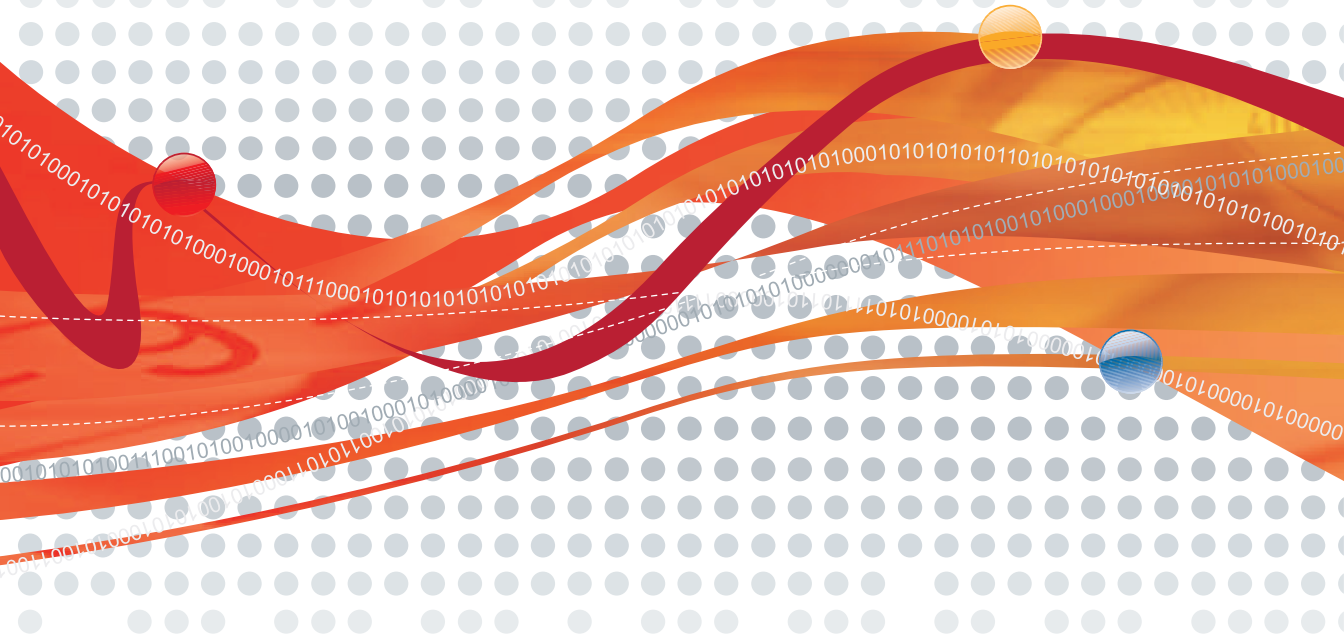
TREND MICRO™

# Core Protection Module
## *for Mac*[1]
for Endpoint Security Platform

## Administrator's Guide



Endpoint Security

Document Part No. APEM14350/91118

Release Date: December 2009

### Related Documents

Use this Administrators's Guide to upgrade, install and/or configure Trend Micro Core Protection Module *for Mac* (CPM for Mac) on an existing ESP Server. This Administrators's Guide also covers ESP client deployment, Web Reputation updates and configuration.

For related information, see:

- **ESP 7.2 Administrator's Guide**—Contains deployment strategies, installation instructions, and common configuration tasks.
- **ESP 7.2 Console Operator's Guide**—Contains information for using the ESP Console to administer protected endpoints.

### Feedback

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 3: CPM for Mac Clients: Installing and Updating



## Chapter 4: Configuring and Managing CPM for Mac

## Chapter 5: Configuration Wizards Reference



## Chapter 6: Using Web Reputation



## Chapter 7: Setting Up and Using Locations



## Chapter 8: Troubleshooting

## Appendix B: Reference Tables

# Chapter 1

# Introducing Core Protection Module *for Mac*

This chapter introduces Trend Micro Core Protection Module for Mac (CPM for Mac) and provides information on the following topics:

# Overview

Trend Micro™ Core Protection Module *for Mac* (CPM *for Mac*) is an anti-malware application for Trend Micro Endpoint Security Platform (ESP). It works with ESP to protect the desktop and notebook Macs on your network from security risks such as malware.

ESP is built on the BigFix® Enterprise Suite (BES) to provide extended management capabilities to the CPM *for Mac* server and clients. The CPM *for Mac* client provides real-time, on-demand, and scheduled malware protection. In addition, you can protect your users against visiting malicious Web sites by enabling CPM *for Mac*'s Web Reputation.

Using a single agent and management console, Trend Micro ESP can support over 250,000 endpoints. From the management console, you can track the progress of each computer as updates or configuration policies are applied.

## Key Differences Between CPM and CPM *for Mac*

If you are migrating from CPM to CPM *for Mac*, the main differences you will notice between the two products are located in the following features:

### Overview Report

To be determined.

### Version Report

These changes will not display until you have subscribed to the CPM *for Mac* Web site.

- A new pie chart that displays the Anti-virus Pattern Versions for Mac has been added.
- A new pie chart initiated from the CPM tab that displays the CPM *for Mac* Program Version has been added.
- The existing Anti-virus Pattern Versions pie chart has changed to support both Windows and Mac endpoints.
- The existing Spyware Active-monitoring Pattern Versions pie chart has changed to support both Windows and Mac endpoints.

## Infection Report

- A new pie chart that displays the Top Mac Malware Infections has been added, but only the total number of malware infections will display.
- A new data chart that details the Mac Malware Infections has been added.

## Web Reputation

- CPM *for Mac* will only support the Blocked Web Sites chart.

## Wizards

**Global Scan Settings Wizard**

To be determined.

**Real-Time Scan Settings Wizard**

- No additional configuration has been added compared to CPM. CPM *for Mac* supports only a subset of the CPM configuration, listed as follows:
  - Malware scans enabled or disabled
  - User activity on files
  - Scan compressed files enabled or disabled
  - Scan action:
    - Use ActiveAction
    - Use custom actions
      - First action: CPM supports only three types of the first action:

        1: Clean, 2: Delete, 3: Quarantine
      - Second action: CPM *for Mac* supports only two types of the first action:

        1: Delete, 2: Quarantine

        If an unsupported option is selected for the first action, such as Rename, the generated Action will not be applied for this configuration, and the original value will be retained.

### On-Demand Scan Settings Wizard

There are several options and features no longer supported in CPM *for Mac*.

**TABLE 1-1. What's Been Added or Changed**

| OPTION | RESOLUTION |
|---|---|
| All Spyware/Grayware actions/options | Ignored and Virus/Malware settings used |
| Files to Scan (Win. filters by extension, Mac takes lists of filenames) | Different target options between CPM and CPM for Mac are used |
| Scan Compressed files maximum layers | Ignored on Mac |
| Scan Boot Area | Ignored on Mac |
| Enable IntelliTrap | Ignored on Mac |
| CPU Setting "Medium" | Mapped to "Low" |
| Scan Exclusion options | Ignored on Mac |
| "Rename" action option | Ignored on Mac |
| Specific action for virus type | Use defaults (Clean / Quarantine) |
| Backup Files before cleaning | Ignored on Mac |
| Display a notification message | Ignored on Mac |

- CPM *for Mac* also does not support specifying alternate configuration files for running custom scans so the **Scan Now** option only applies to CPM.
- CPM *for Mac* has consolidated All Spyware/Grayware actions and options under the "Virus/Malware" scan options. This option is ignored when constructing Mac actions and relevance in favor of the "Virus/Malware" scan options.

### Pattern Update and Rollback Wizard

After the server components are upgraded, the wizard shows any pattern sets downloaded with the older CPM 1.5 AU server components as well as the new CPM 2.0 AU server components. The rollback feature is supported only by CPM.

- When the CPM *for Mac* site is subscribed to and the Server Components are upgraded to the AU 2.0 plug-in architecture, the successive pattern-sets downloaded will show the Virus Scan Engine for Mac components.
- Older pattern sets downloaded with the CPM 1.5 AU server should still exist.
- Rollback capability for old and new pattern sets are restricted to CPM clients for Windows by applicability relevance.
- Old existing CPM 1.5 pattern sets will not be applicable to CPM *for Mac* clients and are restricted in the applicability relevance.
- Unsubscribing from the CPM *for Mac* site will not automatically remove the Virus Scan Engine for Mac from the pattern updates. If this occurs, you will need to remove the CPM 2.0 AU server components and then re-install the CPM 1.5 AU server components.

**Pattern Update Settings Wizard**

After the server components are upgraded, and a new 2.0 pattern set has been downloaded, the setting to enable/disable the updating of the Virus Scan Engine for Mac will display.

- When CPM *for Mac* site is subscribed to and the Server Components are upgraded to the AU 2.0 plug-in architecture, the successive pattern-set downloaded will show the Virus Scan Engine for Mac components.
- After new pattern sets are downloaded, with the Virus Scan Engine for Mac, this new component will appear to enable and disable the update.
- If the CPM *for Mac* site is unsubscribed to, this setting will disappear.
- Refer to the integrated UI for more information.

# How CPM *for Mac* Works

Trend Micro ESP uses the patented Fixlet® technology from BigFix to identify agents with outdated malware protection. You can trigger 50,000 computers to update their 10MB pattern file and have confirmation of the completed action in as little as 15 minutes.

After CPM *for Mac* is installed, you will find it easy to protect your networked computers and keep them secure, all from the ESP Console. Deploying CPM *for Mac* to ESP-managed endpoints can be accomplished in minutes. After completing this process,

you will be able to track the progress of each computer as you apply CPM *for Mac* component updates. This tracking makes it easy to gauge the level of protection across your entire enterprise. Additionally, the ESP Web Reporting module makes it simple to chart the status of your overall protection with Web-based reports.

# ESP Components

CPM for Mac, as a module in the Trend Micro Endpoint Security Platform (ESP), provides a powerful, scalable, and easy-to-manage security solution for very large enterprises.

This integrated system consists of the following components:

- **The ESP Console** ties all the components together to provide a system-wide view of all the computers on your network, along with security status information.
- **The ESP Server** offers a collection of interacting services, including application services, a Web server, and a database server, that together form the heart of ESP. The ESP Server coordinates the flow of information to and from individual computers and stores the results in the ESP database. ESP Servers also include a built-in Web reporting module. ESP versions 7.2 and later support the deployment of multiple servers to ease administrative burdens.
- **The ESP Agent** is installed on every client computer ESP manages. The ESP Agent, along with the ESP Server and Console, is responsible for deploying, communicating with, and uninstalling all CPM *for Mac* components. The ESP Agent is responsible for relaying the instructions you enter in the ESP Console to all CPM *for Mac* components. It also relays the findings and results of scans and damage cleanup processes back to the ESP Console for reporting and analyses.
- **The CPM** *for Mac* **Client Components** are responsible for managing pattern files, conducting scans, and removing any malware they detect. These components run undetected by end users and use minimal system resources. You need to install a CPM *for Mac* client on each endpoint that you want to protect. These endpoints should already have the ESP Agent installed.
- **ESP Relays** increase the efficiency of the system by spreading the load. Hundreds to thousands of ESP Agents can point to a single ESP Relay for downloads, which in turn, makes only a single request of the server. ESP Relays can connect to other relays as well, further increasing efficiency and can be installed on any Mac with Mac OS X running the ESP Agent.

# Features and Benefits

CPM *for Mac* reduces business risks by preventing infection, identity theft, data loss, network downtime, lost productivity, and compliance violations. Additionally, it provides your large enterprise with a host of features and benefits.

## Ease of Management

- Uses small, state-of-the-art pattern files, enhanced log aggregation for faster, more efficient updates, and reduced network utilization.
- Integrates with the Trend Micro ESP Console to provide centralized security, including the centralized deployment of security policies, pattern files, and software updates on all protected clients and servers.

## Extended Platform Support

Works with most versions of Mac OSX, including;

- Mac OS™ X version 10.4.11 (Tiger) or higher
- Mac OS™ X version 10.5.5 (Leopard) or higher
- Mac OS™ X version 10.6 (Snow Leopard)

## Superior Malware Protection

- Delivers powerful protection against malware as it emerges
- Protects against a wide variety of malware, including adware, dialers, joke programs, remote-access tools, key loggers, and password-cracking applications

## Web Reputation Technology

The CPM *for Mac* 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 the downloading of malicious code.

In addition to file-based scanning, CPM *for Mac* now includes the capability to detect and block Web-based security risks, including phishing attacks. Using the ESP location

awareness features, you can have CPM *for Mac* enforce different Web Reputation policies according to the client computer's location. The client's connection status with the ESP Server or any Relay Server can be used to determine the location of the client.

- Web Reputation opens a blocking page whenever access to a malicious site is detected. This page includes links to the Trend Micro Web Reputation Query system, where end-users can find details about the blocked URL or send feedback to Trend Micro.
- Proxy server authentication for Web Reputation is also supported. You can specify a set of proxy authentication credentials on the Web console. HTTP proxy servers are supported.

# The Trend Micro Pattern Files and Scan Engine

All Trend Micro products, including CPM *for Mac*, can be configured to automatically check the Trend Micro ActiveUpdate (TMAU) server, then download and install updates when found. This process is typically configured to occur in the background, although you can manually update some or all of the pattern files at any time. In addition, pre-release patterns are available for manual download (at your own risk) in the event that a situation such as a malware outbreak occurs. Pre-release patterns have not undergone full testing but are available to stop burgeoning threats.

You can manually download the malware pattern and other files from the following URL.

`http://www.trendmicro.com/download/pattern.asp`

At the same location, you can also check the current release version, date, and review all the new malware definitions included in the files.

## Incremental Malware Pattern File Updates

CPM for Mac, in conjunction with Trend Micro ActiveUpdate, supports incremental updates of the malware pattern file. Rather than download the entire pattern file each time (full pattern files can be more than 70MB), ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file.

## How Scanning Works

The scan engine works together with the malware pattern file to perform the first level of detection, using a process called pattern matching. Because malware contains a unique binary "signature" or string of tell-tale characters that distinguish it from any other code, the malware experts at TrendLabs capture inert snippets of this code to include in the pattern file. The engine then compares certain parts of each scanned file to the data in the malware pattern file looking for a match.

Pattern files use the following naming format:

```
lpt$vpn.###
```

where ### represents the pattern version (for example, 400). If multiple pattern files exist in the same directory, only the one with the highest number is used. Trend Micro publishes new malware pattern files on a regular basis (typically several times per week), and recommends configuring hourly automatic updates. With automatic updates enabled, new updates are downloaded to the server and flow to the endpoints immediately. Updates are available to all Trend Micro customers with valid maintenance contracts.

