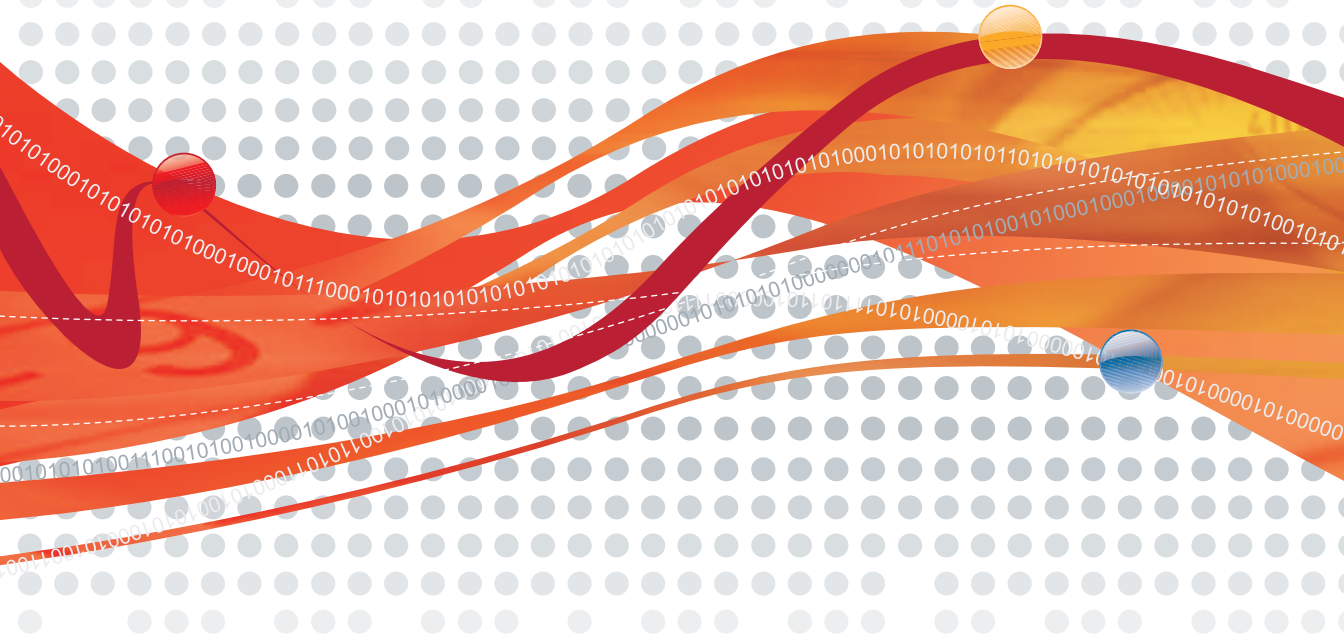
Trend Micro Security[1]

For Enterprise and Medium Business

for Mac

Administrator's Guide



Endpoint Security

Document Part No. TSEM14160/90702

Release Date: August 2009

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 Web site.

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

Contents

Chapter 4: Installing the Trend Micro Security Client

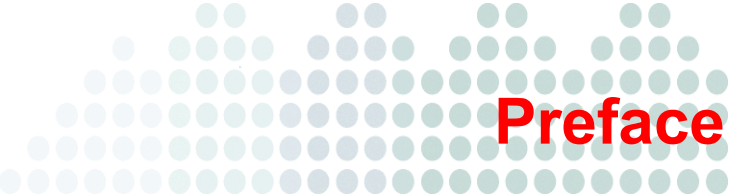
Chapter 5: Keeping Protection Up-to-Date

Chapter 6: Protecting Computers from Security Risks

Chapter 7: Protecting Computers from Web-based Threats

Chapter 8: Managing the Trend Micro Security Server and Clients

Chapter 9: Troubleshooting and Support



Preface

Welcome to the *Administrator's Guide* for Trend Micro™ Security *for Mac*. This document discusses Trend Micro Security server and client installation, getting started information, and server and client management.

Topics in this chapter:

Trend Micro Security Documentation

Trend Micro Security documentation includes the following:

TABLE P-1. Trend Micro Security documentation

DOCUMENTATION	DESCRIPTION
Administrator's Guide	A PDF document that discusses Trend Micro Security server and client installation, getting started information, and server and client management.
Help	HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. The Help is accessible from the Trend Micro Security server and client consoles.
Installation and Configuration Worksheet	A PDF document that provides a checklist of items to guide the administrator in setting up and configuring Trend Micro Security.
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: http://esupport.trendmicro.com/support

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

http://www.trendmicro.com/download

Audience

Trend Micro Security documentation is intended for the following users:

- **Trend Micro Security Administrators:** Responsible for Trend Micro Security management, including server and client installation and management. These users are expected to have advanced networking and server management knowledge.
- **End users:** Users who have the Trend Micro Security client installed on their Macintosh computers. 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 documentation uses the following conventions:

TABLE P-2. 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
TOOLS > CLIENT TOOLS	A "breadcrumb" found at the start of procedures that helps users navigate to the relevant Web console screen. Multiple breadcrumbs means that there are several ways to get to the same screen.
<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.

TABLE P-2. Document conventions (Continued)

CONVENTION	DESCRIPTION
Note: text	Provides configuration notes or recommendations
Tip: text	Provides best practice information and Trend Micro recommendations
WARNING! text	Provides warnings about activities that may harm computers on your network

Terminology

The following table provides the terminology used throughout the Trend Micro Security documentation:

TABLE P-3. Trend Micro Security terminology

TERMINOLOGY	DESCRIPTION
Client	The Trend Micro Security client program installed on a Macintosh computer
Client computer or endpoint	The computer where the Trend Micro Security client is installed
Client user (or user)	The person using the Trend Micro Security client
Server	The Trend Micro Security server program
Server computer	The computer where the Trend Micro Security server is installed

TABLE P-3. Trend Micro Security terminology (Continued)

TERMINOLOGY	DESCRIPTION
Administrator (or Trend Micro Security administrator)	The person managing the Trend Micro Security server
Console	The user interface for configuring and managing Trend Micro Security server and client settings The console for the Trend Micro Security server program is called "Web console", while the console for the client program is called "client console".
Security risk	The collective term for viruses, malware, spyware, and grayware
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
Client installation folder	The following folders on the Macintosh computer that contain the Trend Micro Security client files: • /Library/Application Support/TrendMicro • /Applications/Trend Micro Security

TABLE P-3. Trend Micro Security terminology (Continued)

TERMINOLOGY	DESCRIPTION
Server installation folder	The folder on the server computer that contains the Trend Micro Security server files. After installing Trend Micro Security server, the folder is created on the same OfficeScan server directory. If you accept the default settings during OfficeScan server installation, you will find the server installation folder at any of the following locations: • C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM • C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\TMSM

Chapter 1

Introducing Trend Micro Security *for Mac*

Topics in this chapter:

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. Trend Micro Security *for Mac* integrates with OfficeScan, simplifying the management of Macintosh desktops, laptops, and servers through the same Web console that manages Windows-based clients and servers.

Key Features and Benefits

Trend Micro Security provides the following features and benefits:

Security Risk Protection

Trend Micro Security protects computers 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 notifies you of any outbreak so you can take immediate action, such as cleaning infected computers and isolating them until they are completely risk-free.

Web Reputation

Web reputation technology proactively protects client computers within or outside the corporate network from malicious and potentially dangerous Web sites. Web reputation breaks the infection chain and prevents downloading of malicious code.

Centralized Management

A Web-based management console gives administrators transparent access to all clients on the network. The Web console coordinates automatic deployment of security policies, pattern files, and software updates on every client. Administrators can perform remote administration and configure settings for clients or groups.

The Trend Micro Security Server

The Trend Micro Security server is the central repository for all client configurations, security risk logs, and updates.

The server performs two important functions:

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

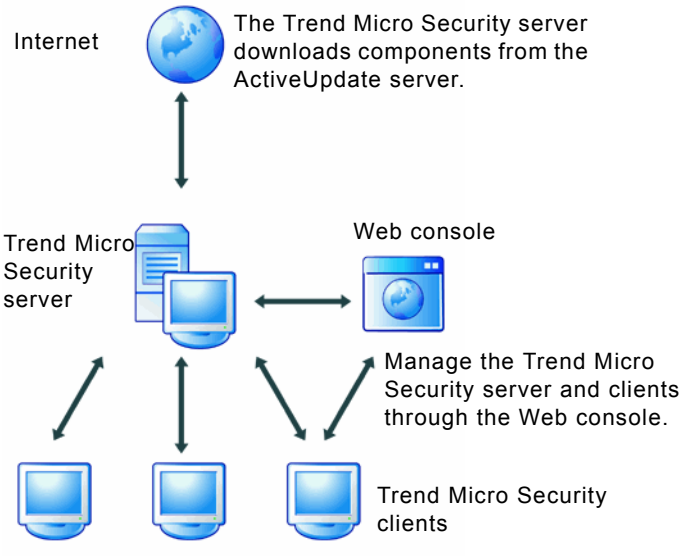


FIGURE 1-1. How the Trend Micro Security server works

Trend Micro Security provides real-time, bidirectional communication between the server and clients. Manage the clients from a browser-based Web console, which you can access from virtually anywhere on the network. The server communicates with the client through the ActiveMQ™ protocol.

