



# Core Protection Module<sup>1</sup>

for Endpoint Security Platform

## Administrator's Guide





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

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Damage Cleanup Services, ScanMail, and TrendLabs are service marks, trademarks or registered trademarks of Trend Micro, Incorporated.

BigFix®, Fixlet® and "Fix it before it fails"® are registered trademarks of BigFix, Inc. iprevention, Powered by BigFix, Relevance Engine, and related BigFix logos are trademarks of BigFix, Inc.

All other product or company names may be trademarks or registered trademarks of their respective owners.

Protected by U.S. Patent No. 5,623,600; 5,889,943; 5,951,698; 6,119,165

Copyright © 2009 Trend Micro Incorporated. All rights reserved.

Document Part No. APEM14023/90302

Release Date: October 2009

## Related Documents

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

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](mailto:docs@trendmicro.com).

Please evaluate this documentation on the following site:

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

# Contents

## **Chapter 1: Introducing Core Protection Module**

Overview .....	1-2
What's New in CPM Version 1.6 .....	1-2
How CPM Works .....	1-2
ESP Components .....	1-3
Features and Benefits .....	1-4
Ease of Management .....	1-4
Extended Platform Support .....	1-5
Superior Malware Protection .....	1-5
Web Reputation Technology .....	1-5
Client-Side Firewall (Optional) .....	1-6
Traffic Filtering .....	1-6
Customizable Profiles and Policies .....	1-6
Stateful Inspection .....	1-6
The Trend Micro Pattern Files and Scan Engine .....	1-7
Incremental Virus Pattern File Updates .....	1-7
How Scanning Works .....	1-7
The Trend Micro Scan Engine and Detection Technologies .....	1-8
Scan Engine Updates .....	1-8
Trend Micro Damage Cleanup Services .....	1-9
GeneriClean .....	1-9
Rootkit Detection .....	1-9
IntelliTrap .....	1-9

## **Chapter 2: ESP Server: Installing and Updating**

Open the ESP Console .....	2-2
Add the CPM Site to the ESP Server .....	2-2
Install and Update CPM on the ESP Server .....	2-4
Overview of Procedures .....	2-4
Install CPM Components on the ESP Server .....	2-4

Upgrading CPM from Version 1.0 to Version 1.6 .....	2-5
What Has Changed and Requires Action .....	2-6
What Has Not Changed for Version 1.6 .....	2-7
Upgrading CPM from Version 1.5 to Version 1.6 .....	2-8
What Has Changed And Requires Action .....	2-8
What Has Not Changed .....	2-8
Update Pattern Files on the Server .....	2-9
Choose an Update Source and Proxy .....	2-9
Prepare the ESP Server and Update the Pattern Files .....	2-11
Running the CPM Automatic Update Setup Script .....	2-13
Enabling Automatic Updates on the ESP Server .....	2-14
Enabling Automatic Updates on Endpoints .....	2-15
Updating the Pattern File and Make the Action Automatic .....	2-17
Running the “Apply Automatic Updates” Task .....	2-20
Activate CPM Analyses .....	2-22
Removing CPM Server Components .....	2-23
Removing the Core Protection Module Site .....	2-23

### **Chapter 3: CPM Clients: Installing and Updating**

About CPM Client Deployment .....	3-2
CPM Console and Client System Requirements .....	3-2
Compatibility with Trend Micro OfficeScan .....	3-2
Incompatible or Conflicting Programs .....	3-2
Overview of Deployment Steps .....	3-3
Assess Endpoint Readiness .....	3-3
Remove Conflicting Products .....	3-3
Deploy CPM Clients to the Endpoints .....	3-5
Pattern File and Engine Updates .....	3-7
Pattern Rollbacks .....	3-7
Incremental Updates .....	3-7
Updates from the "Cloud" .....	3-7
Procedure Overview .....	3-8
Update Pattern Files on the CPM Client .....	3-8
Show the CPM Icon on Endpoints .....	3-12
Removing CPM Clients .....	3-13
System Requirements .....	3-14
Conflicting or Incompatible Programs .....	3-26

	Spyware, Virus, and Malware Programs .....	3-26
	Trend Micro Software .....	3-26
	Programs Incompatible with CPM on the ESP Server .....	3-27
<b>Chapter 4:</b>	<b>Configuring and Managing CPM</b>	
	Using the CPM Dashboard and Menu .....	4-2
	Tips for Navigating the CPM Console .....	4-2
	How CPM Task Flows Work .....	4-3
	Configure Global Settings .....	4-3
	The Global Settings Analysis .....	4-5
	Configure and Run Malware Scans .....	4-6
	Configuring the Default Scan Settings .....	4-8
	Starting a Scan of Relevant Endpoints (Scan Now) .....	4-10
	Creating an On-Demand Scan .....	4-10
	Running an On-Demand Scan .....	4-10
	Scheduling an On-Demand Scan (Automatic Scanning) .....	4-11
	Configure Client Updates from the Cloud .....	4-12
	Configuring Endpoints to Update Pattern File from the Cloud .....	4-13
	Use a Previous Pattern File Version .....	4-14
	Reverting to a Previous Version of the Pattern File .....	4-15
	Re-enabling Updates Following a Rollback .....	4-16
	Deploying Selected Pattern Files .....	4-17
	Exempting Programs From Spyware Detection .....	4-18
	Restoring Programs Incorrectly Detected as Spyware .....	4-20
<b>Chapter 5:</b>	<b>Configuration Wizards Reference</b>	
	The CPM Health Monitor .....	5-2
	Global Scan Settings Wizard .....	5-3
	Scan Settings .....	5-3
	Virus/Malware Scan Settings Only .....	5-4
	Spyware/Grayware Scan Settings Only .....	5-4
	Reserved Disk Space Settings .....	5-5
	Client Console Settings .....	5-5
	On-Demand & Real-Time Scan Settings Wizards .....	5-5
	Scan Target Tab .....	5-7
	User Activity on Files (Real-Time Scans Only) .....	5-7
	Files to Scan .....	5-7

Scan Settings .....	5-7
CPU Usage (On-Demand Scans Only) .....	5-8
Scan Exclusions Tab .....	5-8
AV/Spyware Scan Exclusion .....	5-8
Scan Action Tab .....	5-9
Virus/Malware Action .....	5-9
Spyware/Grayware Action .....	5-11
Spyware White List Wizard .....	5-11
Web Reputation Blacklist-Whitelist .....	5-12
ActiveUpdate Server Settings Wizard .....	5-13
Source .....	5-13
Proxy .....	5-14
Others .....	5-14
Common Firewall Settings .....	5-14

## **Chapter 6: Using Web Reputation**

How Web Reputation Works .....	6-2
Migrating WPM Standalone Settings .....	6-2
Procedures Overview .....	6-2
Web Reputation Security Levels .....	6-7
How Web Reputation Works .....	6-7
Using Web Reputation in CPM .....	6-9
Blacklist and Whitelist Templates .....	6-10
Creating and Deploying a New Template .....	6-11
Importing Lists of Web Sites .....	6-12
Viewing an Existing Template .....	6-14
Copying and Editing a Template .....	6-14
Editing Custom Actions .....	6-15
About Analyses .....	6-17

## **Chapter 7: Install and Manage the Client Firewall**

About the CPM Firewall and Policies .....	7-2
Add the Firewall Masthead to the ESP Server .....	7-2
Remove Conflicting Firewalls .....	7-4
Creating Firewall Policies .....	7-4
Governing Logic .....	7-5
Policy Verification .....	7-7



---

Global Exceptions .....	7-7
Create and Deploy a Firewall Policy .....	7-8
Create and Deploy Smart Policies: Example .....	7-10
Global Exception Rules .....	7-14
All Existing Rules .....	7-14
Firewall Policy Settings Wizard .....	7-15
Firewall Policy Configuration .....	7-17
Exception Rules Configuration .....	7-18
Uninstalling the Common Firewall .....	7-19
Disabling the Firewall from Endpoints .....	7-20
Removing the Firewall Site .....	7-20
<b>Chapter 8: Setting Up and Using Locations</b>	
Overview .....	8-2
Creating Locations .....	8-2
Creating Location-Specific Tasks .....	8-5
How Location Properties Work .....	8-6
<b>Chapter 9: Using the Client Console</b>	
Overview .....	9-2
CPM Client Dashboard vs. CPM Client Console .....	9-3
Accessing the Client Console .....	9-3
Client Connection with CPM Server .....	9-4
Manual Scans .....	9-4
Initiating a Manual Scan from the System Tray Icon .....	9-5
Initiating a Manual Scan from Windows Explorer .....	9-5
Manual Scan Results .....	9-6
Viewing Scan Results .....	9-7
Testing the CPM Client Console .....	9-7
Update Now .....	9-8
<b>Chapter 10: Troubleshooting</b>	
Installation .....	10-2
Install Status .....	10-2
Error Codes .....	10-2
Installing the CPM Server on a Non-default Drive .....	10-3
Virus, Malware, and Spyware Scanning .....	10-3

Virus/Spyware Logs on the CPM Client .....	10-4
Debug Logs .....	10-4
Components Installation Debug Logs (CPM Server) .....	10-5
Components Installation Debug Logs (CPM Client) .....	10-5
CPM Clients .....	10-5
Pattern Updates .....	10-6
General .....	10-7
Automatic Updates .....	10-8
Proxy Servers .....	10-8
Additional Information .....	10-8
Client-Side Logging: ActiveUpdate .....	10-9
Additional Files .....	10-9
Firewall Troubleshooting .....	10-9
General .....	10-10
Client is not Connecting to the ESP Server or Relays .....	10-10

## Chapter 11: Contacting Trend Micro

Technical Support .....	11-2
Contact Information .....	11-2
Speeding Up Your Support Call .....	11-2
Sending Suspicious Files to Trend Micro .....	11-3
Documentation Feedback .....	11-3
The Trend Micro Knowledge Base .....	11-3
TrendLabs .....	11-4
Security Information Center .....	11-4
Security Risks .....	11-4
Phish Attacks .....	11-5
Spyware and Grayware .....	11-5
Types of Spyware/Grayware .....	11-6
Viruses and Malware .....	11-6
Guarding Against Spyware/Grayware and Other Threats .....	11-7

## Appendix A: Routine CPM Tasks (Quick Lists)

Scan Management .....	A-2
General Scan Configurations .....	A-2
Real-time and On-Demand Scans .....	A-3
Spyware Handling and Correction .....	A-4

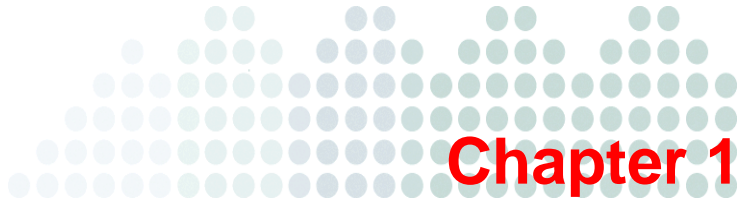
---

CPM Server Management .....	A-4
CPM Client Management .....	A-5
Pattern File Management .....	A-8
Web Reputation .....	A-10
CPM Firewall .....	A-10

## **Appendix B: Reference Tables**

Default ActiveAction Behaviors .....	B-2
Available Virus/Malware Scan Actions .....	B-3
Pattern and Scan Engine Files .....	B-4
Scan Action Results for Compressed Files .....	B-6
Default Firewall Global Exceptions .....	B-7





# Introducing Core Protection Module

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

- [Overview on page 1-2](#)
- [What's New in CPM Version 1.6 on page 1-2](#)
- [How CPM Works on page 1-2](#)
- [ESP Components on page 1-3](#)
- [Features and Benefits on page 1-4](#)
- [The Trend Micro Scan Engine and Detection Technologies on page 1-8](#)

## Overview

Trend Micro™ Core Protection Module (CPM) is an anti-malware application for Trend Micro Endpoint Security Platform (ESP). It works with ESP to protect the desktop and notebook computers on your network from security risks, including spyware, viruses, Trojans, worms, malicious Java applets, and ActiveX controls.

ESP is built on the BigFix® Enterprise Suite (BES) to provide extended management capabilities to the CPM server and clients. The CPM 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's Web Reputation. CPM also provides a policy-based firewall that you can deploy on your endpoints to control port access.

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.

## What's New in CPM Version 1.6

- Windows 7® and Windows 2008 R2® platform support

---

**Note:** Upgrade to ESP 7.2.5 agent which supports Windows 7 and Windows 2008 R2 operating systems before attempting to install CPM.

---

- New client console for endpoints with manual scan, scan results, and update now features
- Web Reputation allows enabling and disabling the collection of visited sites.

## How CPM Works

Trend Micro ESP uses the patented Fixlet® technology from BigFix to identify agents with outdated antivirus and 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.

Once CPM is installed, you will find it easy to protect your networked computers and keep them secure, all from the ESP Console. Deploying CPM 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 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, 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.

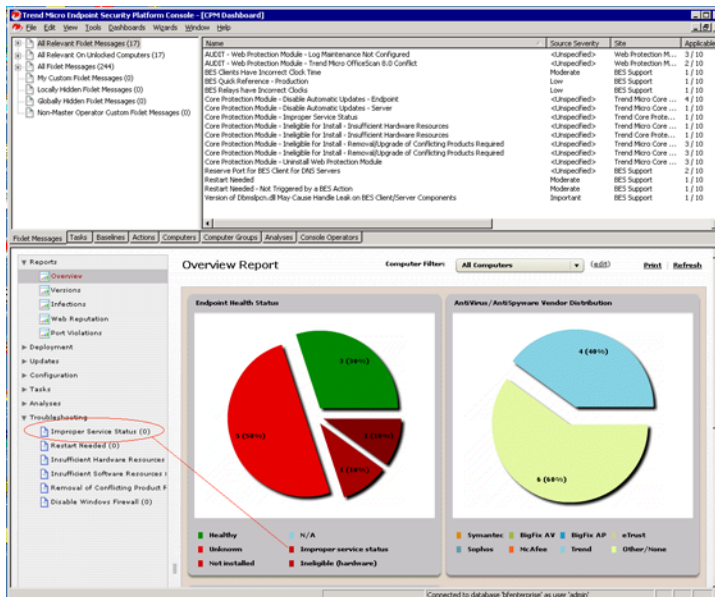


FIGURE 1-1 A screenshot showing the CPM Health Monitor.

- **The ESP Server** offers a collection of interacting services, including application services, a Web server, and a database server, which 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 version 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 components. The ESP Agent is responsible for relaying the instructions you enter in the ESP Console to all CPM 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 Client Components** are responsible for managing pattern files, conducting scans, and with the help of Trend Micro Damage Cleanup services, removing any malware that they detect. These components run undetected by end users and use minimal system resources. You need to install a CPM 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 Microsoft Windows 2000, Windows XP, Windows Server 2003, or Windows Server 2008 computer running an ESP Agent.

## Features and Benefits

CPM 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 and enhanced log aggregation for faster, more efficient updates and reduced network utilization.
- Supports native 64-bit and 32-bit processing for optimized performance.



- 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 Microsoft® Windows®, including;

- Microsoft® Windows 2000®
- Microsoft® Windows XP ®32/64-bit
- Microsoft® Windows Vista® 32/64 bit
- Microsoft® Windows 2000® Server
- Microsoft® Windows Server 2003® and Window Server 2008® 32/64-bit
- Microsoft® Windows 2008 R2®
- Microsoft® Windows 7®
- 

## Superior Malware Protection

- Delivers powerful protection against viruses, Trojans, worms, and new variants as they emerge
- Protects against a wide variety of spyware/grayware, including adware, dialers, joke programs, remote-access tools, key loggers, and password-cracking applications
- Detects and removes active and hidden rootkits
- Cleans endpoints of malware, including processes and registry entries that are hidden or locked

## Web Reputation Technology

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

In addition to file-based scanning, CPM 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 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.

## Client-Side Firewall (Optional)

The CPM firewall protects clients and servers on the network using stateful inspection. You can create rules to filter connections by IP address, port number, or protocol, and then apply the rules to different users and groups.

Contact your Trend Micro sales representative if you do not have the Firewall masthead for CPM 1.6 but are interested in using it.

## Traffic Filtering

The CPM firewall can filter all incoming and outgoing traffic, providing the ability to block certain types of traffic based on the following criteria:

- Direction (inbound/outbound)
- Protocol (TCP/UDP)
- Destination ports
- Source and destination computers

## Customizable Profiles and Policies

The CPM firewall gives you the ability to configure policies to block or allow specified types of network traffic. This provides a highly customizable means of organizing and configuring client firewall settings.

## Stateful Inspection

The CPM firewall is a stateful inspection firewall; it monitors all connections to the client and records all connection states. It can identify specific conditions in any

connection, predict what actions should follow, and detect disruptions in normal connections. Filtering decisions, therefore, are based not only on profiles and policies, but also on the context established by analyzing connections and filtering packets that pass through the firewall.

## The Trend Micro Pattern Files and Scan Engine

All Trend Micro products, including CPM, 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 virus outbreak occurs. Pre-release patterns have not undergone full testing but are available to stop burgeoning threats.

You can manually download the virus pattern and other files from the URL provided below. At the same location, you can also check the current release version, date, and review all the new virus definitions included in the files.

<http://www.trendmicro.com/download/pattern.asp>

## Incremental Virus Pattern File Updates

CPM, in conjunction with Trend Micro ActiveUpdate, supports incremental updates of the virus pattern file. Rather than download the entire pattern file each time (full pattern files can be more than 20MB), 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 virus pattern file to perform the first level of detection, using a process called pattern matching. Because each virus contains a unique binary “signature” or string of tell-tale characters that distinguishes it from any other code, the virus 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 virus 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 virus pattern files on a regular basis (typically several times per week), and recommends configuring hourly automatic updates. With automatic update enabled, new updates will be 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

At the heart of all Trend Micro products lies a scan engine. Originally developed in response to early file-based computer viruses, the scan engine now detects Internet worms, mass-mailers, Trojan horse threats, phishing sites, spyware, and network exploits as well as viruses. 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 "virus" characteristics and the exact location within a file that the malicious code inserts itself. CPM can usually remove this virus/malware upon detection and restore the integrity of the file (that is, "clean" the file).

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

### Scan Engine Updates

By storing the most time-sensitive virus/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 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

## Trend Micro Damage Cleanup Services

CPM uses Trend Micro™ Damage Cleanup Services (DCS) to clean computers of file-based and network viruses plus viruses and worm remnants—Trojans, registry entries, viral files—through a fully-automated process. DCS:

- Detects and removes live Trojans
- Kills processes that Trojans create
- Repairs system files that Trojans modify
- Deletes files and applications that Trojans drop

Because DCS runs automatically in the background, you do not need to configure it. Users are not even aware when it runs.

## GeneriClean

Also known as referential cleaning, GeneriClean is a new way of removing viruses/malware without the availability of virus cleanup components. Using a detected file as basis, GeneriClean determines if the detected file has a corresponding process/service in memory and a registry entry, and then removes them altogether.

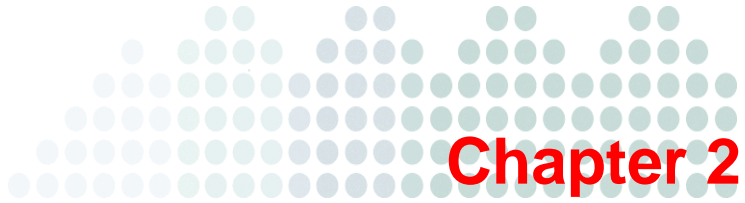
## Rootkit Detection

CPM also detects and removes rootkits. Currently on the rise, rootkits corrupt regular operating system functions that the application programs assumes are still valid to gain various levels of control of a user's computer. Without adequate protection, rootkits are extremely hard to remove without reformatting the infected computer's hard drive.

## IntelliTrap

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of virus/malware entering your network by blocking files with real-time compressed executable files.





## 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 (CPM) server components on the ESP Server, updating the related files, and preparing endpoints to receive the ESP client. Topics include:

- [Open the ESP Console on page 2-2](#)
- [Add the CPM Site to the ESP Server on page 2-2](#)
- [Install CPM Components on the ESP Server on page 2-4](#)
- [Install and Update CPM on the ESP Server on page 2-4](#)
- [Upgrading CPM from Version 1.0 to Version 1.6 on page 2-5](#)
- [Upgrading CPM from Version 1.5 to Version 1.6 on page 2-8](#)
- [Choose an Update Source and Proxy on page 2-9](#)
- [Prepare the ESP Server and Update the Pattern Files on page 2-11](#)
- [Activate CPM Analyses on page 2-22](#)

## 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 Site to the ESP Server

You install the Trend Micro Core Protection Module by adding its site masthead to the list of managed sites in the ESP Console. If you do not have the Core Protection Module and Reporting mastheads, contact your Trend Micro sales representative to obtain them. The Trend Micro Common Firewall is also available for CPM. The firewall provides client-level access control for your ESP endpoints.

CPM 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 may 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.

---

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 can not, the request will remain pending until the connection is made.

### To add the CPM site:

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

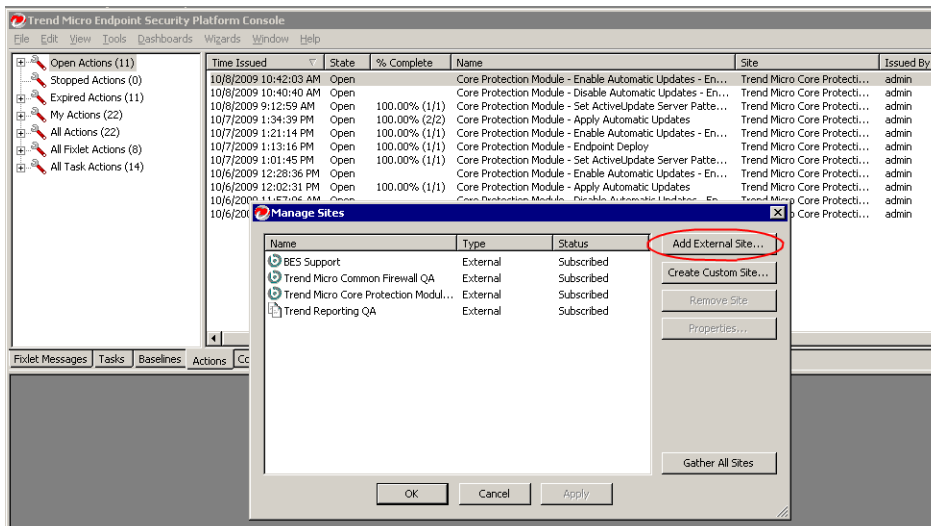


- In the **Add Site** window that opens, locate the masthead file(s) you received from the Trend Micro Sales Representative. The following mastheads are available (file names are shown here):

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

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

- Click the **Gather All Sites** button, and then **OK**.



**FIGURE 2-1** Add CPM sites to make them available in the ESP console.

- When prompted, type your private key password and click OK. The ESP Server will begin gathering the associated files and content associated with the masthead(s) you added and install them on the server.

## Install and Update CPM on the ESP Server

After adding the CPM Site(s) to the ESP Console, you need to install the CPM server components on the ESP Server, update the CPM pattern files, and then prepare and deploy CPM clients to your endpoints that are running the ESP Agent

### Overview of Procedures

- Install the CPM components. (See [page 2-4](#).)
- Do one of the following, if necessary:
  - Upgrade from CPM 1.0 to CPM 1.6. (See [page 2-5](#).)
  - Upgrade from CPM 1.5 to CPM 1.6. (See [page 2-8](#).)
- Update the pattern files on the ESP Server: (Starts on [page 2-9](#).)
  - 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 clients. (See [page 3-1](#).)