## The Trend Micro Scan Engine and Detection Technologies

A scan engine lies at the heart of all Trend Micro products. The scan engine checks for threats "in the wild," or actively circulating, and those that are "in the zoo," or known, theoretical, threat types typically created as a proof of concept.

Rather than scanning every byte of every file, the engine and pattern file work together to identify tell-tale "malware" characteristics and the exact location within a file that the malicious code inserts itself. CPM *for Mac* can usually remove malware upon detection.

International computer security organizations, including ICSA (International Computer Security Association), certify the Trend Micro scan engine annually.

### Scan Engine Updates

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

- Incorporation of new scanning and detection technologies into the software
- Discovery of new, potentially harmful malware unhandled by the current engine
- Enhancement of the scanning performance
- Addition of file formats, scripting languages, encoding, and compression formats

# Chapter 2

# ESP Server: Installing and Updating

Before beginning these procedures, you should have Trend Micro Endpoint Security Platform (ESP) installed, including the ESP Server, ESP Console, and ESP Agents.

This chapter covers installing the Trend Micro Core Protection Module *for Mac* (CPM *for Mac*) server components on the ESP Server, updating the related files, and preparing the endpoints to receive the ESP client. Topics include:

# Open the ESP Console

If you are logging into the ESP Server using an administrator account, you can use NT Authentication instead of entering a password. If you are running the ESP Console remotely, you will need a user name and password.

**To open the ESP Console:**

1. On the Windows desktop, click the Windows Start button, then **Programs> Trend Micro Endpoint Security Platform > ESP Console**.
2. Connect to the ESP Server database by entering the user name you created when installing the ESP Server (if you installed the evaluation version, type `EvaluationUser` for the user name) and then click **OK**.
3. The ESP Console opens.

# Add the CPM *for Mac* Site to the ESP Server

Install the Trend Micro Core Protection Module *for Mac* by adding its site masthead to the list of managed sites in the ESP Console. If you do not have the Core Protection Module *for Mac* and Reporting mastheads, contact your Trend Micro sales representative to obtain them.

CPM *for Mac* now includes a Web Reputation component that replaces the stand-alone version. You will be able to migrate any existing WPM blacklists and whitelists you might have.

**Note:** If you are a current Web Protection Module (WPM) customer, you will need to remove any installed clients and then the WPM site prior to installing CPM *for Mac*.

Before adding the site, make sure that the ESP Server can connect to the source of the masthead files (that is, can connect to the Internet). If it cannot, the request remains pending until the connection is made.

**To add the CPM *for Mac* site:**

1. From any computer with the ESP Console installed, locate and double-click the masthead file to add automatically its site.
2. Alternatively, in the ESP Console menu, click **Tools > Manage Sites...** and then the **Add External Site...** button.

3. In the **Add Site** window that opens, locate the masthead file(s) you received from your Trend Micro Sales Representative. The following masthead is available (file name is shown here):

   ```
   Trend Micro Core Protection Module.efxm
   Trend Reporting.efxm
   Trend Common Firewall.efxm (optional)
   ```

   If you are already a CPM user, you will only need to add CPM *for Mac* and `Trend Micro Core Protection Module for Mac.efxm`

   The masthead(s) you selected appear in the Manage Site window.

4. Click **Gather All Sites**, and then **OK**.

5. When prompted, type your private key password and click **OK**. The ESP Server begins gathering the associated files and content associated with the masthead(s) you added and installs them on the server.

# Install CPM *for Mac* on the ESP Server

After adding the CPM *for Mac* Site(s) to the ESP Console, you need to upgrade the core protection module server on the ESP Server to get core protection module for Mac components, and then prepare and deploy the CPM *for Mac* clients to your endpoints that are running the ESP Agent.

## Overview of Procedures

- Install the CPM *for Mac* components. (See page 2-4.)
- Update the pattern files on the ESP Server: (Starts on page 2-4.)
  - Configure a proxy server and identify a pattern update source.
  - Run a script to set up the ESP server for automatic updates.
  - Update the pattern files manually.
  - Set up automatic pattern updates.
- Deploy and update CPM *for Mac* clients. (See page 3-1.)

## Install CPM *for Mac* Components on the ESP Server

After adding the mastheads to the ESP Server, the next step is to open the ESP Console and update the CPM *for Mac* Server with the required components. You will need at least one relevant computer. In this case, the ESP Server to which you just added the CPM *for Mac* masthead should be relevant. If it is not, resolve this issue before you begin. For example, check that the server has an ESP Agent installed or previous core protection module server has already been installed.

**To install the CPM *for Mac* server components:**

1. From the ESP Console menu, click **Dashboard > CPM Dashboard**.
2. Click **Deployment > Upgrade > Upgrade CPM Server**.
3. Below **Actions,** click the hyperlink to open the **Take Action** window.
4. Select **Specify computers selected in the list below**.

   Because you are updating only the ESP Server with CPM *for Mac* components, only that computer will be relevant and appear in the list of Applicable Computers.
5. Click **OK**, and then when prompted, enter your private key password to initiate the Task.

   A status summary page appears when the Task is finished.
6. Close any open windows to return to the Dashboard view.

# Update Pattern Files on the Server

It is critically important to keep the ESP Server, Relays, and all CPM *for Mac* clients up-to-date with the current pattern and engine files from Trend Micro. CPM *for Mac* uses three different pattern files to identify malware threats. (See Security Risks starting on page 9-4 for the complete list.) Not all patterns are updated every day. There are days, however, such as when a new threat is released and hackers are writing hundreds of variations to try and avoid detection, that one or all the patterns are updated often over the course of a day or week.

Trend Micro recommends that you update the malware pattern file on the ESP Server immediately after installing CPM *for Mac*, and then set the task to repeat hourly. The same holds true for all CPM *for Mac* clients.

## Choose an Update Source and Proxy

By default, the core protection module server is configured to use the Trend Micro ActiveUpdate (AU) server for pattern updates. Although you can use an intranet source (for example by manually downloading the pattern files to an internal computer and then pointing the ESP Server to that source), Trend Micro recommends that you use the AU server. This is the only official source for pattern updates, and in conjunction with CPM *for Mac*, AU provides several layers of authentication and security to prevent forged or unsupported patterns.

You can and should configure the core protection module server to contact frequently the AU server to check for and download pattern and component updates. If there is a proxy server between the ESP Server and the Internet, you need to identify it and provide any required log on credentials. The proxy server you identify here is not "inherited" for use by other CPM *for Mac* components, including the client settings for Web Reputation. That is a separate configuration. Likewise, if you have configured a proxy to enable BESGather service (typically identified during install), those settings will not be inherited for pattern updates, even if the same proxy is being used.

In the procedures that follow, you will configure the core protection module server to get pattern updates, apply the configuration to the ESP server, and run script to set the environment, and then configure and deploy the pattern update. These steps typically only need to be performed once.

**To configure a proxy server and an update location:**

1. In the CPM Dashboard, click **Configuration > ActiveUpdate Server Settings > Change ActiveUpdate Server Settings...**. to open the Server Settings Wizard.
2. Under **Source**, choose **Trend Micro's ActiveUpdate Server**.

   See ActiveUpdate Server Settings Wizard on page 5-5 for information about all the configuration choices available on this page.
3. Under **Proxy**, click **Use a proxy server for pattern and engine updates** and provide the following (there is no validation checking; be sure of the settings you configure here):
   - **Proxy Protocol**—Choose the option that reflects your proxy server.
   - **Server Name or IP**—Use an IP address if you have not configured the ESP Server to recognize host names.
   - **Port**—Typically, this is port 80 or 8080.

- **User Name**—Type a name with access rights to the proxy.
- **Password**—The password is encrypted when stored and transmitted.

4. Click **Create Server Configuration Action...**

   The **Take Action** window opens.

5. Select the ESP server and click **OK**.
6. When prompted, type your private key credential.

   The **Action | Summary** tab appears. Check the **Status** after a few minutes to confirm that the Action is completed.

7. Close the window to return to the Dashboard view.

## Prepare the ESP Server and Update the Pattern Files

This procedure requires running a setup program to prepare the ESP Server for recurring automatic pattern updates that are then used for CPM *for Mac* client updates. Trend Micro recommends that you enable the automatic pattern updates, and that you use this script to do it.

---

**Note:** The file and folder paths mentioned in this section assume that you have installed the components of ESP and CPM *for Mac* in their standard locations. If you installed them in other locations, you must adjust the paths accordingly.

The section also assumes you have a basic knowledge and understanding of ESP and ESP-related terminology. If you are not familiar with the product's overall architecture and/or terminology, review the *Endpoint Security Platform Administrator's Guide* and the *Endpoint Security Platform Console Operator's Guide*.

---

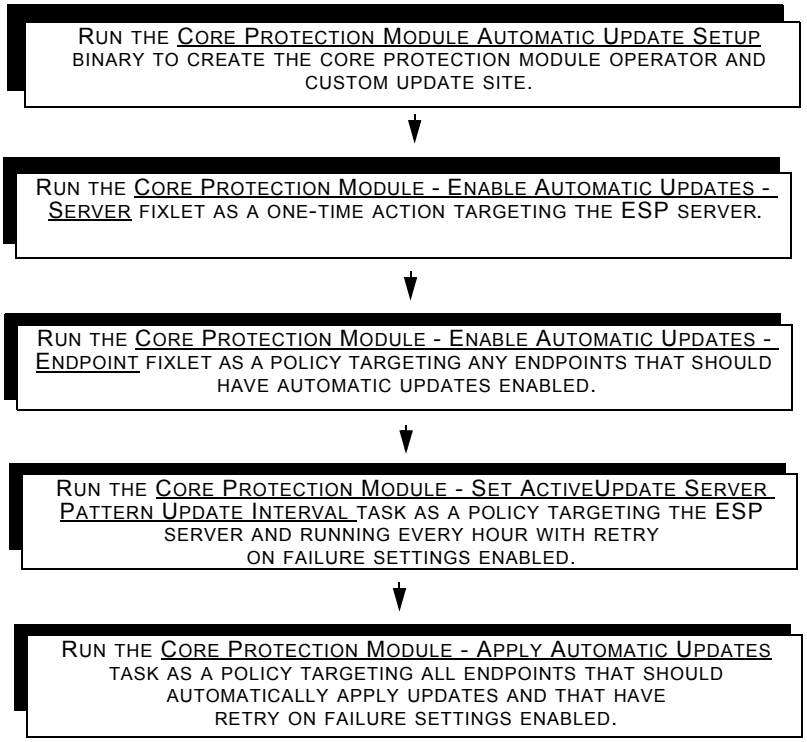



**FIGURE 2-1 Update Overview**

Alternatively, you can download the setup program and run it independently of this procedure. You can even manually perform the steps automated by the script. The URL that follows contains instructions for the manual procedure and a link to the script download.

`http://support.bigfix.com/cpm_update.html`

---

**Note:** Pattern updates to the ESP Server always include all 15 patterns. When configuring updates for CPM *for Mac* clients, you can select patterns individually and selectively

update different clients with different patterns (although it is typical to update all patterns).

## Running the CPM *for Mac* Automatic Update Setup Program

Before you can download updates from the Trend Micro ActiveUpdate servers and distribute them to endpoints, you must first run a setup program that creates a custom site and a user that has privileges to propagate files to that site.

**To run the CPM *for Mac* automatic update setup binary:**

1. Log on to the server running ESP.
2. Download the **CPM Automatic Update Setup** script from the URL that follows and save it to the desktop:

   `http://software.bigfix.com/download/bes/cpm/CPMAutoUpdateSetup2_1.0.0.0.exe`

3. Double-click the name of the program to start it. The program prompts you to create a new user account in ESP.
   a. To use the default account and password, select the checkbox (recommended.)
   b. Enter any password you would like for **CPM Admin Password**.

      You might want to choose something more secure than "trendmicro."
   c. Enter any email address as the **CPM Admin Email Address**.

      ESP only uses this address to generate a public key certificate for the user. It does not send alerts or email to this address.
   d. Browse to the location of the **`license.pvk`** file for your ESP server.

      This file is usually in this folder `C:\Documents and Settings\<Windows login>\My Documents\BESCredentials`, where `<Windows login>` is the account you used to login with when you originally installed ESP.
   e. Enter your **Site Admin** password.

      Be sure that you use the correct password and not your ESP console password. If you are unsure of which password to use, start the ESP Administration Tool. The password you use to start this tool is the same one you should enter here.

**Note:** Using an incorrect password results in an error, and the binary will not complete.

**f.** Click **OK**.

## Enabling Automatic Updates on the ESP Server

Running the "Enable Automatic Updates - Server" task enables automatic updates on the ESP server. If you do not enable automatic updates on the server, clients will not be updated automatically.

**To enable automatic updates on the ESP server:**

1. Log on to the ESP console.
2. Navigate to **Dashboards > CPM Dashboards**.
3. In the CPM Dashboard, click **Updates > Automatic Update Tasks > Enable Automatic Updates - Server...**.

   The Task **Description** tab opens.
4. Find the action to enable automatic updates on the server.
5. Below **Actions,** click the **here** hyperlink to open the **Take Action** window.
6. Leave the default settings in the **Take Action** dialog.
7. Select the ESP server and click **OK**.
8. When prompted, type your private key credential.

   The **Action | Summary** tab appears. Check the **Status** after a few minutes to confirm that the Action is "Fixed." You do not have to wait for the task to complete before continuing.
9. Close the open windows to return to the Dashboard view.

## Enabling Automatic Updates on Endpoints

Next, you must set up a policy to enable automatic updates on the endpoints you want to manage with ESP. Note that this task only enables updates. It is not responsible for downloading or applying updates.

**Note:** Be sure that any firewall running locally on or between the ESP agents and the ESP server has the ESP communication port (52311 by default) open for both TCP and

UDP traffic. Failure to do so could cause significant delays in the agents receiving the pattern and/or engine updates.

**To run the "Enable Automatic Updates - Endpoint" task:**

1. Navigate to **Dashboards > CPM Dashboard**.
2. After the dashboard appears, navigate to **Updates > Automatic Update Tasks > Enable Automatic Updates - Endpoint**.
3. Find the action to enable automatic updates on the server and click the **here** link.
4. Make this task a policy, and use the settings that follow as recommended by Trend Micro.