The Trend Micro Security Client

Protect Macintosh computers from security risks by installing the Trend Micro Security client on each computer. The client provides three scan types: Real-time Scan, Scheduled Scan, and Manual Scan.

The client reports to the parent server from which it was installed. The client sends events and status information to the server in real time. Clients communicate with the server through the ActiveMQ protocol.

Chapter 2

Installing the Trend Micro Security Server

Topics in this chapter:

Server Installation Requirements

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

TABLE 2-1. Server installation requirements

RESOURCE	REQUIREMENTS
OfficeScan server	Version 10.0 or 8.0 Service Pack 1 Refer to the OfficeScan Installation and Upgrade Guide for instructions on installing the OfficeScan server.
Plug-in Manager	Version 1.0 with the latest patch Refer to the Plug-in Manager readme for instructions on installing Plug-in Manager.

Hardware	RAM: 512MB minimum, 1GB recommended
	Available disk space:
	• 1.4GB minimum if the OfficeScan server is installed on the system drive (usually, C: drive)
	• If the OfficeScan server is not installed on the system drive:
	  • 600MB minimum on the drive where the OfficeScan server is installed. The Trend Micro Security server will be installed on this drive.
	  • 800MB minimum on the system drive. Third-party programs used by Trend Micro Security server (such as Microsoft SQL Server 2005 Express™) will be installed on this drive.

TABLE 2-1. Server installation requirements

RESOURCE	REQUIREMENTS

Others	• Microsoft™ .NET Framework 2.0
	• Java runtime environment™ (JRE) 1.6 Update 14 or above required on computers running Windows Server 2008. For other operating systems, JRE 1.6 Update 14 will automatically be installed if not present on the computer or if a different version exists. If a different version exists, the installation package does not uninstall the other JRE version.
	• The following third-party programs will be installed automatically:
	  • Microsoft SQL Server 2005 Express
	  • Apache™ ActiveMQ 5.2.0
	  • Microsoft Data Access Components (MDAC) 2.81 on Windows 2000 computers
	  • Microsoft Visual C++ 2005 Redistributable

Update Source

Before installing Trend Micro Security 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:

ActiveUpdate Server

The Trend Micro ActiveUpdate server is the default update source for OfficeScan. Internet connection is required to connect to this server. 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:

- 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.
- 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 installation package.

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:

- Check if there is functional connection between the server computer and the update source.
- 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 installation package.

For assistance in setting up the intranet source, contact your support provider.

Server Installation

Install the Trend Micro Security server by performing the following steps:

To install Trend Micro Security server:

1. Open the OfficeScan Web console and click **Plug-in Manager** on the main menu.

FIGURE 2-1. OfficeScan Web console main menu

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

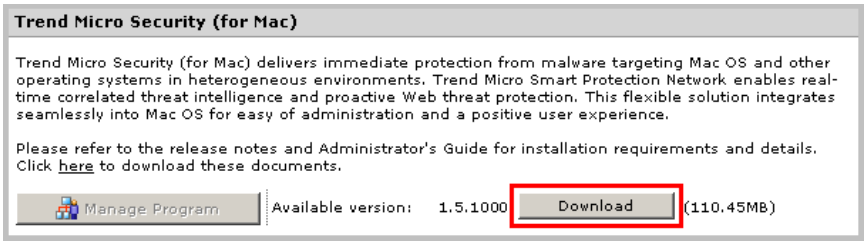


FIGURE 2-2. Trend Micro Security download button

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

<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.

FIGURE 2-3. Download progress

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 Logs**.

4. After Plug-in Manager downloads the package, a new screen with the following options displays: **Install Now** or **Install Later**.

FIGURE 2-4. Download complete

5. If you click **Install Now**, agree to the license agreement and then check the installation progress.

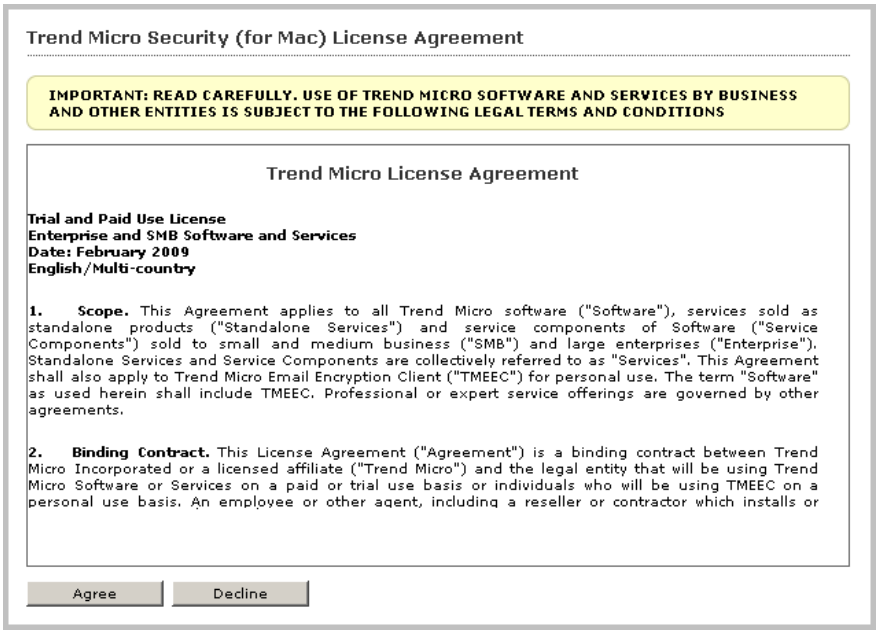


FIGURE 2-5. License Agreement screen

6. If you click **Install Later**:
   a. Open the OfficeScan Web console and click **Plug-in Manager** on the main menu.
   b. Go to the **Trend Micro Security (for Mac)** section and click **Install**.
   c. Agree to the license agreement and then check the installation progress.

After the installation, the Trend Micro Security version displays.

Server Post-installation

Perform the following tasks immediately after installing the Trend Micro Security server:

1. Verify the following:
   - The following services display on the Microsoft Management Console:
     - ActiveMQ for Trend Micro Security
     - SQL Server (TMSM)
     - Trend Micro Security for (Mac)
   - When you open Windows Task Manager, the **TMSMMainService.exe** process is running.
   - The following registry key exists: HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_TMSM
   - The Trend Micro Security server files are found under the <Server installation folder>.
2. Open the OfficeScan Web console and click **Plug-in Manager** on the main menu.

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

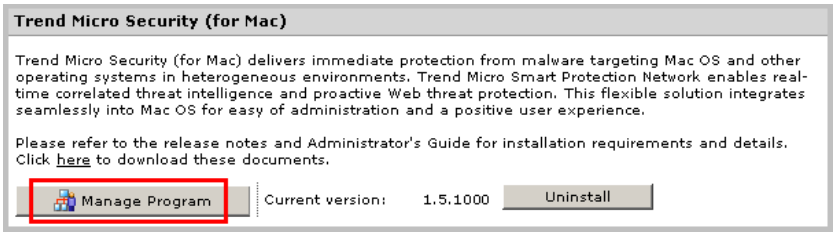


FIGURE 2-6. Manage Program button

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

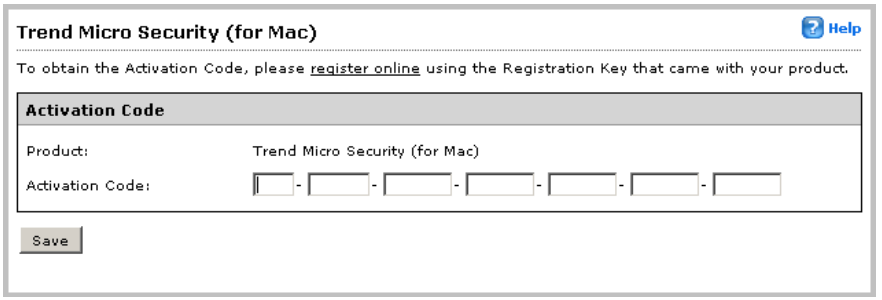


FIGURE 2-7. Activation Code screen

If you do not have the Activation Code, click the **register online** link to access the Trend Micro registration Web site. 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.

If the Activation Code is correct, a screen with the license details displays.

