for `db_TMSM` and then use the **backup** function in SQL Server Management Studio to back up the database files.

   See the SQL Server Management Studio documentation for details.
4. Start the stopped services.

# Restoring the Server Database

### Before you begin

Prepare the backup of the database files created during backup. For details, see *Backing Up the Server Database on page 8-9*.

---

**Procedure**

1. Stop the following services from Microsoft Management Console:
   - **ActiveMQ for Trend Micro Security**
   - **Trend Micro Security for (Mac)**
2. Open SQL Server Management Studio (for example, from **Windows Start menu** > **Programs** > **Microsoft SQL Server {version}** > **SQL Server Management Studio**.
3. Search for `db_TMSM` and then use the **detach** option in SQL Server Management Studio to detach the current database files.

   See the SQL Server Management Studio documentation for details.
4. Use the **attach** option to attach the backup of the database files.
5. Start the stopped services.

---

# 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 8-12*.

See the Control Manager documentation for details.

**Note**

You can also specify Control Manager as the Trend Micro Security (for Mac) server's update source. For details, see *Configuring the Server Update Source on page 5-5*.

# 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

Configure the server settings for the widget to get information from the Trend Micro Security (for Mac) server.

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 **Server Settings** from the top-right menu ( ) of the widget.
4. Click **Check Server Visibility**.
5. Click **Add**.
6. Configure the server settings:
   - **Server Name**: The FQDN or IP address and the port number for the OfficeScan server on which Trend Micro Security (for Mac) is installed
   - **Server Type**: Select **Security (for Mac)** from the list
   - **Account**: The user name required to log on to the server
   - **Password**: The password required to log on to the server

7. Click **Save**.
8. If your network requires a proxy server, click the expand (⌄) icon and configure the proxy server settings.
9. Click **Apply**.

> **Note**
> To add more Trend Micro Security (for Mac) servers, click **Add**.

10. Click **Close**.
11. Select **Server Settings** from the top-right menu (▼) of the widget.
12. Select one or more Trend Micro Security (for Mac) servers and 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 8-1. KPI Widget Indicator Tasks**

| TASK | STEPS |
|---|---|
| Add a new indicator | 1. Click **Add Indicator**. The **Add Indicator** screen appears.<br>2. Select an option from the **Name** drop-down list and optionally customize settings.<br>3. Click **Save**. |
| Edit an indicator | 1. Click the indicator in the list. The **Edit Indicator** screen appears.<br>2. Customize settings.<br>3. Click **Save**. |

| TASK | STEPS |
|---|---|
| Delete an indicator | 1. Click the indicator in the list. The **Edit Indicator** screen appears.<br>2. Click **Delete**.<br>3. Click **OK**. |
| Configure event threshold settings | 1. On the **Add Indicator** or **Edit Indicator** screen, select **Enable alerts at the following thresholds**.<br>2. Type the minimum number of event occurrences for each event type.<br>3. Click **Save**.<br><br>**Note**<br>The important or critical icon displays in the **Occurrences** column if both of the following are true:<br>• The number of event occurrences that match this indicator is equal to or more than the threshold.<br>• **Enable alerts at the following threshold** is selected. |

## 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 8-2. 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.<br><br>**Tip**<br>To manually refresh the widget data, click the refresh ( ) icon. |

# Configuring Agent-Server Communication Settings

Agents identify the server that manages them by the server's name or IPv4/IPv6 address. During the Trend Micro Security (for Mac) server installation, the installer identifies the server computer's IP addresses, which are then displayed on the web console's Agent-Server Communication screen.

The server communicates with agents through the listening port, which is port number 61617 by default.

Notes and reminders:

- If you change the port number, ensure that it is not currently in use to prevent conflicts with other applications and agent-server communication issues.
- If a firewall application is in use on the server computer, ensure that the firewall does not block agent-server communication through the listening port. For example, if the OfficeScan agent firewall has been enabled on the endpoint, add a policy exception that allows incoming and outgoing traffic through the listening port.
- You can configure agents to connect to the server through a proxy server. A proxy server, however, is usually not required for agent-server connections within the corporate network.
- If you plan to update or replace all of the existing server names and IPv4/IPv6 addresses or change the listening port or proxy settings, do so before installing

agents. If you have installed agents and then make changes, agents will lose connection with the server and the only way to re-establish connection is to re-deploy the agents.