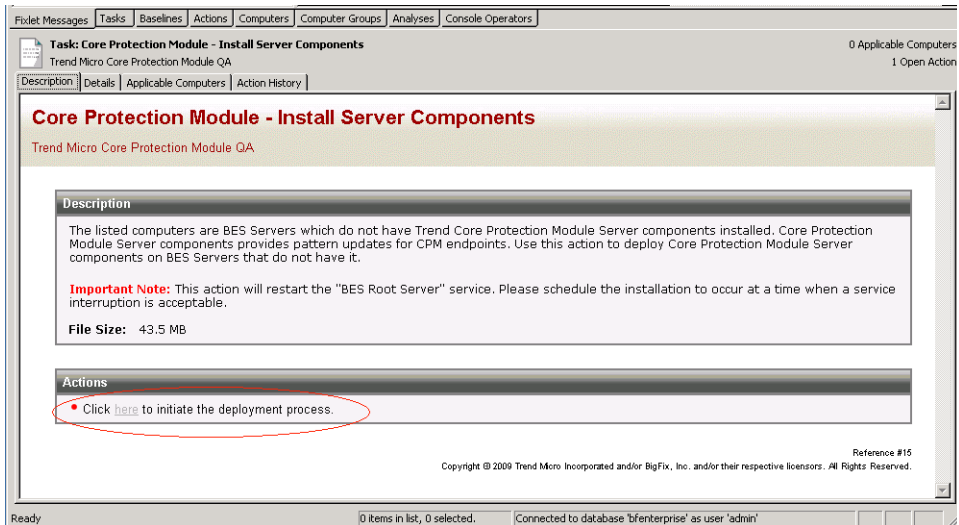
### Install CPM Components on the ESP Server

After adding the mastheads to the ESP Server, the next step is to open the ESP Console and update the CPM 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 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 that the CPM components have not already been updated on the server.

#### **To install the CPM server components:**

1. From the ESP Console menu, click **Dashboard > CPM Dashboard**.

2. Click **Deployment > Install > Install CPM Server**. The Install Server Components window opens to the **Description** tab.



**FIGURE 2-2** Begin by deploying CPM components to the ESP Server.

3. Below **Actions**, click the hyperlink to open the **Take Action** window.
4. Select **Specify computers selected in the list below**.  
Since you are updating only the ESP Server with CPM 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.

## Upgrading CPM from Version 1.0 to Version 1.6

When new CPM site content is published on the BigFix host, it automatically becomes available in the ESP Console. You should upgrade the CPM server components to

version 1.6, and then deploy the upgrade to your CPM clients. See [About CPM Client Deployment on page 3-2](#) for important information about client update strategies.

No concomitant upgrades to the ESP Server software are necessary.

---

**Note:** You may upgrade directly from CPM 1.0 to CPM 1.6. No intermediate upgrade to CPM 1.5 is necessary.

---

## What Has Changed and Requires Action

The following CPM features are new or have changed, and require action to ensure they remain synchronized with the upgrade:

- **CPM clients**—Run the Task Core Protection Module - Upgrade Client Components. See [Deploy CPM Clients to the Endpoints on page 3-5](#) for details.

---

**WARNING!** After upgrading the CPM 1.6 server components, you need to upgrade your installed CPM client base from version 1.0 to 1.6 to ensure access to the latest pattern files. Patterns updates, even manual, cannot occur if the CPM server components have been upgraded to version 1.6, but the endpoints are running CPM client 1.0. Contact Support for a workaround if you have already updated the CPM server components ahead of the clients.

---

- **CPM server components**—Run the Task Core Protection Module - Upgrade Server Components. See [Install CPM Components on the ESP Server on page 2-4](#).
- **Web Reputation**—If you are currently using Trend Micro Web Protection Module (WPM) standalone version, you will need to migrate your existing blacklist and whitelists to use them in CPM 1.6. See [Migrating WPM Standalone Settings on page 6-2](#) for instructions on migrating and configuring WPM in CPM 1.6.
- **WPM**—(Current standalone users only) Migrate any black/white lists to CPM 1.6, unsubscribe from the WPM site, and uninstall WPM clients before upgrading the endpoints to CPM 1.6.
- **Common Firewall**—If you have purchased and installed the Trend Micro Common Firewall, you will need to add that masthead and create firewall policies. See [Install and Manage the Client Firewall starting on page 7-1](#) for details.

- **Activate New Analyses**—Any existing analyses that you have activated in CPM version 1.0 will remain. However, to support new features in version 1.6, you should activate the following Analyses after upgrading and configuring the new features:
  - Core Protection Module – Spyware/Grayware Restore Information
  - Web Reputation – Client Information
  - Web Reputation – Site Statistics
  - Common Firewall – Endpoint Firewall Settings
  - Common Firewall – Inbound Port Violations
  - Common Firewall – Outbound Port Violations
- **CPM Client Console**—The new console on the endpoint machines allows manual scanning of files and folders for virus/malware and spyware/grayware, the ability to review the results and see what actions were taken on the infected files, and a feature that allows the client machine to update immediately to the latest version of protection components. See [Click the Create Firewall Policy Task... button at the top of the screen. on page A-11](#) and [Using the Client Console on page 9-1](#) for details.
- **New platforms supported**—Windows 7® and Windows 2008 R2® platform support added. See [System Requirements on page 3-14](#) for details.

---

**Note:** Upgrade to ESP 7.2.5 agent which supports Windows 7 and Windows 2008 R2 operating systems before attempting to install CPM.

---

- **Enable/disable Web Reputation logging**—The collection of visited sites can be enabled and disabled using the Task pane. See [About Analyses on page 6-17](#) for details.

## What Has Not Changed for Version 1.6

The following CPM settings are retained and do not need to be modified to remain synchronized with the upgrade:

- **Global Settings**, and any saved Tasks
- **On-Demand Settings**, and any saved Tasks
- **Real-Time Settings**, and any saved Tasks
- **Spyware White Lists**, and any saved Tasks
- **ActiveUpdate Server Settings** (proxy and AU server location)

- **Logs and Reports**
- **Analyses** that have already been run (however, see above for new analyses)
- Other existing **Fixlets, Tasks, Actions** (including relevance statements, target definitions, and other embedded logic) and **Baselines**.

## Upgrading CPM from Version 1.5 to Version 1.6

If you are currently running CPM 1.5, there are no steps to upgrade. You will receive the CPM 1.6 content once it propagates to your site. At that point, you can enable the new feature shown in the following section. You should upgrade the CPM server components to version 1.6, and then deploy the upgrade to your CPM clients.

### What Has Changed And Requires Action

- **CPM Client Console**—The new console on the endpoint machines allows manual scanning of files and folders for virus/malware and spyware/grayware, the ability to review the results and see what actions were taken on the infected files, and a feature that allows the client machine to update immediately to the latest version of protection components. See [Using the Client Console on page 9-1](#) for details.
- **New platforms supported**—Windows 7® and Windows 2008 R2® platform support added. See [System Requirements on page 3-14](#) for details.

---

**Note:** Upgrade to ESP 7.2.5 agent which supports Windows 7 and Windows 2008 R2 operating systems before attempting to install CPM.

---

- **Enable/disable Web Reputation logging**—The collection of visited sites can be enabled and disabled using the Task pane. See [About Analyses on page 6-17](#) for details.

### What Has Not Changed

The following CPM settings are retained and do not need to be modified to remain synchronized with the upgrade:

- **Global Settings**, and any saved Tasks
- **On-Demand Settings**, and any saved Tasks

- **Real-Time Settings**, and any saved Tasks
- **Spyware White Lists**, and any saved Tasks
- **ActiveUpdate Server Settings** (proxy and AU server location)
- **Logs and Reports**
- **Analyses** that have already been run (however, see above for new analyses)
- Other existing **Fixlets, Tasks, Actions** (including relevance statements, target definitions, and other embedded logic) and **Baselines**.

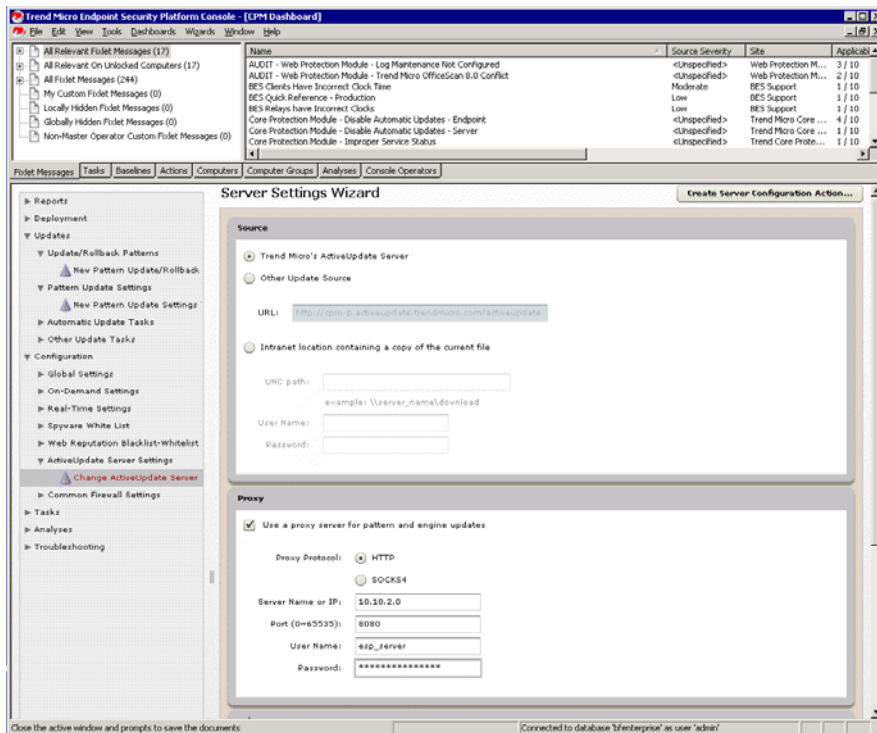
## Update Pattern Files on the Server

It is critically important to keep the ESP Server, Relays, and all CPM clients up-to-date with the current pattern and engine files from Trend Micro. CPM uses as many as 14 different pattern files to identify viruses, spyware, and other malware threats. (See [Security Risks starting on page 11-4](#) 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 virus pattern file on the ESP Server immediately after installing CPM, and then set the task to repeat hourly. The same holds true for CPM clients.

## Choose an Update Source and Proxy

By default, CPM 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 a 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, AU provides several layers of authentication and security to prevent forged or unsupported patterns.



**FIGURE 2-3** Identify a source for pattern file updates and the proxy server, if any, between CPM and the Internet.

You can and should configure the CPM server to frequently contact 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 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 below, you will configure CPM to get pattern updates, apply the configuration to the ESP server, 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 5-13](#) 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 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 the **Create Server Configuration Action...** button.  
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.

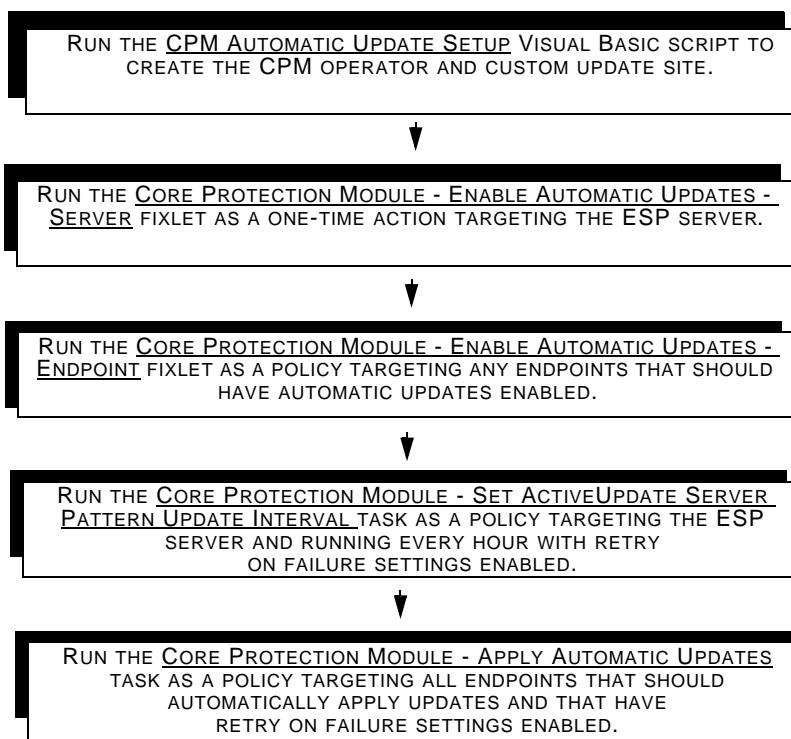
## Prepare the ESP Server and Update the Pattern Files

This procedure requires running a script to prepare the ESP Server for recurring automatic pattern updates, which are then used for CPM client updates. Trend Micro recommends that you enable 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 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 2-4** Update overview

Alternatively you can download the script and run it independent of this procedure. You can even manually perform the steps automated by the script. The URL below contains instructions for the manual procedure and a link to the script download.

[http://support.bigfix.com/cpm\\_update.html](http://support.bigfix.com/cpm_update.html)

---

**Note:** Pattern updates to the ESP Server always include all 14 patterns. When configuring updates for CPM 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 Automatic Update Setup Script

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

### To run the CPM automatic update setup Visual Basic script:

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

[http://software.bigfix.com/download/bes/cpm/CPMAutoUpdateSetup\\_1.5.vbs](http://software.bigfix.com/download/bes/cpm/CPMAutoUpdateSetup_1.5.vbs)

3. Double-click the name of the script to start it. The script prompts you to create a new user account in ESP.
  - a. Unless you have a good reason to change it, leave **CPM Admin Username** set to **cpm\_admin**.
  - b. Enter any password you would like for **CPM Admin Password**.  
You may want to choose something more secure than “trendmicro.”
  - c. Enter any email address for **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\\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.

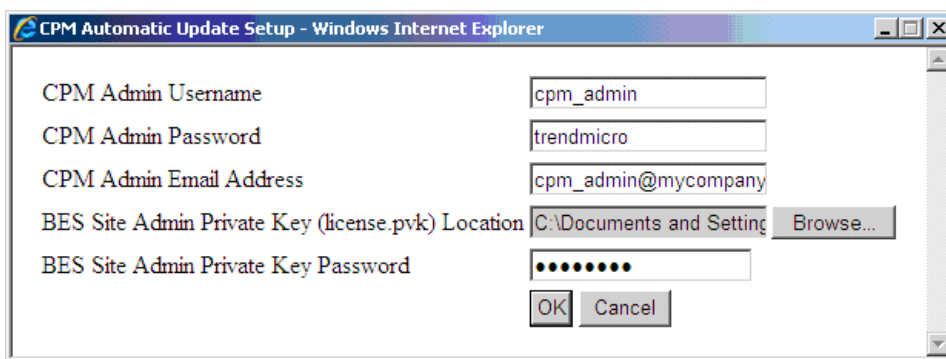
Be sure that you use the correct password and not your ESP console password. If you are unsure of which password to use, start the ESP Administration Tool. The password you use to start this tool is the same one you should enter here.

---

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

---

- f. Click **OK**.



CPM Automatic Update Setup - Windows Internet Explorer

CPM Admin Username: cpm\_admin

CPM Admin Password: trendmicro

CPM Admin Email Address: cpm\_admin@mycompany

BES Site Admin Private Key (license.pvk) Location: C:\Documents and Settings\ Browse...

BES Site Admin Private Key Password: ●●●●●●

OK Cancel

**FIGURE 2-5** Use the correct, Site Admin password.

## 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 update 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. (See [Figure 2-6](#).)

4. Find the action to enable automatic updates on the server.

- Below **Actions**, click the [here](#) hyperlink to open the **Take Action** window.

## Core Protection Module - Enable Automatic Updates - Server

Trend Micro Core Protection Module

**Description**

Take the first action below to enable automatic updates on the Core Protection Module server. After running this action, when new patterns are downloaded by the CPM server they will be made available for application by endpoints that have also been configured for automatic updates.

**Important Note:** Enabling automatic updates on the CPM Server additionally requires manual download and execution of the CPMAutoUpdateSetup script. Please use the link below to download the setup script to the CPM Server. Instructions for running the automatic update setup script can be found [here](#).

**Important Note:** Please validate file integrity with the following information  
 Filename: CPMAutoUpdateSetup\_1.6.vbs  
 SHA1: 1C97D104FDED722D2ADD2C14C08C3B0FE1EDA947

**Actions**

- Click [here](#) to enable automatic updates on the server.
- Click [here](#) to download the CPM Automatic Updates Setup Script.

**FIGURE 2-6 Use the “Enable Automatic Updates - Server” task**

- Leave the default settings in the **Take Action** dialog.
- Select the ESP server and click **OK**.
- 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.
- 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 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 agents receiving pattern and/or engine updates.

---

**To run the “Enable Automatic Updates - Endpoint” task:**

1. Navigate to **Dashboards > CPM Dashboard**.
2. Once 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.

### Core Protection Module - Enable Automatic Updates - Server

Trend Micro Core Protection Module

The screenshot shows a task configuration window with two main sections: 'Description' and 'Actions'. The 'Description' section contains instructions on how to enable automatic updates on the CPM server, including an important note about downloading and executing the CPMAutoUpdateSetup script. The 'Actions' section lists two actions: 'Click here to enable automatic updates on the server' and 'Click here to download the CPM Automatic Updates Setup Script'. The first action is circled in red.

**Description**

Take the first action below to enable automatic updates on the Core Protection Module server. After running this action, when new patterns are downloaded by the CPM server they will be made available for application by endpoints that have also been configured for automatic updates.

**Important Note:** Enabling automatic updates on the CPM Server additionally requires manual download and execution of the CPMAutoUpdateSetup script. Please use the link below to download the setup script to the CPM Server. Instructions for running the automatic update setup script can be found [here](#).

**Important Note:** Please validate file integrity with the following information  
Filename: CPMAutoUpdateSetup\_1.6.vbs  
SHA1: 1C97D104FDED722D2ADD2C14C08C3B0FE1EDA947

**Actions**

- Click [here](#) to enable automatic updates on the server.
- Click [here](#) to download the CPM Automatic Updates Setup Script.

**FIGURE 2-7 Use the “Enable Automatic Updates - Endpoints” task**

4. Make this task a policy, and use the settings below recommended by Trend Micro.

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

---

- a. Change the name of the action to **[POLICY] Core Protection Module - 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 or 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 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.

## Core Protection Module - Set ActiveUpdate Server Pattern Update Interval

Trend Micro Core Protection Module

**Description**

Take the action below to check the Trend Micro ActiveUpdate Server (TMAU Server) for updates to the following:

- Virus Pattern
- Intellitrapp Pattern
- Intellitrapp Exception Pattern
- Virus Scan Engine
- Spyware Pattern
- Spyware Active-Monitoring Pattern
- Spyware Scan Engine
- Virus Cleanup Template
- Virus Cleanup Engine
- Anti-rootkit Driver
- Common Firewall Pattern (versions 1.5 and higher)

When this action is run, the Core Protection Module server component will check to see if any new patterns have been published by Trend Micro. If there are new patterns, they will be downloaded and made available for deployment using the Pattern Update/Rollback Wizard in the CPM Dashboard. Additionally, if automatic updates have been configured and enabled for the server components, the patterns will be published such that endpoints configured for automatic updates will download and apply the new patterns immediately.

**Important Note:** You should set this action to run as a policy with periodic reapplicability behavior. It is recommended you apply this Task with the following action parameters:

- never expire
- run once an hour
- retry up to 99 times on failure
- reapply an unlimited number of times

If you do not set this action to run periodically new pattern sets will not be available for deployment to your endpoints.

---

**Actions**

- [Click here to check the TMAU Server for updates.](#)

**FIGURE 2-8 Set the AU server pattern update interval and make it a policy**

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 - 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 shown in [Figure 2-9](#), 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**.

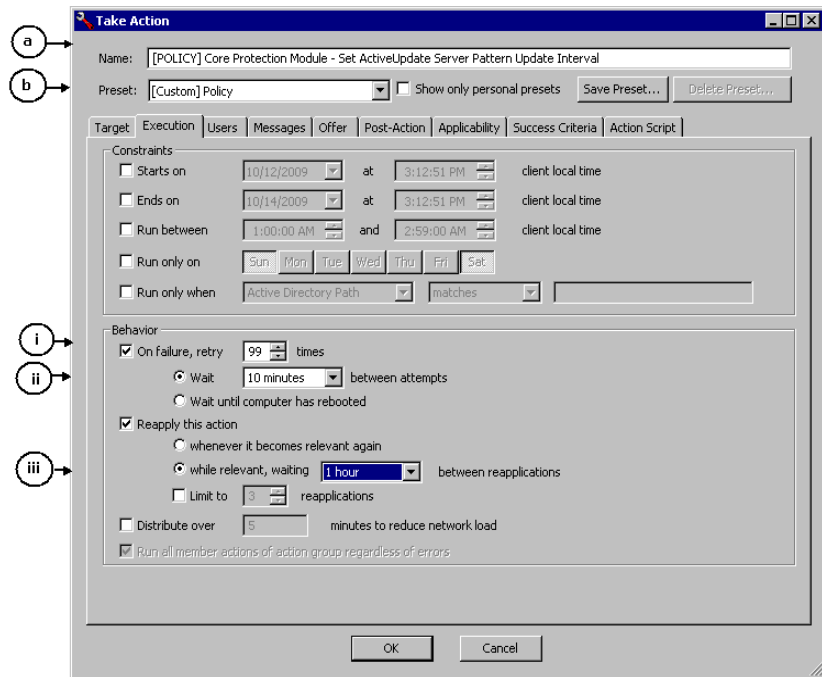
If you want to check for updates more or less frequently, increase or decrease this interval.

---

**Note:** If you are configuring CPM for 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**.



**FIGURE 2-9** Schedule the ESP Server to automatically check the Trend Micro Active Update Server for pattern updates.

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 below indicate, you can still deploy it as a policy targeting all computers or a particular group of computers. Once 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. Once 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.

## Core Protection Module - Apply Automatic Updates

Trend Micro Core Protection Module

**Description**

Use this task to apply pattern updates to Core Protection Module endpoints that have been configured for automatic updates.

**Important Note:** This action requires that the endpoint has been configured to allow automatic updates using the 'Enable Automatic Updates - Endpoint' task. Additionally the server components must also have automatic updates configured and enabled.

**Important Note:** You should set this action to run as a policy with reapplicability behavior. It is recommended you apply this Task with the following action parameters:

- never expire
- reapply whenever relevant
- retry up to 99 times on failure
- reapply an unlimited number of times

**If you do not set this action with the above settings new pattern sets will not be automatically downloaded and applied by your endpoints.**

---

**Actions**

- Click [here](#) to initiate the deployment process.

**FIGURE 2-10 Apply Automatic Updates**

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 Analyses

The Core Protection Module 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, spyware, and virus events. Analyses must be activated before they can be used.

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

### To activate all CPM 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** 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 CPM Server Components

Use the Remove Server Components Task to uninstall CPM 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 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 removal.

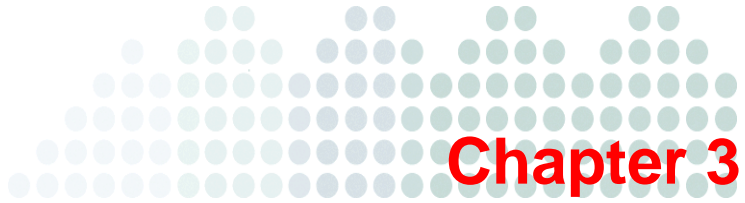
## Removing the Core Protection Module Site

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

### To remove the CPM masthead:

1. In the ESP Console menu, click **Tools > Manage Sites...** and select **Trend Micro Core Protection Module**.
2. Click the **Remove Site** button and then **OK**.
3. Enter your private key password and click **OK** to remove the CPM masthead.





## CPM Clients: Installing and Updating

There are any number of ways to handle the deployment of CPM 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 clients on all your endpoints.

Topics in this chapter include:

- [About CPM Client Deployment on page 3-2](#)
- [Assess Endpoint Readiness on page 3-3](#)
- [Remove Conflicting Products on page 3-3](#)
- [Deploy CPM Clients to the Endpoints on page 3-5](#)
- [Pattern File and Engine Updates on page 3-7](#)
- [Update Pattern Files on the CPM Client on page 3-8](#)
- [Show the CPM Icon on Endpoints on page 3-12](#)
- [Removing CPM Clients on page 3-13](#)
- [System Requirements on page 3-14](#)
- [Conflicting or Incompatible Programs on page 3-26](#)

## About CPM Client Deployment

The Tasks created in the procedures described below can only be deployed to relevant computers (the number of which is indicated after the Task name). In the ESP environment, relevance is determined by a “relevance statement” which defines certain conditions that the computer must meet. 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 XP computers, in California, that are part of the User group.”