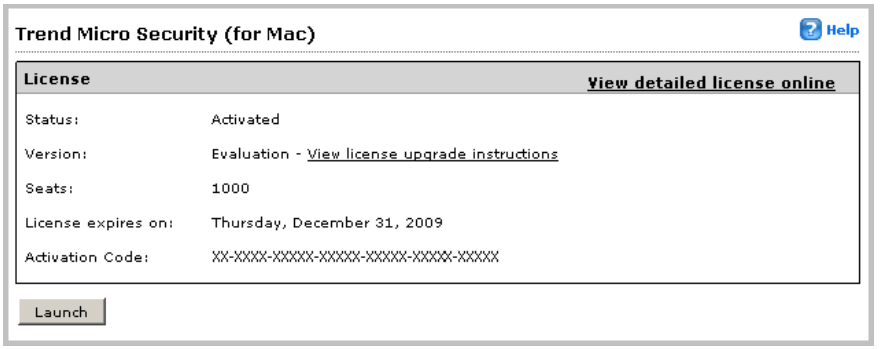


FIGURE 2-8. License details screen

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

Server Uninstallation

You can uninstall Trend Micro Security server from the Plug-in Manager screen on the Web console.

To uninstall the Trend Micro Security server:

1. Open the OfficeScan Web console and click **Plug-in Manager** 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 server is again available for installation.

Note: The uninstallation package does not remove Java runtime environment (JRE) 1.6 Update 14. You can remove JRE if no other application is using it.

Chapter 3

Getting Started with Trend Micro Security

Topics in this chapter:

The Web Console

The Web console is the central point for monitoring Trend Micro Security clients and configuring settings to be deployed to clients. 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 clients installed on Macintosh computers
- Organize clients into logical groups for simultaneous configuration and management
- Set scan configurations and initiate scanning on a single or multiple computers
- Configure security risk notifications and view logs sent by clients
- Configure outbreak criteria and notifications

Open the Web console from any computer on the network that has the following resources:

- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft™ Internet Explorer™ 6.0 or later

To open the Web console:

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 Web console or click **Summary** in the main menu.

Tip: Refresh the screen periodically to get the latest information.

Networked Computers

The **Networked Computers** section displays the following information:

- The connection status of all Trend Micro Security clients with the Trend Micro Security server. Clicking a link opens the client tree where you can configure settings for the clients.
- The number of detected security risks and Web threats
- The number of computers with detected security risks and Web threats

Components and Program

The **Update Status** table contains information about Trend Micro Security components and the client program that protects Macintosh computers from security risks.

Update outdated components immediately. You can also upgrade clients to the latest program version or build if you recently upgraded the server. For client upgrade instructions, see *Upgrading the Server and Clients* on page 8-2.

To launch an update from the Summary screen:

1. Go to the **Update Status for Networked Computers** section and click the link under the **Outdated** column. The client tree opens, showing all the clients that require an update.
2. Select the clients that you want to update.
3. Click **Tasks > Update**. Clients that receive the notification start to update. On Macintosh computers, the Trend Micro Security icon on the menu bar indicates that the product is updating. Users cannot run any task from the console until the update is complete.

The Trend Micro Security Client Tree

The client tree displays all the clients that the server currently manages. All clients belong to a certain group. Use the menu items above the client tree to simultaneously configure, manage, and apply the same configuration to all clients belonging to a group.

Client Tree General Tasks

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

- Click the root icon  to select all groups and clients. When you select the root icon and then choose a menu item above the client tree, a screen for configuring settings displays. On the screen, choose from the following general options:
  - **Apply to All Clients:** Applies settings to all existing clients and to any new client 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 clients added to future groups. This option will not apply settings to new clients added to an existing group.
- To select multiple adjacent groups or clients, click the first group or client in the range, hold down the SHIFT key, and then click the last group or client in the range.
- To select a range of non-contiguous groups or clients, hold down the CTRL key and then click the groups or clients that you want to select.
- Search for a client to manage by specifying a full or partial client name in the **Search for computers** text box. A list of matching client names will appear in the client tree.
- Sort clients based on column information by clicking the column name.

Client Tree Specific Tasks

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

TABLE 3-1. Client tree specific tasks

MENU BUTTON	TASK
Tasks	• Run Scan Now on client computers. For details, see *Scan Now* on page 6-9. • Update client components. For details, see *Client Update* on page 5-6.

Settings	• Configure scan settings. For details, see the following topics:
	  • *Real-time Scan* on page 6-6
	  • *Manual Scan* on page 6-7
	  • *Scheduled Scan* on page 6-8
	  • *Scan Exclusions* on page 6-12
	• Configure Web reputation policies. For details, see *Web Reputation Policies* on page 7-3.

Logs	View the following log types: • *Security Risk Logs* on page 6-18 • *Web Reputation Logs* on page 7-4
Manage Client Tree	Manage Trend Micro Security groups. For details, see *Trend Micro Security Groups* on page 3-6.

Trend Micro Security Groups

A group in Trend Micro Security is a set of clients that share the same configuration and run the same tasks. By organizing clients into groups, you can simultaneously configure, manage, and apply the same configuration to all clients belonging to the groups.

For ease of management, group clients based on their departments or the functions they perform. You can also group clients 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 clients to a different group, or remove clients permanently. A client removed from the client tree is not automatically uninstalled from the client computer. The Trend Micro Security client can still perform server-dependent tasks, such as updating components. However, the server is unaware of the existence of the client and therefore cannot send configurations or notifications to the client.

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

To add a group:

PATH: CLIENT MANAGEMENT > MANAGE CLIENT TREE > ADD GROUP

1. Type a name for the group you want to add.
2. Click **Add**. The new group appears in the client tree.

To delete a group or client:

PATH: CLIENT MANAGEMENT > MANAGE CLIENT TREE > REMOVE GROUP/CLIENT

1. Before deleting a group, check if there are clients that belong to the group and then move them to another group. The procedure for moving clients is found below.
2. When the group is empty, select the group and click **Remove Group/Client**.
3. To delete a client, select the client and click **Remove Group/Client**.

To rename a group:

PATH: CLIENT MANAGEMENT > MANAGE CLIENT TREE > RENAME GROUP

1. Type a new name for the group.
2. Click **Rename**. The new group name appears in the client tree.

To move a client:

PATH: CLIENT MANAGEMENT > MANAGE CLIENT TREE > MOVE CLIENT

1. Select the group to which to move the client.
2. Decide whether to apply the settings of the new group to the client.

Tip: Alternatively, drag and drop the client to another group in the client tree.

3. Click **Move**.

Chapter 4

Installing the Trend Micro Security Client

Topics in this chapter:

Client Installation Requirements

The following are the requirements for installing the Trend Micro Security client on a Macintosh computer.

TABLE 4-1. Client installation requirements

RESOURCE	REQUIREMENT
Operating system	• Mac OS™ X version 10.4.11 (Tiger™) or later • Mac OS X version 10.5.5 (Leopard™) or later
Hardware	• Processor: PowerPC™ or Intel™ core processor • RAM: 256MB minimum • Available disk space: 30MB minimum
Others	• Java for Mac OS X 10.4, Release 9 • Java for Mac OS X 10.5, Update 4

Client Installation Methods

There are two ways to install the Trend Micro Security client.

- Install on a single computer by launching the installation package on the Macintosh computer
- Install on several computers by using Apple Remote Desktop

Note: To upgrade clients, see *Upgrading the Server and Clients* on page 8-2.

Obtain the client installation package (**tmsminstall.mpkg.zip**) from the Trend Micro Security server and copy it to the Macintosh computer. To obtain the package, perform any of the following steps:

- On the Trend Micro Security Server Web console, navigate to **Administration > Client Setup Files** and click the link under **Client Installation File**.

  Note: The link to the client uninstallation file is also available on this screen. Use this program to remove the client program from the Macintosh computer. For information on uninstalling the Trend Micro Security client, see *Client Uninstallation* on page 4-12.

- Navigate to <Server installation folder>\TMSM_HTML\ClientInstall and search for the file **tmsminstall.mpkg.zip**.

Installing on a Single Computer

The process of installing Trend Micro Security client on a single computer is similar to the installation process for other Macintosh software.

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

To install on a single Macintosh computer:

1. Check for and uninstall any security software on the Macintosh computer.
2. Obtain the client installation package **tmsminstall.mpkg.zip**. For information on obtaining the package, see *Client Installation Methods* on page 4-2.
3. Copy and then launch the package on the Macintosh computer. Launching the package unarchives the file **tmsminstall.mpkg**.