   **Note:** Making this task a policy allows you to install CPM *for Mac* on a new machine and have the new machine automatically download updates.

   a. Change the name of the action to **[POLICY] Core Protection Module for Mac - Enable Automatic Updates - Endpoint** to distinguish the open action as a policy.

   b. Change the **Preset** from **Default** to **Policy**.

   c. On the **Target** tab, select the **All computers with the property values selected in the tree below** option.

   d. Choose a group, property, or Active Directory container to target some or to target all computers.

   e. Click **OK**.

5. Type your private key credential when prompted.

   The Action | Summary tab appears. Check the Status after a few minutes to confirm that the Action is "Fixed." You do not have to wait for the task to complete before continuing.

6. Close the open windows to return to the Dashboard view.

## Updating the Pattern File and Make the Action Automatic

Next, you need to set up a policy that periodically checks for and downloads updates as they become available. This task is only responsible for downloading updates from the

Trend Micro ActiveUpdate servers and then publishing them to the custom CPM *for Mac* update site.

**To run the "Set ActiveUpdate Server Pattern Update Interval" task:**

1. Navigate to **Dashboards > CPM Dashboard**.
2. In the CPM Dashboard, click **Deployment > Install > Set ActiveUpdate Server Pattern Update Interval...**.

   The Task **Description** tab opens.
3. Below **Actions,** click the **here** hyperlink to open the **Take Action** window.
4. Make this task a policy to allow the ESP server to check the Trend Micro ActiveUpdate servers periodically for new updates.

---

**Note:** You can set any parameters you want, but Trend Micro recommends the following settings:

---

   a. Change the name of the action to **[POLICY] Core Protection Module for Mac - Set ActiveUpdate Server Pattern Update Interval**.

      This helps to distinguish the open action as a policy.

   b. Change the **Preset** from **Default** to **Policy**.

   c. On the **Target** tab, select the **ESP** server.

   d. On the **Execution** tab, make the following changes:

      i. Check **On failure, retry** and set it to **99** times.

      ii. Select **Wait... between attempts** when there is a failure and choose **10** minutes.

      iii. Select **while relevant, waiting... between reapplications** and choose **1** hour.

      If you want to check for updates more or less frequently, increase or decrease this interval.

---

**Note:** If you are configuring CPM *for Mac* for testing, a Proof of Concept installation, or simply reviewing the features in the product, you can change this interval to **10 minutes** to check for updates more frequently.

---

d. Click **OK**.

5. When prompted, type your private key password and click **OK**.

   The **Action** window opens. Check the **Status** after a few minutes to confirm that the Action is "Running" and then "Completed." You do not have to wait for the task to complete before continuing.

6. Close any open windows to return to the Dashboard view.

## Running the "Apply Automatic Updates" Task

The last step in the configuration procedure is to set up a policy to download updates from the ESP server as soon as they become available. This task is responsible for downloading updates from the ESP server and applying them to your endpoints.

---

**Note:** This task does not appear as relevant in the ESP console until the Set ActiveUpdate Server Pattern Update Interval task completes at least once and downloads new pattern files from the Trend Micro ActiveUpdate servers. However, as the steps that follow indicate, you can still deploy it as a policy targeting all computers or a particular group of computers. After you download the new pattern files, this task then becomes relevant on all endpoints that do not yet have the new pattern files.

---

### To run the "Apply Automatic Updates" task:

1. Navigate to **Dashboards > CPM Dashboard**.
2. After the dashboard appears, navigate to **Updates > Automatic Update Tasks > Apply Automatic Updates**.
3. Below **Actions,** click the **here** hyperlink to open the **Take Action** window.
4. Make this task a policy to allow the endpoints to download the updates automatically as soon as they become available.

   ---

   **Note:** You can set any parameters you want, but Trend Micro recommends the following settings:

   ---

   a. Change the name of the action to **[POLICY] Core Protection Module - Apply Automatic Updates**. This helps distinguish the open action as a policy.

   b. Change the **Preset** from **Default** to **Policy**.

c. On the **Target** tab, select the **All computers with the property values selected in the tree below** option and then choose a group, property, or Active Directory container to target. You can also target all computers.

d. On the **Execution** tab, make the following changes:

i. Check **On failure, retry** and set it to **99** times.

ii. Select **Wait... between attempts** when there is a failure and choose 10 minutes.

iii. Do **not** change any other settings on this tab.

d. Click **OK**.

5. When prompted, type your private key password and click **OK**.

   The **Action** window opens. Check the **Status** after a few minutes to confirm that the Action is "Running" and then "Completed." You do not have to wait for the task to complete before continuing.

6. Close any open windows to return to the Dashboard view.

# Activate CPM *for Mac* Analyses

The Core Protection Module *for Mac* includes a number of Analyses that are used to collect statistics from target computers. Analyses data are used to display information, typically in Reports, about endpoint scan and configuration settings, server settings, and malware events. Analyses must be activated before they can be used.

**To activate CPM *for Mac* analyses:**

1. In the CPM Dashboard, click **Analyses > CPM Server > [analysis name]**.

   The Analysis **Description** tab opens.

2. Below the **Description**, click the hyperlink to activate the analysis.
3. Type your private key password and click **OK**.
4. Close any open windows to return to the Dashboard view.

## Shortcut

You can activate all CPM *for Mac* analyses at once, thus avoiding the need to repeatedly type your private key password and click **OK**. You can activate the CPM *for Mac* client Analyses anytime—before or after the CPM *for Mac* clients have been deployed.

**To activate all CPM *for Mac* analyses:**

1. In the ESP Console navigation pane, click the **Analyses** tab. A list of available analyses appears.
2. Click the **Name** column header to sort the analyses in alphabetical order, then scroll down the list and select all the Core Protection Module and Core Protection Module *for Mac* analyses.
3. Right-click the list you have selected. In the pop-up menu that appears, click **Activate**.
4. When prompted, type your private key password and click **OK** to activate all the Analyses.

# Removing Core Protection Module Server Components

Use the Remove Server Components Task to uninstall Core Protection Module server components from the ESP Server (seldom used).

**To remove CPM server components:**

1. From the main ESP Console menu, open the Tasks tab and then click **All Tasks > By Site > Trend Micro Core Protection Module.**
2. Locate **Core Protection Module - Remove Server Components** in the list of **Actions** that appears and click it to open the **Description**.
3. Click the hyperlink under **Action** to open the **Take Action** screen.
4. Select the CPM server and click **OK**.
5. When prompted, enter your password to initiate the component removal.

## Removing the Core Protection Module *for Mac* Site

Remove the Core Protection Module *for Mac* and/or Trend Reporting site from the ESP Console by deleting the mastheads from the list of managed sites.

**To remove the CPM *for Mac* masthead:**

1. In the ESP Console menu, click **Tools > Manage Sites...** and select **Trend Micro Core Protection Module for Mac**.

2. Click the **Remove Site** button and then **OK**.
3. Enter your private key password and click **OK** to remove the CPM *for Mac* masthead.

# Chapter 3

# CPM *for Mac* Clients: Installing and Updating

There any number of ways to handle the deployment of Core Protection Module *for Mac* (CPM *for Mac*) clients to your endpoints, and you will need to decide on the one that works best for you and your organization. However, Trend Micro does recommend that you start off incrementally, deploying and then configuring a small number of clients and then either gradually or in batches, proceed until you have installed CPM *for Mac* clients on all your endpoints.

Topics in this chapter include:

# About CPM *for Mac* Client Deployment

The Tasks created in the procedures described in the following sections can only be deployed to relevant computers (the number of which is indicated after the Task name). In the ESP environment, a "relevance statement" which defines certain conditions that the computer must meet determines relevance. Any computers running an ESP Agent can receive relevance statements, and when they do, they perform a self-evaluation to determine whether they are included in the criteria. Relevant computers will complete whatever Action has been specified.

When targeting more than a few computers, Trend Micro suggests that you target endpoints by property rather than by list. Targeting by property does not require that any computers appear as relevant; instead, you can use logic such as, "Install on all iMacs, in California, that are part of the User group."

## CPM *for Mac* Console and Client System Requirements

A complete list of system requirements can be found in System Requirements starting on page 3-8.

For information on ESP Server and ESP Console requirements, refer to the *Trend Micro Endpoint Security Platform Administrator's Guide*.

## Incompatible or Conflicting Programs

For a complete list of incompatible or conflicting programs, see Conflicting or Incompatible Programs starting on page 3-8. The following is a short list of software that you should remove from the endpoints before deploying the CPM *for Mac* client.

- Trend Micro Smart Surfing for Mac and Trend Micro Security for Macintosh
- AntiVirus software for Mac, including Symantec AntiVirus, McAfee VirusScan, Sophos Antivirus, and Intego VirusBarrier

# Overview of Deployment Steps

1. Assess endpoint readiness.
2. Remove conflicting products.
3. Deploy CPM *for Mac* clients.

4. Check the deployment status and results.

## Assess Endpoint Readiness

The CPM *for Mac* client supports most operating systems and typically does not require system resources in excess those of required by the host operating system. However, there are some factors that can preclude otherwise eligible endpoints from receiving the CPM *for Mac* client. Perform the procedures that follow to identify which of your endpoints, if any, need to be modified in order for the client to be installed. Do this before removing any existing security products to ensure a continuation of your endpoint security.

### To identify ineligible endpoints:

1. In the CPM Dashboard, click **Troubleshooting > Insufficient Hardware Resources**. The Fixlet **Description** opens.
2. Click the **Applicable Computers** tab.

   A list appears with the endpoints running conflicting software.
3. Below **Actions**, click the hyperlink if you want to connect to the Support Web page for more information. Otherwise, just close any open windows to return to the Dashboard view.
4. Repeat steps 1-3 for any Tasks that pertain to endpoint readiness, for example, **Troubleshooting > Insufficient Software Resources**.

## Remove Conflicting Products

Before deploying the CPM *for Mac* client to your endpoints, you need to uninstall any programs that conflict with the CPM *for Mac* functions. See Conflicting or Incompatible Programs starting on page 3-8 for more information.

### To identify endpoints with conflicting software:

1. In the CPM Dashboard, click **Troubleshooting > Removal of Conflicting Product Required**.

   The Fixlet **Description** opens.
2. Click the **Applicable Computers** tab.

   A list of endpoints running conflicting software appears.

3. Below **Actions**, click the hyperlink if you want to connect to the Support Web page for more information.
4. Close any open windows to return to the Dashboard view.

**To remove the conflicting software:**

1. For information on how to remove conflicting software, go to `http://support.bigfix.com/cgi-bin/kbdirect.pl?id=560`.

## IDeploy CPM *for Mac* Clients to the Endpoints

Use the Core Protection Module *for Mac* Endpoint Deploy Task to deploy CPM *for Mac* to all computers you want to secure against malware. The CPM *for Mac* client package is about 24.2MB, and each endpoint is directed to download the file from the ESP Server or Relay.

If you target your endpoints using properties rather than by computer (which is the recommended behavior) any endpoint that subsequently joins the network automatically receives the CPM *for Mac* client.

Installation takes about five minutes, and the CPM *for Mac* client can be installed with or without the target user's consent. Installation does not typically require a reboot.

---

**Note:** Prior to deploying the CPM *for Mac* client, be sure your targeted endpoints are not running a conflicting product (see Conflicting or Incompatible Programs on page 3-8) and that they meet the hardware and software requirements as explained in Assess Endpoint Readiness on page 3-3.

---

**To deploy CPM *for Mac* to your endpoints:**

1. In the CPM Dashboard, click **Deployment > Install** and pause for a second to note the number of eligible clients in the parenthesis after the task name.
2. Click **Install CPM** *for Mac* **Endpoints.**

   The Task **Description** tab opens.
3. Below **Actions**, click the hyperlink to open the **Take Action** window.

   In the **Target** tab that opens, a list of eligible endpoints appears. The default behavior is to install the CPM *for Mac* client on every relevant endpoint, regardless of who is logged on to the computer and whether the user is present or not.

4. Use the following deployment options if you want to change the target:
   - **Target**—Click **All computers with the property values selected in the tree list below** and then choose a property that includes all the computers to which you want to deploy this Action.
   - **Execution**—Sets the deployment time and retries behavior, if any.
   - **Users**—This option works in combination with Target, linked by the AND operand (both conditions must be present for the install to occur).
   - **Messages**—Configure these options to notify passively the user that the install is going to occur, or to ask users to stop using their computer while the install occurs.
   - **Offer**—Configure these options if you want the user to be able to choose whether the client is installed. A pop-up message is displayed on the target endpoints. (Requires that the client is enabled for offers.)
5. When finished, type your private key password and click **OK** to initiate the action.
6. In the **Action | Summary** window that opens, check the **Status** after a few minutes to confirm that the Action is "Running" and then "Completed."
7. Close any open windows to return to the Dashboard view.

# Pattern File and Engine Updates

It is important to keep your CPM *for Mac* clients current with the latest pattern and engine files from Trend Micro. The update process can be scheduled to occur automatically and is transparent—there is no need to remove the old pattern or install the new one.

## Incremental Updates

To reduce network traffic generated when downloading the latest pattern, the Trend Micro ActiveUpdate server includes incremental pattern updates along with the full pattern file. Updates represent the difference between the previous pattern file and the current one. Like the full pattern file, incremental updates are automatically downloaded and applied. Incremental updates are available to both the ESP Server (which typically downloads pattern updates from the ActiveUpdate server) and to CPM *for Mac* clients that are configured to get their updates from the ESP Server.

## Updates from the "Cloud"

Clients typically receive their updates from the ESP Server or Relays, but CPM *for Mac* also supports client-updates from the "cloud," that is, directly from the Trend Micro ActiveUpdate server. Note, however, that updating clients from the cloud is not recommended as the default behavior. Pattern files can exceed 20MB/client, so frequent, direct client downloads from the AU server are usually not preferred. Instead, you can use the cloud as a fall-back for clients to use whenever they are not able to connect to the ESP Server. Updates from the cloud support incremental pattern updates, however, it does not allow you to update only certain pattern types.

### Procedure Overview

1. Enable CPM *for Mac* clients to receive automatic pattern updates.
2. Schedule and apply automatic pattern file updates.
3. Manually update CPM *for Mac* clients with the latest pattern files.

## Update Pattern Files on the CPM *for Mac* Client

Before performing the client update procedures that follow, be sure that you have updated the pattern files on the CPM *for Mac* Server and that you have enabled that server to perform automatic updates. See Update Pattern Files on the Server on page 2-4 for details.

Trend Micro recommends that you perform the first full pattern-file update on a small number of CPM *for Mac* clients, and then repeat the procedure on an expanded scope as you become more familiar with the procedures.