## CPM Console and Client System Requirements

A complete list of system requirements can be found in [System Requirements starting on page 3-14](#).

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

## Compatibility with Trend Micro OfficeScan

Trend Micro CPM is intended to replace OfficeScan clients with CPM clients, which can be managed using the scalability and flexibility of the ESP Console.

Before deploying CPM clients, you should use the native OfficeScan uninstall program to remove all installed OfficeScan clients and then reboot them.

## Incompatible or Conflicting Programs

For a complete list of incompatible or conflicting programs, see [Conflicting or Incompatible Programs starting on page 3-26](#). Below is a short list of software that you should remove from the endpoints before deploying the CPM client.

- Trend Micro OfficeScan and Trend Micro PC-cillin



- AntiVirus software, including Symantec AntiVirus, McAfee VirusScan, Sophos Antivirus, and eTrust Antivirus

## Overview of Deployment Steps

1. Assess endpoint readiness.
2. Remove conflicting products.
3. Deploy CPM clients.
4. Check the deployment status and results.

## Assess Endpoint Readiness

The CPM 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 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 client to your endpoints, you need to uninstall any programs that will conflict with the CPM functions. See [Conflicting or Incompatible Programs starting on page 3-26](#) 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. In the CPM Dashboard, click **Deployment > Uninstall > [product name]**. The Fixlet **Description** tab opens, showing a list of the endpoints currently running the program.
  - Alternatively, you can click the Fixlet Messages tab and then navigate to **All Fixlet Messages > By Site > Trend Core Protection Module**. In the list of Fixlets that appears in the right window pane, select **Core Protection Module - Uninstall [product name]** by double-clicking it.
2. Below **Actions**, click the hyperlink to open the Take Action window.
3. In the **Target** tab, a list of the endpoints that are running the selected program appears. Click **Applicable Computers** to choose all relevant computers. In addition, you may also want to configure other options, as described below:
  - **Execution**—Set the deployment time and retry behavior.
  - **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 passively notify the user that the uninstall is going to occur, to obtain consent, 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 or not the program is removed. A pop-up message will be displayed on the target endpoints. (Requires that the client is enabled for offers.)
4. Click **OK**, and then 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.

## Deploy CPM Clients to the Endpoints

Use the Core Protection Module Endpoint Deploy Task to deploy CPM to all computers you want to secure against viruses and spyware. The CPM client package is about 65MB, and each endpoint will be 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 will automatically receive the CPM client.

Installation takes about five minutes, and the CPM client can be installed with or without the target user's consent. Installation does not typically require a reboot, however, a DOS-style command console may open on the client as the install scripts are run. In addition, the client will be briefly disconnected from the network.

---

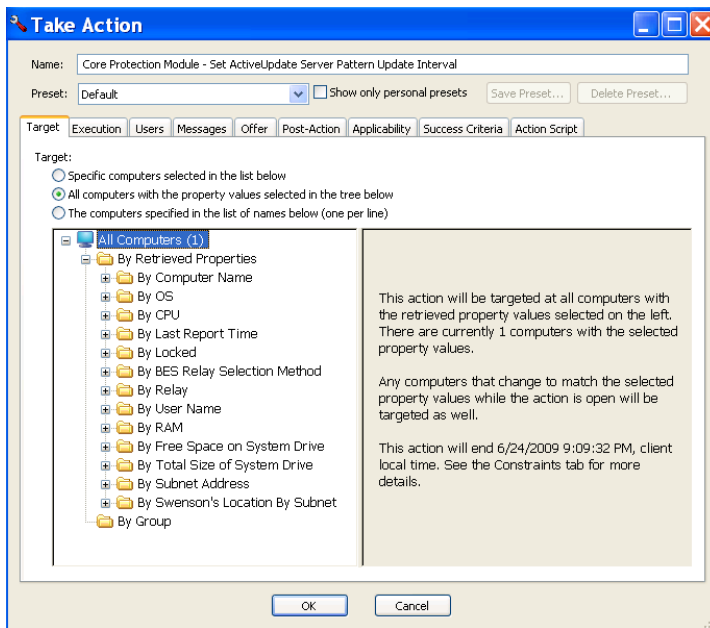
**Note:** Prior to deploying the CPM client, be sure your targeted endpoints are not running a conflicting product (see [Conflicting or Incompatible Programs on page 3-26](#)) and that they meet the hardware and software requirements as explained in [Assess Endpoint Readiness on page 3-3](#).

---

### To deploy CPM 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 Endpoint**.  
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 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 will include all the computers you want to deploy this Action to.



**FIGURE 3-1 Taking Action on the basis of computer properties means the action will automatically be applied whenever the property becomes true (e.g. a new computer is added to the network).**

- **Execution**—Set the deployment time and retry 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 passively notify 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 or not the client is installed. A pop-up message will be 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 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.

### Pattern Rollbacks

CPM supports pattern "rollbacks," that is, swapping out the current pattern to a different one. Although seldom used, it is useful in case there is a problem with the pattern file, for example to address an issue of false positives. The default is to keep 15 patterns on the server for clients to rollback to if necessary, but you can set this number as high as 100 (in the CPM Dashboard, click **Configuration > ActiveUpdate Server Settings > Change ActiveUpdate Server Settings...** and scroll to the bottom of the screen).

### 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 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 1.6 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 may 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 clients to receive automatic pattern updates.
2. Schedule and apply automatic pattern file updates.
3. Manually update CPM clients with the latest pattern files.

## Update Pattern Files on the CPM Client

Before performing the client update procedures below, be sure that you have updated the pattern files on the CPM Server and that you have enabled that server to perform automatic updates. See [Upgrading CPM from Version 1.0 to Version 1.6 on page 2-5](#) for details.

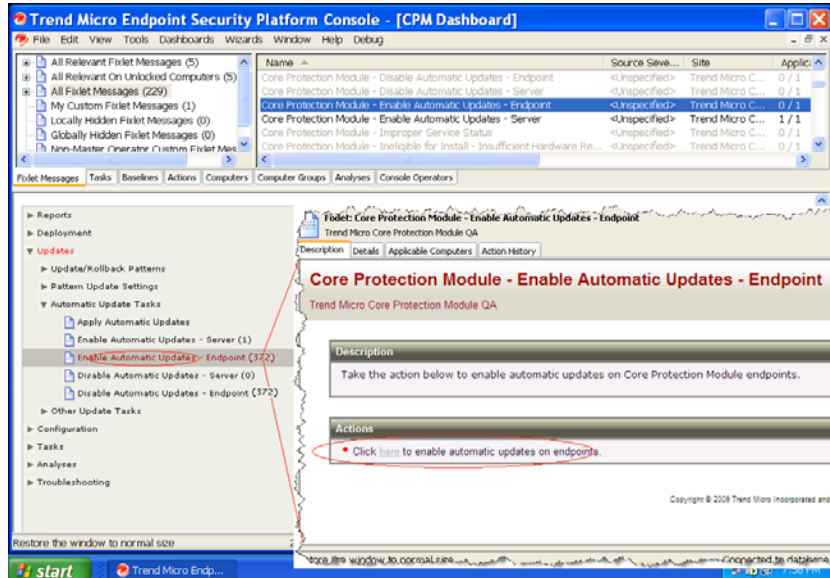
Trend Micro recommends that you perform the first full pattern-file update on a small number of CPM clients, then repeat the procedure on an expanded scope as you become more familiar with the procedures.

### To enable CPM 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.

- Below **Actions**, click the hyperlink to open the **Take Action** window.



**FIGURE 3-2** This composite screen shows the Dashboard Task and Fixlet that open after steps 1 and 2.

- On the **Target** tab, choose **All computers with the property values selected in the tree list below**.
- Choose a property that will include all the computers you want to deploy this Action to and click **OK**.
- When prompted, type your private key credential and click **OK**.  
The **Action | Summary** tab appears.
- Check the **Status** and **Count** after a few minutes to confirm that the Action is “Fixed.”
- Close the open windows to return to the Dashboard view.

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

- 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.

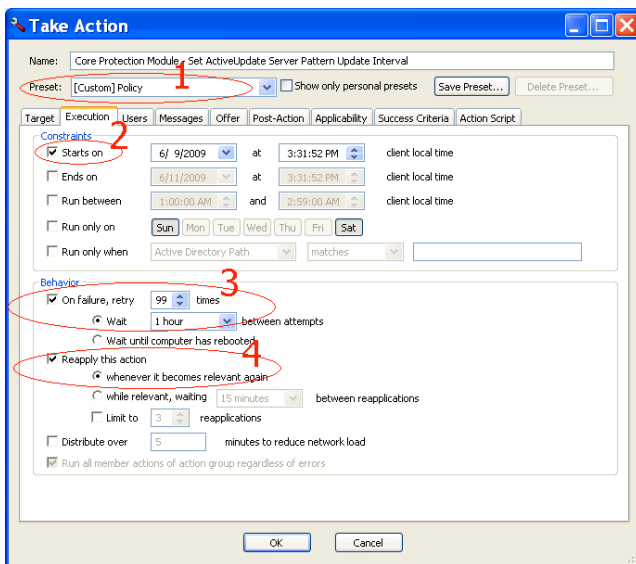
3. On the **Target** tab, choose **All computers with the property values selected in the tree list below** and then select **All Computers**.

---

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

---

4. Click the **Execution** tab to display scheduling options as shown below:



**FIGURE 3-3** Schedule the CPM clients to automatically check the ESP Server for pattern updates.

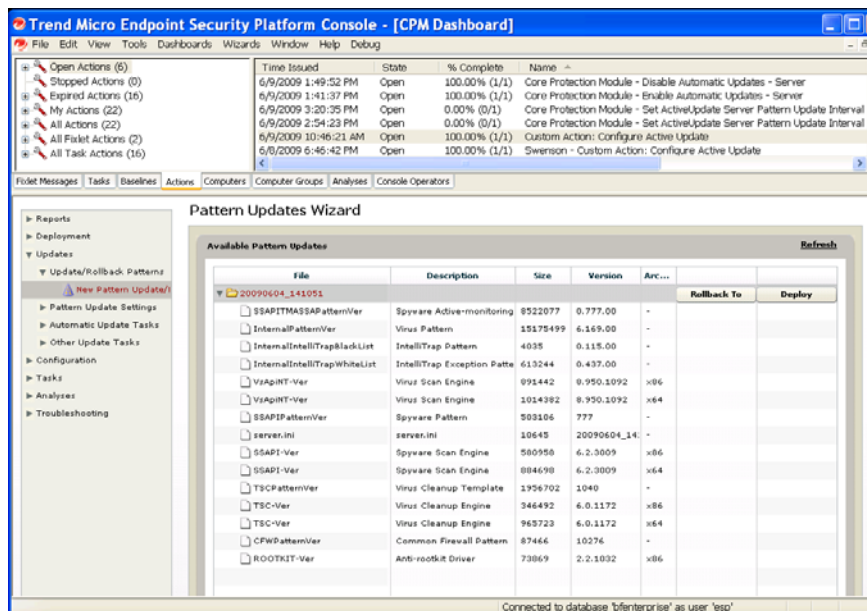
- a. Change **Preset: Policy** as shown by the number 1 in the Figure above.
- b. Enable **Starts on** and choose the current date and time (do not set **Ends on**).
- c. Enable **On failure, retry 99** times.
- d. Choose to **Wait 1 hour** between attempts.



- 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.

### To manually update CPM clients with the latest pattern files:

1. In the CPM Dashboard, click **Updates > Update/Rollback Patterns > New Pattern Update/Rollback Task...** The Pattern Updates Wizard opens.



**FIGURE 3-4** You can deploy or rollback individual pattern files, which are grouped in folders that start with the date.

2. In the list of folders that appears, click the ">" icon next to most recent folder to expand and display individual patterns as shown in [Figure 3-4](#).

If you recently updated the pattern file for the first time, there will be only one folder available.

3. Click the **Deploy** button across from the folder. In the pop-up window that appears, choose:
  - **Deploy a one time action** to open the Take Action window and select the computers you want to apply this one-time Action to. Any computers included in the Target that are not relevant for the Action at the time of deployment will respond with a “not relevant” statement. Click **OK**.
  - **Create an update Fixlet** to open **Edit Fixlet Message** window and configure a Fixlet that will deploy the Action whenever the selected clients become relevant. When finished, click **OK** and in the window that opens, click the hyperlink that appears below **Actions** to open the **Take Action** window.
4. In the **Target** tab that opens, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
  - **Execution**—Set the time and retry behavior for the update, (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).
5. After selecting the computers to update, click **OK** and when prompted, type your private key password and click **OK**.
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.

## Show the CPM Icon on Endpoints

By default, the CPM agent running on your endpoints is in “stealth” mode— it is not visible to the end-users, and they do not have any control over the settings. If you want users to know that CPM is running on their computer, however, you can display a CPM icon in the Windows taskbar. Users can right-click the icon to view basic information about the client in the Client Dashboard, including recent detections and the CPM client version.

When displayed, the CPM icon also includes a hidden "Technical" mode that Support or the CPM administrator can use to see a variety of information, including a list of Fixlets that are relevant on that computer. Useful, for example, to help understand and troubleshoot a client-side issue. After deploying the Task as described in the procedure

below, simultaneously press the following keys on the client's keyboard to display the Technical mode screen:

`Ctrl Alt Shift T`

#### To show a CPM icon on your endpoints' taskbars:

1. In the CPM Dashboard, click **Tasks > Enable Client Dashboard**. The **Task Description** opens.
2. Below **Actions**, click the hyperlink to open the **Take Action** window.
3. In the **Target** tab that opens, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
  - **Execution**—Do not select a retry behavior.
  - **Users**—This option works in combination with **Target**, linked by the AND operand (both conditions must be present for the install to occur).
4. When finished, click **OK** to initiate the action and 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.

## Removing CPM Clients

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

#### To uninstall CPM clients from one or more endpoints:

1. From the CPM Dashboard menu, click **Deployment > Uninstall > CPM 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 back their **Action** status.

## System Requirements

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

- [Windows 2000®](#)
- [Windows XP®/Windows 2003®, 32-bit version](#)
- [Windows XP®/Windows 2003®, 64-bit version](#)
- [Windows Vista®, 32-bit and 64-bit versions](#)
- [Windows 2008®, 32-bit version](#)
- [Windows 2008®/Windows 2008 R2®, 64-bit version](#)
- [Windows 7®, 32-bit version](#)
- [Windows 7®, 64-bit version](#)

Also included is a list of software programs that should be removed before installing the CPM client. Most of the programs on this list have duplicate or competing functions, including Trend Micro's OfficeScan and PC-cillin/Internet Security programs.

- Trend Micro OfficeScan
- Trend Micro Internet Security 2008
- Trend Micro Pc-cillin 2007
- Symantec Software Virtualization Solution, Symantec AntiVirus
- McAfee VirusScan
- Sophos Antivirus
- eTrust Antivirus

**TABLE 3-1. Windows 2000®**

<b>RESOURCE</b>	<b>REQUIREMENT</b>
Operating system	<ul style="list-style-type: none"> <li>• Windows 2000 with Service Pack 4</li> <li>• Windows 2000 Professional with Service Pack 4</li> <li>• Windows 2000 Cluster Server with Service Pack 4</li> <li>• Windows 2000 Advanced Server with Service Pack 4</li> <li>• CPM supports client installation on guest Windows 2000 operating systems hosted on the following virtualization applications:               <ul style="list-style-type: none"> <li>• Microsoft Virtual Server 2005 R2 with Service Pack 1</li> <li>• VMware™ ESX™/ESXi Server 3.0 or 3.5 (Server Edition)</li> <li>• VMware Server 1.0.3 or later (Server Edition)</li> <li>• VMware Workstation and Workstation ACE Edition 6.0</li> <li>• Microsoft Windows Server 2008 64-bit Hyper-V environment</li> </ul> </li> </ul>
Hardware	<p><b>Processor</b> 300MHz Intel™ Pentium™ processor or equivalent</p> <p><b>RAM</b> 512MB recommended</p> <p><b>Available disk space</b> 700MB recommended</p> <p><b>Others</b> Monitor that supports 800 x 600 resolution at 256 colors or higher</p>

**TABLE 3-2. Windows XP®/Windows 2003®, 32-bit version**

RESOURCE	REQUIREMENT
Operating system	<ul style="list-style-type: none"><li>• Windows XP Professional with Service Pack 2 or later</li><li>• Windows XP Home with Service Pack 3 or later</li><li>• Windows Server™ 2003 (Standard, Enterprise, Datacenter, and Web Editions) with Service Pack 2 or later</li><li>• Windows Server 2003 R2 (Standard, Enterprise, and Datacenter Editions) with Service Pack 2 or later</li><li>• Windows Storage Server 2003</li><li>• Microsoft Cluster Server 2003</li><li>• CPM supports client installation on guest Windows XP/2003 operating systems hosted on the following virtualization applications:<ul style="list-style-type: none"><li>• Microsoft Virtual Server 2005 R2 with Service Pack 1</li><li>• VMware ESX/ESXi Server 3.0 or 3.5 (Server Edition)</li><li>• VMware Server 1.0.3 or later (Server Edition)</li><li>• VMware Workstation and Workstation ACE Edition 6.0</li><li>• Microsoft Windows Server 2008 64-bit Hyper-V environment</li></ul></li></ul>

**TABLE 3-2. Windows XP®/Windows 2003®, 32-bit version (Continued)**

<b>RESOURCE</b>	<b>REQUIREMENT</b>
Hardware	<p><b>Processor</b> 300MHz Intel Pentium or equivalent AMD™ 64 or Intel 64 processor architectures</p> <p><b>RAM</b> 512MB recommended</p> <p><b>Available disk space</b> 700MB recommended</p> <p><b>Others</b> Monitor that supports 800 x 600 resolution at 256 colors</p>

**TABLE 3-3. Windows XP®/Windows 2003®, 64-bit version**

<b>RESOURCE</b>	<b>REQUIREMENT</b>
Operating system	<ul style="list-style-type: none"> <li>• Windows XP Professional with Service Pack 2 or later</li> <li>• Windows Server 2003 (Standard, Enterprise, Datacenter, and Web Editions) with Service Pack 2 or later</li> <li>• Windows Server 2003 R2 (Standard, Enterprise, and Datacenter Editions) with Service Pack 2 or later</li> <li>• Windows Storage Server 2003</li> <li>• Microsoft Cluster Server 2003</li> <li>• CPM supports client installation on guest Windows XP/2003 operating systems hosted on the following virtualization applications:               <ul style="list-style-type: none"> <li>• VMware ESX/ESXi Server 3.0 or 3.5 (Server Edition)</li> <li>• VMware Server 1.0.3 or later (Server Edition)</li> <li>• VMware Workstation and Workstation ACE Edition 6.0</li> <li>• Microsoft Windows Server 2008 64-bit Hyper-V environment</li> </ul> </li> </ul>
Hardware	<p><b>Processor</b></p> <ul style="list-style-type: none"> <li>• Intel x64 processor</li> <li>• AMD64 processor</li> </ul> <p><b>RAM</b></p> <p>512MB recommended</p> <p><b>Available disk space</b></p> <p>700MB recommended</p> <p><b>Others</b></p> <p>Monitor that supports 800 x 600 resolution at 256 colors</p>



**TABLE 3-4. Windows Vista®, 32-bit and 64-bit versions**

<b>RESOURCE</b>	<b>REQUIREMENT</b>
Operating system	<ul style="list-style-type: none"><li>• Windows Vista™ Business Edition with Service Pack 1 or later</li><li>• Windows Vista Enterprise Edition with Service Pack 1 or later</li><li>• Windows Vista Ultimate Edition with Service Pack 1 or later</li><li>• Windows Vista Home Premium Edition with Service Pack 1 or later</li><li>• Windows Vista Home Basic Edition with Service Pack 1 or later</li><li>• CPM supports client installation on guest Windows Vista operating systems hosted on the following virtualization applications:<ul style="list-style-type: none"><li>• VMware ESX/ESXi Server 3.0 or 3.5 (Server Edition)</li><li>• VMware Server 1.0.3 or later (Server Edition)</li><li>• VMware Workstation and Workstation ACE Edition 6.0</li><li>• Microsoft Windows Server 2008 64-bit Hyper-V environment</li></ul></li></ul>

**TABLE 3-4. Windows Vista®, 32-bit and 64-bit versions (Continued)**

RESOURCE	REQUIREMENT
Hardware	<p><b>Processor</b></p> <ul style="list-style-type: none"> <li>• 800MHz Intel Pentium or equivalent</li> <li>• AMD64 or Intel 64 processor architectures</li> </ul> <p><b>RAM</b></p> <p>1GB minimum</p> <p><b>Available disk space</b></p> <p>700MB recommended</p> <p><b>Others</b></p> <p>Monitor that supports 800 x 600 resolution at 256 colors</p>

**TABLE 3-5. Windows 2008®, 32-bit version**

RESOURCE	REQUIREMENT
Operating system	<ul style="list-style-type: none"> <li>• Windows Server 2008 (Standard, Enterprise, Datacenter and Web Editions) with Service Pack 1 or later</li> <li>• CPM supports client installation on guest Windows Vista operating systems hosted on the following virtualization applications: <ul style="list-style-type: none"> <li>• VMware ESX/ESXi Server 3.0 or 3.5 (Server Edition)</li> <li>• VMware Server 1.0.3 or later (Server Edition)</li> <li>• VMware Workstation and Workstation ACE Edition 6.0</li> <li>• Microsoft Windows Server 2008 64-bit Hyper-V environment</li> </ul> </li> </ul> <hr/> <p>Note: CPM cannot be installed if Windows 2008 runs in the Server Core environment.</p> <hr/>

**TABLE 3-5. Windows 2008®, 32-bit version (Continued)**

<b>RESOURCE</b>	<b>REQUIREMENT</b>
Hardware	<p><b>Processor</b></p> <ul style="list-style-type: none"><li>• Minimum 1.4GHz Intel Pentium or equivalent, 2GHz recommended</li><li>• AMD64 and Intel 64 processor architectures</li></ul> <p><b>RAM</b></p> <p>1GB recommended</p> <p><b>Available disk space</b></p> <p>700MB recommended</p> <p><b>Others</b></p> <p>Monitor that supports 800 x 600 resolution at 256 colors</p>

**TABLE 3-6. Windows 2008®/Windows 2008 R2®, 64-bit version**

RESOURCE	REQUIREMENT
Operating system	<hr/> <p data-bbox="396 386 1085 414">Note: Windows 2008 R2 requires ESP agent 7.2.5 (or later.)</p> <hr/> <ul data-bbox="409 441 1068 922" style="list-style-type: none"><li data-bbox="409 441 1068 500">• Windows Server 2008 Standard, Enterprise, Datacenter and Web Editions) with Service Pack 1 or later</li><li data-bbox="409 516 1068 574">• Windows Server 2008 R2 (Standard, Enterprise, Datacenter, and Web Editions)</li><li data-bbox="409 591 1068 672">• CPM supports client installation on guest Windows 2008 operating systems hosted on the following virtualization applications:<ul data-bbox="436 688 1055 922" style="list-style-type: none"><li data-bbox="436 688 1055 716">• Microsoft Virtual Server 2005 R2 with Service Pack 1</li><li data-bbox="436 732 1055 760">• VMware ESX/ESXi Server 3.0 or 3.5 (Server Edition)</li><li data-bbox="436 776 1055 803">• VMware Server 1.0.3 or later (Server Edition)</li><li data-bbox="436 820 1055 847">• VMware Workstation and Workstation ACE Edition 6.0</li><li data-bbox="436 863 1055 922">• Microsoft Windows Server 2008 64-bit Hyper-V environment</li></ul></li></ul> <hr/> <p data-bbox="396 971 1081 1019">Note: CPM cannot be installed if Windows 2008 runs in the Server Core environment.</p> <hr/>

**TABLE 3-6. Windows 2008®/Windows 2008 R2®, 64-bit version (Continued)**

<b>RESOURCE</b>	<b>REQUIREMENT</b>
Hardware	<p><b>Processor</b></p> <ul style="list-style-type: none"><li>• Minimum 1.4GHz Intel Pentium or equivalent, 2GHz recommended</li><li>• AMD64 and Intel 64 processor architectures</li></ul> <p><b>RAM</b></p> <p>1GB recommended</p> <p><b>Available disk space</b></p> <p>700MB recommended</p> <p><b>Others</b></p> <p>Monitor that supports 800 x 600 resolution at 256 colors</p>

**TABLE 3-7. Windows 7®, 32-bit version**

RESOURCE	REQUIREMENT
Operating system	<hr/> <p>Note: Windows 7 requires ESP agent 7.2.5 (or later.)</p> <hr/> <ul style="list-style-type: none"> <li>• Windows 7 build 7600.16385 (Starter, Home Basic, Home Premium, Ultimate, Professional, Enterprise)</li> <li>• CPM also supports XP mode running in Windows 7</li> <li>• CPM supports client installation on guest Windows 7 operating systems hosted on the following virtualization applications: <ul style="list-style-type: none"> <li>• Microsoft Virtual Server 2005 R2 with Service Pack 1</li> <li>• VMware ESX/ESXi Server 3.0 or 3.5 (Server Edition)</li> <li>• VMware Server 1.0.3 or later (Server Edition)</li> <li>• VMware Workstation and Workstation ACE Edition 6.0</li> <li>• Microsoft Windows Server 2008 64-bit Hyper-V environment</li> </ul> </li> </ul>
Hardware	<p><b>Processor</b> Minimum 1GHz Intel Pentium or equivalent, 2GHz recommended</p> <p><b>RAM</b> 1GB minimum, 2GB recommended</p> <p><b>Available disk space</b> 16GB minimum</p>

**TABLE 3-8. Windows 7®, 64-bit version**

<b>RESOURCE</b>	<b>REQUIREMENT</b>
Operating system	<p data-bbox="494 386 1103 412">Note: Windows 7 requires ESP agent 7.2.5 (or later.)</p> <ul style="list-style-type: none"> <li data-bbox="505 440 653 466">• Windows 7</li> <li data-bbox="505 485 1099 511">• CPM also supports XP mode running in Windows 7</li> <li data-bbox="505 531 1153 613">• CPM supports client installation on guest Windows 7 operating systems hosted on the following virtualization applications: <ul style="list-style-type: none"> <li data-bbox="532 633 1150 659">• Microsoft Virtual Server 2005 R2 with Service Pack 1</li> <li data-bbox="532 678 1150 704">• VMware ESX/ESXi Server 3.0 or 3.5 (Server Edition)</li> <li data-bbox="532 724 1067 750">• VMware Server 1.0.3 or later (Server Edition)</li> <li data-bbox="532 769 1163 795">• VMware Workstation and Workstation ACE Edition 6.0</li> <li data-bbox="532 815 1083 867">• Microsoft Windows Server 2008 64-bit Hyper-V environment</li> </ul> </li> </ul>
Hardware	<p data-bbox="494 896 615 922"><b>Processor</b></p> <p data-bbox="494 935 973 961">Minimum 2GHz Intel Pentium or equivalent</p> <p data-bbox="494 974 551 1000"><b>RAM</b></p> <p data-bbox="494 1013 650 1039">2GB minimum</p> <p data-bbox="494 1052 736 1078"><b>Available disk space</b></p> <p data-bbox="494 1091 663 1117">20GB minimum</p>

## Conflicting or Incompatible Programs

Remove the following programs before deploying CPM to the endpoints.