WARNING! **The files on the package may become corrupted if users launch the package using archiving tools not built-in on the Mac. Instruct users to launch the package using built-in archiving tools, such as Archive Utility.**

4. Launch **tmsminstall.mpkg**. When a message prompting you to continue with installation displays, click **Continue**.

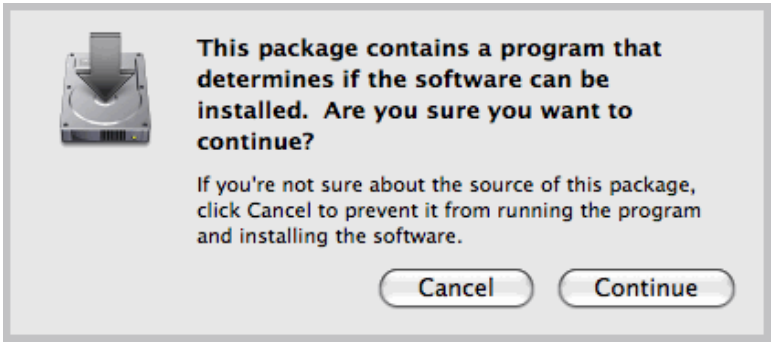


FIGURE 4-1. Confirm installation message

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

FIGURE 4-2. Introduction screen

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

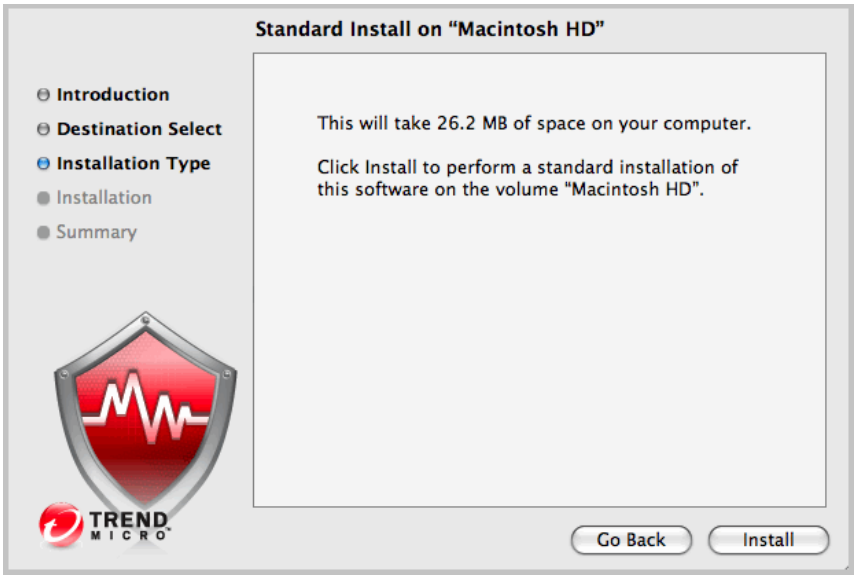


FIGURE 4-3. Installation Type screen

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

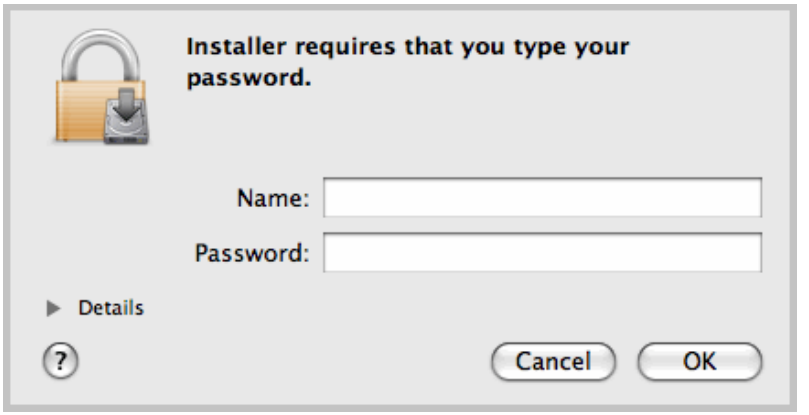


FIGURE 4-4. Message prompting for user name and password

Note: Specify the name and password for an account with administrative rights on the Macintosh computer.

8. If the installation was successful, click **Close** to finish the installation process. The client automatically registers to the server where the client installation package was obtained. The client also updates for the first time.

FIGURE 4-5. Installation Succeeded screen

9. Perform client post-installation tasks.

Installing on Several Computers

The process of installing Trend Micro Security client on several computers can be simplified by using Apple Remote Desktop.

To install on several Macintosh computers:

1. Check for and uninstall any security software on the Macintosh computers.
2. Obtain the client installation package **tmsminstall.mpkg.zip**. For information on obtaining the package, see *Client Installation Methods* on page 4-2.
3. Copy and then launch the package on the Macintosh computer with Apple Remote Desktop. Launching the package unarchives the file **tmsminstall.mpkg**.

WARNING! **The files on the package may become corrupted if users launch the package using archiving tools not built-in on the Mac. Instruct users to launch the package using built-in archiving tools, such as Archive Utility.**

---

4. Open Apple Remote Desktop on the Macintosh computer.
5. Select the computers to which to install the Trend Micro Security client and then click **Install**.

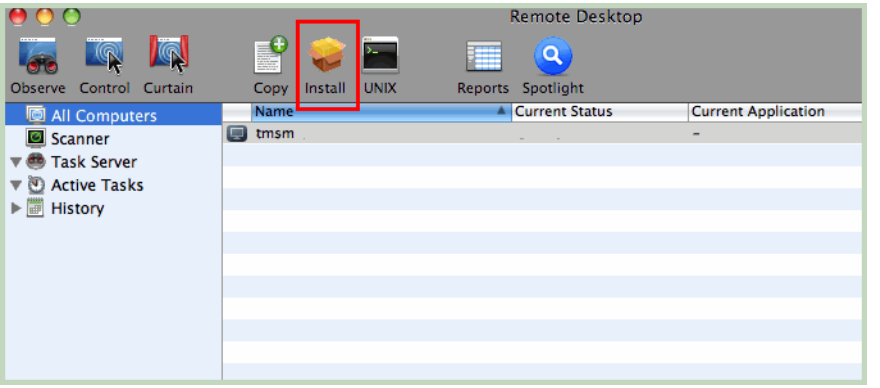


FIGURE 4-6. Remote Desktop screen

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

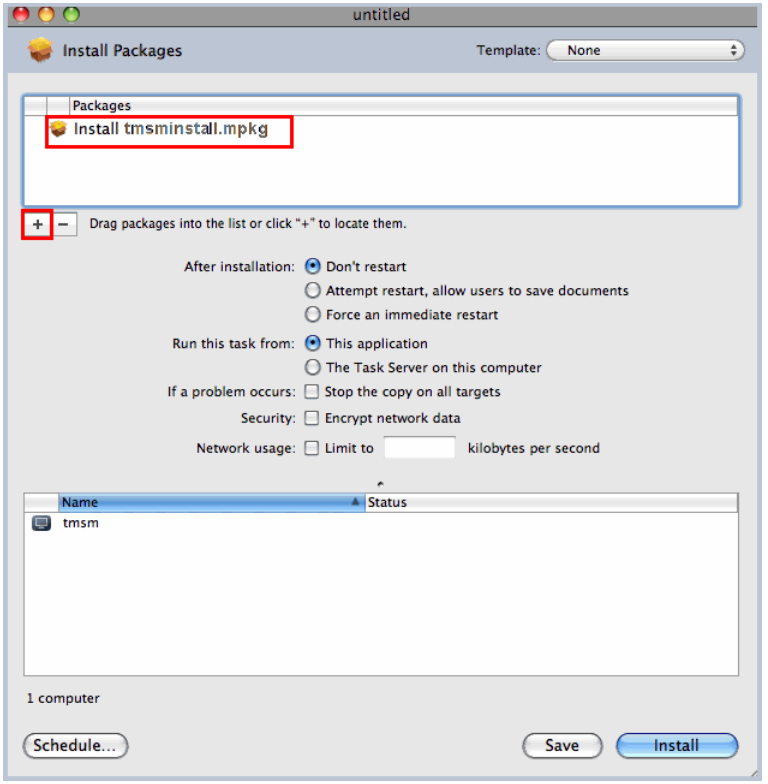


FIGURE 4-7. Install Packages screen

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

8. Click **Install**. The Apple Remote Desktop starts installing the client to the selected computers. If the installation was successful on all computers, the message **Install Packages: Succeeded on all** appears. Otherwise, **Successful** appears under **Task Status** for each computer to which the installation was successful.

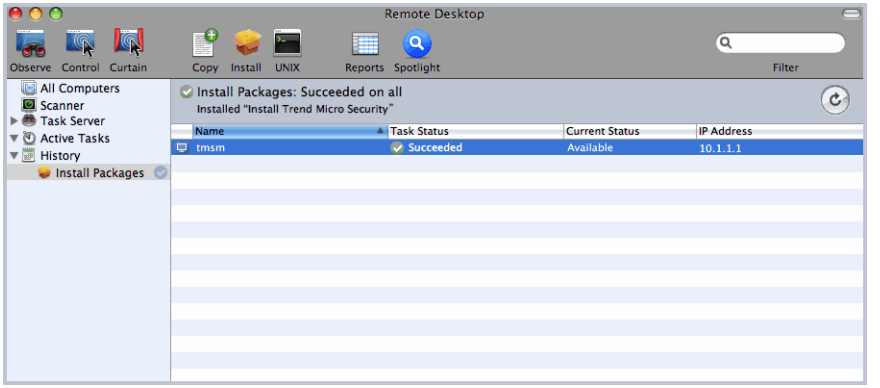


FIGURE 4-8. Successful Installation screen

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

9. Perform client post-installation tasks.

Client Post-installation

Perform the following tasks immediately after installing the Trend Micro Security client:

1. Verify the following:
   - The Trend Micro Security client icon displays on the menu bar of the Macintosh computer.

   - The Trend Micro Security client files are found under the <Client installation folder>.
   - The client appears on the Web console's client tree. To access the client tree, click **Client Management** on the main menu.