**To enable CPM *for Mac* clients to receive automatic pattern updates:**

1. In the CPM Dashboard, click **Updates > Automatic Update Tasks > Enable Automatic Updates - Endpoint...**.

   The Fixlet **Description** tab opens.
2. Below **Actions,** click the hyperlink to open the **Take Action** window.
3. On the **Target** tab, choose **All computers with the property values selected in the tree list below.**
4. Choose a property that includes all the computers you want to deploy this Action to and click **OK**.

5. When prompted, type your private key credential and click **OK**.

   The **Action | Summary** tab appears.

6. Check the **Status** and **Count** after a few minutes to confirm that the Action is "Fixed."

7. Close the open windows to return to the Dashboard view.

### To schedule and apply automatic pattern file updates:

1. In the CPM Dashboard, click **Updates > Automatic Update Tasks > Apply Automatic Updates...**.

   The Task **Description** tab opens.

2. Below **Actions,** click the hyperlink to execute the Action.

   The **Take Action** window opens.

3. On the **Target** tab, choose **All computers with the property values selected in the tree list below** and then select **All Computers**.

---

**Note:** It is important to target **All Computers** for this action; only endpoints with the CPM *for Mac* client installed and that have automatic updates enabled will be relevant.

---

4. Click the **Execution** tab to display the scheduling options.

   a. Change **Preset**: Policy.

   b. Enable **Starts on** and choose the current date and time (do not set **Ends on**).

   c. Enable **On failure, retry 99 times.**

   d. Choose to **Wait 1 hour between attempts**.

   e. Enable **Reapply this action... whenever it becomes relevant again**.

5. Click **OK**, and when prompted, type your private key password and click OK.

6. In the **Action | Summary** window that opens, check the **Status** and **Count** after a few minutes to confirm that the Action is "Running" and then "Completed."

7. Close any open windows to return to the Dashboard view.

# Removing CPM *for Mac* Clients

To uninstall CPM *for Mac* from the ESP Server, you first remove all the CPM *for Mac* clients deployed to the endpoints, and then remove the CPM *for Mac* server components from the server, including any mastheads. You can do the former by running the Endpoint Uninstall Task.

**To uninstall CPM *for Mac* clients from one or more endpoints:**

1. From the CPM Dashboard menu, click **Deployment > Uninstall > CPM for Mac Endpoints**. The Task **Description** window opens.
2. Click the hyperlink under **Action** to open the Take Action screen.
3. Select the computers you want to target and click **OK**.
4. When prompted, enter your password. The uninstall sequence begins.
5. In screen that appears, click the **Reported Computers** tab to follow the status of the scan. It usually takes a few minutes for targeted computers to report their **Action** status.

# System Requirements

A quick list of supported operating systems is provided as follows. Click each for details and hardware requirements.

- Mac OS™ X version 10.4.11 (Tiger) or higher
- Mac OS™ X version 10.5.5 (Leopard) or higher
- Mac OS™ X version 10.6 (Snow Leopard)

# Conflicting or Incompatible Programs

Remove the following programs before deploying CPM *for Mac* to the endpoints.

## Spyware, Virus, and Malware Programs

- Norton AntiVirus 11 for Mac
- Norton Internet Security 4 For Mac
- Intego VirusBarrier X4

- Intego VirusBarrier X5
- Intego NetBarrier X4
- Intego NetBarrier X5
- Sophos Anti-Virus for Mac OS X 7.1.1
- avast! Mac Edition 2.7.4
- Kaspersky 7.0 beta
- Kaspersky 8.0.1.358
- MacScan 2.6
- MacScan 2.7
- MacAfee ViruScan for Mac 8.6
- PCTools iAntivirus 1.36
- ClamXav 1.1.1 with ClamAV 0.95.2 backend

## Trend Micro Software

These software programs should be removed from the endpoints before deploying CPM for Mac clients to those computers. Use the program's native uninstaller to remove them.

- Trend Micro Security for Macintosh 1.0
- Trend Micro Security for Macintosh 1.5
- Trend Micro Smart Surfing for Mac 1.0
- Trend Micro Smart Surfing for Mac 1.5
- Trend Micro Smart Surfing for Mac 1.6

## Programs Incompatible with CPM for Mac on the ESP Server

- Trend Micro ServerProtect
- ServerProtect for Windows NT

# Chapter 4

# Configuring and Managing CPM *for Mac*

Before using this chapter, you should already have the ESP Server, ESP Console, and at least one ESP Agent installed. In addition, you should have already installed the Core Protection Module *for Mac* (CPM *for Mac*) server and deployed CPM *for Mac* clients (and updated their pattern files). If you have not, see Chapters 2 and 3 for the procedures.

Topics in this chapter include:

# Using the ESP Console and Menu

- Open the ESP Console by clicking the Windows **Start** button, then **Programs > Trend Micro Endpoint Security Platform > ESP Console**. When prompted, log in as the Master Console Operator.
- Display the CPM Dashboard by clicking **Dashboards > CPM Dashboard** in the Console menu.

## How CPM *for Mac* Task Flows Work

In general, you start by using the CPM Dashboard to make configuration settings. Then you bundle the settings into a **Task**, which delivers an **Action** to targeted computers. **Tasks** also include a **Relevance**, which provides an additional layer of logic that can further define eligible targets. All **ESP Agents** (on which the **CPM for Mac client** runs) receive **Tasks**, but then each agent makes its own determination as to whether its host endpoint meets the conditions of the **Task**, that is, whether the **Action** is **Relevant** or not.

- **Relevance** is determined by checking whether a given set of conditions is true for a particular endpoint. If all the conditions are true, the endpoint is designated as eligible for whatever **Task**, **Fixlet**, or **Action** did the checking.
- **Fixlets** are a way of polling endpoints to see if they are **Relevant** for an **Action**. In other words, Fixlets make **Actions** in a **Task** possible when conditions are right.
- Fixlets can be grouped into **Baselines** to create a sequence of Fixlet Actions.
- **Offers** are a way of obtaining end-users consent before taking an action.

# Configure and Run Malware Scans

CPM *for Mac* provides two types of malware scans, On-Demand and Real-Time. In addition, you can schedule On-Demand scans to reoccur automatically. You can apply the same scan to all endpoints, or create different scan configurations and apply them to different sets of endpoints based on whatever criteria you choose. Users can be notified before a scheduled or an on-demand scan runs, but do not explicitly receive notifications whenever detection occurs on their computer.

**Note:** See Removing CPM for Mac Clients on page 3-8 for information on making some detection information visible to your end users.

Detections are logged and available for review in CPM *for Mac* Reports.

**Note:** On-Demand scans can be CPU intensive on the client. Although you can moderate the affect by configuring the CPU Usage option (sets a pause between each file scanned), you might also want to configure an Offer as part of the Task. The Offer allows users to initiate the scan themselves.

As with most Tasks in the ESP Console, you can associate any of these scans with selected computers, users, or other conditions. As a result, you can define multiple scan settings and then attach a particular scan configuration to a given set of computers. Scan settings are saved in the CPM Dashboard.

The configuration settings you define for these scans apply in conjunction with whatever Global Settings you have configured.

- **On-Demand scans**—Use On-Demand scans to configure the client. Launch the default scan with the **Scan Now** task - a one-time scan. On-Demand scans can take from a few minutes to a few hours to complete, depending on how many files are scanned and client hardware.
- **Scheduled scans**— You can schedule an On-Demand scan to trigger at a given time, day, or date. You can also have the scan automatically reoccur according to the schedule you set.
- **Real-Time scans**— This scan checks files for malicious code and activity as they are opened, saved, copied or otherwise being accessed. These scans are typically imperceptible to the end-user. Real-time scans are especially effective in protecting against Internet-borne threats and harmful files being copied to the client. Trend Micro recommends that you enable real-time scanning for all endpoints.

## Configuring the Default Scan Settings

Whenever you run the default on-demand scan, the settings applied are those that you configured for the default On-Demand Scan Settings.

1. In the CPM Dashboard, click **Configuration > On-Demand Settings > New On-Demand Settings Task**. The On-Demand Scan Settings Wizard appears.
2. Make your configurations choices.
3. Click the **Create Configuration Task...** button.

   The **Edit Task** window opens
4. Because this is the default **Endpoint Deploy** Task, keep the existing name and click **OK** to accept the default **Actions** and **Relevance.**

   The Task is set to be relevant to all CPM *for Mac* clients.
5. Click **OK** when prompted.
6. Go back to the CPM Dashboard to perform the previously created tasks on the selected endpoint.
7. Type your private key password, and click **OK**.
8. After the task has executed on the target computer, the Summary window appears.
9. In the **Action | Summary** window that opens, check the **Status** and **Count** after a few minutes to confirm that the Action is "Running" and then "Completed."
10. Close any open windows to return to the Dashboard view.

## Starting a Scan of Relevant Endpoints (Scan Now)

**To start a scan of relevant endpoints:**

In the CPM Dashboard, click **Tasks > Core Protection Module > Start Scan**.

## Creating an On-Demand Scan

This scan configuration will be saved apart from the default scan now settings. You can run it from the CPM Dashboard anytime to initiate an On-Demand scan that uses the saved settings and applies to the selected computers.

**To create an On-Demand Scan:**

1. In the CPM Dashboard, click **Configuration > On-Demand Settings > New On-Demand Settings Task**.

   The On-Demand Scan Settings Wizard appears.
2. Click the **Create Scan Now Task...** button. The **Edit Task** window opens.

3. Edit the **Name** the **Description** fields so they clearly identify the scan parameters you have selected and the computers you will target in this Task.
4. Select all the relevant computers and click **OK.** When prompted, type your private key password and click **OK**.
5. After the task has executed on the target computer, the Summary window appears.
6. In the **Action | Summary** window that opens, check the **Status** and **Count** after a few minutes to confirm that the Action is "Running" and then "Completed."
7. Close any open windows to return to the Dashboard view.

## Running an On-Demand Scan

**To run an On-Demand Scan:**

1. Click **Configuration > On-Demand Settings > [scan name]** in the CPM Dashboard.
2. Under **Actions**, click the link to initiate the scan.
3. In the **Take Action** window, select the computers you want to target (typically, by Properties) and then click **OK.** When prompted, type your private key password and click **OK**.
4. In the **Action | Summary** window that opens, check the **Status** and **Count** after a few minutes to confirm that the Action is "Running" and then "Completed."
5. Close any open windows to return to the Dashboard view.

## Scheduling an On-Demand Scan (Automatic Scanning)

A scheduled scan runs automatically according to the schedule you set. Although it appears in the CPM Dashboard along with any other On-Demand scans, you do not need to trigger it.

**To schedule an On-Demand Scan:**

1. Schedule an On-Demand scan by clicking **Tasks > Core Protection Module > Start Scan** in the CPM Dashboard.
2. In the window that opens, under **Actions**, click the link to initiate the scan.
3. In the **Take Action** window, click the **Execution** tab.

- Choose a **Start** date, and optionally, configure the days you want the scan to run in the **Run only on** field.
- Select **Reapply this action while relevant, waiting 2 days between reapplications** (choosing whatever period suits you).

> **WARNING!** Do not select the "whenever it becomes relevant again" option because the scan might run continuously.

- If you want to let users initiate the scan, click the **Offer** tab and select **Make this action an offer**.

**a.** Click any of the other Tabs to modify the trigger time and applicable users.

4. Select all the relevant computers and click **OK.** When prompted, type your private key password and click **OK**.
5. In the **Action | Summary** window that opens, check the **Status** and **Count** after a few minutes to confirm that the Action is "Running" and then "Completed."
6. Close any open windows to return to the Dashboard view.

# Configure Client Updates from the Cloud

Receiving pattern updates from the "cloud" is not recommended as the default behavior. However, there are some cases, such as when an endpoint is not connected to the ESP Server or Relay; you might want the endpoint to fail-over to updates from the cloud. The most typical use case is to support roaming clients, for example those being taken off-site for travel.

> **Note:** Perhaps the best method for updating roaming endpoints is to place an ESP Relay in your DMZ. This way, endpoints are able to maintain continuous connectivity with the ESP architecture and can receive their updates through this Relay just as they would if located inside the corporate network.

There are several reasons updating from the cloud is not recommended for daily use by all endpoints:

1. The Update from the cloud Task is not restricted only to roaming clients. You will need to target your endpoints carefully to avoid triggering a bandwidth spike.

2. Full pattern and engine file updates can be 15MB or more.
3. Updates from the cloud will always include all patterns (you cannot update selected patterns as you can from the ESP server).
4. Updates from the cloud are typically slower than updates from the ESP server.

Two additional points are relevant to cloud updates:

1. The endpoint needs an Internet connection. If the endpoint has a proxy configured, those settings are automatically used.
2. The CPM *for Mac* client verifies the authenticity of the pattern from the cloud.

## Configuring Endpoints to Update Pattern File from the Cloud

**To update endpoint pattern files from the cloud:**

1. From the CPM Dashboard menu, click **Updates > Other Update Tasks > Update From Cloud.** The **Task Description** window opens.
2. Below **Actions**, click the hyperlink to open the **Take Action** window.
3. In the **Target** tab, choose **All computers with the property values selected in the tree list below** and then select the property that you want to apply (for example, one that distinguishes between corporate and non-corporate Internet connections).
   - **Execution**—Schedule the time and duration of the cloud updates, as well as the retry behavior. This setting can be very useful for cloud updates.
   - **Users**—Select the computers you want to convert to cloud-updates by User. This option works in combination with Target, linked by the AND operand (both conditions must be present for the install to occur).
4. Click **OK** when finished, and then, when prompted, type your private key password and click **OK**.
5. The **Action | Summary** window that opens, check the **Status** after a few minutes to confirm that the Action is "Running" and then "Completed."
6. Close any open windows to return to the Dashboard view.

# Deploying Selected Pattern Files

By default, all pattern files are included when the pattern is deployed from the ESP Server to CPM *for Mac* clients. You can, however, select and deploy a subset of patterns.

**Note:** This Task is typically only used to address special cases, and as a result is seldom used. When used, this Task tends to be targeted narrowly.

### To deploy a specific pattern file:

1. From the CPM Dashboard menu, click **Updates > Pattern Update Settings > New Pattern Update Settings Task**.

   The Update Settings Wizard screen opens.
2. In the list of components that appears, select the pattern types that you want to allow updates for whenever pattern updates are applied. By default, all pattern files are selected.
3. Click the **Create Update Settings Task. . .** button in the upper right corner. The Edit Task window opens.
4. Modify the default name in the **Name** field so that it clearly defines the purpose of this custom Task.
5. Edit the **Description** and the **Relevance** tabs if necessary, to reflect your goals.
6. Click **OK** and then enter your private key password when prompted.