**Procedure**

1. Navigate to **Administration** > **Agent-Server Communication**.
2. Type the server's name or IPv4/IPv6 address(es), and listening port.

   **Note**

   If there are multiple entries in the **Server name (or IP address)** field, the agent randomly selects an entry. Ensure that agent-server connection can be established using all the entries.

3. Select whether agents connect to the server through a proxy server.
   a. Select the proxy server protocol.
   b. Type the proxy server name or IPv4/IPv6 address, and port number.
   c. If the proxy server requires authentication, type the user name and password in the fields provided.
4. Click **Save**.
5. If you are prompted to restart Trend Micro Security (for Mac) services for the settings to take effect, perform the following steps:
   a. Navigate to the <*Server installation folder*>.
   b. Double-click `restart_TMSM.bat`.
   c. Wait until all the services have restarted.

# 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 endoint 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.<br><br>For details, see *Managing Licenses on page 8-7*. |
| | | The agent has not been registered to its parent server. The product license may or may not have been activated.<br><br>If an agent is not registered to its parent server, 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 9

## 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. Check if the endpoint meets the requirements for installing and running Trend Micro Security (for Mac) server.

   For details, see *Server Installation Requirements on page 2-2*.

2. Check if the following services have been started:

   - **ActiveMQ for Trend Micro Security**
   - **OfficeScan Plug-in Manager**
   - **SQL Server (TMSM)**
   - **Trend Micro Security for (Mac)**

3. Collect debug logs. Use 'error' or 'fail' as keyword when performing a search on the logs.

   - **Installation logs**: `C:\TMSM*.log`
   - **General debug logs**: <*Server installation folder*>`\debug.log`
   - **OfficeScan debug logs**: `C:\Program Files\Trend Micro \OfficeScan\PCCSRV\Log\ofcdebug.log`

     a. If the file does not exist, enable debug logging. On the banner of the OfficeScan web console, click the first "c" or "O" in "OfficeScan", specify debug log settings, and click **Save**.

     b. Reproduce the steps that led to the web console access problem.

c. Obtain the debug logs.

4. Check the Trend Micro Security (for Mac) registry keys by navigating to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TMSM`.

5. Check the database files and registry keys.

   a. Check if the following files exist under `C:\Program Files\Microsoft SQL Server\MSSQL.x\MSSQL\Data\` or `C:\Program Files(x86)\Microsoft SQL Server\MSSQL.x\MSSQL\Data\`:

      - `db_TMSM.mdf`
      - `db_TMSM_log.LDF`

   b. Check if the Trend Micro Security (for Mac) database instance on the Microsoft SQL server registry key exists:

      - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\TMSM`
      - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\ TMSM\ MSSQLServer\CurrentVersion`

6. Send the following to Trend Micro:

   - Registry files

     a. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Microsoft SQL server\TMSM`.

     b. Click **File** > **Export** and then save the registry key to a `.reg` file.

   - Server computer information

     - Operating system and version
     - Available disk space
     - Available RAM
     - Whether other plug-in programs, such as Intrusion Defense Firewall, is installed

7. Restart the Trend Micro Security (for Mac) services.
   a. Navigate to the <*Server installation folder*>.
   b. Double-click `restart_TMSM.bat`.
   c. Wait until all the services have restarted.
8. The Trend Micro Security (for Mac) service should always be running. If this service is not running, there may be a problem with the ActiveMQ service.
   a. Back up ActiveMQ data in `C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM\apache-activemq\data\*.*`.
   b. Delete the ActiveMQ data.
   c. Try to restart the Trend Micro Security (for Mac) service by double-clicking `restart_TMSM.bat`.
   d. Try to access the web console again to check if the access problem has been resolved.

---

## Server Uninstallation

**Problem**:

The following message displays:

```
Unable to uninstall the plug-in program. The uninstallation
command for the plug-in program is missing in the registry key.
```

---

**Procedure**

1. Open registry editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Wow6432Node\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`.
2. Reset the value to `1.0.1000`.