### Spyware, Virus, and Malware Programs

- Symantec Software Virtualization Solution
- Symantec AntiVirus
- McAfee VirusScan
- Sophos Antivirus
- eTrust Antivirus
- Bit9 Parity Agent
- Computer Associates ARCserve Backup
- HSM (Hierarchical Storage Management) Backup Software

### Trend Micro Software

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

- OfficeScan versions 8 and 10
- Internet Security 2008
- Pc-cillin 2007
- Pc-cillin 2006
- Pc-cillin 2005
- Pc-cillin 2004 (AV)
- Pc-cillin 2004 (TIS)
- PC-cillin 2003
- PC-cillin 2002
- PC-cillin 2000 (WinNT)
- PC-cillin 2000 7.61 (WinNT)
- PC-cillin 98 Plus (WinNT)
- PC-cillin NT 6

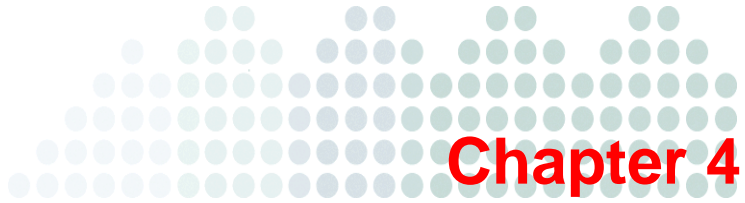


- PC-cillin NT
- HouseCall Pro
- Virus Buster 2000 for NT ver.1.20-
- Virus Buster 98 for NT
- Virus Buster NT

### **Programs Incompatible with CPM on the ESP Server**

- Trend Micro ServerProtect
- ServerProtect for Windows NT





## Configuring and Managing CPM

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 CPM server and deployed CPM 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 CPM Dashboard and Menu on page 4-2](#)
- [Configure Global Settings on page 4-3](#)
- [The Global Settings Analysis on page 4-5](#)
- [Configure and Run Malware Scans on page 4-6](#)
- [Configure Client Updates from the Cloud on page 4-12](#)
- [Use a Previous Pattern File Version on page 4-14](#)
- [Deploying Selected Pattern Files on page 4-17](#)
- [Exempting Programs From Spyware Detection on page 4-18](#)
- [Restoring Programs Incorrectly Detected as Spyware on page 4-20](#)

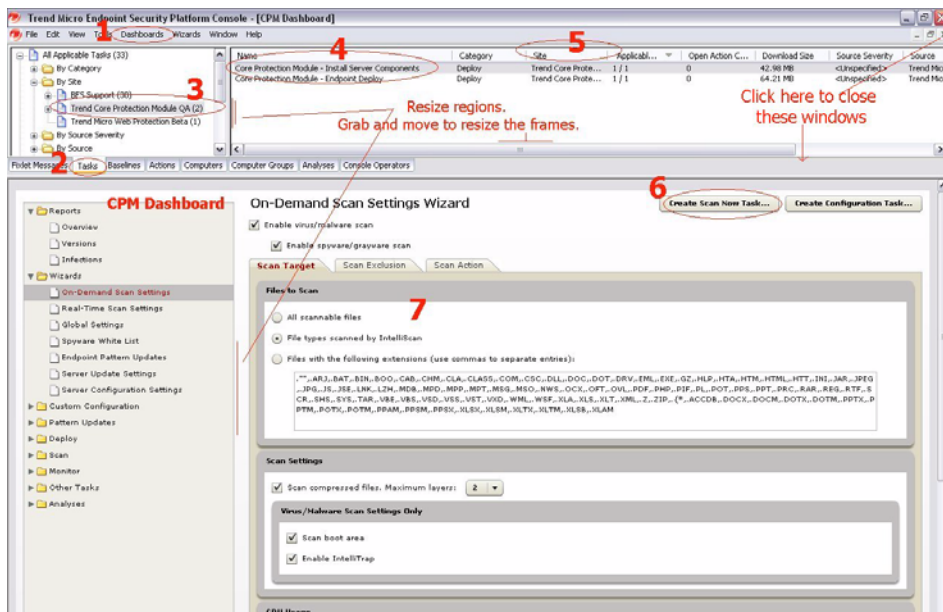
## Using the CPM Dashboard and Menu

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

## Tips for Navigating the CPM Console

When you open the ESP Console, you will notice that there are two systems of navigation: the CPM Dashboard, and a classic folder tree. Both are shown in [Figure 4-1](#).

- Display the CPM Dashboard by clicking **Dashboards > CPM Dashboard** in the Console menu.
- Switch between **Navigation Views** such as Fixlet Messages, Task, and Actions.
- Find any Task, including custom Tasks, by browsing the folder tree. Click the **Task** tab and then click **All Tasks > By Site > Trend Core Protection Module**.



**FIGURE 4-1** CPM provides a Dashboard and classic tree navigation.

4. Click a **Task** to open it and view the description.
5. Run the **Task** by clicking the link that appears below the **Action** window.
  - Target certain computers when the Task is open by clicking one of the sub-tabs that appears: **Description** (default), **Details**, **Applicable Computers**, and **Action History**.
6. Add or remove display columns by right-clicking and then selecting or de-selecting from the pop-up menu that appears.
7. Bundle configuration settings into a Task, attach it to selected endpoints, and schedule it to run automatically.
8. Use the CPM Dashboard to make your security and firewall configurations, for example, setting up the behavior of client scans.
9. Close configuration windows by clicking the X in the upper right corner.

## How CPM 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 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 Global Settings

Global settings apply to all On-Demand and Real-Time scans. You can think of them as a superset, or background, against which all scan policies and associated Tasks are applied. Global settings also apply to both virus/malware and spyware/grayware.

Set your global configurations before creating any on-demand or real-time scans, then create and deploy a Task. You can also create multiple Global Settings Tasks, which are saved in the Dashboard. For example if you want to apply different scan policies to different endpoints according to location (See [Chapter 8 for more information.](#)) In this case, you need to be mindful about keeping each global setting aligned with its corresponding scan policy and its location.

**Note:** Avoid overlapping two Global Scans on the same client when deploying. If you do, only the last deployed settings will apply, or the overlapped endpoints may constantly cycle between different applicable settings.

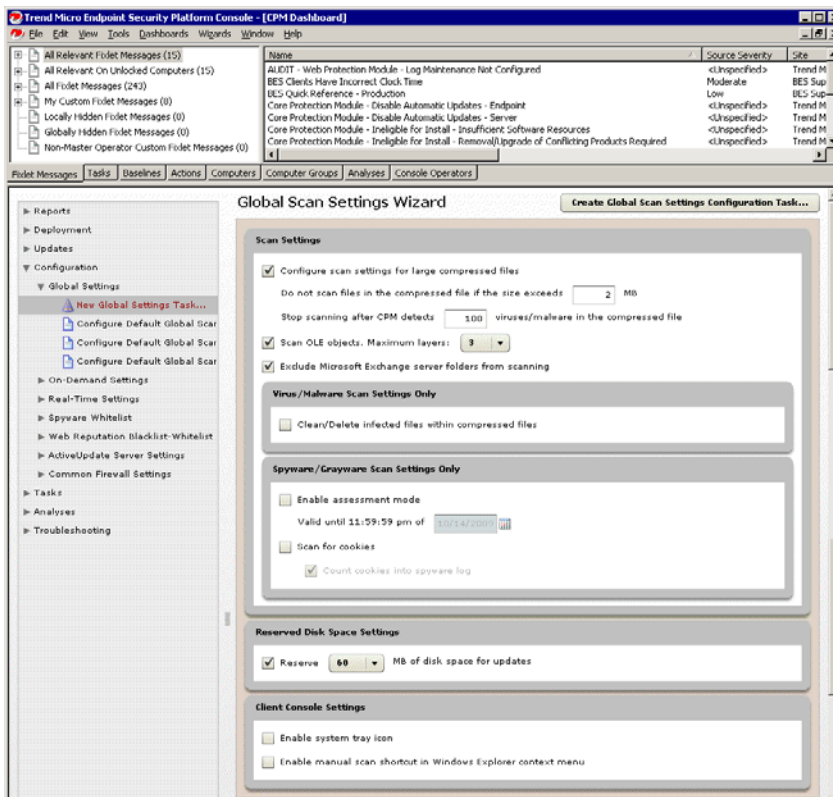


FIGURE 4-2 Configure a Task from the Global Scan Settings Wizard.

**To create a Global Settings configuration Task:**

1. In the CPM Dashboard, click **Configuration > Global Settings > New Global Settings Task**.  
The Global Scan Settings Wizard appears. (See [Figure 4-2](#).)
2. Make your configurations choices (options are detailed in: [Configure and Run Malware Scans on page 4-6](#)).
3. Click the **Create Global Scan Settings Configuration Task...** button. The **Edit Task** window opens.
4. Above the **Description** tab, name the Task and then click **OK** to accept the default **Actions** and **Relevance**. By default, the Task will be relevant to any CPM clients that do not already have the Global Setting parameters set in their registry.
5. Click **OK** to save the Task.

**To deploy the Global Settings to CPM clients:**

1. Deploy the Global Settings by clicking **Configuration > Global Settings > [scan name]** 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 that opens, click **OK** to deploy the configuration to all relevant CPM clients (by default, that is all CPM clients).
4. Check the **Action History** tab to see which CPM clients received the update or, if using multiple Tasks to deploy different sets of Global Settings, which settings are in effect for a given endpoint.

## The Global Settings Analysis

When the CPM client is installed, it includes a default configuration for Global Settings. If you have changed any of these settings and updated your clients, you will need to explicitly deploy these updates to any new computers as they are added to the network—unless you select the Target by property (recommended) rather than by computer. You can check which configuration is in place using the Global Settings Analysis.

**To enable the Global Settings Analysis:**

1. In the CPM Dashboard, click **Analyses > CPM Endpoint > Global Client Settings**.

The Analysis window opens.

2. Under **Actions**, click the link to activate the analysis, and type your private key password and click **OK** when prompted.
3. In the **Take Action** window that opens, click **OK** to deploy the configuration to all relevant CPM clients (by default, that is all CPM clients).

Core Protection Module - Endpoint Protection: Global Client Settings	
Assessment Valid Until X	<none>
Clean Compressed Files	False
Configure Scan Settings for Large Compressed Files	True
Configure Scan Settings: Do not scan if file > X MB	2
Configure Scan Settings: Stop scanning if > X virus in a compressed file	100
Count Cookies into Spyware Log	<none>
Enable Scan for Cookies	False
Enable Spyware/Grayware Assessment Mode	False
Exclude Microsoft Exchange Server Folders from Scanning	True
Reserve X MB of Disk Space for Updates	60
Scan Up to X OLE Layer(s)	3

**FIGURE 4-3** This screen shows an example Global Settings Analysis.

## Configure and Run Malware Scans

CPM provides two types of malware scans, On-Demand and Real-Time. In addition, you can schedule On-Demand scans to automatically reoccur. 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 on-demand scan runs, but do not explicitly receive notifications whenever a detection occurs on their computer.

---

**Note:** See [Show the CPM Icon on Endpoints on page 3-12](#) for information on making some detection information visible to your end users.

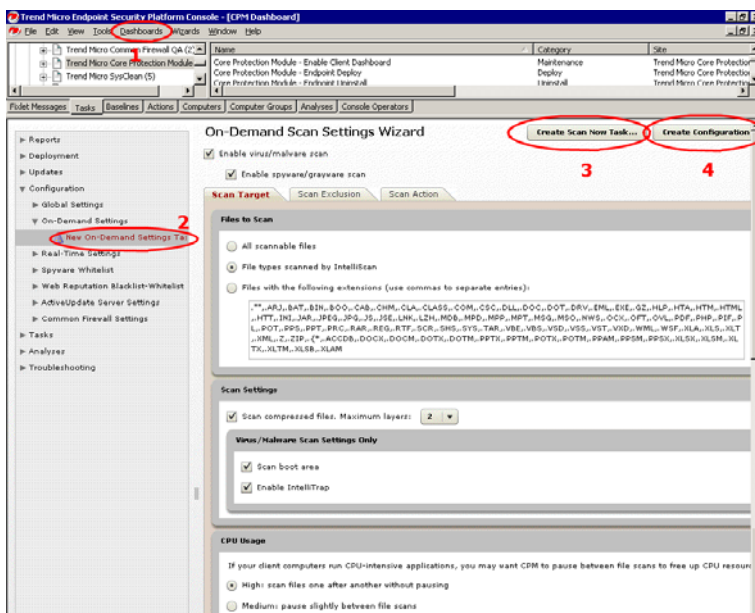
---

Detections are logged and available for review in CPM 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 may also want to configure an Offer as part of the Task. The Offer will allow 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.



**FIGURE 4-4** The numbered taskflow illustrates how to save a scan configuration as the default Task, or create custom configuration.

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

- **On-Demand scans**—Use On-Demand scans to run a one-time scan of client hard drives and/or the boot sector. Launch the default scan with the **Scan Now** Task.

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.

---

**Note:** When an end-user initiates a Manual Scan from the CPM client console, the scan settings reflect the latest settings configured by the administrator for an On-Demand Scan.

For example, an administrator might schedule an On-Demand Scan on every Thursday 12:00 PM that scans all file types. Then the administrator might run an On-Demand scan with different scan settings, maybe scanning only for .EXE files, at 14:00 PM. If an end-user runs a Manual Scan at 15:00 PM, and the administrator has not changed the settings, the end-user's Manual Scan will only scan for .EXE files, not all file types.

---

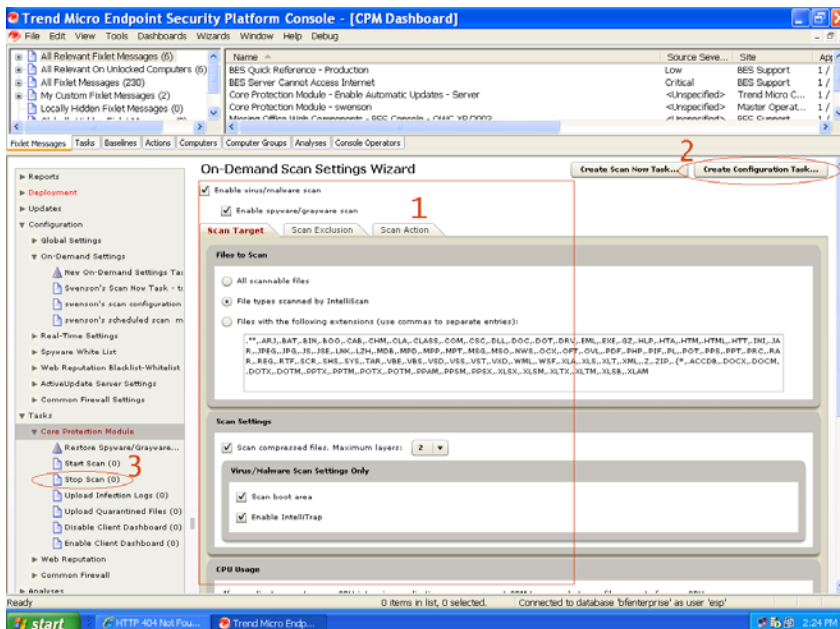
- **Scheduled scans**— You can schedule an On-Demand scan to trigger at a given time, day, or date. You can also have the scan automatically reoccur according to the schedule you set.
- **Real-Time scans**— This scan checks files for malicious code and activity as they are opened, saved, copied or otherwise 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. The relationship between these is shown in [Figure 4-5](#).

### To configure the default on 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.



**FIGURE 4-5** The scan configuration (1), is bundled into a Task (2) that is run whenever you click Scan Now (3).

2. Make your configurations choices.  
Options are detailed in: [To add spyware/grayware to the approved list: on page 4-19.](#)
3. Click the **Create Configuration Task...** button.  
The **Edit Task** window opens
4. Since this is the default **Start Scan Now** Task, keep the existing name and click **OK** to also accept the default **Actions** and **Relevance**.  
The Task is set to be relevant to all CPM clients.
5. Click **OK** 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.

## 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. Make your configurations choices (options are detailed in: [To add spyware/grayware to the approved list: on page 4-19](#)).
3. Click the **Create Scan Now Task...** button. The **Edit Task** window opens.
4. 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.
5. Select all the relevant computers and click **OK**. 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.

## 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 will run automatically according to the schedule you set. Although it will appear 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 **Configuration > On-Demand Settings > [scan name]** 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. (See [Figure 4-6](#).)
  - 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 time period suits you).

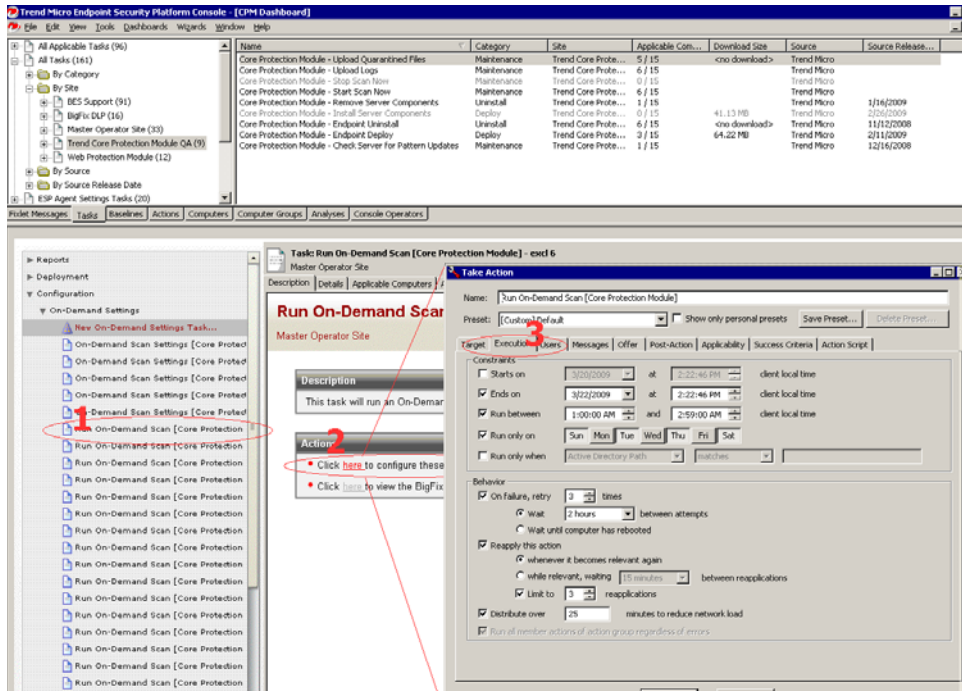
---

**WARNING!** Do not select "whenever it becomes relevant again" or the scan may 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.



**FIGURE 4-6** Schedule a complete On-Demand scan to occur weekly.

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 may 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.

Three additional points are relevant to cloud updates:

1. The endpoint will need an Internet connection. If the endpoint has a proxy configured for Internet Explorer, those settings will be automatically used.
2. As with any pattern update, following a pattern rollback, further updates will be prohibited until the rollback condition has been lifted by running the Task, **Core Protection Module - Clear Rollback Flag**.
3. The CPM client will verify 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.

## Use a Previous Pattern File Version

Problems with the scan engine and/or pattern files are very uncommon. However if a problem does occur, it is likely to be due either to file corruption or false positives (incorrect detection of malware in non-problematic files).

If a problem does arise, you can deploy an **Action** to affected endpoints that will delete the file(s) in question and replace them with a different version. This action is called a pattern rollback, and you can rollback all or selected pattern files. By default, the CPM server keeps 15 previous versions of the pattern and engine file for rollbacks (set this at the bottom of the Server Settings Wizard: **Configuration > ActiveUpdate Server Settings > Change ActiveUpdate Server Settings...**).

There are several things to bear in mind with regards to rolling back a pattern update:

1. Part of the rollback process is to lock-down endpoints to prevent any further pattern updates until the lock has been cleared. The lock serves as a safeguard against re-introducing whatever issue it was that triggered the need for a rollback. Once the issue has been resolved, either by changing something on the endpoints or by acquiring a different version of the pattern file, you will need to run the **Clear Rollback Flag Task** to re-enable updates.
2. If your clients are not all running the same version of the pattern file, that is, some have the current pattern and some have a much older version, and you perform a



rollback to the previous version, those with the current version will be *reverted* to the previous version, while those with the older version will be *updated* to the version.