2. Update Trend Micro Security components. The client downloads components from the Trend Micro Security server. See *Client Update* on page 5-6 for details.

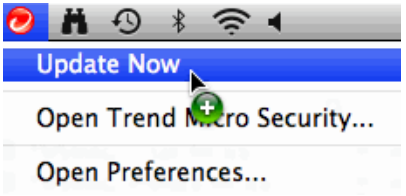


FIGURE 4-9. Update Now menu item

If the client 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. Initiate Scan Now on the client computer or instruct the user to run Manual Scan.

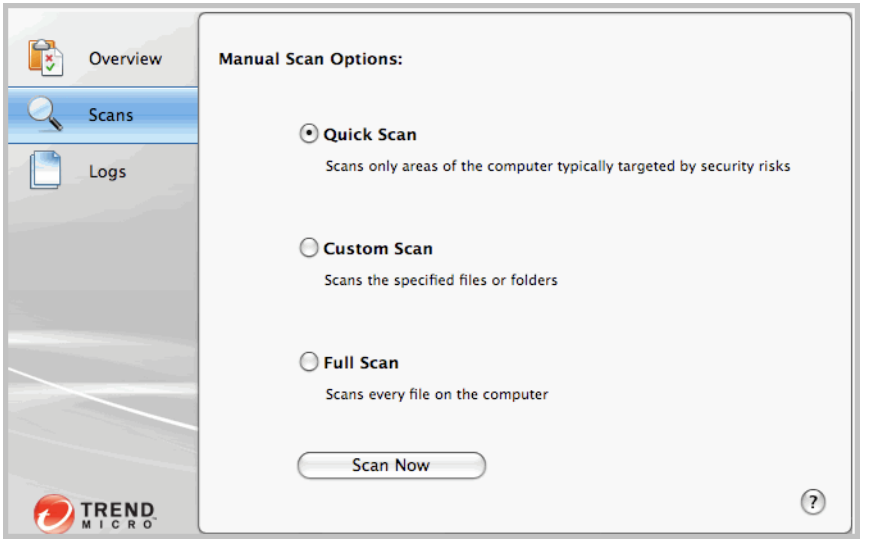


FIGURE 4-10. Manual Scan screen on the endpoint

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

Client Uninstallation

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

To uninstall the client:

1. Obtain the client uninstallation package **tmsmuninstall.mpkg.zip** from the Trend Micro Security server. On the Web console, navigate to **Administration > Client Setup Files** and click the link under **Client Uninstallation File**.
2. Copy and then launch the package on the Macintosh computer.
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 Macintosh computer.

4. If the uninstallation was successful, click **Close** to finish the uninstallation process.
5. Unregister the client from the server.
   a. On the Web console, click **Client Management** and select the client that was uninstalled.
   b. Click **Manage Client Tree > Remove Group/Client**.

Chapter 5

Keeping Protection Up-to-Date

Topics in this chapter:

Components

Trend Micro Security makes use of components to keep client computers 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 clients also receive updated configuration files from the Trend Micro Security server. Clients need the configuration files to apply new settings. Each time you modify Trend Micro Security settings through the Web console, the configuration files change.

Virus Pattern

The Virus Pattern contains information that helps Trend Micro Security 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.

Spyware Active-monitoring Pattern

The Spyware Active-monitoring Pattern contains information that helps Trend Micro Security identify spyware and grayware.

Virus Scan Engine

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.

Updating the Scan Engine

By storing the most time-sensitive information about security risks in the pattern files, Trend Micro minimizes the number of scan engine updates while keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. Trend Micro releases new engines under the following circumstances:

- Incorporation of new scanning and detection technologies into the software
- Discovery of a new, potentially harmful security risk that the scan engine cannot handle

- Enhancement of the scanning performance
- Addition of file formats, scripting languages, encoding, and/or compression formats

Client Program

The Trend Micro Security client program provides the actual protection from security risks.

Update Overview

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

You can configure the Trend Micro Security 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 server and clients:

TABLE 5-2. Server-client update options

UPDATE OPTION	DESCRIPTION
ActiveUpdate server | Trend Micro Security server | Clients	The Trend Micro Security 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 clients.
ActiveUpdate server | Clients	Trend Micro Security clients receive updated components directly from the ActiveUpdate server if they cannot connect to the Trend Micro Security server.

Server Update

The Trend Micro Security server downloads the following components and deploys them to clients:

- Virus Pattern
- Spyware Active-monitoring Pattern
- Virus Scan Engine

View the current versions of components on the Web console's Summary screen, and determine the number of clients 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.

Server Update Source

Configure the Trend Micro Security server to download components from the Trend Micro ActiveUpdate server or from another source.

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

To configure the server update source:

PATH: SERVER UPDATES > UPDATE SOURCE

1. Select the location from where you want to download component updates.

   If you choose ActiveUpdate server, ensure that the server has Internet connection and, if you are using a proxy server, test if Internet connection can be established using the proxy settings. For details, see *Proxy for Server Update* on page 5-5.

   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.

2. Click **Save**.

Proxy for Server Update

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

To configure proxy settings:

PATH: ADMINISTRATION > EXTERNAL PROXY SETTINGS

1. Select the check box to enable the use of a proxy server.
2. Specify the proxy IP address and port number.
3. If the proxy server requires authentication, type the user name and password in the fields provided.
4. Click **Save**.

Server Update Methods

Update Trend Micro Security 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 *Manual Update* on page 5-6 for details.

Scheduled Update

The Trend Micro Security server connects to the update source during the scheduled day and time to obtain the latest components. See *Scheduled Update* on page 5-5 for details.

Scheduled Update

Configure the Trend Micro Security 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.

To configure server update schedule:

PATH: SERVER UPDATES > SCHEDULED UPDATE

1. Select the components to update.
2. Specify the update schedule. For daily, weekly, and monthly updates, the period of time is the number of hours during which Trend Micro Security will perform the update. Trend Micro Security updates at any given time during this time period.
3. Click **Save**.

Manual Update

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

To update the server manually:

PATH: SERVER UPDATES > MANUAL UPDATE

1. Select the components to update.
2. Click **Update**. The server downloads the updated components.

Client Update

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

In addition to components, Trend Micro Security clients also receive updated configuration files during updates. Clients need the configuration files to apply new settings. Each time you modify Trend Micro Security settings on the Web console, the configuration files change.

Before updating the clients, check if the Trend Micro Security server has the latest components. For information on how to update the Trend Micro Security server, see *Server Update* on page 5-4.

Note: Trend Micro Security clients can use proxy settings during an update. Proxy settings are configured on the client console.

There are several ways to update clients.

- **Server-initiated update:** You can initiate an update from the Web console by navigating to **Client Management > Tasks > Update**.
- **Automatic update:** After the server finishes an update, it immediately notifies clients to update.
- **Manual update:** Users launch the update from their Macintosh computers.

During an update, The Trend Micro Security icon on the menu bar of the Macintosh computer indicates that the product is updating. If an upgrade to the client program is available, clients 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 clients have been updated.

Chapter 6

Protecting Computers from Security Risks

Topics in this chapter:

About Security Risks

Security risk includes viruses, malware, spyware, and grayware. Trend Micro Security protects computers from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak, which Trend Micro Security can help contain by enforcing outbreak prevention policies and isolating infected computers 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. Computer viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and Web sites.

Trend Micro Security protects computers from the following virus/malware types:

TABLE 6-1. 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 a computer monitor.
Trojan Horse Program	A Trojan horse is an executable program that does not replicate but instead resides on computers to perform malicious acts, such as opening ports for hackers to enter. This program often uses Trojan Ports to gain access to computers. An application that claims to rid a computer of viruses when it actually introduces viruses to the computer is an example of a Trojan program. Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those already running on the system.

TABLE 6-1. Virus/Malware types

VIRUS/MALWARE TYPES	DESCRIPTION
Virus	A virus is a program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes. • Boot sector virus: A virus that infects the boot sector of a partition or a disk. • Java malicious code: Operating system-independent virus code written or embedded in Java™. • Macro virus: A virus encoded as an application macro and often included in a document. • VBScript, JavaScript, or HTML virus: A virus that resides on Web pages and downloads through a browser. • Worm: A self-contained program or set of programs able to spread functional copies of itself or its segments to other computers, often through email
Test Virus	A test virus is an inert file that is detectable by virus scanning software. Use test viruses, such as the EICAR test script, to verify that the antivirus installation scans properly.
Packer	Packers are compressed and/or encrypted Windows or Linux™ executable programs, often a Trojan horse program. Compressing executables makes packers more difficult for antivirus products to detect.
Probable Virus/Malware	Suspicious files that have some of the characteristics of virus/malware are categorized under this virus/malware type. For details about probable virus/malware, see the following page on the Trend Micro online Virus Encyclopedia: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS

TABLE 6-1. Virus/Malware types

VIRUS/MALWARE TYPES	DESCRIPTION
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 computers 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 computer vulnerabilities to attack.

Trend Micro Security protects computers from the following spyware/grayware types:

TABLE 6-2. 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 a computer 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 a computer.
Remote Access Tool	A remote access tool helps hackers remotely access and control a computer.