3. Delete the plug-in program registry key; for example, `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx`.

4. Restart the OfficeScan Plug-in Manager service.

5. Download, install, and then uninstall the plug-in program.

## 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.

# The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro website, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

http://esupport.trendmicro.com/en-us/business/default.aspx

Trend Micro updates the contents of the Knowledge Base continuously and adds new solutions daily. If you are unable to find an answer, however, you can describe the problem in an email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

# Technical Support

Learn about the following topics:


- *Troubleshooting Resources on page 9-8*
- *Contacting Trend Micro on page 9-9*
- *Sending Suspicious Content to Trend Micro on page 9-10*
- *Other Resources on page 9-11*

# 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<br>225 E. John Carpenter Freeway, Suite 1500<br>Irving, Texas 75062 U.S.A. |
| Phone | Phone: +1 (817) 569-8900<br>Toll-free: (888) 762-8736 |
| Website | http://www.trendmicro.com |
| Email address | support@trendmicro.com |

- 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

# Appendix A

## 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.

# IPv6 Support for Trend Micro Security (for Mac) Server and Agents

IPv6 support for Trend Micro Security (for Mac) started in version 2.0. Earlier Trend Micro Security (for Mac) versions do not support IPv6 addressing. IPv6 support is automatically enabled after installing or upgrading the Trend Micro Security (for Mac) server and agents that satisfy the IPv6 requirements.

# Trend Micro Security (for Mac) Server IPv6 Requirements

Trend Micro Security (for Mac) server must be installed with an OfficeScan server version that supports IPv6.

IPv6 support in OfficeScan started in version 10.6. Earlier OfficeScan versions that are compatible with Trend Micro Security (for Mac) (see *Server Installation Requirements on page 2-2*) do not support IPv6 addressing.

See the OfficeScan 10.6 or later documentation for details about IPv6 support.

# 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 Server Limitations

The following table lists the limitations when the Trend Micro Security (for Mac) server only has an IPv6 address.

**TABLE A-1. Pure IPv6 Server Limitations**

| ITEM | LIMITATION |
|---|---|
| Agent management | A pure IPv6 server cannot manage pure IPv4 agents. |
| Updates and centralized management | A pure IPv6 server cannot update from pure IPv4 update sources or report to pure IPv4 central management products, such as:<br>• Trend Micro ActiveUpdate Server<br>• Any pure IPv4 custom update source<br>• Pure IPv4 Control Manager 6.0 |
| Product registration, activation, and renewal | A pure IPv6 server cannot connect to the Trend Micro Online Registration Server to register the product, obtain the license, and activate/renew the license. |
| Proxy connection | A pure IPv6 server cannot connect through a pure IPv4 proxy server. |

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 Trend Micro Security (for Mac) server and the entities to which it connects or the entities that it serves.

# Pure IPv6 Agent Limitations

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

**TABLE A-2. 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:<br>• Trend Micro ActiveUpdate Server<br>• A pure IPv4 Trend Micro Security (for 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.

- 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.

# Index


**A**

agent tree, 3-4
    general tasks, 3-4

**C**

components, 3-13
contacting, 9-7
    Knowledge Base, 9-7
    Trend Micro, 9-7
Control Manager integration, 8-11
conventional scan, 6-5–6-7
    switching to smart scan, 6-7
CPU usage, 6-18

**D**

Damage Cleanup Services, 1-3, 1-6
documentation feedback, 9-11

**F**

File Reputation Services, 3-15

**I**

IntelliScan, 6-16
IPv6 support, A-2
    limitations, A-3

**K**

Knowledge Base, 9-7

**P**

performance control, 6-18
programs, 3-13

**S**

scan criteria
    CPU usage, 6-18
    files to scan, 6-16
    schedule, 6-19
    user activity on files, 6-16
scan method
    default, 6-5
scan types, 6-11
Smart Feedback, 3-15
Smart Protection
    File Reputation Services, 3-15
    Web Reputation Services, 3-15
smart scan, 6-5–6-7
    switching from conventional scan, 6-7
support
    resolve issues faster, 9-9

**T**

Trend Micro
    Knowledge Base, 9-7
Trojan horse program, 1-3, 1-6

**V**

virus/malware scan
    results, 6-34

**W**

web console, 3-2
    about, 3-2
web reputation, 7-2
Web Reputation Services, 3-15
web threats, 7-2
widgets, 3-10, 3-13, 3-14

**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: TSEM37299/160114