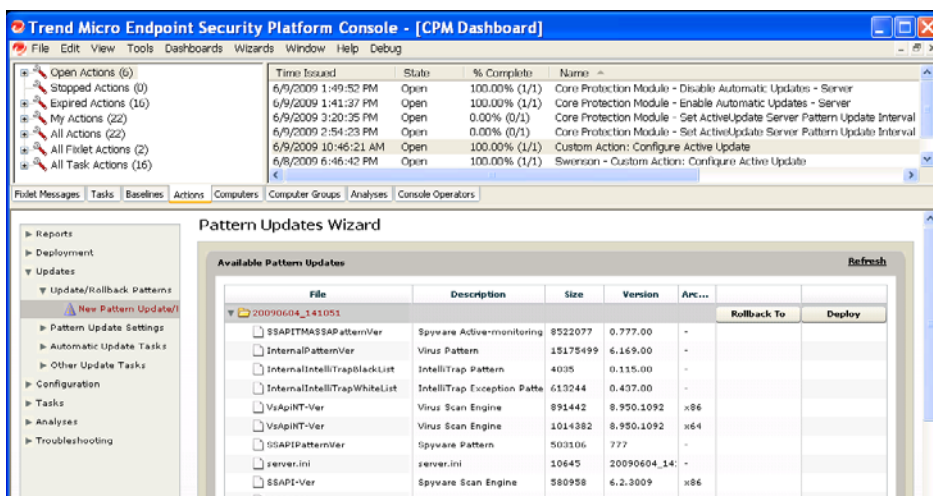
3. You can rollback all or selected pattern files. However, even if you only rollback one pattern file, you will still need to reset the rollback flag for all pattern files.

## Reverting to a Previous Version of the Pattern File

To revert to a previous pattern file:

1. In the CPM Dashboard, click **Updates > Update/Rollback Patterns > New Pattern Update/Rollback Task...**

The Pattern Updates Wizard opens.



**FIGURE 4-7** You can deploy or rollback all or selected pattern files.

2. In the list of folders that appears, click the “>” icon to expand and display the pattern files you want to rollback to, as shown in [Figure 4-7](#).
3. Click the **Rollback To** button across from the folder. In the pop-up window that appears, choose:
  - **Deploy a one time action** to open the Take Action window and the computers you want to apply this one-time Action to. Any computers included

in the **Target** that are not relevant for the Action at the time of deployment will respond with a "not relevant" statement. Click **OK**.

- **Create an update Fixlet** to open **Edit Fixlet Message** window and configure a Fixlet that will deploy the Action whenever the selected clients become relevant. When finished, click **OK** and in the window that opens, click the hyperlink that appears below **Actions** to open the **Take Action** window.
4. In the **Target** tab that opens, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
    - **Execution**—Set the time and retry behavior for the update, (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).
  5. After selecting the computers you want to update, click **OK** and when prompted, type your private key password and click **OK**.
  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.

## Re-enabling Updates Following a Rollback

After a rollback, you must clear the rollback flag setting attached to patterns on your CPM clients to re-enable manual, cloud, and/or automatic pattern updates. The same holds true even for pattern files that were not included in the rollback: all pattern files updates will be on hold after a rollback until their individual flags have been lifted. You can lift the flag on all pattern files at once or on selected files.

### To clear the rollback flag:

1. In the CPM Dashboard, click **Updates > Other Update Tasks > Clear Rollback Flag**. The **Task Description** window opens.
2. Below **Actions**, click the hyperlink to open the **Take Action** window.
3. In the **Target** tab, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
4. Click **OK**, and then when prompted, type your private key password and click **OK**. The **Action | Summary** window opens.

5. 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 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.

The screenshot shows the 'Update Settings Wizard' window in the Trend Micro Security Platform Console. The window title is 'Update Settings Wizard' and it has a 'Create Update Settings Task...' button in the top right. On the left is a navigation pane with 'New Pattern Update Settings' selected. The main area contains a table titled 'Components to Update' with columns for 'Components', 'Current Version', and 'Last Update'. The table lists various components with checkboxes for selection.

Components	Current Version	Last Update
Components		
Virus Patterns		
Virus Pattern	5.889.00	12 Mar 2009 02:12:14 +0000
IntelliTrap Pattern	0.109.00	01 Dec 2008 12:45:34 +0000
IntelliTrap Exception Pattern	0.409.00	12 Mar 2009 02:12:15 +0000
Virus Scan Engine (32-bit)	8.910.1002	01 Dec 2008 12:45:34 +0000
Virus Scan Engine (64-bit)	8.910.1002	01 Dec 2008 12:45:34 +0000
Anti-spyware		
Spyware Pattern	743	09 Mar 2009 20:21:52 +0000
Spyware Active-monitoring Pattern	0.743.00	09 Mar 2009 20:22:50 +0000
Spyware Scan Engine (32-bit)	6.1.2025	03 Dec 2008 12:45:34 +0000
Spyware Scan Engine (64-bit)	6.1.2025	03 Dec 2008 12:45:34 +0000
Damage Cleanup Services		
Virus Cleanup Template	1018	12 Mar 2009 02:12:16 +0000
Virus Cleanup Engine (32-bit)	6.0.1172	09 Mar 2009 20:22:07 +0000

**FIGURE 4-8** You can choose the pattern/engine files you want to update.

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 will include all the computers you want to deploy this Action to.
  - **Execution**—Set the deployment time and retry 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 passively notify 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.

## Exempting Programs From Spyware Detection

You can add programs that you don't want CPM to detect as spyware to the Spyware Whitelist (the whitelist is analogous to exceptions in the CPM Firewall). In addition, you can create different sets of whitelists and target them to different computers. This is especially useful, for example, if you want your Help Desk people to be able to use

certain diagnostic tools, but also want those same tools to be removed from any non-authorized computers.

**To add spyware/grayware to the approved list:**

1. In the CPM Dashboard, click **Configuration > Spyware White List > New Spyware White List Task...**  
The **Spyware White List Wizard** opens.
2. Select spyware from the reference list on the left list and click **Add** to include it in the spyware list on the right (those programs on the right will be exempted from future detection). Choose multiple names by holding the **Ctrl** key while selecting.
3. Click the button, **Create Spyware White List Configuration Task...** when you are finished selecting programs for exclusion. 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 **New Spyware White List Task...** 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 will include all the computers you want to deploy this Action to.
  - **Execution**—Set the deployment time and retry 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 passively notify 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 include in the exception, 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.

## Restoring Programs Incorrectly Detected as Spyware

CPM will keep up to 15 copies per client of the files it detects as spyware. If CPM incorrectly classified a program running on the endpoints as spyware, you can undo the action (that is, replace the file on the endpoint) by running the **Restore Spyware/Grayware...** task. Before running the restore, be sure to add the program(s) in question to the Spyware White List so the mis-detection will not occur again.

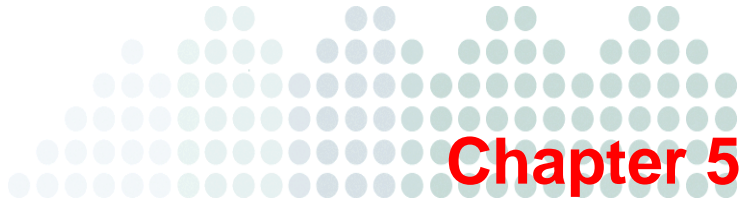
---

**Note:** If the same program was detected on many different endpoints, or if you choose to restore many different programs at the same time, it may take a while for the restoration to finish on the targeted computers.

---

### To restore files incorrectly detected as spyware:

1. In the CPM Dashboard, click **Configuration > Spyware White List > New Spyware White List Task...**  
The **Spyware White List Wizard** opens.
2. Select the snapshot(s) that contain the software you want to restore to the computers from which it was removed.
3. Click the button, **Restore Selected Snapshots...** 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.
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 will include all the computers you want to deploy this Action to.
9. 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.



## Configuration Wizards Reference

The 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 scan engine CPM usage, and designate the action to take whenever a threat is discovered. Individual scan configurations can also be saved as a Task, which is then available in the main Task List.

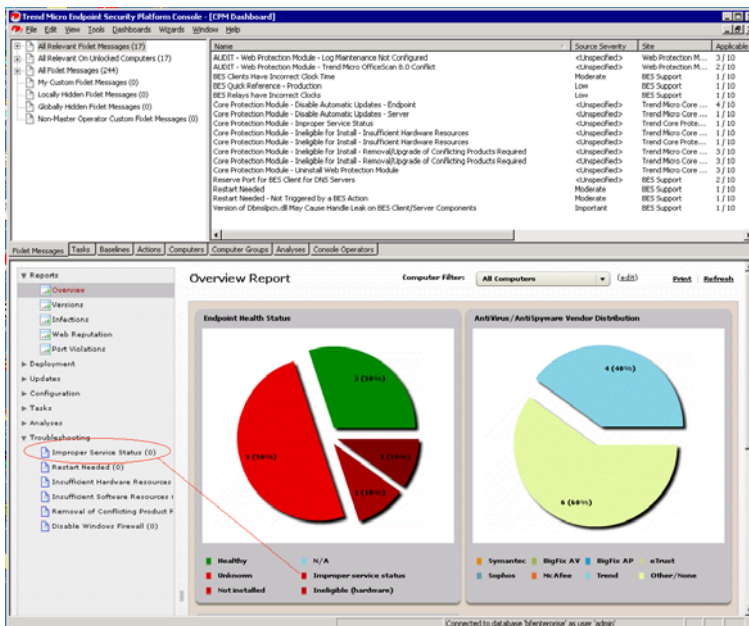
Use the CPM Health Monitor, for example, to get a quick overview of endpoint statuses or as a Troubleshooting aid.

Topics in this chapter include:

- [The CPM Health Monitor on page 5-2](#)
- [Global Scan Settings Wizard on page 5-3](#)
- [On-Demand & Real-Time Scan Settings Wizards on page 5-5](#)
- [Spyware White List Wizard on page 5-11](#)
- [ActiveUpdate Server Settings Wizard on page 5-13](#)

## The CPM Health Monitor

The CPM 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 clients on the network.



**FIGURE 5-1** The Health Monitor provides a quick overview of endpoint statuses and can serve as an impetus to Troubleshooting.

Available health status:

- **Healthy**—Computers are considered healthy if they are relevant to at least one Fixlet, Task, or Analysis in the CPM 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 client but the client has not been deployed. As such, there is no CPM information available for that endpoint.



- **Conflicting product**—The CPM 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 client is not installed. See [System Requirements starting on page 3-14](#).
- **Ineligible (software)**—CPM client is not installed. See [System Requirements starting on page 3-14](#).
- **Improper service status**—One or more client services for the ESP Agent or CPM 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 client. The CPM client may not be installed or the endpoint may be offline.
- **N/A**—The computer(s) are not relevant to any Fixlet, Task, or Analyses in the CPM Site.

## Global Scan Settings Wizard

The Global Scan Settings Wizard page contains sections for setting the following parameters:

- [Scan Settings on page 5-3](#)
- [Virus/Malware Scan Settings Only on page 5-4](#)
- [Spyware/Grayware Scan Settings Only on page 5-4](#)
- [Reserved Disk Space Settings on page 5-5](#)
- [Client Console Settings on page 5-5](#)

## Scan Settings

- **Configure scan settings for large compressed files**—CPM checks the file size and security risk count limit to determine whether to scan individual files contained in a compressed file.
  - **Do not scan files in the compressed file if the size exceeds X MB:** Some compressed files can expand to 100 or even 10,000 times their compressed size

(innocently, or maliciously, in what is known as the “zip of death”.) Scanning these files can be dangerous and inefficient.

- **Stop scanning after CPM detects X viruses/malware in the compressed file:** This option provides a reduced scan time, which can be intensive for compressed files. If a file is found to contain a lot of threats, it can be summarily deleted.
- **Scan OLE objects. Maximum layers <drop-down list>**—Object Linking and Embedding (OLE) allows users to create objects with one application and then link or embed them in a second application, creating “layers.” For example, a Microsoft Word document that contains an Excel spreadsheet, which, in turn, contains another embedded object.
- **Exclude Microsoft Exchange server folders from scanning**—Select this option to prevent CPM from scanning Microsoft Exchange 2000/2003 server folders on the client. For example, if you already use Trend Micro™ ScanMail for Exchange to protect email. For Microsoft Exchange 2007 folders, you need to manually add the folders to the scan exclusion list. For scan exclusion details, see:

<http://technet.microsoft.com/en-us/library/bb332342.aspx>

## Virus/Malware Scan Settings Only

- **Clean/Delete infected files within compressed files**—Selecting this option can slow scan processing time. For a list of secondary actions (if clean or delete fails,) see [Security Risks starting on page 11-4](#).

## Spyware/Grayware Scan Settings Only

- **Enable assessment mode**—CPM audits spyware/grayware detections. This can be especially useful for identifying and observing suspect programs for individual handling. It also prevents any service interruption that may otherwise occur during the cleaning, as well as the unexpected termination of any running processes or deleted registry keys. Assessment also allows you to recognize and exonerate files that were incorrectly detected as spyware/grayware by adding them to the Spyware White List (as described on [page 5-11](#).) If enable, set the **Valid until 11:59:59 pm of <select date>** field.

---

**Note:** Assessment mode overrides the user-configured scan action. If you have a scan action set to Clean, but have also enabled the Assessment mode, On-Demand Scans will use the Pass action and Real-Time Scans will use the Deny Action.

---

During assessment mode, CPM performs the following scan actions:

- **Pass:** (On-Demand Scans)
- **Deny Action:** (Real-Time Scans)

**Tips:**

- Avoid running the Assessment Mode for long periods because spyware/grayware will not be removed. Instead, use it for periodic evaluations.
- If unsure of the risk posed by a detected file, send it to Trend Micro for analysis.
- **Scan for cookies**—Select this option to have CPM scan and evaluate cookies.
- **Count cookies into spyware log**—Disable this option to reduce the number of spyware logs that are generated.

## Reserved Disk Space Settings

- **Reserve X MB of disk space for updates**—Sets the amount of client disk space that will be saved for CPM pattern files, scan engines, and program updates.

## Client Console Settings

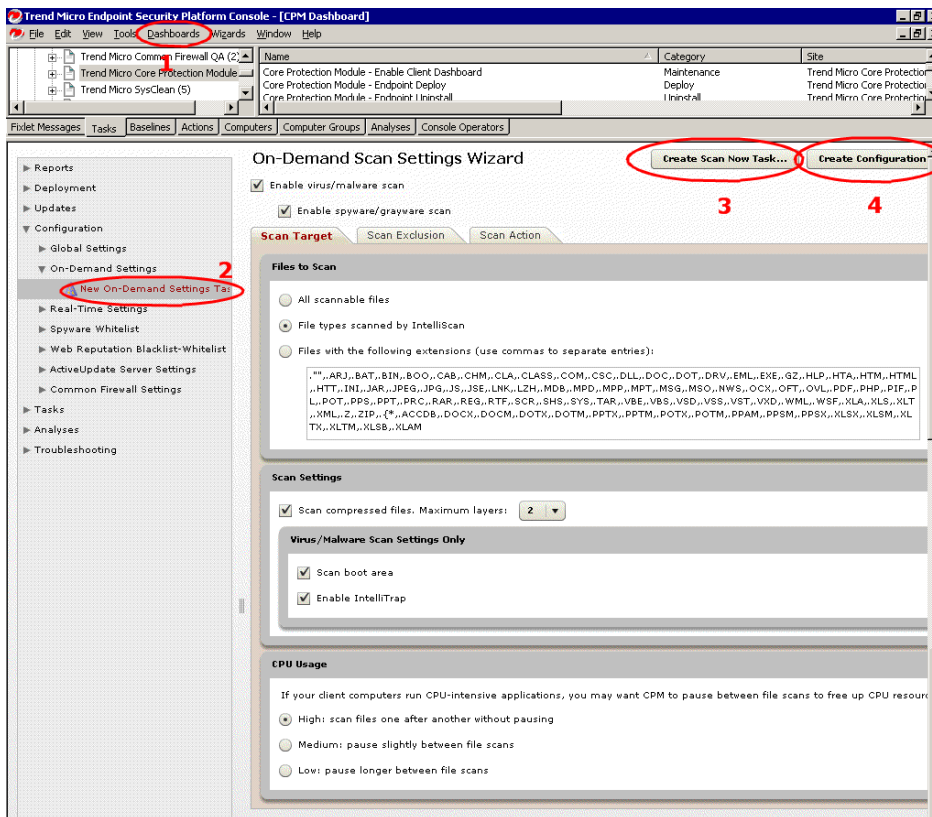
- **Enable system tray icon**—Displays the icon used to access the client console on the relevant endpoints.
- **Enable manual scan shortcut in Windows Explorer context menu**—Allows initiating a manual scan from Windows Explorer.

## On-Demand & Real-Time Scan Settings Wizards

---

**Note:** When an end-user initiates a Manual Scan from the CPM client console, the scan settings reflect the latest settings configured by the administrator for an On-Demand Scan.

For example, an administrator might schedule an On-Demand Scan on every Thursday 12:00 PM that scans all file types. Then the administrator might run an On-Demand scan with different scan settings, maybe scanning only for .EXE files, at 14:00 PM. If an end-user runs a Manual Scan at 15:00 PM, and the administrator has not changed the settings, the end-user's Manual Scan will only scan for .EXE files, not all file types.



**FIGURE 5-2** There are different scanning options available for On-Demand and Real-Time Scan.

- **Enable virus/malware scan** (recommended)—The different types of viruses and malware threats are described in [Security Risks starting on page 11-4](#).
- **Enable spyware/grayware scan** (recommended)—The different types of spyware and grayware are described in [Security Risks starting on page 11-4](#), which also contains information about excluding programs you know to be safe from spyware detection.

## 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

- **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 can not be infected.
- **File types scanned by IntelliScan**—Scans only files known to potentially harbor malicious code, even those disguised by an innocuous-looking extension name. IntelliScan examines the file meta data to determine file type.
- **Files with the following extensions**—Scans files based on their extensions. If selected, only file types listed in this field will be scanned. For example, you can specify certain file types as a shortcut to excluding all those file types not on the list.

### Scan Settings

- **Scan floppy disk during system shutdown**—Real-Time scans only.
- **Scan network drive**—Real-Time scans only. Includes client file activity as it extends to mapped network drives.
- **Scan compressed files. Maximum layers <drop-down list>**—CPM will scan up to a specified number of compression layers and skip scanning any excess layers. For example, if the maximum is two layers and a compressed file to be scanned has six layers, CPM scans two layers and skips the remaining four.

---

**Note:** Choose this option to enable scanning of the following file type: **Microsoft Office 2007 files in Office Open XML format**. These are considered compressed because Office Open XML includes ZIP compression technologies. for Office 2007 applications such as Excel, PowerPoint, and Word.

---

- **Scan boot area**—(On-Demand scans only) Scans the boot sector of the client computer hard disk.
- **Enable IntelliTrap**—Blocks real-time compressed executable files and pairs them with other malware characteristics. Trend Micro recommends quarantining (not deleting or cleaning) files when you enable IntelliTrap. Do not use IntelliTrap if your users frequently exchange real-time compressed executable files.

## CPU Usage (On-Demand Scans Only)

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

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

## Scan Exclusions Tab

To increase scanning performance and reduce false alarms, you can exclude certain files, file extensions, and directories from scanning. There are different exclusion lists for different scans. These exclusions do not apply to spyware. See [Spyware White List Wizard on page 5-11](#) to understand how to prevent false positives by excluding certain program files from spyware detection.

## AV/Spyware Scan Exclusion

By default, CPM will excludes its own directories. The recommended setting are:

- Exclude Trend Micro directories
- Exclude BigFix directories (Real-Time scans only)

Remove any conflicting antivirus products or add them to the scan exclusion list.

---

**Note:** If you are running Trend Micro ScanMail for Exchange, you can configure CPM to exclude Microsoft Exchange 2000/2003 directories from On-Demand and Real-time Scans. For Microsoft Exchange 2007, you need to manually add the directory to the scan exclusion list. For more information, see:  
<http://technet.microsoft.com/en-us/library/bb332342>.

---

## Scan Action Tab

### Virus/Malware Action

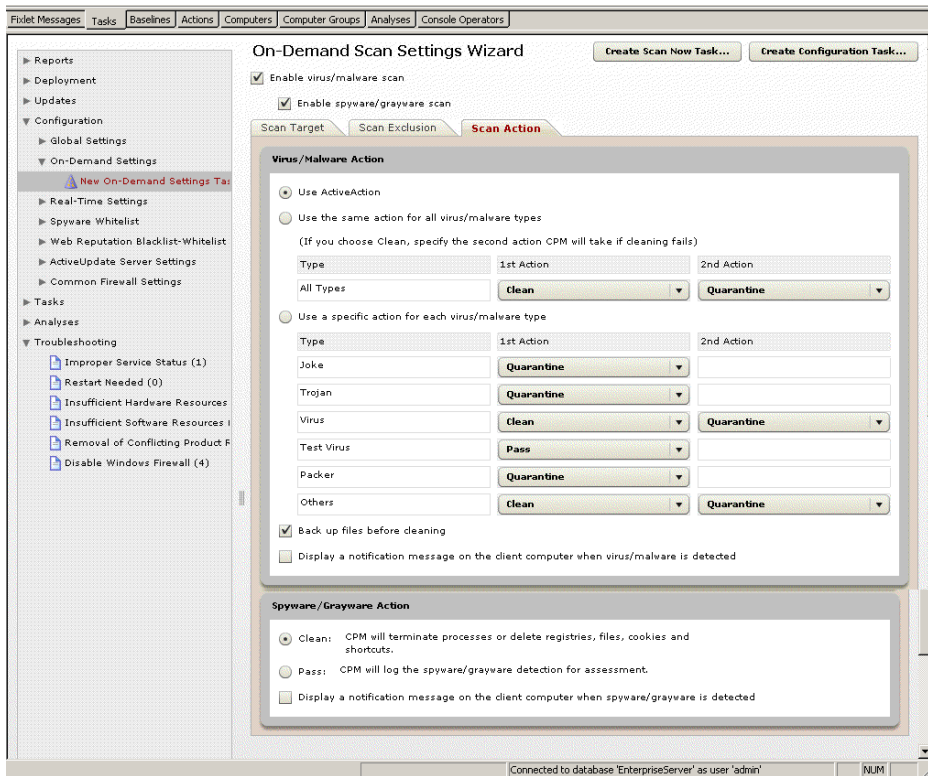
The default scan action CPM performs depends on the virus/malware type and the scan type that detected the virus/malware. For example, because Trojan horse programs cannot be cleaned (there is no virus code to remove from an infected file), the default action is to Quarantine them. The default action for viruses, however, is to clean them. If that fails, the backup action is to quarantine them.

---

**Note:** **Quarantining files**—You can have CPM quarantine any harmful files that it detects. These files will be encrypted and moved to a directory on the endpoint that prevents users from opening them and spreading the virus/malware to other computers in the network. Trend Micro provides a tool for decrypting quarantined files called `VSEncode.exe`. See [To decrypt quarantined files: on page A-6](#) for more information.

---

- **Use ActiveAction**—ActiveAction is a set of pre-configured scan actions for specific types of viruses/malware. Trend Micro recommends using ActiveAction if you are not sure which scan action is suitable for each type of virus/malware. See [Default ActiveAction Behaviors starting on page B-2](#) for a list threat types and their associated ActiveAction.



**FIGURE 5-3** Trend Micro recommends that you use ActiveAction if you are not sure which scan action is suitable for each type of virus/malware.

- **Use the same action for all virus/malware types**—If the first action fails, CPM will automatically take the second action. For example say the first action is Clean and the second is Quarantine. If CPM detects a virus but the code cannot be removed, (that is, the file cannot be “cleaned”), the file will be quarantined. See [Available Virus/Malware Scan Actions starting on page B-3](#) for more information.
- **Use a specific action for each virus/malware type**—Choose this option and specify a 1st action and 2nd action for each threat type. See [Available Virus/Malware Scan Actions starting on page B-3](#) for more information.



- **Back up files before cleaning**—CPM will encrypt the original file and make an encrypted copy on the client computer before it attempts to clean the file. For instructions on decrypting backup copies, see [To activate analyses: on page A-5](#).
- **Display a notification message on the client computer when virus/malware is detected**—Enabling this option allows CPM to display a notification message for end users to see when virus or malware has been detected on their client machine.