TABLE 6-2. Spyware/Grayware types

SPYWARE/ GRAYWARE TYPES	DESCRIPTION
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 Types

Trend Micro Security provides the following scan types to protect client computers from security risks:

TABLE 6-3. Scan types

SCAN TYPE	DESCRIPTION
Real-time Scan	Automatically scans a file on the computer as it is received, opened, downloaded, copied, or modified See *Real-time Scan* on page 6-6 for details.
Manual Scan	A user-initiated scan that scans a file or a set of files requested by the user See *Manual Scan* on page 6-7 for details.
Scheduled Scan	Automatically scans files on the computer based on the schedule configured by the administrator See *Scheduled Scan* on page 6-8 for details.
Scan Now	An administrator-initiated scan that scans files on one or several target computers See *Scan Now* on page 6-9 for details.

Real-time Scan

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If Trend Micro Security does not detect a security risk, the file remains in its location and users can proceed to access the file. If Trend Micro Security 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 clients and groups, or to all clients that the server manages.

To configure Real-time Scan settings:

PATH: CLIENT MANAGEMENT > SETTINGS > REAL-TIME SCAN SETTINGS

1. Select the check box to enable Real-time Scan.
2. Configure the following scan criteria:
   - User Activity on Files that will trigger Real-time Scan
   - Scan Settings
3. Click the **Action** tab to configure the scan actions Trend Micro Security performs on detected security risks.
4. If you selected group(s) or client(s) on the client tree, click **Save** to apply settings to the group(s) or client(s). If you selected the root icon  , choose from the following options:
   - **Apply to All Clients:** Applies settings to all existing clients and to any new client 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 clients added to future groups. This option will not apply settings to new clients 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 client console. The time it takes to complete scanning depends on the number of files to scan and the client computer's hardware resources.

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

To configure Manual Scan settings:

PATH: CLIENT MANAGEMENT > SETTINGS > MANUAL SCAN SETTINGS

1. On the **Target** tab, configure the following scan criteria:
   - Scan Settings
   - CPU Usage
2. Click the **Action** tab to configure the scan actions Trend Micro Security performs on detected security risks.
3. If you selected group(s) or client(s) on the client tree, click **Save** to apply settings to the group(s) or client(s). If you selected the root icon  , choose from the following options:
   - **Apply to All Clients:** Applies settings to all existing clients and to any new client 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 clients added to future groups. This option will not apply settings to new clients 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 client and improve scan management efficiency.

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

To configure Scheduled Scan settings:

PATH: CLIENT MANAGEMENT > SETTINGS > SCHEDULED SCAN SETTINGS

1. Select the check box to enable Scheduled Scan.
2. Configure the following scan criteria:
   - Schedule
   - Scan Target
   - Scan Settings
   - CPU Usage
3. Click the **Action** tab to configure the scan actions Trend Micro Security performs on detected security risks.
4. If you selected group(s) or client(s) on the client tree, click **Save** to apply settings to the group(s) or client(s). If you selected the root icon  , choose from the following options:
   - **Apply to All Clients:** Applies settings to all existing clients and to any new client 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 clients added to future groups. This option will not apply settings to new clients added to an existing group.

Scan Now

Scan Now is initiated remotely by a Trend Micro Security administrator through the Web console and can be run on one or several client computers.

Initiate Scan Now on computers that you suspect to be infected. To initiate Scan Now, navigate to **Client Management > Tasks > Scan Now**.

All the Scheduled Scan settings, except the actual schedule, are used during 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 clients and groups, or to all clients 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 computer.

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 computer (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 computer 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. See *IntelliScan* on page A-2 for details.
- **File or folder name with full path:** Only scan the specified file or files found in a specific folder.

Scan Settings

Trend Micro Security can scan individual files within compressed files. Trend Micro Security supports the following compression types:

TABLE 6-4. Supported compressed files

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	

TABLE 6-4. Supported compressed files (Continued)

EXTENSION	TYPE
.eml; .mht	MIME
.td0	Teledisk format
.bz2	Unix BZ2 Bzip compressed file
.uu	UUEncode
.ace	WinAce

CPU Usage

Trend Micro Security 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 and what time Scheduled Scan will run. Select from the following options and then select the start time:

- Daily
- Weekly
- Monthly

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 checks the scan exclusion list to determine which files on the computer will be excluded from scanning.

When you enable scan exclusion, Trend Micro Security will not scan a file under the following conditions:

- The file name matches any of the names in the exclusion list.
- The file extension matches any of the extensions in the exclusion list.

Scan Exclusion List (Files)

Trend Micro Security will not scan a file if its file name matches any of the names included in this exclusion list. If you want to exclude a file found under a specific location on the computer, include the file path, such as \Users\tmsm\Desktop\test.ppt.

You can specify a maximum of 64 files.

Scan Exclusion List (File Extensions)

Trend Micro Security will not scan a file if its file extension matches any of the extensions included in this exclusion list. You can specify a maximum of 64 file extensions. A period (.) is not required before the extension.

Scan Actions

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

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

Actions

The following are the actions Trend Micro Security can perform against security risks:

Delete

Trend Micro Security removes the infected file from the computer.

Quarantine

Trend Micro Security renames and then moves the infected file to the quarantine directory on the client computer located in <Client installation folder>/common/lib/vsapi/quarantine.

Once in the quarantine directory, Trend Micro Security can perform another action on the quarantined file, depending on the action specified by the user. Trend Micro Security can delete, clean, or restore the file. Restoring a file means moving it back to its original location without performing any action. Users may restore the file if it is actually harmless. Cleaning a file means removing the security risk from the quarantined file and then moving it to its original location if cleaning is successful.

Clean

Trend Micro Security removes the security risk from an infected file before allowing users to access it.

If the file is uncleanable, Trend Micro Security performs a second action, which can be one of the following actions: Quarantine, Delete, and Pass. To configure the second action, navigate to **Client Management > Settings > {Scan Type} > Action** tab.

Pass

Trend Micro Security performs no action on the infected file but records the detected security risk in the logs. The file stays where it is located.

Trend Micro Security 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 to perform the appropriate scan action. If actually harmless, probable virus/malware will no longer be detected.

For example:

Trend Micro Security 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 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

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

Use ActiveAction

ActiveAction is a set of pre-configured scan actions for different types of security risks. If you are unsure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction.

ActiveAction settings are constantly updated in the pattern files to protect computers against the latest security risks and the latest methods of attacks.

Use the same action for all security risk types

Select this option if you want the same action performed on all types of security risks, except probable virus/malware. For probable virus/malware, the action is always "Pass".

If you choose "Clean" as the first action, select a second action that Trend Micro Security performs if cleaning is unsuccessful. If the first action is not "Clean", no second action is configurable.

Display a Notification Message When a Security Risk is Detected

When Trend Micro Security detects a security risk during Real-time Scan, it can display a notification message to inform the user about the detection.

Allow Users to Postpone or Cancel Scheduled Scan

Trend Micro Security displays a notification message five minutes before Scheduled Scan runs. Users can postpone scanning to a later time and will be reminded again before the scan runs. Users can also cancel the scan.

Security Risk Notifications

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

Administrator Notification Settings

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

To configure administrator notification settings:

PATH: NOTIFICATIONS > GENERAL SETTINGS

Specify information in the fields provided.

1. In the **SMTP server** field, type either an IP address or computer name.
   a. Type a port number between 1 and 65535.
   b. Type the sender's email address in the **From** field.
2. Click **Save**.

Security Risk Notifications for Administrators

Configure Trend Micro Security 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 to successfully send notifications through email. For details, see *Administrator Notification Settings* on page 6-15.

To configure security risk notifications for administrators:

PATH: NOTIFICATIONS > STANDARD NOTIFICATIONS

1. In the **Criteria** tab, specify whether to send notifications each time Trend Micro Security detects a security risk, or only when the action on the security risks is unsuccessful.
2. Click **Save**.
3. In the **Email** tab:
   - Enable notifications to be sent through email.
   - Specify the email recipients and accept or modify the default subject.

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

TABLE 6-5. Token variables for security risk notifications

VARIABLE	DESCRIPTION
%v	Security risk name
%s	The computer where the security risk was detected
%m	Client tree group to which the computer belongs
%p	Location of the security risk
%y	Date and time of detection

4. Click **Save**.

Outbreak Criteria and 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 to notify you and other Trend Micro Security administrators of an outbreak so you can respond immediately.

You can receive notifications through email. Configure administrator notification settings to allow Trend Micro Security to successfully send notifications through email. For details, see *Administrator Notification Settings* on page 6-15.

To configure the outbreak criteria and notifications:

PATH: NOTIFICATIONS > OUTBREAK NOTIFICATIONS

1. 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 declares an outbreak and sends a notification message when the number of detections is exceeded. For example, if you specify 100 detections, Trend Micro Security sends the notification after it detects the 101st instance of a security risk.
2. Click **Save**.
3. 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.