   The Task **Description** window opens, and the Task is added below **Pattern Update Settings** in the CPM Dashboard.
7. Below **Actions**, click the hyperlink to open the Take Action window.
8. In the **Target** tab, click **All computers with the property values selected in the tree list below** and then choose a property that includes all the computers to which you want to deploy this Action.
   - **Execution**—Sets the deployment time and retries the behavior (if any).
   - **Users**—This option works in combination with Target, linked by the AND operand (both conditions must be present for the install to occur).
   - **Messages**—Configure these options to notify passively the user that the install is going to occur, to obtain consent, or to ask users to stop using their computer while the install occurs.

9. When finished identifying the computers you want to receive the selected patterns, click **OK** and when prompted, type your private key password and click **OK**.
10. The **Action | Summary** window that opens, check the **Status** after a few minutes to confirm that the Action is "Running" and then "Completed."
11. Close any open windows to return to the Dashboard view.

# Chapter 5

# Configuration Wizards Reference

The Core Protection Module (CPM) Dashboard includes Wizards to help you understand and organize scan-related configuration choices. It also provides a Health Monitor for quick reference.

Use the On-Demand Scan Settings Wizard, for example, to define which files to scan, how to manage the Core Protection Module *for Mac* (CPM *for Mac*) scan engine usage, and designate the action to take whenever a threat is discovered. Individual scan configurations can also be saved as a Task, which are then available in the main Task List.

Use the CPM *for Mac* Health Monitor, for example, to get a quick overview of endpoint statuses or as a Troubleshooting aid.

Topics in this chapter include:

# The CPM *for Mac* Health Monitor

The CPM *for Mac* Console provides rich reporting features, including graphical representations and drill-down granularity. The Health Monitor provides a quick summary showing you the overall condition of CPM *for Mac* clients on the network.

Available health status:

- **Healthy**—Computers are considered healthy if they are relevant to at least one Fixlet, Task, or Analysis in the CPM *for Mac* site and are using the current pattern files.
- **Restart needed**—Identifies endpoints that must be rebooted before a pending Action can be completed. Use the Troubleshooting Task in the Dashboard to reboot the endpoints identified here.
- **Not Installed**—The endpoint is eligible for a CPM *for Mac* client but the client has not been deployed. As such, there is no CPM *for Mac* information available for that endpoint.
- **Conflicting product**—The CPM *for Mac* client is not installed because ESP has detected one or more incompatible programs. Run the existing Uninstall Task(s) on the endpoints, or if a Task is not available for that particular program, uninstall it manually.
- **Ineligible (hardware)**—CPM *for Mac* client is not installed. See System Requirements starting on page 3-8.
- **Ineligible (software)**—CPM *for Mac* client is not installed. See System Requirements starting on page 3-8.
- **Improper service status**—One or more client services for the ESP Agent or CPM *for Mac* client on the endpoint are not reporting. The service(s) likely need to be restarted. Services include the BES Client and BES FillDB.
- **Unknown**—The ESP Agent is installed on the endpoint but there is no information about the CPM *for Mac* client. The CPM *for Mac* client could not be installed or the endpoint could be offline.
- **N/A**—The computer(s) are not relevant to any Fixlet, Task, or Analyses in the CPM *for Mac* Site.

# On-Demand & Real-Time Scan Settings Wizards

- **Enable virus/malware scan** (recommended)—The different types of malware threats are described in Security Risks starting on page 9-4.

## Scan Target Tab

### User Activity on Files (Real-Time Scans Only)

- **Scan files being...**
  - **Created**-scans new files and files as they are copied to the client.
  - **Modified**-scans files that are opened as they are saved to the client.
  - **Received**-scans files as they are moved or downloaded to the client.

### Files to Scan

This feature only applies to On-demand scans and not Real-time scans, and considers the full path filename as the target file rather than just the file extension.

- All scannable files—This option is the safest, but will also have the greatest effect on client performance; all files are scanned (On-Demand) or monitored (Real-Time), even file types that cannot be infected.
- Target Files—Use file extensions for Windows files and full paths for Mac files. CPM *for Mac* does not support a file extension scan. You have to specify the whole filename for a target scan.

### CPU Usage (On-Demand Scans Only)

On-Demand scans can be CPU intensive and clients might notice a performance decrease when the scan is running. You can moderate this affect by introducing a pause after each file is scanned, which allows the CPU to handle other tasks. Consider factors such as the type of applications to be run on the computer, the CPU speed, the RAM speed, and what time the scan is to be run.

- **High—**No pausing between scans
- **Low—**Pause longer between scans

## Scan Action Tab

### Malware Action

CPM *for Mac* performs a scan action on the malware. The default action for malware is to clean it. If that fails, the backup action is to quarantine them.

---

**Note:** **Quarantining files**—You can have CPM *for Mac* quarantine any harmful files that it detects. These files are encrypted and moved to a directory on the endpoint that prevents users from opening them and spreading the malware to other computers in the network.

---

- **Use ActiveAction**—ActiveAction is a set of pre-configured scan actions for specific types of malware. Trend Micro recommends using ActiveAction if you are not sure which scan action is suitable for each type of malware.
- **Use the same action for all virus/malware types**—If CPM *for Mac* detects malware but the code cannot be removed, (that is, the file cannot be "cleaned"), the file is quarantined. See Available Malware Scan Actions starting on page B-2 for more information.

CPM *for Mac* performs the specified action for all types of malware. Because malware does not "infect" files, there are only four possible actions:

- **Clean**—Recommended. CPM *for Mac* terminates processes or deletes registries, files, and shortcuts.
- **Pass**—On-Demand scans only. CPM *for Mac* takes no action on the detected malware, but records the detection in the logs.
- **Delete**—If a file is found to contain a lot of threats and is uncleanable, it can be summarily deleted.
- **Quarantine**— If CPM *for Mac* detects a virus but the code cannot be removed, (that is, the file cannot be "cleaned"), the file will be quarantined. See Available Malware Scan Actions starting on page B-2 for more information.

# Web Reputation Blacklist-Whitelist

For information on using Web Reputation Blacklist-Whitelist, see Blacklist and Whitelist Templates on page 6-4.

# ActiveUpdate Server Settings Wizard

Use this Wizard to select the location from where you want to download component updates. You can choose to download from the Trend Micro ActiveUpdate (AU) server, a specific update source, or a location on your company intranet.

## Source

- **Trend Micro's ActiveUpdate Server**—This location contains the latest available patterns and is typically the best source.
- **Other Update Source**—(seldom used) The default location is:

  `http://esp-p.activeupdate.trendmicro.com/activeupdate`

- **Intranet location containing a copy of the current file**—If you want to use an Intranet source for obtaining the latest pattern file update, specify that location here. This is typically used on a temporary basis for one-time updates unless the Intranet source is configured to poll and receive updates from the Trend Micro ActiveUpdate server on a regular basis.

## Proxy

- **Use a proxy server for pattern and engine updates**—If there is a proxy server between the ESP Server and the pattern update source you selected previously, enable this option and provide the location and proxy access credentials.

## Others

- **Log Rolling Frequency (1-90)**—To keep the cumulative size of log files from occupying too much space on the server, you can specify how many days to retain logs. The newest logs will replace the oldest logs after this number of days. The default is 10 days. Logs are stored in the following directory:

  `\TrendMirrorScript\log`

- **Number of Updates to Keep on Server (1-100)**— You can store previous pattern file sets on the server in case you ever need to revert, or roll back to an older file. By default, CPM *for Mac* keeps the current pattern and 15 "snapshots" of the pattern set.

# Chapter 6

# Using Web Reputation

This chapter helps you optimize the features of Web Reputation (WR) for your environment by detailing how to manage Blacklist and Whitelist templates, Analyses, and the Core Protection Module (CPM) Dashboard.

Topics in this chapter include:

# How Web Reputation Works

The Trend Micro Web Reputation (WR) technology joins its real-time visibility and control capabilities with Core Protection Module *for Mac* (CPM *for Mac*) to prevent Web-based malware from infecting your users' computers. WR intercepts malware "in-the-cloud" before it reaches your users' systems, reducing the need for resource-intensive threat scanning and clean-up. Specifically, WR monitors outbound Web requests, stops Web-based malware before it is delivered, and blocks users' access to potentially malicious Web sites in real time.

Web Reputation is requires no pattern updates. It checks for Web threats when a user accesses the Internet by performing a lookup on an "in-the-cloud" database. Web Reputation uses the site's "reputation" score and a security level set by the Console Operator to block access to suspicious sites. The Web Reputation database lookups are optimized to use very little bandwidth (similar in size to a DNS lookup) and have a negligible impact on network performance.

**Note:** Users who are logged on to their computer with Administrator rights can disable Web Reputation.

## Web Reputation Security Levels

After enabling WR on your endpoints, you can raise the security level to Medium or High (the default is Low) to increase the degree of sensitivity that WR uses when evaluating URLs.

### How Web Reputation Works

Whenever an end user tries to open an Internet site, the requested URL is scored at the proxy, in real-time, and that score is then evaluated against the security level. URLs with a score that exceeds the level you select will be prevented from opening. Note that this scoring is relative to security, not whether a site might contain objectionable content.

**Note:** As you set the security level higher, the Web threat detection rate improves but the likelihood of false positives also increases.

You can override incorrect blocking by adding the URL to the whitelist. Likewise, you can force blocking of a site by adding it to the blacklist.

URLs are scored on a security scale that runs from 0 to 100.

- **Safe**—Scores range from 81 to 100. Static and normal ratings. URLs are confirmed as secure; however, the content could be anything (including objectionable content.)
- **Unknown**—Score equals 71. Unknown ratings. These URLs are not included in the rating database.
- **Suspicious**—Scores range from 51 to 80. URLs that have been implicated in Phishing or Pharming attacks.
- **Dangerous**—Scores range from 0 to 49. Static and malicious ratings. URLs are confirmed as malicious, for example a known vector for malware.

Security Levels range from high to low and have the following default actions:

- **High**—blocks unknown, suspicious, and dangerous sites
- **Medium**—blocks dangerous and suspicious sites.
- **Low**—blocks only dangerous sites.

For example, if you set the Security Level to Low, Web Reputation only blocks URLs that are known to contain malicious software or security threats.

### To configure a default security level:

1. In the CPM Dashboard, click **Tasks > Web Reputation > Configure Web Reputation Security Level**.

   The Task **Description** opens.
2. Below **Actions**, choose a Security Level by clicking the hyperlink.

   The **Take Action** window opens.
3. In the **Target** tab, select all **Applicable Computers** to apply the WR security level to all your endpoints.
4. Click **OK.** When prompted, type your private key password and click **OK**.
5. In the **Action | Summary** window that opens, check the **Status** after a few minutes to confirm that the Action is "Running" and then "Completed."
6. Close any open windows to return to the Dashboard view.

# Using Web Reputation in CPM *for Mac*

The following rules apply when creating whitelists and/or blacklists:

- The prefix, "http://" will automatically be affixed to URLs added to the list.
- Secure URLs, that is, those starting with **https:** are not supported.
- Include all subdirectories by using the * wildcard:

  ```
  "http://www.example.com/*"
  ```

- Include all subdomains by using the * wildcard

  ```
  "http://*.example.com"
  ```

  ```
  Not valid: https://www.example.??
  ```

- To import a URL that uses a non-standard port, use the following format:

  ```
  "http://www.example.com:8080"
  ```

- URLs can be up to 1024 characters long.
- List each URL on a new line.
- You can add or import up to 500 URLs in a given list.

## Blacklist and Whitelist Templates

The Web Reputation Blacklist-Whitelist Wizard enables you to create and maintain global lists of Web sites in the form of templates that you can use to control your users' Web access. After you have defined these templates, you use them to create Custom Tasks, which you can then apply to your endpoints.

There are two types of URL lists that you can create and group into templates using this Wizard:

- **Blacklists**—These are lists of blocked Web sites. If the endpoint tries to access a site in one of these lists, they receive a message in their Web browser indicating that access to the site is blocked.
- **Whitelists**—These are lists of Web sites you allow your endpoints to access without restriction.

---

**Note:** Use care when selecting sites for Whitelists. After a site is added to a Whitelist, it will no longer be checked. Therefore, endpoints connecting to that site would no longer

be protected by WR, should that site become a host for malware at some point in the future.

By creating multiple tasks, you can apply different sets of Blacklist and Whitelist templates to different users or groups of users. You can perform the following tasks:

- Create and deploy a New Blacklist / Whitelist Template
- Create and deploy a New Blacklist / Whitelist Template by importing an existing list
- View an existing Blacklist / Whitelist Template
- Copy a Blacklist / Whitelist Template
- Copy and edit a Blacklist / Whitelist Template
- Delete a Blacklist / Whitelist Template

## Creating and Deploying a New Template

### To create a new Blacklist / Whitelist Template:

1. In the CPM Dashboard, click **Configuration > Web Reputation Blacklist-Whitelist > New Web Reputation Blacklist-Whitelist Task...**

   The Web Reputation Blacklist-Whitelist Wizard window opens, showing a list of your currently available templates.

2. Click **Add Template**.

   The Blacklist-Whitelist Template–Add Template page opens.

3. Enter a name for your template in the Template Name field.

4. In the Blacklist pane, enter or copy/paste the URLs you want to block.

   You can enter up to 500 URLs. To block all the pages for a site, enter the name of the domain followed by /* :

   Example:

   ```
   "http://www.badURL.com/*"
   ```

**Note:** You can include up to 500 URLs in a single template, and can create multiple templates for use. However, only one template can be active on an endpoint at the same time.

5. To enter a Whitelist, in the Whitelist pane, enter or copy/paste the URLs you want your users to be able to access without restriction. You can enter up to 499 URLs per template. To grant access to all the pages on a site, enter the name of the domain followed by /* :

   Example:

   ```
   "http://www.goodURL.com/*"
   ```

6. When you are finished creating your template, click **Save**.

   The Blacklist-Whitelist Templates window returns.

7. Click the **Create Task From Template...** button.

   The Edit Task window opens.

8. Click **OK**, type your Private Key Password, and click **OK**. A **Task** window appears.

9. Click the *here* link in the **Actions** window.

   The **Take Action** window opens.

10. Select the computer or computers in the window to which you want to deploy your Blacklist / Whitelist template and set any desired options.

    **Note:** For more information about setting options using tabs in the **Take Action** window, see the *BigFix Console Operator's Guide*.

11. When you have finished selecting options, click **OK**.

12. Enter your Private Key Password and click **OK**.

    An Action window appears in which you can track the progress as BES deploys your Blacklist / Whitelist template to your endpoints. After deployment, the status shows "Completed."