## Spyware/Grayware Action

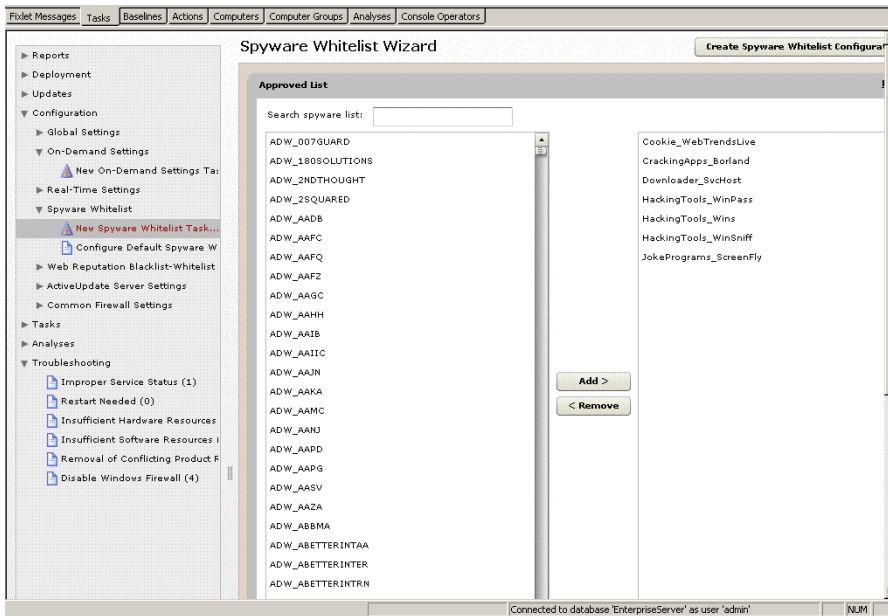
CPM performs the specified action for all types of spyware/grayware. Because spyware/grayware does not “infect” files, there are only three possible actions:

- **Clean**—Recommended. CPM terminates processes or deletes registries, files, cookies, and shortcuts.
- **Pass**—On-Demand scans only. CPM takes no action on the detected spyware/grayware, but records the detection in the logs
- **Deny access**—(Real-Time scans only.) CPM leaves the file in its original location but prevents non-Administrator users from opening, deleting, copying or moving the file.
- **Display a notification message on the client computer when spyware/grayware is detected**—Enabling this option allows CPM to display a notification message for end users to see when spyware or grayware has been detected on their client machine.

## Spyware White List Wizard

CPM classifies applications as spyware or grayware based on their function and/or on the basis of code analysis. The Spyware Whitelist allows you to prevent CPM from treating whitelisted applications as spyware or grayware. For example, say you have a utility installed on clients that performs behavior that, under a different set of circumstances, would be malicious or dangerous. You can add that file to the whitelist to allow it to run. CPM will continue to detect the file as spyware, but it will not take the configured action.

**Note:** The Spyware/Grayware Approved list will only be populated (as seen in [Figure 5-4](#)) after you have downloaded at least one set of pattern files to the server.



**FIGURE 5-4** The Spyware/Grayware Approved list is populated with names after updating the pattern file on the ESP Server.

A good way to identify which programs (innocuous and malicious) are being detected as spyware/grayware is to check your Spyware/Grayware Logs.

CPM can accommodate a maximum of 1024 spyware/grayware in the white or black lists.

## Web Reputation Blacklist-Whitelist

For information on using Web Reputation Blacklist-Whitelist, see [Blacklist and Whitelist Templates on page 6-10](#).

## 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.

The screenshot displays the 'Server Settings Wizard' window. The left sidebar shows a navigation tree with 'ActiveUpdate Server Settings' selected, and a sub-option 'Change ActiveUpdate Server' highlighted. The main content area is divided into three sections:

- Source:** Contains three radio button options:
  - Trend Micro's ActiveUpdate Server
  - Other Update Source
  - Intranet location containing a copy of the current file
 Below these are input fields for 'URL:' (pre-filled with `http://cmrnc.activeupdate.trendmicro.com/activeupdate`), 'UNC path:' (with an example `\\server_name\download`), 'User Name:', and 'Password:'.
- Proxy:** Starts with a checkbox 'Use a proxy server for pattern and engine updates'. Below it are radio buttons for 'Proxy Protocol:' (selected: HTTP, unselected: SOCKS4), and input fields for 'Server Name or IP:', 'Port (0-65535):' (pre-filled with 80), 'User Name:', and 'Password:'.
- Others:** Contains two input fields: 'Log Rolling Frequency (1-90):' (pre-filled with 10) and 'Number of Updates to Keep on Server (1-100):' (pre-filled with 15).

**FIGURE 5-5** Choose the location you will receive pattern updates from.

- **Other Update Source**—(seldom used) The default location is:  
`http://cpm15-p.activeupdate.trendmicro.com/activeupdate`  
`http://cpm-p.activeupdate.trendmicro.com/activeupdate [ver 1.0]`
- **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 above, enable this option and provide the location and proxy access credentials.

## Others

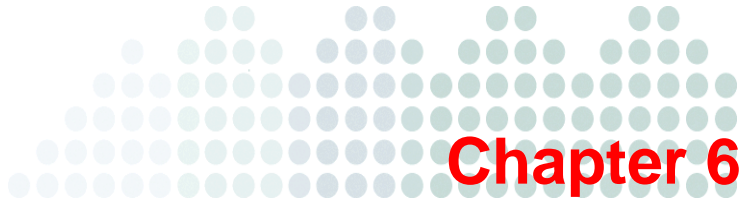
- **Log Rolling Frequency (1-90)**—To keep the cumulative size of log files from occupying too much space on the server, you can specify how many days to retain logs. The newest logs will replace oldest after this number of days. The default is 10 days. Logs are stored in the following directory:

`\TrendMirrorScript\log`

1. **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 keeps the current pattern and 15 “snapshots” of the pattern set.

## Common Firewall Settings

For more information on Common File Settings, see [Install and Manage the Client Firewall on page 7-1](#).



## Using Web Reputation

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

Topics in this chapter include:

- [How Web Reputation Works](#) on page 6-2
- [Migrating WPM Standalone Settings](#) on page 6-2
- [Web Reputation Security Levels](#) on page 6-7
- [Using Web Reputation in CPM](#) on page 6-9
- [Importing Lists of Web Sites](#) on page 6-12
- [Viewing an Existing Template](#) on page 6-14
- [About Analyses](#) on page 6-17
- [To view the Client Information Analysis:](#) on page 6-18
- [To view the Site Statistics Analysis:](#) on page 6-18

## How Web Reputation Works

The Trend Micro Web Reputation (WR) technology joins its real-time visibility and control capabilities with CPM 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 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.

---

## Migrating WPM Standalone Settings

Some customers start with an evaluation copy of Web Reputation, called the Web Protection Module (WPM), before moving to CPM. You can migrate blacklists and whitelists created in WPM standalone version to Web Reputation (WR) on CPM. The alternative is to create new lists in the WR wizard. In the wizard, you can also import lists from a text file.

---

**Note:** Perform the migration *before* you unsubscribe from the WPM site. However, Trend Micro recommends that you do not stay subscribed to both sites, and that you do not run both WPM and WR at the same time (either on the same endpoints or by having a mix of endpoints).

---

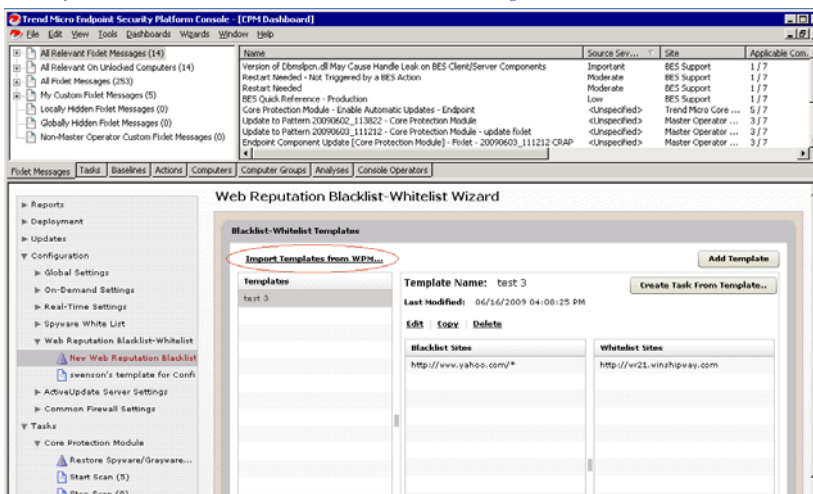
## Procedures Overview

1. Migrate black and/or white lists from WPM standalone to CPM 1.6. (See [page 6-3](#).)

2. Unsubscribe from the WPM site. (See [page 6-4](#).)
3. Uninstall WPM standalone. (See [page 6-4](#).)
4. Install or upgrade to CPM 1.6 clients on your endpoints. (See [page 6-4](#).)
5. Enable Web Reputation. (See [page 6-5](#).)
6. Redeploy your WPM policies to CPM clients. (See [page 6-5](#).)
7. Configure new proxy settings for WR. (See [page 6-6](#).)
8. Configure a default security level for new WR templates. (See [page 6-9](#).)

### 1) To migrate black and/or white lists from WPM standalone to CPM 1.6:

1. In the CPM Dashboard, click **Configuration > Web Reputation Blacklist-Whitelist > New Web Reputation Blacklist-Whitelist Task...** The Web Reputation Blacklist-Whitelist Wizard screen opens.
2. Click the link, **Import Templates from WPM...** which will only appear in the screen if you have any existing blacklists/whitelists that were created with, and currently exist on, the standalone WPM site. See [Figure 6-1](#).



**FIGURE 6-1** You can migrate existing lists from WPM standalone to CPM.

## 2) To unsubscribe from the WPM site:

Remove the standalone Web Protection Module site from the ESP Console by deleting the mastheads from the list of managed sites.

1. In the ESP Console menu, click **Tools > Manage Sites...** and select the Web Protection Module.
2. Click the **Remove Site** button, and then **OK**.
3. Enter your private key password. The ESP Server will remove the WPM masthead.

## 3) To uninstall the standalone WPM:

Before you can install or upgrade CPM 1.6 endpoints, you must uninstall any existing WPM standalone clients.

1. In the CPM Dashboard, click **Deployment > Uninstall > Web Protection Module**. The Fixlet opens, the Applicable Computers tab will show a list of endpoints that have WPM standalone installed.
2. Below **Actions**, click the hyperlink to open the **Take Action** window.
3. Choose all Applicable Computers and then click **OK**.
4. When prompted, type your private key password and click **OK**. The **Action | Summary** tab appears. Check the **Status** after a few minutes to confirm that the Action is “Fixed.”
5. Close the open windows to return to the Dashboard view.

## 4) To install or upgrade to CPM 1.6 endpoints:

1. Install or upgrade CPM 1.6 endpoints:
  - **Install**—From the CPM Dashboard, click **Deployment > Install > Install CPM Endpoints**.
  - **Upgrade**—From the CPM Dashboard, click **Deployment > Upgrade > Upgrade CPM Endpoints**.
2. Below **Actions**, click the hyperlink to initiate the deployment process and open the Take Action window.
3. Choose all Applicable Computers and then click **OK**.
4. When prompted, type your private key password and click **OK**. The **Action | Summary** tab appears.
5. Check the Status after a few minutes to confirm that the Action is “Fixed.”



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

### 5) To enable Web Reputation on your CPM clients:

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

The Task **Description** screen opens.

2. Below **Actions**, click the hyperlink to open the **Take Action** window.
3. In the **Target** tab, a list shows the CPM clients without Web Reputation installed.
4. Select all the Applicable Computers and click **OK**. 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 "Evaluating," "Running," and then "Completed."
6. Close any open windows to return to the Dashboard view.

### 6) To redeploy your WPM policies to CPM clients:

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

The Web Reputation Blacklist-Whitelist Wizard screen opens.

2. Select the template(s) you want to deploy and then click the **Create Task From Template** button.

The Edit Task window opens.

3. Modify the default name in the **Name** field so that it clearly defines the purpose of this custom Task.
4. Edit the **Description** tab to reflect your goals (if necessary).
5. Click **OK** and then enter your private key password and click **OK** when prompted.  
The Task **Description** window opens, and the new **Task** is added below **Web Reputation Blacklist-Whitelist** in the CPM Dashboard.
6. Below **Actions**, click the hyperlink to open the Take Action window.
7. In the **Target** tab, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
  - **Execution**—Set the deployment time and retry the behavior (optional).

- **Users**—This option works in combination with the Target, linked by the AND operand (both conditions must be present for the install to occur).
  - **Messages**—Configure these options to passively notify 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.
8. When finished identifying the computers you want to receive the lists, click **OK** and when prompted, type your private key password and click **OK**.
  9. The **Action | Summary** window that opens, check the **Status** 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.

### 7) To configure new proxy settings for Web Reputation:

If your endpoints connect to the Internet through a proxy server, you will need to identify that proxy and provide log on credentials. The credentials will be used by those CPM clients you target with this Action to connect to the Internet.

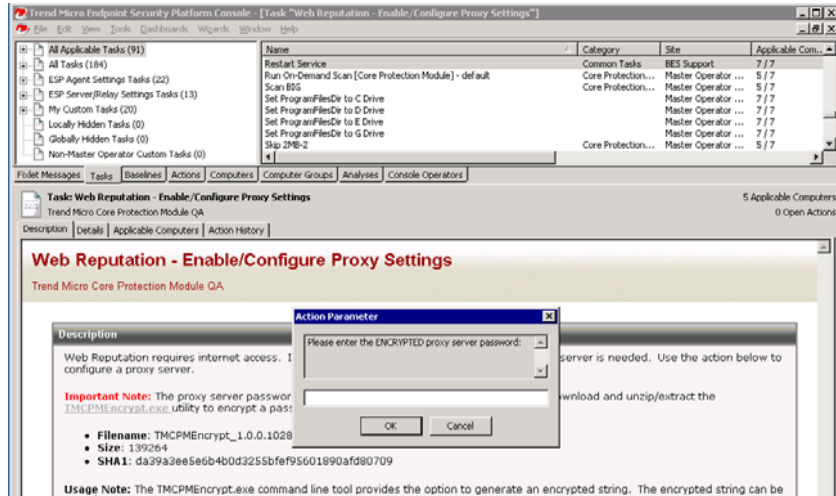
---

**Note:** You will be prompted to provide a password for the proxy server. Be sure to encrypt the password using the utility provided in the Task before deploying the Task (user name and password will be visible in the Action's Summary Details).

---

1. In the CPM Dashboard, click **Tasks > Web Reputation > Enable/Configure Proxy Settings**.  
The Task **Description** page opens.
2. Download and expand the encryption program, which will have a name such as the following: TMCPMEncrypt\_1.0.0.1038.zip.
  - a. Run the program, and when prompted, type your password in the field.
  - b. Copy the encrypted results (you will be prompted to paste them later).
3. Back in the Task **Description** window, below **Actions**, click the hyperlink and when prompted, provide the following:
  - Proxy IP address or host name
  - Proxy port
  - User name for proxy authentication

- Encrypted password (paste the password you encrypted)



**FIGURE 6-2** Paste the password you encrypted for the proxy server.

4. The **Take Action** window opens. In the **Target** tab, a list of endpoints that are running the CPM client appears.
5. Select all applicable computers (those that are running WR) and then click **OK**.
6. When prompted, type your private key password and click **OK**.
7. In the **Action | Summary** window that opens, check the **Status** after a few minutes to confirm that the Action is "Running" and then "Completed."
8. Close any open windows to return to the Dashboard view.

## 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 may 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.



**FIGURE 6-3** End users who visit a blocked site will see a message like this.

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 content may 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 spyware or viruses.

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

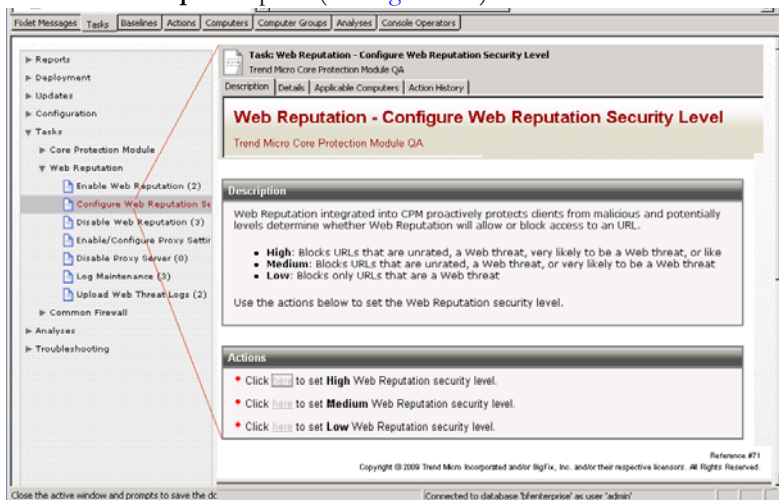
- **High**—blocks unknown, suspicious, and dangerous sites
- **Medium**—blocks dangerous and suspicious sites.
- **Low**—blocks only dangerous sites.

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

## 8) To configure a default security level:

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

The Task **Description** opens. (See [Figure 6-4](#).)



**FIGURE 6-4** You can change the security level from the default of **Low**.

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

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 2083 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. Once 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 you can create and group into templates using the 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. Once 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 may enter up to 500 URLs. You also must have “http://” before each URL entry. 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 may enter up to 499 URLs per template. You also must have “http://” before each URL entry. 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.
11. Click **Yes** to import the file. If you click **No**, to import the list you must re-launch the Wizard and perform the import process again.
12. After you click **Yes**, the Blacklist / Whitelist Wizard displays the contents of the tab associated with the file.
13. Click **Finish** to end the import process and start generating the relevant Custom Action.

---

**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 may 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:

Follow the steps below 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 completely remove the Blacklist-Whitelist template from your endpoints, follow the steps below.

---

#### **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 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 client.

- In the CMS 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 will be 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 **Trend Micro CPM** 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.

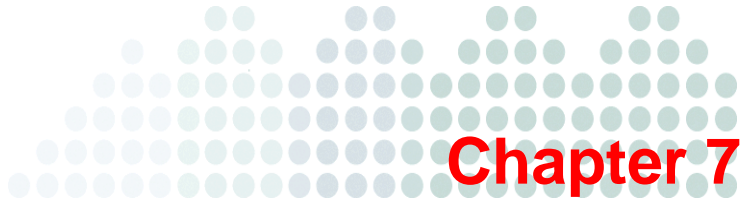
### To view the Site Statistics Analysis:

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 two Web Reputation properties you can view with the analysis:
  - Blocked Web sites
  - Visited 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.







## Install and Manage the Client Firewall

Trend Micro Core Protection Module provides an optional, policy-based CPM firewall that allows you to enable client-level firewall protection.

Topics in this chapter include:

- [About the CPM Firewall and Policies on page 7-2](#)
- [Add the Firewall Masthead to the ESP Server on page 7-2](#)
- [Remove Conflicting Firewalls on page 7-4](#)
- [Creating Firewall Policies on page 7-4](#)
- [Create and Deploy Smart Policies: Example on page 7-10](#)
- [Global Exception Rules on page 7-14](#)
- [Firewall Policy Settings Wizard on page 7-15](#)
- [Firewall Policy Configuration on page 7-17](#)

## About the CPM Firewall and Policies

The CPM firewall is optionally available with the Trend Micro Core Protection Module and allows you to enable client-level firewall protection. It is policy-based, and provides bi-directional port-control to all or selected endpoints. You can also apply policies selectively and automatically in real-time, according to the user's current IP address. For example, you can have one policy for in-office network connections and another for unsecured connections such as in an airport. The appropriate policy will automatically be applied as the end-user changes location.

The firewall configuration is not available from the ESP Console by default; you need to add the firewall site before the Wizard will appear in the CPM Dashboard. Firewall policies are automatically enabled and active when you deploy them to the endpoints. There are no installation steps required.

Several examples of the firewall versatility are worth pointing out. Procedures for each appear later in this chapter:

- **Uniform security**—You can create a policy, apply it to all your endpoints, enable one or more of the global exceptions, and then deploy the policy to all your endpoints in just a few minutes.
- **Targeted security**—You can create multiple policies, each with a different set of ports enabled, and then use different Tasks to selectively target the different policies to different endpoints.
- **Smart (flexible) security**—You can create two policies, each with different rules, and create two Tasks, each of which deploys one of the policies to the same endpoints. By attaching a different Location Property to each Task prior to deployment, the targeted endpoints will receive both policies. Whenever conditions on an endpoint change to those set for one of the Locations, the policy in affect for that endpoint will also change. In this way, you can create different policies for the same computer, and they will automatically adapt to different conditions.

## Add the Firewall Masthead to the ESP Server

Install the Trend Micro Common Firewall by adding its site masthead to the list of managed sites in the ESP Console. If you do not have the Common Firewall masthead, contact your Trend Micro sales representative to obtain it.

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 will remain pending until the connection is made.

### To add the CPM Firewall site:

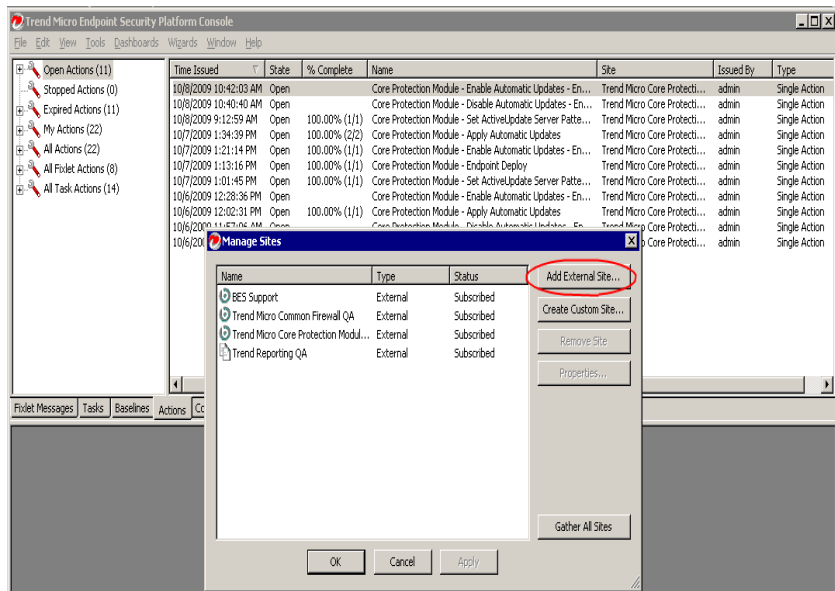
1. In the ESP Console menu, click **Tools > Manage Sites...** and then the **Add External Site...** button.

The **Add Site** window opens.

2. Locate and select the Common Firewall masthead file you received from Trend Micro:

Trend Micro Common Firewall.efxm (optional)

The selected masthead appears in the Manage Site window as shown in [Figure 7-1](#).



**FIGURE 7-1** Add the firewall site to make it available in the ESP console.

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

The ESP Server will begin gathering the files and content associated with the masthead you added and install them on the server.

## Remove Conflicting Firewalls

You should only deploy the CPM firewall on endpoints that do not have another firewall installed, regardless of whether that firewall is active (for example, the driver and services may continue to load, although no firewall policies are in place).

If the endpoints to be protected already have a firewall such as Windows Firewall installed, you need to open port 52311 to allow the ESP server to communicate with the endpoint before enabling the CPM firewall.

CPM provides a Fixlet for disabling the Windows Firewall. For other firewalls, you can use the same program that was used to install it to uninstall it, or create a custom Fixlet.

### To disable the Windows firewall:

1. In the CPM Dashboard, click **Troubleshooting > Disable Windows Firewall**.  
The Task **Description** opens.
2. Below **Actions**, click the hyperlink to open the Take Action window.  
A list of the endpoints that are running the Windows Firewall appears under the **Target** tab.
3. Select all Applicable Computers and 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.

## Creating Firewall Policies

Configure firewall settings for your endpoints by creating one or more firewall policies in the Firewall Policy Settings Wizard. Next, create a Task to deploy the action. Structure the policy to Allow or Deny all inbound and outbound network connections by setting the Security Level. A security level of High creates a default behavior of Deny for all ports, while Low does the opposite. From there, you can add individual port exceptions

and/or use any of the 30 pre-set exceptions for common ports (such as HTTP, FTP, SMTP) that are available as Global exception rules. Completed policies are available in the Policy List. You can select one or more policies from the list to include in a Task for deployment to the endpoints you specify.