TABLE 6-6. Token variables for outbreak notifications

VARIABLE	DESCRIPTION
%CV	Total number of security risks detected
%CC	Total number of computers with security risks

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

Security Risk Logs

Trend Micro Security generates logs when it detects security risks. 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 8-5.

To view security risk logs:

PATH: CLIENT MANAGEMENT > LOGS > SECURITY RISK LOGS

1. Specify the log criteria and click **Display Logs**.
2. View logs. Logs contain the following information:
   - Date and time of security risk detection
   - Computer 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
   - Platform

Scan Results

Security risk logs indicate any of the following scan results:

A. If Scan Action is Successful

The following results display if Trend Micro Security was able to perform the configured scan action:

Deleted

The first action is Delete and the infected file was deleted.

The first action is Clean but cleaning was unsuccessful. The second action is Delete and the infected file was deleted.

Quarantined

The first action is Quarantine and the infected file was quarantined.

The first action is Clean but cleaning was unsuccessful. The second action is Quarantine and the infected file was quarantined.

Cleaned

An infected file was cleaned.

Passed

The first action is Pass. Trend Micro Security did not perform any action on the infected file.

The first action is Clean but cleaning was unsuccessful. The second action is Pass so Trend Micro Security did not perform any action on the infected file.

B. If Scan Action is Unsuccessful

The following results display if Trend Micro Security was unable to perform the configured scan action:

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 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 security risk may spread other computers 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 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 security risk may spread to other computers on the network.

Unable to clean the file

The file may be uncleanable. For details and solutions, see *Uncleanable Files* on page A-6.

Chapter 7

Protecting Computers from Web-based Threats

Topics in this chapter:

About Web Threats

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

In recent years, individuals once characterized as hackers, virus writers, spammers, and spyware makers are now known as cyber criminals. Web threats help these individuals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is leakage of confidential information in the form of identity loss. The infected computer may also become a vector to deliver phish attack 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

Trend Micro Security leverages Trend Micro's extensive Web security databases to check the reputation of Web sites that users are attempting to access. The Web site's reputation is correlated with the specific Web reputation policy enforced on the computer. Depending on the policy in use, Trend Micro Security will either block or allow access to the Web site. Policies are enforced based on the client's location.

Web Reputation Policies

Web reputation policies dictate whether Trend Micro Security will block or allow access to a Web site. To determine the appropriate policy to use, Trend Micro Security checks the client's location. A client's location is "internal" if it can connect to the Trend Micro Security server. Otherwise, a client's location is "external".

To configure a Web reputation policy:

PATH: CLIENT MANAGEMENT > SETTINGS > WEB REPUTATION SETTINGS

1. Configure a policy for **External Clients** and **Internal Clients**.
2. Select the check box to enable the Web reputation policy.
3. Select from the available Web reputation security levels: High, Medium, or Low

   The security levels determine whether Trend Micro Security will allow or block access to a URL. For example, if you set the security level to Low, Trend Micro Security 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.
4. For internal clients, select whether to allow the Trend Micro Security client to send Web Reputation Logs to the server. Allow clients to send logs if you want to analyze URLs being blocked by Trend Micro Security and take the appropriate action on URLs you think are safe to access.
5. If you selected group(s) or client(s) on the client tree, click **Save** to apply settings to the group(s) or client(s). If you selected the root icon  , choose from the following options:
   - **Apply to All Clients:** Applies settings to all existing clients and to any new client 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 clients added to future groups. This option will not apply settings to new clients added to an existing group.

Approved URLs

Approved URLs bypass Web Reputation policies. Trend Micro Security does not block these URLs even if the Web Reputation policy is set to block them. Add URLs that you consider safe to the approved URL list.

To configure the approved URL list:

PATH: ADMINISTRATION > WEB REPUTATION APPROVED URL LIST

1. Specify a URL in the text box. You can add a wildcard character (*) anywhere on the URL.

   Examples:

   - www.trendmicro.com/* means that all pages under www.trendmicro.com will be approved.
   - *.trendmicro.com/* means that all pages on any sub-domain of trendmicro.com will be approved.

2. Click **Add**.
3. To delete an entry, click the icon next to an approved URL.

4. Click **Save**.

Web Reputation Logs

Configure internal clients to send Web reputation logs to the server. Do this if you want to analyze URLs that Trend Micro Security blocks and take appropriate action on URLs you think are safe to access.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see *Managing Logs* on page 8-5.

To view Web reputation logs:

PATH: CLIENT MANAGEMENT > LOGS > WEB REPUTATION LOGS

1. Specify the log criteria and click **Display Logs**.
2. View logs. Logs contain the following information:

- Date/Time Trend Micro Security blocked the URL
- Computer 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

Chapter 8

Managing the Trend Micro Security Server and Clients

Topics in this chapter:

Upgrading the Server and Clients

The Plug-in Manager console displays any new Trend Micro Security build or version. Upgrade the server and clients immediately when the new build or version becomes available.

To upgrade the server:

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

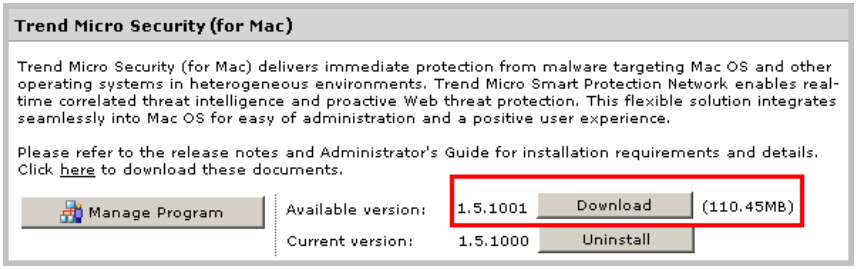


FIGURE 8-1. Web console displaying a new Trend Micro Security build

---

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

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

---

2. 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 Logs**.

3. After Plug-in Manager downloads the package, a new screen displays, providing you the following options: **Upgrade Now** or **Upgrade Later**.

4. If you choose to immediately upgrade, check the upgrade progress.

5. If you choose to upgrade at a later time:
   a. Open the OfficeScan Web console and click **Plug-in Manager** on the main menu.
   b. Go to the **Trend Micro Security (for Mac)** section and click **Upgrade**.
   c. Check the upgrade progress.

After the upgrade, the Trend Micro Security version displays.

To upgrade clients:

1. Navigate to <Server installation folder>\TMSM_HTML\ActiveUpdate\ and create a new folder named **Product**.
2. Navigate to <Server installation folder>\TMSM_HTML\ClientInstall and copy the file **tmsminstall.mpkg.zip** to the folder created in step 1.
3. Record the file size in bytes (NOT the size on disk) of **tmsminstall.mpkg.zip**. You will need this information when you modify the **server.ini** file. To check the file size, right-click the file and click **Properties**.

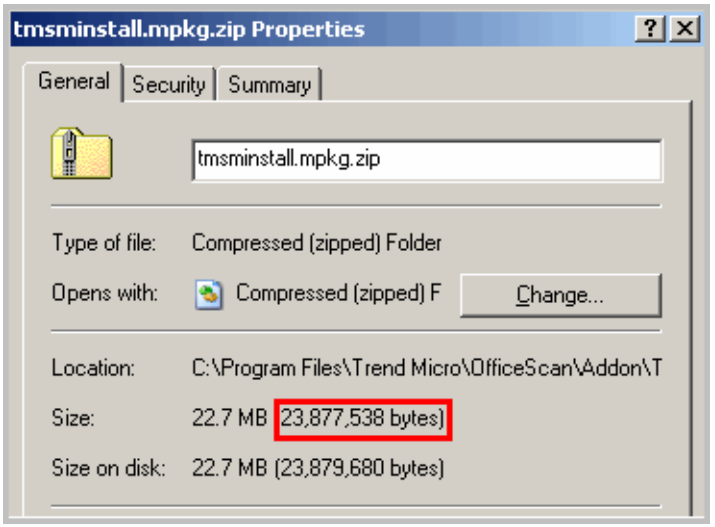


FIGURE 8-2. Sample package file size

4. Navigate to <Server installation folder>\TMSM_HTML\ActiveUpdate\ and modify the **server.ini** file as follows:

```
[All_Product]
MaxProductID=465
Product.465=TMSMCLIENT, 1.0, 1.9

[Info_465_10000_1_4865]
Version=x
Build=y
Path=product/tmsminstall.mpkg.zip,z
```

Where:

x = Trend Micro Security version (for example, 1.5)

y = Build number

z = File size in bytes, excluding commas (for example, 23877538)

5. Upgrade clients by instructing users to click **Update Now** from the client console. Clients begin to upgrade to the new build or version.

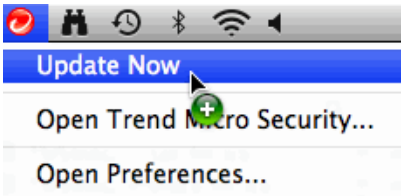


FIGURE 8-3. Update Now menu item

You can also launch an upgrade from the Web console's Summary screen by performing the following steps:

a. Go to the **Update Status for Networked Computers** section and click the link under the **Not Upgraded** column. The client tree opens, showing all the clients that require an upgrade.

b. Select the clients that you want to upgrade.

c. Click **Tasks > Update**. Clients that receive the notification start to upgrade. On the Macintosh computer, the Trend Micro Security icon on the menu bar indicates that the product is updating. Users cannot run any task from the console until the upgrade is complete.