# Importing Lists of Web Sites

Web Reputation allows you to import URLs for new Blacklist and Whitelist templates from new line-delimited files.

**To create a new Template by importing lists of blacklisted and whitelisted Web sites:**

1. Create two text files - one for the Web sites you want this template to block and another for the Web sites to which you want to give your users unrestricted access.

   **Note:** If you do not want to include a Whitelist in the template, you can skip this part of the process. Web Reputation allows you to create Blacklist / Whitelist Templates with both list types (a blacklist and a whitelist), only a blacklist, or only a whitelist.

2. Press **Enter** or place a "newline" code at the end of each line to separate each entry. You must have "http://" before each URL entry. To block all the pages for a site, enter the domain name followed by "/*", for example:

   ```
   "http://www.badURL.com/*."
   ```

3. Click **Configuration > Web Reputation Blacklist-Whitelist > Web Reputation Blacklist-Whitelist Task...** to open the Web Reputation Blacklist-Whitelist Wizard.
4. Click the **Add Template** button or **Edit**.

   The Blacklist-Whitelist Templates – Add Template window opens.
5. Click **Bulk Import Sites from external file...**.

   The Import Sites from External File window appears.
6. Select the text file you wish to import by clicking **Browse** next to the Select Import File field.

   The Open window appears.
7. Use the Open window to navigate to the location where you have stored the text file.
8. Select the file and click **Open**.

   The path to the selected file appears in the Select Import File field.
9. Choose **Blacklist** or **Whitelist** from the List Type.
10. Click the **Add Sites from File** button. The list displays and returns you to the page that allows you to add a new page.

**Note:** To see the process required to finish generating your Custom Action and deploying the template, start at Step 7 in the Creating and Deploying a New Template section.

## Viewing an Existing Template

**To view an existing Blacklist / Whitelist template:**

1. Click **Configuration > Web Reputation Blacklist-Whitelist > New Web Reputation Blacklist-Whitelist Task...** to open the Web Reputation Blacklist-Whitelist Wizard.
2. Click the name of the Blacklist / Whitelist template you want to examine.

   The Blacklist-Whitelist Templates – Add Template window appears.

## Copying and Editing a Template

Web Reputation enables you to create copies of existing Blacklist / Whitelist templates. Use this feature to create copies of existing templates or to create slightly modified versions of existing templates.

**To create a copy of an existing Blacklist / Whitelist template:**

1. Click **Configuration > Web Reputation Blacklist-Whitelist > Web Reputation Blacklist-Whitelist Task...** to open the Web Reputation Blacklist-Whitelist Wizard.
2. Select the name of the Blacklist / Whitelist template you want to duplicate and click **Copy**.

   The name of the template appears in the form of "Copy of…" followed by the template name you chose to copy. Web Reputation automatically copies the contents of the Blacklist and Whitelist fields into the new template.
3. Change the name in the **Template Name** field to a descriptive template name.
4. Make other necessary changes to the template.

   For example, in copied templates, you can:

   - Add new URLs to the copied blacklist or whitelist.
   - Remove URLs from the blacklist or whitelist.

- Import and append either an external blacklist or an external whitelist to your blacklist and whitelist entries.

5. When you have modified the template, click **Finish** to end the process and to start generating the relevant **Custom Action**.

## Editing Custom Actions

The Blacklist / Whitelist Wizard allows you to edit existing blacklist or whitelist templates.

You can edit these Custom Actions in two different ways:

- By making modifications using the **Edit Task** window immediately after you click **Finish** to create the Custom Task
- By accessing the **Edit Task** window AFTER you have completely generated the **Custom Task**.

  To make modifications using the Edit Task window, either access it as part of Custom Task generation process or select it by right-clicking on the name of an existing Custom Task and selecting Edit.

The Edit Task window consists of four tabs:

- **Description**—Use the Description tab to make modifications to the task name, title, and description.
- **Actions**—Use the Actions tab to view or change the Action this Custom Task performs. For example, use this window to add or remove blacklisted or whitelisted URLs from the presented Action Script.
- **Relevance**— Use the Relevance tab to view and make modifications to the relevance for a Custom Task. By default, the relevance for the blacklist or whitelist is static. Its purpose is to detect endpoints for Web Reputation.
- **Properties**—Use the Properties tab to view and modify the properties for this custom task.

When you have finished making modifications, click **OK**. When the Private Key Password window appears, enter your password and click **OK** again. The edited/changed Blacklist / Whitelist template appears.

### To delete a template:

Complete the following steps to delete an existing blacklist or whitelist template from the Wizard's Template list:

1. Click **Configuration > Web Reputation Blacklist-Whitelist > Web Reputation Blacklist-Whitelist Task...** to open the Web Reputation Blacklist-Whitelist Wizard.
2. Select the name of the blacklist or whitelist template you want to delete and click **Delete**.

   The Delete window appears.
3. Click **Yes**. Web Reputation removes the template from the Blacklist-Whitelist Wizard Template Management window.

---

**Note:** The Blacklist-Whitelist Wizard Delete feature only deletes the template from the Management list. It does not delete the Custom Task you created with the template. To remove completely the Blacklist-Whitelist template from your endpoints, complete the steps that follow.

---

### To delete a custom task:

1. Select the name of the template you wish to delete in the My Custom Tasks list and right-click.

   The right-click menu appears.
2. Select **Remove** from the right-click menu.

   The Remove Task confirmation window appears.
3. Click **OK**.

   The Private Key Password window appears.
4. Enter your Private Key Password and click **OK**.

   A series of messages displays when the Custom Task is removed from the affected CPM *for Mac* clients and the List Panel.

# About Analyses

Web Reputation allows you to view detailed information about an endpoint or group of endpoints protected by Web Reputation. Use the Client Information analysis to view information about each endpoint protected by a CPM *for Mac* client.

- In the CPM Dashboard, click **Reports > Web Reputation.**

The following Properties are available for each endpoint:

- **WR Installation Date**—The date Web Reputation was installed.
- **Number of Web Threats Found**—The number of Web threats encountered and recorded in the endpoint's storage file
- **Web Reputation Enabled/Disabled**—The status of the agent's Web Reputation feature (Enabled/Disabled)
- **Web Reputation Security Level**—The security level for the Web Reputation feature (High, Medium, or Low)
- **Proxy Server Enabled/Disabled**—If a proxy server is enabled/disabled
- **Proxy Server Address**—The address of the proxy server
- **Proxy Server Port**—The port being used by the proxy server
- **Proxy Server User Name**—The user name used by the client to connect to the proxy server
- **Blacklist-Whitelist Template**—The name of all blacklist and whitelist templates deployed to the Agent
- **Number of Days since Last Log Maintenance**—The number of days that have elapsed since you last performed Log Maintenance
- **Log Age Deletion Threshold**—The number of days that logs are kept on the endpoint before they are deleted (the log age deletion threshold)

The Site Statistics analysis displays statistical information about the number of Web sites accessed by an endpoint. You can use this analysis to view the following:

1. **Blocked Sites**—Shows the time a block occurred and the URL that was blocked.
2. **Visited Sites**—Shows each domain visited and the number of visits

---

**Note:** Enable or disable the collection of visited sites in the task pane by selecting either "Web Reputation - Enable Collection of Visited Sites" or

"Web Reputation - Disable Collection of Visited Sites" and applying it to the appropriate endpoint(s).

**To view the Client Information Analysis:**

1. Click the **Analyses** tab.

   The List Panel changes to show all available analyses.
2. Click **All Applicable Analyses**.
3. Click the "+" sign and then click **By Site.**
4. Click the **Trend Micro Core Protection Module** site. Two analyses are available:
   - Web Reputation—Client Information
   - Web Reputation—Site Statistics
5. Click the **Web Reputation—Client Information** analyses link.

   The Web Reputation—Client Information window appears.
6. To view the view details about each property, click the Results tab.
7. You can view the analysis property results in either List or Summary format. To select a perspective, choose the desired format from the drop-down box in the upper-right corner of the analysis in the Results tab.
8. To deactivate the analysis, return to the "click here: link in the Action window.

## To view the Site Statistics Analysis:

1. Click the **Analyses** tab. The **List Panel** shows all available analyses.
2. Click **All Applicable Analyses**.
3. Click the "**+**" sign and then click By Site.
4. Click **Web Reputation** to see a list of both available analyses.

5. Click the **Web Reputation – Site Statistics** analyses link.

   The Web Reputation – Site Statistics window appears. The window displays information on the Web Reputation property you can view with the analysis:

   - Blocked Web sites

6. You can view the analysis property results in a list or in summary form. To select a perspective, choose the desired format from the drop-down box in the upper-right corner of the analysis in the Results tab.
7. To deactivate the analysis, return to the "click here" link in the Action window.

# Chapter 7

# Setting Up and Using Locations

This chapter contains information about creating locations, managing tasks related to the locations, and how to use the locations.

Topics in this chapter include:

# Overview

You can have ESP apply different Core Protection Module *for Mac* (CPM *for Mac*) security configuration on the basis of the client's current geographical location. For example, say an organization has offices in California, New York, and Germany, and that travel between offices is common. In California and New York, the corporate security policy requires that suspicious files be quarantined. In Germany such files must be deleted. In locations other than California or Germany, incidents should be logged but no action taken. You can accommodate all these regulations by creating Location Properties. In short, a client can disconnect from the corporate network in the California one day and reconnect in Germany the next, and his or her computer automatically picks up the correct security policy for the new location.

This same idea also applies to firewall configurations, and other CPM *for Mac* security features. So, for example, in addition to location-specific configurations, you can create NIC-specific security policies. If you want to have one set of malware and firewall settings to that govern wireless connections and another set for wired connections. Your LAN and W-LAN settings can be the same for all geographic locations, or they too can vary to reflect a local security policy.

For example, wireless connections in New York could have one set of rules and wired connections mighty have a different set of rules. In Germany, there might be completely different rules for both wired and wireless connections - two locations, but four sets of rules that might apply.

# Creating Locations

Use the ESP Location Property wizard to create one or more named properties that allow the ESP Agents to identify themselves according to their current network location or status. As soon as the property is created, it will be propagated to all clients and applicable computers will pick up the setting (that is, their configuration status might change according to the choices you have in place.)

Before you begin, you should know or have a list of the subnets used in your organization and their respective geographic locations. Alternatively, you can create a custom relevance expression to map dynamically retrieved client properties using a key/value set. See the *ESP Administrator's Guide* for more information.

**Note:** The purpose of the procedure that follows is to create a property that defines the geographic location of an endpoint according to its subnet. Using the same principles, you could also create a property based on connection type, relay, operating system, or any other characteristics and use it in conjunction with the CPM *for Mac* firewall, CPM *for Mac* malware protection, and CPM *for Mac* Web Reputation.

### To create a location property:

1. Log on to the ESP Console as Master Console Operator, open the CPM *for Mac* console, and then click **Wizards > Location Property Wizard**. The Location Property Wizard screen opens.
2. Choose one of the following and then click **Next**.
   - **Create a retrieved property that maps subnet to location—**For each location you want to identify, type the subnet IP address. If a single location includes more than one subnet, type each subnet IP address (followed by the same location name) on a new line. Clients will self-determine their relevance to a given location by comparing their current IP address with the value(s) specified here. Note that clients with multiple NICs might self-identify using their W-LAN or LAN IP address, so you might need to include both subnets.
   - **Create a retrieved property that maps subnet to location using only the first two octets**—Use this option to support a larger block of IP addresses. As shown previously, clients will self-identify their relevance to this IP address block. Clients not included in the block will either inherit the default configuration that is not location-specific, or not be covered by any location property.
   - **Create a retrieved property that maps IP address range to location**—only one range per line is supported (do not delimit multiple ranges).
   - **Create a retrieved property that uses a custom relevance expression and maps the result using a key/value set**—See the *ESP Administrator's Guide* for more information.
3. Give the property a name that clearly identifies its purpose and click **Next**.
4. For each location, type the subnet address(es); click the **Insert Tab** button, and then type a name. Use only one IP/location pair per line. Create multiple lines for the same location if it uses multiple subnets.

Be careful not to "overlap" any IP addresses when specifying ranges. Computers included in multiple locations will constantly be updated as they re-evaluate and recognize their relevance to one location and then another.

5. Click **Next**, and if no valid IP/location pairs are displayed, click **Next** again.
6. Accept the defaults that are selected in the Extra Options window and click **Finish**. The **Import Content** window opens.
7. In the **Import Content** window, enable **Open documents after creation**. Do not miss this step, or it prevents the location property from being deployed to your endpoints and your locations will not be relevant for any of your **Actions**.
8. Click **OK** and then type your private key password and click **OK** to deploy the Action.
9. In the **Action | Summary** window that opens, check the **Status** and **Count** after a few minutes to confirm that the Action is "Running" and then "Completed."
10. Close any open windows to return to the Dashboard view.

Now that locations have been defined, the next step is to create a couple of different configuration settings and bundle them into a Task. You can then associate these Tasks with the Locations you just created.

# Creating Location-Specific Tasks

In the procedures that follow, the goal is to create two different configurations and tasks, and then attach them to different locations. The result is that users in Location 1 will automatically pick up Configuration 1, and users in Location 2 will pick up Configuration 2. If a user from Location 2 travels to Location 1, he or she will automatically pick up Configuration 1 when connecting to the network.

## How Location Properties Work

Each ESP Agent, on which the CPM *for Mac* client resides, receives a complete list of all the Actions deployed from the ESP Server through the various Tasks. The individual Agents check themselves against the list and create a short-list of only those Actions that apply to them. In the current example, relevance is determined by IP address. Configuration 1 is going to be deployed to all Agents, but only those Agents running on an endpoint with an IP address in the subnet defined for San Francisco will pick up the configuration. You will be able to see this self-selection at work when you create the

second configuration and apply it to a different Location. One Action will be picked up by San Francisco endpoints and the other by German endpoints.

ESP Agents remain in sync with new relevance expressions by frequently checking the ESP server for updates. Agents also maintain a detailed description of themselves that might include hundreds of values describing their hardware, the network, and software.

In short:

- First, define some locations.
- Second, configure your scan or URL filtering settings.
- Next, save the settings to a Task and create an Action to target some given endpoints.

When you deploy the Task, the ESP Server converts the Action details into a relevance expression, which is sent to all Agents at the endpoints. Each Agent checks itself against the relevance expression and takes the Action required for every match found.