## Governing Logic

There are several sets of logic that affect policy targeting. When creating and deploying a firewall policy, the chronological order is:

- Create a policy.
- Add it to a task.
- Deploy it

The endpoint, which makes the final determination of relevance, is more-or-less autonomous.

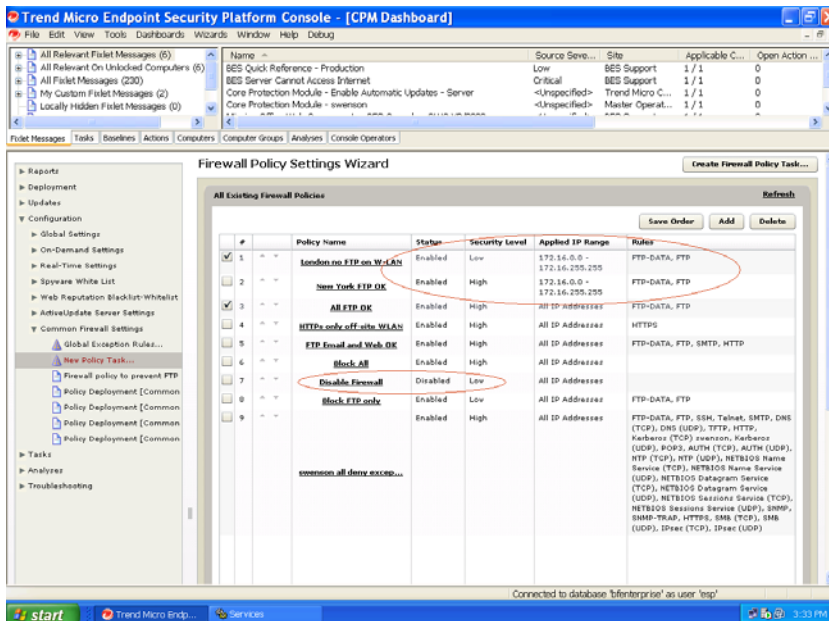
Irrespective of this chronology, however, is the determination of applicability. Whether or not a given policy is in fact applied to a given endpoint is determined by the population of endpoints that remains after configuring the Task and Action. This is important because it means that simply including an IP address in a firewall policy does not mean that the IP address will receive the policy.

The list below shows the order of inheritance. The Task defines the population within which the Action can occur, and the Action defines the population within which IP addresses defined in the policy can occur. The Policy sets the population of IP addresses available for the Task. Knowing exactly which endpoints will ultimately receive your policy can be complex.

To determine which endpoints receive a policy depends on:

1. **The Policy List**—Only one policy will ever be in effect for a given client at a given time. The policy in effect is the first policy on the policy list that contains the IP address of a targeted endpoint. This condition makes the order of policies in the Policy List significant. Evaluation occurs from the top down and stops once a policy has been found that applies to an endpoint IP addresses. Always put policies that specify fewer than “All Possible IPs” above those that specify all IP addresses

(which is, typically, most if not all policies). If you do not, the policy that includes specific IP addresses will never be applied.



**FIGURE 7-2** Firewall policies are evaluated in top down order.

2. **The Policy**—Within a firewall policy, include all possible IP addresses or a range of IP addresses. Policy IP addresses will always be limited to the population of IP addresses defined in the Task that deploys it.
3. **The Task**—You can make the Task relevant to all or certain computers. By default, tasks created for a firewall policy will use a relevance statement that is made up of conditions from the firewall policy.
4. **The Action**—When you deploy a Task, you select your targets from the population of endpoints made available in the Task. You can reduce the population of endpoints to those that you want the policy to target, and the conditions under which you want the policy to apply. For example, you can filter the possible endpoints by selecting a different target, by defining user eligibility, or by setting execution or offer conditions.

5. **The Endpoint**—The ESP Agent installed on the endpoint keeps a detailed list of computer-specific parameters against which it continuously evaluates the relevance statements of all Tasks deployed to it. If the endpoint finds that it is not relevant, it will not incorporate the policy. This is significant when you deploy multiple firewall policies to co-exist on the same endpoint (as opposed to one policy replacing another). The endpoint selects which policy to apply based on its current status, for example, the IP address it is currently using to connect to the network.

## Policy Verification

It is possible to create a condition wherein no policies are applied to a given IP address, or the wrong policy is inadvertently applied to a given IP address. Trend Micro recommends that following deployment, you confirm your policy coverage by using a port scanning program such as Nmap (<http://nmap.org>) to verify that the policy has been applied to the computers and ports and is functioning as you expect.

## Global Exceptions

You can add rules from the Global Exceptions list to individual firewall policies. These rules are available when you create a new policy, however, only those rules that you have actually enabled in that policy will remain after you save it.

**FIGURE 7-3** You can add or remove rules from the Global Exception Rules list.

Global Exception Rules are not altered by editing a rule from within a policy. Add or edit rules in the Global Exception list to have the change available for all new policies

(global exception rules already attached to a policy will not change, even if they are edited in the rule list).

One other point to keep in mind is that global exception rules have a pre-defined action, either Allow or Deny. Be sure this action agrees with the fundamental construct of your policy. For example, if you set the policy **Security Level = Low**, that is, allow traffic to and from all ports, you need to change any exception rules imported from the global list to *Deny* traffic for your exception ports. See [Global Exception Rules on page 7-14](#) for configuration details.

## Create and Deploy a Firewall Policy

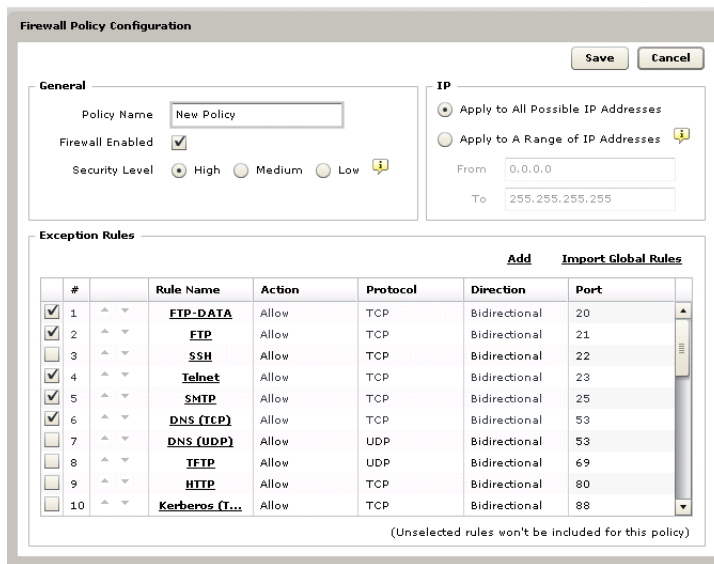
The procedure below is for creating a single firewall policy that will be applied to all endpoints. You can use these same instructions to create multiple policies and target them to different endpoints. The difference occurs according on the policies you enable in the Policy List when creating a Task, and the computers you target with that Task. See [Firewall Policy Configuration on page 7-17](#) for details.

### To create a firewall policy:

1. In the ESP Console menu, click **Common Firewall Settings > New Policy Task...**  
The Firewall Policy Settings Wizard appears.
2. Click the **Add** button, and in the window that appears, give the policy a name that will make its function clear when it appears in the Policy List.
3. Configure the following:
  - **Firewall Enabled**—This option must be selected for the policy to be “on.” In addition, the policy must be selected in the Policy List. *Both* conditions must apply for the policy to be used.
  - **Security Level**—
    - Choose **High** to block all traffic to all ports, and then use Exceptions to enable specific ports (inbound, outbound, or both.)
    - Choose **Medium** to block all inbound traffic to all ports, but allow all outbound traffic to all ports; use Exceptions to alter specific ports. To achieve the opposite, choose High and create a single exception rule to Allow all inbound traffic for all ports (and enable this rule in the Exception Rules list).



- Choose **Low** to allow all traffic to all ports, and then use Exceptions to block specific ports (inbound, outbound, or both.)
- **Apply to All Possible IP Addresses**—Choose this option for most cases. An IP address is “possible” only if it is also included in the Task.



**FIGURE 7-4** Create a firewall policy and add exceptions, if any.

- **Apply to A Range of IP Addresses**—Only use this option if you are creating a policy to bind to one of several possible IP addresses that an endpoint may use (due to Dual NICs, variable locations, etc. as described in [Create and Deploy Smart Policies: Example on page 7-10](#))
- **Exception Rules**— Only enabled rules will be included in the policy. Select an existing rule from the list of Global Exception rules that appears, or add a new one. In either case, be sure your exceptions are in fact the opposite of the Security Level you have set for the policy. For example, the default action for most rules in the Global Exception list is Allow. Enabling this rule for a policy where Security Level = Low would produce no effect.

- **Rule Name**—Click an existing rule to modify it. Any modifications made to a global rule from within the policy will apply only to that policy (the global rule itself will not change).
  - **Add**—Click this button to create and enable a new exception rule.
  - **Import Global Rules**—Click this button to repopulate the Exception Rules list with exceptions from the Global Exception Rules list.
4. Click **Save**. The Firewall Policy List becomes active.

#### To deploy the firewall policy to endpoints:

1. Enable the policy you just created in the Policy List by selecting it. All enabled policies will be bundled into the Task when you create it. Disable any policies in the list that you do not want in the Task. (Deleting a policy will make it unavailable for other Tasks.)
2. Move your policy to the top of the list and click the **Save Order** button.
3. Click the **Create Firewall Policy Task...** button at the top of the screen.  
The Policy Deployment **Description** appears.
4. Accept the defaults and click **OK**. When prompted, type your private key password and click **OK**. The Task **Description** window appears.
5. Below **Actions**, click the hyperlink to open the Take Action window, which opens to the **Target** tab.
6. Click **Applicable Computers** or whichever option will include all endpoints with the firewall installed.
7. Click **OK**, and when prompted, type your private key password and click **OK**.
8. 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.”
9. Close any open windows to return to the Dashboard view.

## Create and Deploy Smart Policies: Example

In this procedure you will create four firewall policies, one for each of the policy goals listed below.

**Usage scenario:** Endpoints are comprised of desktop computers and laptops. All are running the CPM Firewall. Desktops have a single, wired, LAN. The laptops have both a LAN and W-LAN. The laptops, being mobile, often travel to different corporate offices

(London and New York). In addition, they are used outside the corporate network (Airport.)

Create one firewall policy for each of the following cases:

- **Policy 1**—Prevent wireless FTP connections in London
- **Policy 2**—Allow wired and wireless FTP connections in New York
- **Policy 3**—Allow wired FTP connections in London and New York
- **Policy 4**—Prevent all but HTTPS connections in unknown locations (wireless)

When targeting specific IP addresses in a firewall policy, be sure that the IP address ranges specified are mutually exclusive— that the same IP address is not included in related policies.

- **London** = 10.10.0.0–10.10.255.255
- **New York** = 192.168.0.0– 192.168.255.255
- **Unknown** = Not London or New York

#### To create a policy for each case:

The steps for creating the first policy are provided below. Repeat steps 2 and 3, modifying as needed, to create the remaining three policies.

1. In the ESP Console menu, click **Common Firewall Settings > New Policy Task...**

The Firewall Policy Settings Wizard appears.

2. Click the **Add** button, and in the window that appears, give the policy a name that will make its function clear when it appears in the Policy List, for example, *No FTP over W-LAN in London*. The Firewall Policy Configuration screen opens.
3. Configure the following (see [Firewall Policy Configuration on page 7-17](#) for configuration details):
  - Select **Firewall Enabled**
  - Select **Security Level = High** to block all traffic to all ports
  - Select **Apply to A Range of IP Addresses** and enter the IP address range for London, **From:** 10.10.0.0 **To:** 10.10.255.255.
    - If in fact you have a location that includes multiple ranges, create a parallel firewall policy for each range (differentiate the name by adding a number).

- If you are using a subnet to represent the location, enter the subnet IP in both the From: and To: fields.

---

**Note:** Subnet notations such as 172.16.0.0/16 and 172.16 are not supported.

---

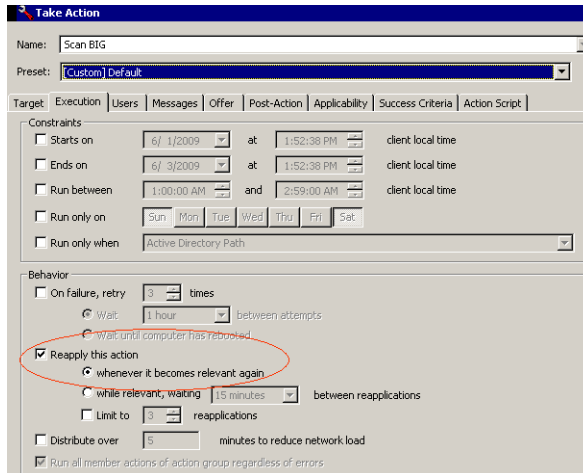
- From the **Exception Rules**, enable FTP-Data and FTP.
4. Click **Save**. The Firewall Policy List becomes active.

#### **To create Tasks for the different locations:**

In this procedure, you will create different Tasks and include in them different combinations of the policies created above. The combinations you select for a Task are important, as they determine the policies a given endpoint will have available to use.

1. In the Firewall Policy Settings Wizard screen, do the following:
  - a. Be sure the policies are ordered correctly, that is, put the policy with an IP address range above the one for all IP addresses.
  - b. Select both London policies (Policies 1 and 3).
    - For New York, use Policies 2 and 3
    - For Unknown, use Policies 1, 2, and 4
2. Click the **Create Firewall Policy Task...** button at the top of the screen.  
The Policy Deployment **Description** appears.
3. In the **Name** field, give the Task descriptive name, such as *Firewall policy to prevent FTP over WLAN at London office*.
4. Below **Description**, edit the text to provide, for example, the rationale for the policy to other console operators.
5. Below **Actions**, edit **Link 1**. For example, Click \_\_\_ to deploy firewall policy.
6. Click **OK** to close the windows, and when prompted type your private key password and click **OK**.  
The Task **Description** window appears.
7. Below **Actions**, click the hyperlink to open the Take Action window.
8. Click **Applicable Computers** or whichever option will include all endpoints with the firewall installed.

9. Click the **Execution** tab to make it active. 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.**



**FIGURE 7-5** Choose “Reapply this action” so the endpoint Agent will always monitor its IP address relative to the firewall policies in the Task.

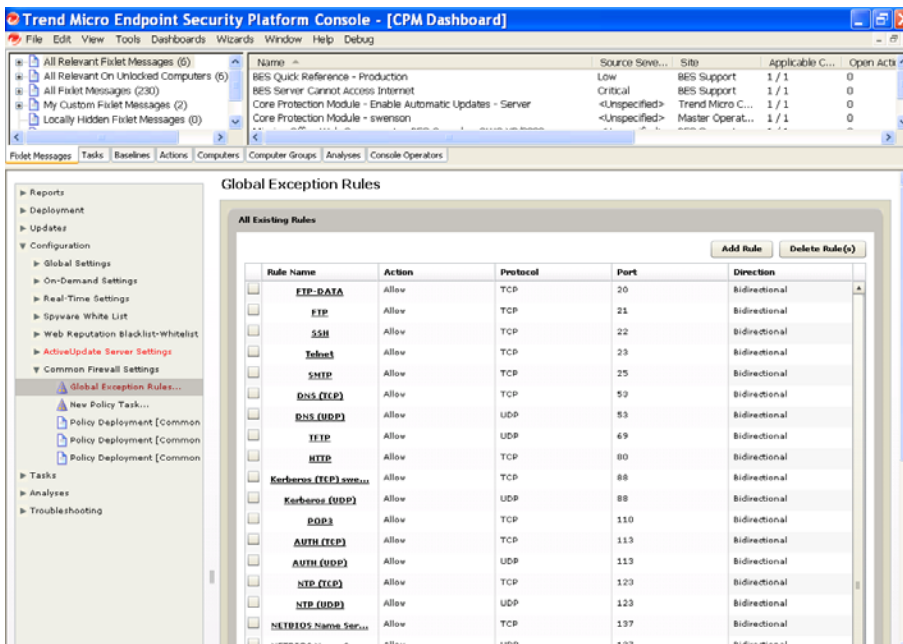
10. Click **OK**, and when prompted, type your private key password and click **OK**.
11. In the **Action | Summary** window that opens, check the **Status** and **Count** after a few minutes to confirm that the Action is “Running” and then “Completed.”
12. Close any open windows to return to the Dashboard view.

## Global Exception Rules

The list of 30 or so default global exception rules appears whenever you create a new firewall policy. You can use the rules to quickly add commonly used UDP and TCP ports to your policy, for example, those used for SMTP, FTP, and HTTP traffic.

## All Existing Rules

You can add, modify, or remove unused exception rules from the global list.



**FIGURE 7-6** Global Exception Rules are available in new policies. Once attached to a policy, the rule will not change within that policy.

New rules and those modified in the Global Exceptions Rules list are available to all new policies. However, if from within a policy, you modify a rule imported from the Global Exception Rules list, that modification will not be applied to the global rule. Likewise, if

you modify a rule in the global list, any version of that rule that has been saved in an individual policy will not change.

#### To add or change global exception rules:

1. In the ESP Console menu, click **Common Firewall Settings > Global Exception Rules...**
  - Click a Rule **Name** in the list to open that rule for editing.
  - Click the **Add** button to create a new rule.
  - Click the **Delete Rule(s)** button to remove selected rule(s).
2. When finished, click the **Save Rule** button.

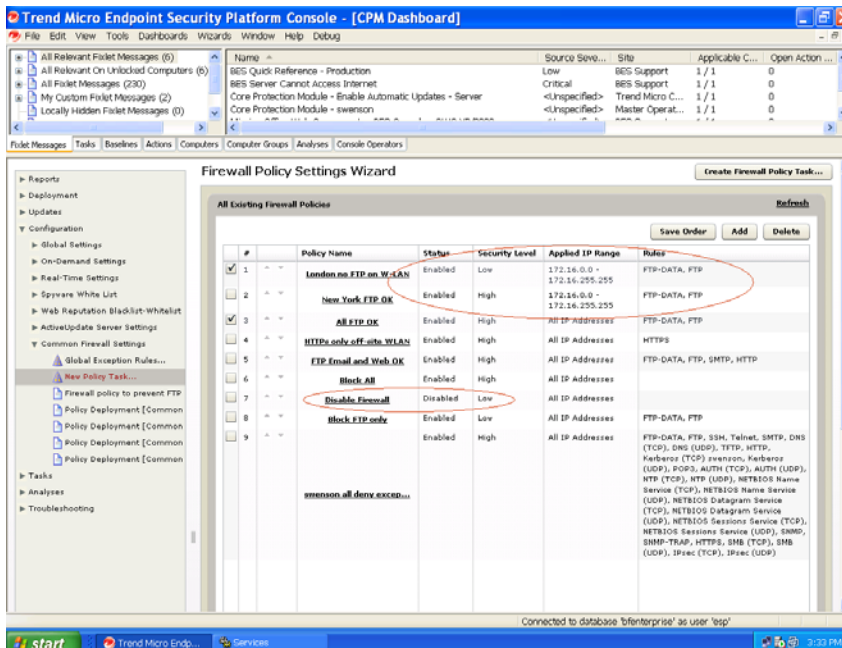
## Firewall Policy Settings Wizard

Use the Firewall Policy Settings Wizard to create one or more firewall policies. You can structure the policy to Allow or Deny all inbound and outbound network connections by setting the Security Level, and then individual port exceptions. Completed policies appear in the Policy List, as shown in [Figure 7-7](#). Select policies from the list to include in a Task and deploy to your endpoints.

The following buttons and functions are available in the Firewall Policy Settings Wizard:

- **Create Firewall Policy Task**—Only policies that have been bundled into a Task can be deployed to endpoints. You can apply different policies to different endpoints by creating multiple Tasks.
- **Save Order**—Because the firewall evaluates applicability by starting at the top of the list and working down, put policies with a smaller Applied IP Range above those that apply to All IPs. Save the order often to avoid losing your changes.
- **Add**—Use this button to create a new policy. You must also select the policy before using it in a Task.
- **Delete**—Select one or more policies from the list and then use this button to remove them. Only use Delete to remove the policy from any further use; disable any policies that you do not want to include in a given Task.

- **Open an existing policy**—Click the **Policy Name** to open an existing policy for viewing or modification. Changes will not be applied to endpoints until you re-deploy the policy.



**FIGURE 7-7** These example firewall policies cover roving endpoints, disabling the firewall, and targeting different policies to different endpoints.



## Firewall Policy Configuration

Create or modify a firewall policy by clicking the **Add** button or a Policy Name in the policy list. The options are explained below.

**Firewall Policy Configuration**

**General**

Policy Name:

Firewall Enabled:

Security Level:  High  Medium  Low

**IP**

Apply to All Possible IP Addresses

Apply to A Range of IP Addresses

From:

To:

**Exception Rules**

[Add](#) [Import Global Rules](#)

#	Rule Name	Action	Protocol	Direction	Port
<input checked="" type="checkbox"/> 1	<b>FTP-DATA</b>	Allow	TCP	Bidirectional	20
<input checked="" type="checkbox"/> 2	<b>FTP</b>	Allow	TCP	Bidirectional	21
<input type="checkbox"/> 3	<b>SSH</b>	Allow	TCP	Bidirectional	22
<input checked="" type="checkbox"/> 4	<b>Telnet</b>	Allow	TCP	Bidirectional	23
<input checked="" type="checkbox"/> 5	<b>SMTP</b>	Allow	TCP	Bidirectional	25
<input checked="" type="checkbox"/> 6	<b>DNS (TCP)</b>	Allow	TCP	Bidirectional	53
<input type="checkbox"/> 7	<b>DNS (UDP)</b>	Allow	UDP	Bidirectional	53
<input type="checkbox"/> 8	<b>FTTP</b>	Allow	UDP	Bidirectional	69
<input type="checkbox"/> 9	<b>HTTP</b>	Allow	TCP	Bidirectional	80
<input type="checkbox"/> 10	<b>Kerberos (T...</b>	Allow	TCP	Bidirectional	88

(Unselected rules won't be included for this policy)

**FIGURE 7-8** Select policies to include in a Task by choosing them in the Firewall Policy Configuration screen.

The following options are available in the Firewall Policy Configuration screen:

### General

- **Policy Name**—The name you type here will appear in the firewall policy list. Once saved, it cannot be changed. Use a name that will make the purpose of the policy clear.
- **Firewall Enabled**—Selected by default, only disable this option in a policy to uninstall the firewall from your endpoints (the Task must be deployed).
- **Security Level**—This option sets the predisposition of the policy, that is, whether it Allows or Denies all traffic to all ports. You can then fine-tune the policy by adding port exceptions (these exceptions should, of course, be the inverse of the action set through the Security Level).

## IP Address

- **Apply to All Possible IP Addresses**—This is the correct choice for most firewall policies. *Possible* IP addresses refers to the limits inherited through the creation of the Task, Policy Action, and the endpoint's own relevance evaluation.
- **Apply to A Range of IP Addresses**—This option is available for creating location-aware policies. Be sure to move these policies to the top of the Policy List to prevent the policy from being missed.

## Exception Rules

All exceptions rules are policy-specific. Exceptions created within a policy are not be available globally. Add them in the Global Exceptions screen.

- **Add** button—Opens a screen for creating a new exception rule that will be unique to the policy. Exceptions that you add will automatically be selected, that is, enabled in the policy. Note that if you disable the exception and save the policy, the exception will be removed from the policy. See more information in [Exception Rules Configuration on page 7-18](#).
- **Import Global Rules** button—Repopulates the Exception Rules list with all exceptions from the Global Exception Rules list (including the defaults and any that you have added). This can be especially useful if you later re-open the policy and want to add additional exceptions (those not included the first time will no longer appear in the list).
- **Editing existing rules**—Modifications made to rules within a policy apply only to that policy, even if the rule is one of the Global Exception Rules.
- **Selecting exception rules**—Select exceptions to include them in a policy.

## Exception Rules Configuration

Add a custom exception rule to the firewall policy by clicking the **Add** button. Click an existing exception rule to open the rule for editing. The options are explained below.