6. Check the upgrade status from the Summary screen.

Managing Logs

Trend Micro Security keeps comprehensive logs about security risk detections and blocked URLs. Use these logs to assess your organization's protection policies and to identify clients 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.

To delete logs based on a schedule:

PATH: ADMINISTRATION > LOG MAINTENANCE

1. Select **Enable scheduled deletion of logs**.

2. Select whether to delete all logs or only logs older than a certain number of days.

3. Specify the log deletion frequency and time.

4. Click **Save**.

Licenses

View, activate, and renew the Trend Micro Security license on the Web console.

To manage product licenses:

PATH: ADMINISTRATION > PRODUCT LICENSE

1. 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 clients installations the license supports
   - **License expires on:** The expiration date of the license
   - **Activation Code:** The code used to activate the license.

2. To specify a new Activation Code, click **New Activation Code**.
3. In the screen that opens, type the Activation Code and click **Save**. This screen also provides a link to the Trend Micro Web site where you can view detailed information about your license.

Client-Server Communication

Clients identify the server that manages them by the server's name or IP address. During the Trend Micro Security server installation, the installer identifies the server computer's IP addresses, which are then displayed on the Web console's Client-Server Communication screen.

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

If you change the port number, ensure that it is not currently in use to prevent conflicts with other applications and client-server communication issues.

If a firewall application is in use on the server computer, ensure that the firewall does not block client-server communication through the listening port. For example, if the OfficeScan client firewall has been enabled on the computer, add a policy exception that allows incoming and outgoing traffic through the listening port.

You can configure clients to connect to the server through a proxy server. A proxy server, however, is usually not required for client-server connections within the corporate network.

If you need to configure the server name/IP address, listening port, and proxy server settings, configure them before installing clients. If you have installed clients and then change any of these settings, clients will lose connection with the server and the only way to re-establish connection is to re-deploy the clients.

To configure client-server communication settings:

PATH: ADMINISTRATION > CLIENT-SERVER COMMUNICATION

1. Type the server's name or IP address(es), and listening port.

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

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

Chapter 9

Troubleshooting and Support

Topics in this chapter:

Troubleshooting

Web Console Access

Problem:

The Web console cannot be accessed.

Solutions:

Perform the following steps:

1. Check if the computer meets the requirements for installing and running Trend Micro Security 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
     - If the file does not exist, enable debug logging. On the banner of the OfficeScan Web console, click the first "c" in "OfficeScan", specify debug log settings, and click **Save**.
     - Reproduce the steps that led to the Web console access problem.
     - Obtain the debug logs.
4. Check the Trend Micro Security registry keys by navigating to HKEY_LOCAL_MACHINE\SOFTWARE\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\:
      - db_TMSM.mdf
      - db_TMSM_log.LDF
   b. Check if the Trend Micro Security database instance on the Microsoft SQL server registry key exists:
      - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names
      - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.x\MSSQLServer\CurrentVersion
6. Send the following to Trend Micro:
   - Registry files
     - Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL server\TMSM.
     - 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 services.
   a. Navigate to the <Server installation folder>.
   b. Double-click **restart_TMSM.bat**. 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.

Solution:

1. Open registry editor and navigate to HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\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\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.

Client Installation

Problem:

The installation was unsuccessful. The installation package (**tmsminstall.mpkg.zip**) was launched using an archiving tool not built-in on the Mac, causing the extracted installation files (files included in **tmsminstall.mpkg**) to become corrupted.

Solutions:

Perform any of the following two tasks:

1. Set the correct permission to execute **tmsminstall.mpkg**.
   a. Open the Terminal utility.
   b. Change to the directory where tmsminstall.mpkg is located.
   c. Type the following:

      ```
      $ chmod +x
      tmsminstall.mpkg\Contents\Resources\integritycheck
      ```

   d. Retry the installation.
2. Remove the extracted folder (**tmsminstall.mpkg**) and then launch the installation package again using a built-in archiving tool such as Archive Utility.

Client Troubleshooting

Problem:

An error or problem was encountered on the client.

Solution:

Run the Trend Micro Security Debug Manager to collect data that may help resolve the error or problem.

To run the tool, open <Client installation folder>/Tools and launch **Trend Micro Debug Manager**. Follow the on-screen instructions to successfully collect data.

Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all registered users.

- Get a list of the worldwide support offices at:

  http://www.trendmicro.com/support

- Get the latest Trend Micro product documentation at:

  http://www.trendmicro.com/download

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

Trend Micro, Inc.

10101 North De Anza Blvd., Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Web address:

http://www.trendmicro.com

Email: support@trendmicro.com

Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, 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

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.

TrendLabs

TrendLabs[SM] is the global antivirus research and support center of Trend Micro. Located on three continents, TrendLabs has a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Email access to antivirus engineers
- Knowledge Base, the Trend Micro online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

Comprehensive security information is available at the Trend Micro Web site.

http://www.trendmicro.com/vinfo/

Information available:

- List of viruses and malicious mobile code currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

Sending Suspicious Files to Trend Micro

If you think you have an infected file but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us. For more information, refer to the following site:

http://subwiz.trendmicro.com/subwiz

You can also send Trend Micro the URL of any Web site you suspect of being a phish site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and viruses).

- Send an email to the following address and specify "Phish or Disease Vector" as the subject.

  virusresponse@trendmicro.com

- You can also use the Web-based submission form at:

  http://subwiz.trendmicro.com/subwiz

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

Glossary

ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of pattern files, scan engines, programs, and other Trend Micro component files through the Internet.

Compressed File

A single file containing one or more separate files plus information for extraction by a suitable program, such as WinZip.

Domain Name

The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).

End User License Agreement

An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product.

Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.

False Positive

A false positive occurs when a file is incorrectly detected by security software as infected.

HTTP

Hypertext Transfer Protocol (HTTP) is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet.

HTTPS

Hypertext Transfer Protocol using Secure Socket Layer (SSL). HTTPS is a variant of HTTP used for handling secure transactions.

IntelliScan

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

Using IntelliScan provides the following benefits:

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

IP

"The internet protocol (IP) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)

Java File

Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets". An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet transfers its code to your computer and the browser's Java Virtual Machine executes the applet.

Listening Port

A listening port is utilized for client connection requests for data exchange. The default Trend Micro Security listening port is 61617. If a firewall application is running on the server computer, ensure that the firewall does not block the listening port to ensure uninterrupted communication between the server and clients.

Mixed Threat Attack

Mixed threat attacks take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the "Nimda" or "Code Red" threats.

Phish Attack

Phish, or phishing, is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site.

In a typical scenario, unsuspecting users get an urgent sounding (and authentic looking) email telling them there is a problem with their account that they must immediately fix to avoid account termination. The email will include a URL to a Web site that looks exactly like the real thing. It is simple to copy a legitimate email and a legitimate Web site but then change the so-called backend, which receives the collected data.

The email tells the user to log on to the site and confirm some account information. A hacker receives data a user provides, such as a logon name, password, credit card number, or social security number.

Phish fraud is fast, cheap, and easy to perpetuate. It is also potentially quite lucrative for those criminals who practice it. Phish is hard for even computer-savvy users to detect. And it is hard for law enforcement to track down. Worse, it is almost impossible to prosecute.

Please report to Trend Micro any Web site you suspect to be a phishing site. See *Sending Suspicious Files to Trend Micro* on page 9-9 for more information.

Proxy Server

A proxy server is a World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, and then returns the URL to the requester.

SSL

Secure Socket Layer (SSL) is a protocol designed by Netscape for providing data security layered between

application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

TCP

Transmission Control Protocol (TCP) is a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols that support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.

Telnet

Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.

Trojan Ports

Trojan ports are commonly used by Trojan horse programs to connect to a computer. During an outbreak, Trend Micro Security blocks the following port numbers that Trojan programs may use:

TABLE A-1. Trojan ports

PORT NUMBER	TROJAN HORSE PROGRAM	PORT NUMBER	TROJAN HORSE PROGRAM
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven

TABLE A-1. Trojan ports (Continued)

PORT NUMBER	TROJAN HORSE PROGRAM	PORT NUMBER	TROJAN HORSE PROGRAM
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Uncleanable Files

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

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 computer systems. The propagation usually takes place through network connections or email attachments. Worms are uncleanable because the file is a self-contained program.

Solution: Trend Micro recommends deleting worms.

Write-protected Infected Files

Solution: Remove the write-protection to allow Trend Micro Security to clean the file.

Password-protected Files

Includes password-protected files or compressed files.

Solution: Remove the password protection for Trend Micro Security to clean these files.

Backup Files

Files with the RB0~RB9 extensions are backup copies of infected files. Trend Micro Security creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.

Solution: If Trend Micro Security successfully cleans the infected file, you do not need to keep the backup copy. If the computer functions normally, you can delete the backup file.

Index