### A. To create the first configuration and Task:

1. From the CPM Dashboard, click **Configuration > Global Settings > New Global Settings Task**. The Global Scan Settings Wizard screen opens.
2. Enable **Configure scan settings for large compressed files** and enter the limits shown here:
   - Do not scan files in the compressed file if the size exceeds 2 MB
   - Stop scanning after CPM *for Mac* detects 2 malware in the compressed file
3. Click the **Create Global Scan Settings Configure Task** button. The **Edit Task** window opens
4. Type a descriptive (or memorable) name for the Task such as, **Skip 2MB-2**.
5. Click **OK** to close the windows, and when prompted type your private key password and click **OK** to create the new global policy.
6. The new policy now appears in the **Configuration > Global Settings** dashboard.

### B. To create the second configuration and Task:

1. From the CPM Dashboard, click **Configuration > Global Settings > New Global Settings Task**. The Global Scan Settings Wizard screen opens.
2. Remove the check from **Configure scan settings for large compressed files**.

3. Click the **Create Global Scan Settings Configure Task** button. The **Edit Task** window opens.
4. Type a descriptive (or memorable) name for the Task such as, **Scan BIG**.
5. Click **OK** to close the windows, and when prompted type your private key password and click **OK** to create the new global policy.
6. The new policy now appears in the **Configuration > Global Settings** Dashboard.

### C. To make the configurations location-specific:

1. In the **Configuration > Global Settings** Dashboard, click the **Skip 2MB-2** task you just created. The **Description** window opens.
2. Under the **Actions** heading, click the hyperlink to configure the policy settings. The **Take Action** window opens to the **Target** tab.
3. Select **All computers with the property values selected in the tree below.**
4. Next, click the **All Computers** tree and then **By Retrieved Properties > By Subnet Address** to open that branch.
5. Choose the Location name you created for the San Francisco subnet (Step 3 on page 7-3).
6. With your location still selected, click the **Execution** tab.
7. Remove any **Constraints** that you do not want to apply (such as a Start and End date), and in the **Behavior** section, make sure only the following option is enabled:

   **Reapply this action... whenever it becomes relevant again**.
8. Click **OK** and then enter your password when prompted.
9. Repeat this procedure for the second configuration and Task (choose **Scan BIG** from the **Global Settings** Dashboard), and use the Location name you used for the Germany subnet.

# Chapter 8

# Troubleshooting

This chapter includes information to help with basic troubleshooting and problem solving.

Topics in this chapter include:

# Installation

The Core Protection Module *for Mac* (CPM *for Mac*) installer writes install logs to the following file:

```
/var/log/TrendMicro/TMMPMInstallResult.log
```

The log typically includes the install start and finish time, status, and any error codes encountered. If the status upon completion is not 5 or 6, an error occurred.

## Install Status

```
0 = Preparing Installation
1 = Installing CPM for Mac Component
2 = Upgrading CPM for Mac Component
3 = Installing OSCE Component
4 = Upgrading OSCE Component
5 = Done
6 = Done But Need Reboot
7 = Installing BF-AU-Server Component
8 = Upgrading BF-AU-Server Component
```

## Error Codes

```
0 = Succeed
-1 = Wrong Platform
-2 = Extracting Package Failed
-3 = Not Enough Disk Space
-4 = No Administrator Privilege
-5 = A Newer Version of Core Protection Module for Mac Exists
-6 = Need Reboot Before Install
-7 = Cannot Start Core Protection Module for Mac Service(s)
-8 = Cannot Stop Core Protection Module for Mac Service(s)
-9 = Wait Installation Time Out
-10 = Another Installer Is Running
-11 = Invalid Command Line Argument
-12 = Copy File Failed
-13 = Unknown Error
-14 = Do not allow installation with other Trend Micro Antivirus
      software installed
```

```
-15 = Do not allow installation with other antivirus software
      installed
-16 = Do not allow CPM for Mac to be uninstalled
```

## Installing the CPM *for Mac* Server on a Non-default Drive

By default, the CPM *for Mac* component files are installed to the local hard drive. However, you can download and import a custom task to enable installation to a different location.

**To download the Task:**

`http://esupport.trendmicro.com/Pages/Installing-CPM-module-to-a-user-defined-drive.aspx`

OR

`http://esupport.trendmicro.com/sadmin/Lists/Solution%20Contribution%20Attachments/Attachments/70/Core%20Protection%20Module%20-%20Endpoint%20Deploy%20-%20Custom%20Install%20Path.bes`

**To import the Task:**

1. In the ESP Console, click **File > Import**.
2. Look for the *.bes file and then click **Open**.
3. Click **OK**.

# Malware Scanning

**To enable debug logging:**

1. Open Terminal.
2. Change your location to the `/var/log/TrendMicro/`directory.
3. Use the root permission to create the "`TmccCore`" folder.
4. The log file is generated in the new folder.

**To disable the debug logging:**

1. Open the Terminal.
2. Remove the directory `/var/log/TrendMicro/TmccCore` with root permission.

## Malware Logs on the CPM *for Mac* Client

The spyware log directory is located here:

```
/var/log/TrendMicro/MPM/
```

The following log is significant in that contains both virus and spyware information:

- malware.log

## Debug Logs

1. BigFix Client Logs:

   ```
   %ProgramFiles%\ BigFix Enterprise\BES
   Client\__BESData\__Global\Logs
   ```

2. TrendMirrorScript logs:

   ```
   C:\Program Files\BigFix Enterprise\TrendMirrorScript\logs
   ```

3. CPM Agent Logs:

   ```
   /Library/Application Support/BigFix/_BESData/_Global/Logs/
   ```

4. CPM AU Server Logs:

   ```
   %ProgramFiles%\Trend Micro\Core Protection Module for Mac
   Server\bin\AU_Data\AU_Log\TmuDump.txt
   ```

### Components Installation Debug Logs (CPM *for Mac* Server)

Get and use the following logs to help understand CPM *for Mac* server installation issues.

Directory = %WINDOWS%

- `CPMInstallResult.log`
- `CPMSrvInstall.log`
- `ClnExtor.log`
- `CPMsrvISSetup.log`

### Components Installation Debug Logs (CPM *for Mac* Client)

Get and use the following logs to help understand CPM *for Mac* client installation issues.

Install logs:

- `/var/log/TrendMicro/TMMPMInstallResult.log`
- `/tmp/TrendMicroMPMInstaller.log`

Log file names followed by an asterisk ( * ) also serve as CPM *for Mac* Client upgrade debug logs. CDT can collect all log files.

## CPM *for Mac* Clients

**To enable debugging on the CPM *for Mac* clients:**

**To collect information by CDT:**

1. While logged in as a "root" permission user, open the terminal.
2. Change the file location to:
   `/Library/Application Support/TrendMicro/MPM/`
3. Run the `CaseDiagnosticTool on` script.
4. Use the root permission level to run:
   `CaseDiagnosticTool collect`
5. Run the `CaseDiagnosticTool off` script.
6. The file will output onto your desktop with a filename of:
   `TMMPMLogCollect.tar.bz2`
7. Send the compressed .tar file to Trend Micro Technical Support.

# Pattern Updates

There are a number of moving parts and components involved with the routine task of updating the pattern files:

- CPM *for Mac* server components include:
  - Proxy Settings
  - TMMPMAuHelper
  - TrendMirrorScript
- CPM *for Mac* console components include:
  - Pattern Update Wizard
  - Pattern-set Loading via Manifest.json
- CPM *for Mac* client components include:
  - BESClient (for dynamic download requests for pattern-sets)
  - TMPMAuUpdater (for request and application of pattern-sets)

## General

- The default ActiveUpdate server (for pattern updates) appears in the ESP Server registry:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CPMSrv\ServerUpdateSource\DefaultAUServer
  ```

- The default ActiveUpdate server URL for CPM *for Mac*:

  ```
  http://esp-p.activeupdate.trendmicro.com/activeupdate
  ```

- **CPM Server**: Check that the server exists in the Windows Registry:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\CPM\server
  ```

- **CPMSvr:** If the automatic update Task is successful, the CPM *for Mac* site exists in the 'bfsites' directory:

  ```
  <%Program Files%>\BigFix Enterprise\BES Server\wwwrootbes\bfsites\CustomSite_FileOnlyCustomSite_CPMSvrAutoUpdate_1
  ```

- **CPM Client:** After automatic updates have been enabled on the client, the CPM *for Mac* site exists in the ESP subscribed sites directory:

  `<%Program Files%>\BigFix Enterprise\BES Client\__BESData`

- Check for pattern updates on the CPM server. From the CPM Dashboard, click **Pattern Updates > New Pattern Update Task** to open the Endpoint Pattern Update Wizard.
  - If there are no new updates, inspect the Task **Core Protection Module for Mac – Check Server for Pattern Updates.**
  - If the Task was run but the updates are not working properly, check the Action or the BigFix Agent logs on the BigFix Server.
  - Check the ESP Server to confirm whether pattern update are being received as expected:

    `wwwrootbes\CPM for Mac\patterns`

- Check the TrendMirrorScript.exe logs.
- Confirm that older pattern files are still located on the ESP Server (by default a reserve of 15 patterns are retained).

## Automatic Updates

1. Check on the ESP Server that the Task, **Core Protection Module for Mac - Check Server for Pattern Updates** has been created and run. This task should be set to automatically reapply at a frequent interval (often, this is hourly), and it should not be restricted in any way that would conflict with the action.
2. Check on the ESP Server that the Task, **Core Protection Module - Apply Automatic Updates** has been run and that the Action has successfully completed.
3. On the CPM server, the user account must be in place for the propagation site. The PropagateManifest registry key must be set to 1:

   `[HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\CPM\server]`

4. For CPM *for Mac* clients that have been enabled for automatic updates, use the following plist file:

   `/Library/Preferences/com.bigfix.BESAgent.plist`

## Proxy Servers

If there is a proxy server between the ESP Server and Internet, two separate configurations are necessary:

- **The BES Server proxy authentication settings** (used by BESGather service, and typically set during the ESP Server install). See the following knowledge base article for more information:

  `http://support.bigfix.com/cgi-bin/kbdirect.pl?id=231`

- **CPM** *for Mac* **server component proxy authentication settings** (used by the update program, TMMPMAuHelper.exe). Set or check this from the CPM Dashboard: **Configuration > ActiveUpdate Server settings > Change ActiveUpdate Server settings.**

### Additional Information

If the latest pattern file already exists on the CPM server, you will need to perform the following manual steps to continue testing.

**To continue testing:**

1. Locate and delete the following folder:

   `%TMMPMAuHelper_install_path%\bin\AU_Data`

2. Delete all files and any subfolders from this directory (but not the folder itself):

   `%TMMPMAuHelper_install_path%\download`

3. From the CPM Dashboard, run the **Check Server for Pattern Updates** Task.

## Client-Side Logging: ActiveUpdate

1. On the CPM *for Mac* server, create/locate and open the following text file:

   `/Library/Application Support/TrendMicro/common/conf/aucfg.ini`

2. Add or change the following parameter:

   ```
   [debug]
   level=-1
   ```

3. Save and close the file.

4. Log output is saved here:

   ```
   /Library/Application
   Support/TrendMicro/common/conf/AU_Data/AU_Log/TmuDump.txt
   ```

### Additional Files

- Create a manifest file and list of URLs by typing the following at a command prompt:

  ```
  TMMPMAuUpdater –pu –m Manifest –f urllist
  ```

- Check the file, server.ini in the following location:

  ```
  /Library/Application Support/TrendMicro/MPM/download/
  ```

## Watchdog Functionality

To provide improved failover defense for the Core Protection Module for Mac, a "watchdog" service has been introduced to monitor the program's own essential service processes, such as the iCoreService. Every 30 seconds, the watchdog checks for the existence of the Core Protection Module for Mac's main service. If the main service has exited abnormally or crashed, the watchdog will restart the CPM for Mac main service guaranteeing the availability of the system.

However, in order to avoid a watchdog restarting loop, if the watchdog detects that the main service has crashed immediately after it was restarted, the watchdog is programmed not to automatically restart the main service.

In the event of a restart, the event will be saved in the `/var/log/TrendMicro/TmccCore/iCoreMonitor.txt` directory.

Under normal circumstances, the log file should be empty. After the watchdog restarts the iCoreService, it generates records similar to those that follow:

```
Tue Feb 02 11:39:15 +0800 2010 Restart /Library/Application
Support/TrendMicro/TmccMac/iCoreService
```

```
Tue Feb 02 11:39:16 +0800 2010 /Library/Application
Support/TrendMicro/TmccMac/iCoreMonitor.rb has been started
```

# Chapter 9

# Contacting Trend Micro

This appendix provides information to optimize the Trend Micro Core Protection Module *for Mac* (CPM for Mac) performance and get further assistance with any technical support questions you might have.

Topics in this chapter include:

# 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.

Worldwide support offices:

http://www.trendmicro.com/support

Trend Micro product documentation:

http://www.trendmicro.com/download

# Contact Information

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: 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:

- Mac OS version and hardware model
- 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

## 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 in the suspicious file.

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 malware).

- Send an email to: virusresponse@trendmicro.com, and specify "Phish or Disease Vector" as the Subject.
- Use the Web-based submission form: 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
```

## 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/enterprise/search.aspx?mode=advance

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 investigates the issue and responds as soon as possible.

# TrendLabs

TrendLabs™ is the global malware 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 malware pattern updates for all known "zoo" and "in-the-wild" computer malware and malicious codes
- Emergency malware outbreak support
- Email access to malware 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:

- List of malware and malicious mobile code currently "in the wild," or active
- Computer malware hoaxes
- Internet threat advisories
- Malware Encyclopedia, which includes a comprehensive list of names and symptoms for known malware and malicious mobile code
- Glossary of terms
- `http://www.trendmicro.com/vinfo/`

# Security Risks

This section describes common security risks (malware and Web threats). CPM *for Mac* protects computers from each of the security risks as described in the following sections.

## Phish Attacks

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 includes 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 back-end—the recipient of 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 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.

## Malware

Client computers are at risk from potential threats other than malware. Malware refers to applications or files not classified as viruses or Trojans, but can still negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization. Often malware 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.

If you find an application or file that CPM *for Mac* does not detect as malware but you believe is a type of malware, send it to Trend Micro for analysis:

http://subwiz.trendmicro.com/SubWiz

### How Malware Gets into the Network

Malware often gets into a corporate network when users download legitimate software that has malware applications included in the installation package. Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the

application and its intended use is to collect personal data; however, users often overlook this information or do not understand the legal jargon.

## Types of Malware

- **Spyware**: Gathers data, such as account user names and passwords, and transmits them to third parties.
- **Adware**: Displays advertisements and gathers data, such as user Web surfing preferences, used for targeting advertisements at the user through a Web browser.
- **Dialer**: Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem. These often pay-per-call or international numbers can result in a significant expense for your organization.
- **Joke program**: Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes.
- **Hacking tool**: Helps hackers enter computers.
- **Remote access tool**: Helps hackers remotely access and control computers.
- **Password cracking application**: Helps hackers decipher account user names and passwords.
- **Others**: Other types of potentially malicious programs.

### Malware Types

Tens of thousands of malware exist, with more being created each day. Although once most common in Windows or Mac OS X environments, computer malware today can also cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and Web sites.

- **Probable malware**: Suspicious files that have some of the characteristics of malware. For details, see the Trend Micro Virus Encyclopedia:

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

- **Trojan horse**: This type of threat often uses ports to gain access to a computer's executable programs. Trojan horse programs do not replicate but instead resides on systems to perform malicious acts, such as opening ports for hackers to enter. Traditional malware solutions can detect and remove malware but not Trojans, especially those already running on the system.

- **Virus**: A program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes, including:
  - **Worm**: A self-contained program or set of programs able to spread functional copies of itself or its segments to other computer systems, often through email.
  - **VBScript, JavaScript or HTML virus**: A virus that resides on Web pages and downloaded through a browser.
  - **ActiveX malicious code**: Code that resides on Web pages that execute ActiveX™ controls.
  - **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.
  - **Test Malware**: An inert file that acts like real virus and is detectable by malware-scanning software. Use test viruses, such as the EICAR test script, to verify that your malware installation scans properly.
  - **Packer**: A compressed and/or encrypted Windows or Linux™ executable program, often a Trojan horse program. Compressing executables makes packer more difficult for malware products to detect.
  - **Others**: Malware not categorized under any of the other malware types.
  - **Boot sector virus**: A virus that infects the boot sector of a partition or a disk.
  - **COM and EXE file infector**: An executable program with .com or .exe extension.
- **Joke program**: A virus-like program that often manipulates the appearance of things on a computer monitor.

## Guarding Against Malware and Other Threats

There are many ways you can prevent the installation of malware onto your computer. Trend Micro suggests the following:

- Configure On-Demand, Real-time, and Scheduled On-Demand Scans to find and remove malware files and applications.
- Educate your client users to do the following:
  - Read the End User License Agreement (EULA) and included documentation of applications they download and install on their computers.

  - Click **No** to any message asking for authorization to download and install software unless client users are certain both the creator of the software and the Web site they view are trustworthy.
  - Disregard unsolicited commercial email (spam), especially if the spam asks users to click a button or hyperlink.
- Configure Web browser settings that ensure a strict level of security. Trend Micro recommends requiring Web browsers to prompt users before installing ActiveX controls.
- If using Microsoft Outlook for Mac, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages.
- Do not allow the use of peer-to-peer file-sharing services. Spyware and other malware applications might be masked as other types of files your users might want to download, such as MP3 music files.
- Periodically examine the installed software on your agent computers and look for applications that might be spyware or other malware.
- Keep your Macintosh operating systems updated with the latest patches from Apple.

# Appendix A

# Routine CPM *for Mac* Tasks (Quick Lists)

The Appendix includes a "quick list" of How To's for the most common and routine management tasks you are likely to encounter.

In addition, you will find several processes that are intended to reduce some procedures to a simple reference. Refer to the complete procedure if you need configuration steps, an explanation of choices, or other details.

Procedure sections in this appendix include:

# Scan Management

Scan management procedures included in this section include:

For Real-time an On-Demand Scans:



## Real-time and On-Demand Scans

**To configure the Scan Now scan:**

- Click **Configuration > On-Demand Settings > New On-Demand Settings Task**.

**To start scanning with the default settings:**

- Click **Tasks > Core Protection Module for Mac > Start Scan**.

**To create and run a custom On-Demand Scan Task:**

- Click **Configuration > On-Demand Settings > New On-Demand Settings Task**.

**To run an On-Demand Scan:**

- Click **Configuration > On-Demand Settings > [scan name]**.

**To schedule an On-Demand Scan:**

1. Click **Configuration > On-Demand Settings > [scan name]**. In the **Take Action** window,
2. In the **Take Action** window,
   - Choose a **Start** date, and optionally, configure the days you want the scan to run in the **Run only on** field.
   - Select **Reapply this action while relevant, waiting 2 days between reapplications** (choosing whatever period suits you).

**To change or configure the following extra scan settings:**

- Client performance (CPU throttling)
- Malware scanning
- How threats are handled (delete, quarantine)
- Real-time scanning (scan files as they are created, modified, or received)
- Which files are scanned (performance, security)
- Network drive scanning
- Compressed files (performance, security)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

1. In the CPM Dashboard, click **Configuration > On-Demand Settings > New On-Demand Settings Task**.
2. Deploy the On-Demand settings by clicking **Configuration > On-Demand Settings > [scan name]**.

OR

1. In the CPM Dashboard, click **Configuration > Real-Time Settings > New Real-Time Settings Task**.
2. Deploy the Real-Time settings by clicking **Configuration > On-Demand Settings > [scan name]**.

# CPM Server Management

The steps that follow are for experienced ESP administrators who just need a list for tasks involving the CPM server.

The procedures include:


- To activate analyses: on page A-4
- To update or remove CPM server components: on page A-4
- To remove the Core Protection Module for Mac site: on page A-4
- To view CPM for Mac hidden client statistics for a given endpoint: on page A-4
- To decrypt quarantined files: on page A-5
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

**To activate analyses:**

1. In the ESP Console navigation pane, click the **Analyses** tab.
2. Sort the Name column in alphabetical order.
3. Select all the **Core Protection Module for Mac** analyses.
4. Right-click the list you have selected and click **Activate**.

**To update or remove CPM server components:**

1. Open the Tasks tab and then click **All Tasks > By Site > Trend Micro Core Protection Module**.
2. Locate **Core Protection Module - Remove Server Components** in the list of **Actions** that appears and double click it to open the **Description**.

**To remove the Core Protection Module for Mac site:**

1. In the ESP Console menu, click **Tools > Manage Sites...** and select the Trend Core Protection Module *for Mac*.
2. Click the **Remove Site** button and then **OK**.

# CPM *for Mac* Client Management

The steps that follow are for experienced ESP administrators who just need a list for tasks involving the CPM *for Mac* clients. Procedures include:


- To view CPM for Mac hidden client statistics for a given endpoint: on page A-4
- To decrypt quarantined files: on page A-5
- To deploy CPM for Mac clients: on page A-6
- To remove CPM for Mac clients: on page A-6


**To view CPM *for Mac* hidden client statistics for a given endpoint:**

- From the endpoint you want to check, press the following keys:

  ```
  Ctrl Alt Shift T
  ```

**To decrypt quarantined files:**

**WARNING!** Decrypting an infected file might spread the malware to other files. Trend Micro recommends isolating the computer with infected files by unplugging it from the network. Move important files to a backup location.

When you decrypt or encrypt a file, CPM *for Mac* creates the decrypted or encrypted file in the same folder. For example: type "VSEncode [-d] [-debug]" to decrypt files in the suspect folder and create a debug log.

The following files are required:

- Main file: `VSEncode.exe`
- Required DLL files: `Vsapi32.dll`

Run Restore Encrypted Virus using the following parameters:

```
no parameter {encrypt files in the Suspect folder}
-d (decrypt files in the Suspect folder)
-debug {create debug log and output in the client temp folder}
/o {overwrite encrypted or decrypted file if it already exists}
/f <filename> {encrypt or decrypt a single file}
/nr {do not restore original file name}
```

When you decrypt Quarantine Files on a Macintosh, the following files are required:

- Main file: `VSEncode`
- Required library: `libvsapi.dylib`

Run the Restore Encrypted Malware files using the following parameters:

### Usage:

```
./VSEncode {-e | -d} srcFile [dstFile]
./VSEncode -v
```

### Options:

**-e** Encodes the srcFile and saves the encoded data to the dstFile. The dstFile will be "srcFile.gen" if it's not provided.

**-d** Decodes the srcFile and saves the decoded data to the dstFile. The dstFile will be "srcFile.org" if it's not provided.

```
-v Indicates the version of this program.
```

**To deploy CPM *for Mac* clients:**

1. Click **Deployment > Install**.
2. Click **Install CPM for Mac Endpoints**.

**To remove CPM *for Mac* clients:**

To uninstall CPM *for Mac*, you first remove all the CPM *for Mac* clients installed on the endpoint, and then the CPM *for Mac* server components from the ESP Server (and any Relays), including the mastheads.

1. From the main ESP Console menu, open the **Tasks** tab and then click **All Tasks > By Site > Trend Core Protection Module for Mac**.
2. Locate **Core Protection Module for Mac - Endpoint Uninstall** in the list of Actions that appears and double click it to open the Description.

# Pattern File Management

The steps that follow are for experienced ESP administrators who just need a list for tasks involving the pattern files. Procedures include:


- To configure updates from the cloud: on page A-6
- To deploy selected pattern files: on page A-6
- To update pattern files on the CPM server: on page A-7
- To update pattern files on the CPM for Mac clients: on page A-7


**To configure updates from the cloud:**

From the CPM Dashboard menu, click **Updates > Other Update Tasks > Update From Cloud**. The Task **Description** window opens.

**To deploy selected pattern files:**

By default, all pattern files are included when the pattern is deployed from the ESP Server to CPM *for Mac* clients. You can, however, select and deploy a subset of patterns.

1. From the CPM Dashboard menu, click **Updates > Pattern Update Settings > New Pattern Update Settings Task.**

2. In the list of components that appears, select those that you want to include in the pattern update. By default, all patterns are selected.
3. Click the **Create Update Settings Task** button in the upper right corner.

#### To update pattern files on the CPM server:

1. Configure the ActiveUpdate server and proxy settings: In the CPM Dashboard, click **Configuration > ActiveUpdate Server Settings > Change ActiveUpdate Server Settings...**.
2. Enable CPM *for Mac* Server updates: Open the **Fixlet Messages** tab > **All Fixlet Messages > Core Protection Module for Mac - Enable Automatic Updates - Server**.
3. Update the pattern file on the CPM *for Mac* server: In the CPM Dashboard, click **Deployment > Install > Set ActiveUpdate Server Pattern Update Interval...**.

#### To update pattern files on the CPM *for Mac* clients:

1. Enable CPM *for Mac* clients to receive automatic pattern updates (this is typically a one-time Task): Click **Updates > Automatic Update Tasks > Enable Automatic Updates - Endpoint...**.
2. Schedule and apply automatic pattern file updates: Click **Updates > Automatic Update Tasks > Apply Automatic Updates...**.
3. Manually update CPM *for Mac* clients with the latest pattern files: Click **Updates > Update Patterns > New Pattern Update Task...**.

## Web Reputation

The steps that follow are for experienced ESP administrators who just need a list for tasks involving the Web Reputation.

#### To enable Web Reputation:

In the CPM Dashboard, click **Tasks > Web Reputation > Enable Web Reputation**.

#### To configure the security level:

In the CPM Dashboard, click **Tasks > Web Reputation > Configure Web Reputation Security Level**. The Task **Description** opens.

# Appendix B

## Reference Tables

The reference tables included in this appendix include:

# Available Malware Scan Actions

| SCAN ACTION | DESCRIPTION |
|---|---|
| Delete | CPM *for Mac* deletes the infected file. |
| Quarantine | CPM *for Mac* renames and then moves infected files to the following, non-configurable, directory on the client's computer:<br>`/Library/Application Support/TrendMicro/com-mon/lib/vsapi/quarantine/`<br>If you need to access any of the quarantined files, you can access the directory using system administrator credentials and restore it using the VSEncode tool (see Scan Action Results for Compressed Files on page B-3). |
| Clean | CPM *for Mac* cleans the infected file before allowing full access to the file. If the file is uncleanable, CPM *for Mac* performs a second action, which can be one of the following actions: Quarantine (typical), Delete, Rename or Pass. |
| Pass | CPM *for Mac* performs no action on the infected file but records the malware detection in the logs. The file stays where it is located.<br>CPM *for Mac* cannot use this scan action during Real-time Scan because performing no action when an attempt to open or execute an infected file is detected allows malware to execute. All the other scan actions can be used during Real-time Scan.<br>For the "probable malware" type, CPM *for Mac* always performs no action on detected files (regardless of the scan type) to mitigate false positives. If further analysis confirms that the probable malware is indeed a security risk, a new pattern will be released to allow CPM *for Mac* to take the appropriate scan action. If actually harmless, the probable malware will no longer be detected. |

# Pattern and Scan Engine Files

| COMPONENT | DESCRIPTION |
|---|---|
| **Malware** | |
| Virus Pattern | A file that helps CPM *for Mac* identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus. |
| Virus Scan Engine | The engine that scans for and takes appropriate action on malware; supports 32-bit and 64-bit platforms |
| **Anti-spyware** | |
| Spyware Pattern | The file that identifies malware in files and programs, modules in memory, Windows registry and URL shortcuts |

# Scan Action Results for Compressed Files

| STATUS OF CLEAN/DELETE INFECTED FILES IN COMPRESSED FILES | CPM *FOR MAC* ACTION | COMPRESSED FILE FORMAT | RESULT |
|---|---|---|---|
| Enabled | Clean or Delete | Not supported<br>Example: *def.rar* contains an infected file *123.doc*. | CPM *for Mac* encrypts *def.rar* but does not clean, delete, or perform any other action on *123.doc*. |
| Disabled | Clean or Delete | Supported/Not supported<br>Example: *abc.zip* contains an infected file *123.doc*. | CPM *for Mac* does not clean, delete, or perform any other action on both *abc.zip* and *123.doc*. |

| **STATUS OF** CLEAN/DELETE **INFECTED FILES IN COMPRESSED FILES** | **CPM *FOR MAC* ACTION** | **COMPRESSED FILE FORMAT** | **RESULT** |
|---|---|---|---|
| Enabled/ Disabled | Not Clean or Delete (in other words, any of the following: Quarantine or Pass) | Supported/Not supported<br>Example: *abc.zip* contains an infected file *123.doc*. | CPM *for Mac* performs the configured action (Quarantine or Pass) on *abc.zip*, not *123.doc*.<br>If the action is:<br>**Quarantine:** CPM *for Mac* quarantines *abc.zip* (*123.doc* and all non-infected files are quarantined).<br>**Pass:** CPM *for Mac* performs no action on both *abc.zip* and *123.doc* but logs the malware detection. |