- **Name**—The name you type here will appear in the Exception Rules list. Once saved, it cannot be changed. Use a name that will make the purpose of the policy clear.
- **Actions**—Deny/Allow. Choose an action that contradicts the prevailing disposition of the policy as set by the Security Level.

- **Protocol**—Select TCP/UDP to affect all traffic on the port, the typical assumption. Otherwise, to block or allow a specific application, match the protocol and port.

**Direction**—Inbound/Outbound or both. Blocking inbound traffic, for example, can prevent unauthorized access on the endpoint, while blocking outbound traffic can be used thwart malicious spyware or programs such as file sharing.

**FIGURE 7-9** Exception rules created within a policy will apply only to that policy. If the rule is later modified, it will not take effect on the targeted endpoints until the policy has been re-deployed.

- **Ports**— (ports 0-1023 are “well-known,” 1024-49151 are registered ports, and those above 49151 are dynamic or private ports.)
  - **All ports**—Includes ports 1 through 65535
  - **Range**—Create multiple, parallel exception rules to include a number of different ranges.
  - **Specified port(s)**—Do not use zero or invalid input such as non-whole numbers.

## Uninstalling the Common Firewall

If you decide not to use the firewall, there is no application that you need to remove, or anything that gets uninstalled. Instead, you simply create a policy with the firewall disabled and deploy it in a Task. In addition, you can remove the CPM firewall site from the ESP Console. Both procedures are provided in the sections that follow.

## Disabling the Firewall from Endpoints

You can disable the CPM firewall by deploying a policy with a disabled firewall status to your endpoints. When you deploy a disabled firewall, the policy will override any existing policy already in effect on the clients. Only one policy with the firewall disabled can be included in any Task.

### To disable the firewall:

1. In the ESP Console menu, click **Common Firewall Settings > New Policy Task...** The Firewall Policy Settings Wizard appears.
2. Click the **Add** button, and in the window that appears, give the policy a name such as *Disable Firewall*.
  - Clear the check from **the Firewall Enabled** check box.
3. Click **Save**. The Firewall Policy List becomes active.
4. Select the policy you just created in the Policy List and clear the check from any other policies if necessary.
5. Click the **Create Firewall Policy Task...** button at the top of the screen. The Policy Deployment **Description** appears.
6. Accept the defaults and click **OK**. When prompted, type your private key password and click **OK**. The Task **Description** window appears.
7. Below **Actions**, click the hyperlink to open the Take Action window.
8. In the **Target** tab that opens, click **Applicable Computers** or whichever option will include all endpoints with the firewall installed.
9. Click **OK**, and when prompted, type your private key password and click **OK**.
10. 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.”
11. Close any open windows to return to the Dashboard view.

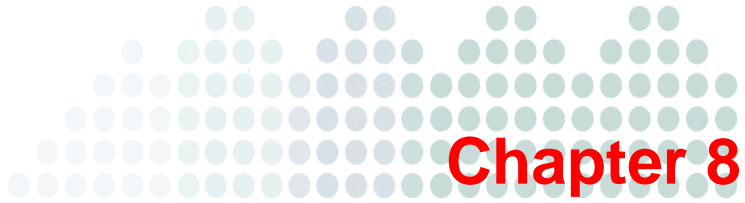
## Removing the Firewall Site

Remove the Common Firewall site from the ESP Console by deleting the masthead from the list of managed sites.

**To remove the firewall masthead:**

1. In the ESP Console menu, click **Tools > Manage Sites...** and select the Trend Micro Common Firewall.  
The **Remove Site** button becomes enabled.
2. Click **Remove Site**, and then the **OK** button.
3. Type your private key password and then click **OK** to remove the firewall components.





## Setting Up and Using Locations

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

Topics in this chapter include:

- [Overview on page 8-2](#)
- [Creating Locations on page 8-2](#)
- [Creating Location-Specific Tasks on page 8-5](#)
- [How Location Properties Work on page 8-6](#)
- [To create a location property: on page 8-3](#)

## Overview

You can have ESP apply different CPM 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 not uncommon. 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 computer will automatically pick up the correct security policy for the new location.

This same idea also applies to firewall configurations, and other CPM 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 might have a different set of rules. In Germany, there may be completely different rules for both wired and wireless connections - two locations, but four sets of rules that may apply.

## Creating Locations

Use the ESP Location Property wizard to create one or more named properties which allow 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 may 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 dynamically map retrieved client properties using a key/value set. See the *ESP Administrator's Guide* for more information.



---

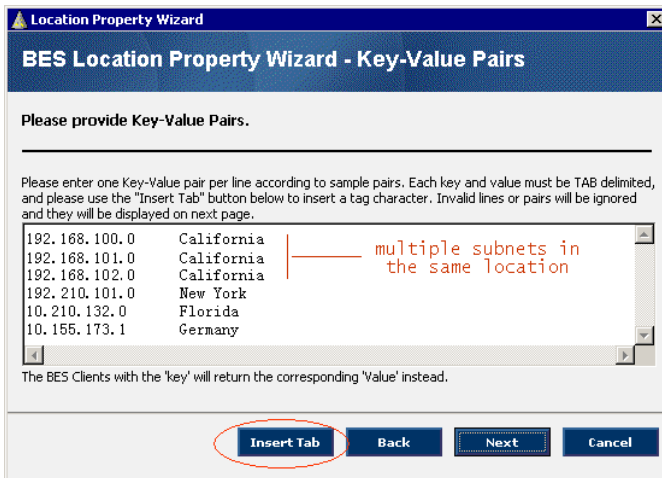
**Note:** The purpose of the procedure below is to create a property that will define the geographic location of an endpoint according to its subnet. Using the same principles, you could also create a property based on connection type, relay, operating system, or any other characteristics and use it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

---

**To create a location property:**

1. Log on to the ESP Console as Master Console Operator, open the CPM 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 may self-identify using their W-LAN or LAN IP address, so you may 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 above, clients will self-identify their relevance to this IP address block. Clients not included in the block will either inherit the default configuration which 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 will clearly identify 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 as shown in [Figure 8-1](#). Create multiple lines for the same location if it uses multiple subnets.

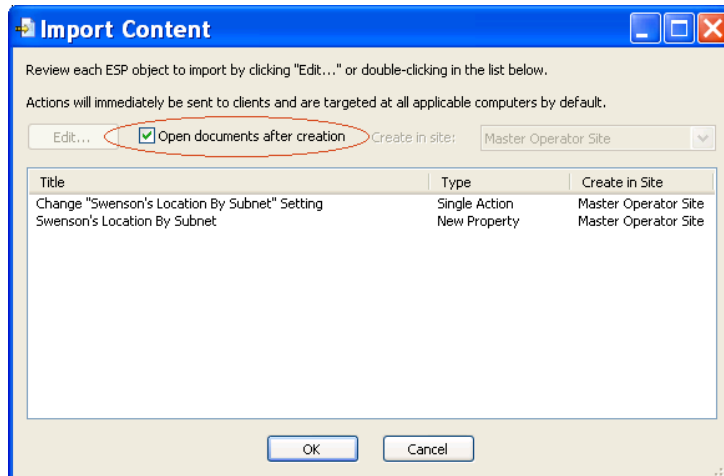


**FIGURE 8-1** Create one or more Location Properties to support site- or NIC-specific CPM configurations.

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** as shown in [Figure 8-2](#). Do not miss this step, or it will prevent the location property

from being deployed to your endpoints and your locations will not be relevant for any of your **Actions**.



**FIGURE 8-2** This option must be selected to deploy the location property you configured to the endpoints.

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

See [Install and Manage the Client Firewall starting on page 7-1](#) for instructions on creating location-specific firewall policies, and NIC-specific and connection-specific policies, such as connecting through the corporate LAN or a coffee shop.

## How Location Properties Work

Each ESP Agent, on which the CPM 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 may include hundreds of values describing their hardware, the network, and software.

In short:

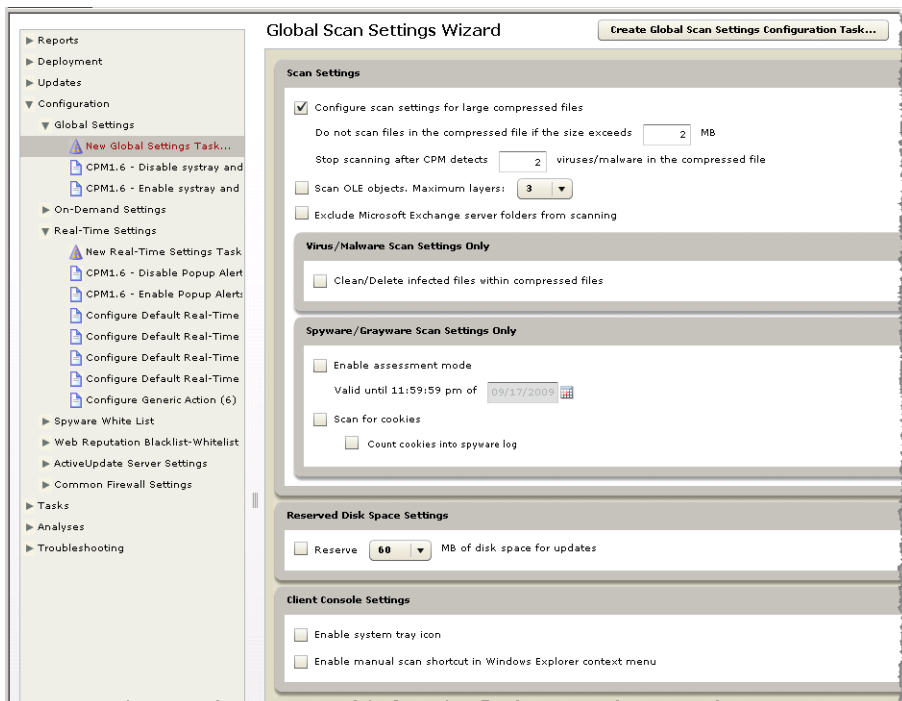
- First, define some locations.
- Second, configure your scan, firewall, or URL filtering settings.
- Next, save the settings to a Task and create an Action to target some given endpoints.

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 detects 2 virus/malware in the compressed file



**FIGURE 8-3** Create location-specific configurations.

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.

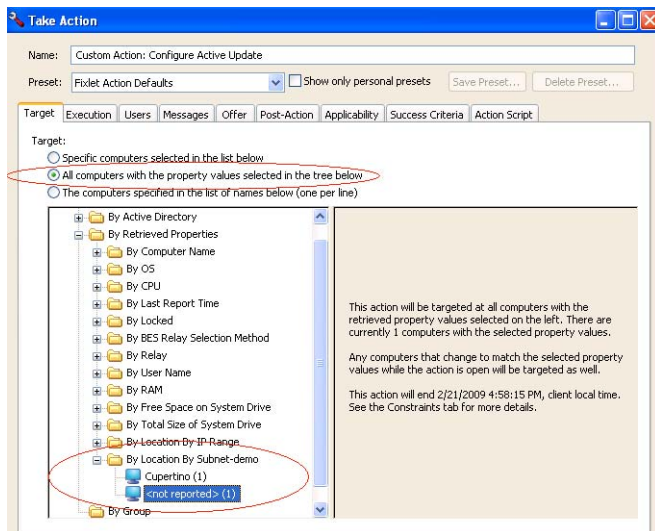
#### **B. To create the second configuration and Task:**

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**.



**FIGURE 8-4** Find the Location you created so you can attach a Task to it.

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 8-3](#)).
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.**

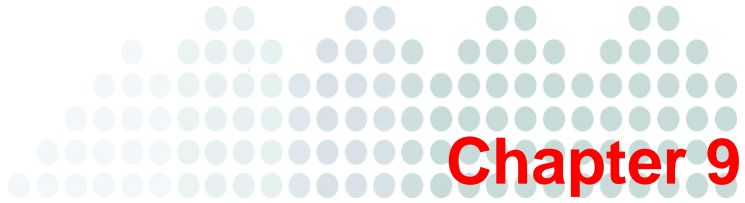
The screenshot shows the 'Take Action' configuration window with the 'Behavior' section expanded. The 'Reapply this action' checkbox is checked, and the radio button for 'whenever it becomes relevant again' is selected. A red circle highlights the 'Reapply this action' checkbox and its associated radio button options. Other options in the 'Behavior' section include 'On failure, retry' (3 times), 'Wait' (1 hour between attempts), 'Wait until computer has rebooted', 'while relevant, waiting' (15 minutes between reapplications), 'Limit to' (3 reapplications), 'Distribute over' (5 minutes to reduce network load), and 'Run all member actions of action group regardless of errors' (checked).

**FIGURE 8-5** Choose “Reapply this action” so the Agent will monitor its IP address relative to the Location rules.

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.







## Using the Client Console

This chapter includes information to help with using the Core Protection Module (CPM) client console that runs on end-users machines.

Topics in this chapter include:

- [Overview on page 9-2](#)
- [Accessing the Client Console on page 9-3](#)
- [Client Connection with CPM Server on page 9-4](#)
- [Manual Scans on page 9-4](#)
- [Testing the CPM Client Console on page 9-7](#)
- [Update Now on page 9-8](#)

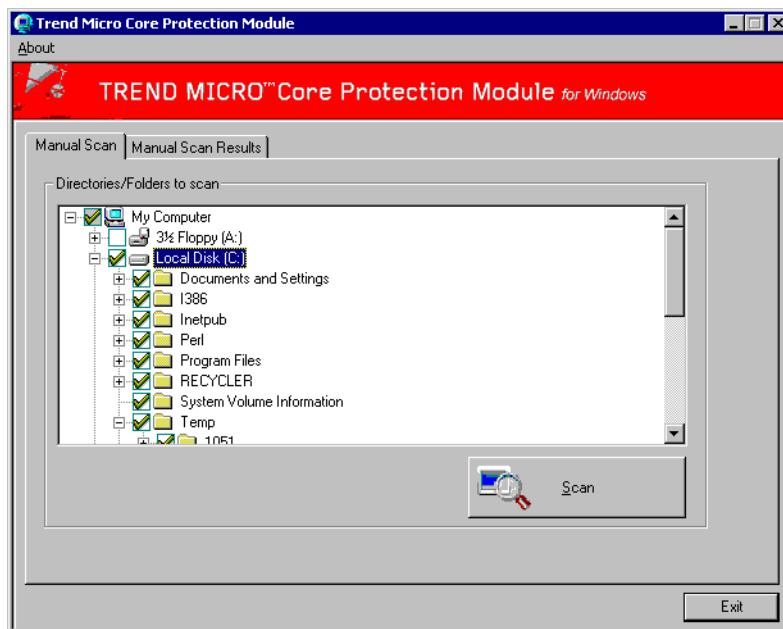
## Overview

The CPM client provides security risk protection and reports events to, and gets updates from, the CPM server. A system tray icon for the client console informs the user of the current scan service status of CPM and gives access to the client console. Also, if enabled, the client console installation allows initiating a manual scan from Windows Explorer.

You can perform the following tasks using the CPM client console:

- Manually scan files and folders for virus/malware and spyware/grayware
- View Manual Scan results and take see the action on infected files
- Update to the latest version of protection components

The CPM client console, shown in [Figure 9-1](#), allows users to initiate scans at any time on the files and folder selected, then view the scan results.



**FIGURE 9-1** The CPM client console accesses Manual Scan and results.

## CPM Client Dashboard vs. CPM Client Console

The CPM Client Dashboard offers display-only information about the client machine to the client machine user and the administrator. Before accessing it, it must be enabled from the CPM dashboard and deployed. For more information about enabling and disabling the CPM Client Dashboard, see "To display the CPM icon on endpoints:" on page A-6. Users right-click the red icon (#1 in Figure 9-2) to access it.

The CPM Client Console provides on-demand scan information about the client machine to the client machine user. Before accessing it, it must be enabled from the CPM Dashboard and deployed. See "To enable the Client Console:" on page A-7 for details. Users right-click the blue icon (#2 in Figure 9-2) to access it.



**FIGURE 9-2** 1 = Client Dashboard, 2 = Client Console

## Accessing the Client Console

### To access the client console:





1. Right-click the icon in the system tray. [Table 9-1](#) shows the icons.
2. Mouse over the icon to display client connection information.
3. Select **Core Protection Module Console**.

The CPM client console opens.

## Client Connection with CPM Server

Icons on the client computer's system tray indicate the client's scan service status with the CPM server.

**TABLE 9-1. Online client icons**

ICON	FOR	DESCRIPTION
	Manual scan	All components are up-to-date and services work properly.
	Manual or On-Demand scan	Scan is in progress
	Real-Time scan	Scan service is disabled.
	All scan types	Improper scan service status. User cannot perform scans.

## Manual Scans

The Manual Scan tab displays a folder tree that shows your disk drives, folders, and files as they appear in Windows Explorer®. Network resources such as Network Neighborhood or My Network Places do not display.

Manual Scan is an on-demand scan that starts immediately after a user clicks the Scan button the client console. The time needed to complete the scan depends on the number of files scanned and the hardware resources of the client computer.

---

**Note:** When an end-user initiates a Manual Scan from the CPM client console, the scan settings reflect the latest settings configured by the administrator for an On-Demand Scan.

For example, an administrator might schedule an On-Demand Scan on every Thursday 12:00 PM that scans all file types. Then the administrator might run an On-Demand scan with different scan settings, maybe scanning only for .EXE files, at


---

14:00 PM. If an end-user runs a Manual Scan at 15:00 PM, and the administrator has not changed the settings, the end-user's Manual Scan will only scan for .EXE files, not all file types.

---

## Initiating a Manual Scan from the System Tray Icon

### To manually scan for security risks:

1. Right-click the client console icon  in the system tray.
2. Select **Core Protection Module Console**.
3. Click the **Manual Scan** tab.
4. Select the drives, folders, and files you want to scan manually.  
If a plus sign [+] appears next to a drive or folder, it means that the drive or folder has at least one subfolder.
5. Click **Scan**.
6. See the **Manual Scan Results** tab immediately after completing the scan. See [Viewing Scan Results on page 9-7](#) for details.

---

**Note:** Scan results are only available during the scan session. If the console is closed, scan results are no longer available.

---

## Initiating a Manual Scan from Windows Explorer

This option must be enabled from the CPM dashboard before it is available to the endpoint user.

### To initiate a scan from Windows Explorer:

1. Open Windows Explorer on the endpoint computer.
2. Right-click on any folder or file to be scanned.
3. Select **Scan with Core Protection Module** to initiate the scan.

Results will let you know if the scan was successful:

- If nothing was found, click **OK** in the confirmation dialog box.
- If the scan found an issue, the action for handling malware (configured by the system administrator) occurs.

- See the **Manual Scan Results** tab immediately after completing the scan for details. See [Viewing Scan Results on page 9-7](#) for more information.

## Manual Scan Results

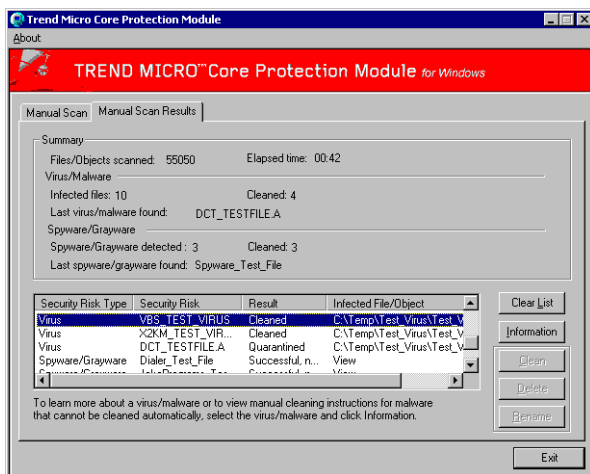
The Manual Scan Results tab displays the result of the most recent Manual Scan. You can choose to view virus/malware or spyware/grayware scanning results.

---

**Note:** Closing the client console removes the information displayed on this screen.

---

The upper half of the screen contains the scan summary and the lower half contains a table with detailed information about any security risk detected during scanning.



**FIGURE 9-3** Scan result details display in the Summary section.

[Table 9-1](#) describe the buttons beside the scan results.

**TABLE 9-2.** Scan results buttons and usage

BUTTON	USAGE
Clear List	Click this button to remove the information in the table.

**TABLE 9-2. Scan results buttons and usage**

BUTTON	USAGE
Information	To learn more about the security risk, click the security risk name and then click this button
<b>Note:</b> The next three buttons apply only to virus/malware scan results if the scan action (configured by the CPM administrator) is Pass. Pass means that CPM detected the file but did not take any action. CPM allows you to clean, delete or rename the file.	
Clear	CPM may not be able to automatically clean some files because the file may be encrypted, in a location that does not allow it to be cleaned, or is a Trojan or worm. (See scan results for details.)
Delete	Delete the virus or malware file.
Rename	Click to change the extension of the file to .VIR, (or to .VIO, .VI1, and so on if there is more than one) to prevent yourself or other users from opening it accidentally.

## Viewing Scan Results

### To view the scan results:

1. Perform a Manual Scan as described in [Initiating a Manual Scan from the System Tray Icon on page 9-5](#).
2. Click the Manual Scan Results tab.  
Summary details display at the top of the screen. See [Figure 9-3](#).
3. (If the CPM configured the scan action to Pass) Select a detected virus or malware.
4. Click **Clean**, **Delete** or **Rename**. See details in [Table 9-2](#).

## Testing the CPM Client Console

After enabling the CPM console, your administrator may test it to verify that antivirus protection works. EICAR, the European Institute for Computer Antivirus Research, developed a test script as a safe way to confirm proper installation and configuration of antivirus software. Visit the EICAR Web site for more information at:

<http://www.eicar.org>

The EICAR test script is an inert text file with a .com extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software reacts to it as if it were a virus.

---

**WARNING!** Never use real viruses to test your antivirus installation.

---

Contact your CPM administrator for information about how to use the EICAR test script.

## Update Now

Keeping client components current is essential to ensuring that your computer stays protected. The Update Now feature allows updating at any time. The client connects to an update source to check for updates to security components that detect the latest viruses, spyware, and malware. If updates are available, the client automatically downloads the components.

---

**Note:** Update Now always updates from the cloud and not the ESP Server, whether the endpoint runs remotely or connects to the LAN.

---

### To update the client manually:

1. Right-click on the CPM client console icon in the system tray.
2. Click **Update Now** from the console menu.
3. In the Update Status tab, click **Update Now**.

When complete, a message displays saying, “Component update is complete.”





# Troubleshooting

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

Topics in this chapter include:

- [Installation on page 10-2](#)
- [Virus, Malware, and Spyware Scanning on page 10-3](#)
- [CPM Clients on page 10-5](#)
- [Pattern Updates on page 10-6](#)
- [Firewall Troubleshooting on page 10-9](#)

## Installation

The CPM installer writes install logs to the following file:

```
%WINDOWS%\CPMInstallResult.log
```

The log typically includes the install start and finish time, current 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 Component
2 = Upgrading CPM 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 Exists
-6 = Need Reboot Before Install
-7 = Cannot Start Core Protection Module Service(s)
-8 = Cannot Stop Core Protection Module 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 = Configuration File Missed
```

## Installing the CPM Server on a Non-default Drive

By default, the CPM component files will be installed to the local c:\ 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**.

## Virus, Malware, and Spyware Scanning

### To enable debug logging:

1. From the CPM client, open Microsoft Regedit.
2. Locate the following entry:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tmfilter\Parameters\
```

3. Double-click **DebugLogFlags** and type the following under **Value Data**:

```
0x3EFF
```

4. Save and close as necessary. A log file will be created in the following location:

```
C:\Windows\TMfilter.log  
C:\WinNT\TMfilter.log
```

## Virus/Spyware Logs on the CPM Client

The virus/spyware log directory is located here:

```
%Program Files%\Trend Micro\OfficeScan Client\Misc
```

The following logs are significant:

- Pccnt35.log  

```
20090108< />1131< />JS_AMILALA.A< />1< />1< />0< />C:\Documents and Settings\Administrator.QAL-22-13.001\Local Settings\Temporary Internet Files\Content.IE5\WPIBG52Z\trojan[1].htm< />
```
- Spyware.log  

```
20090108< />1140< />JokePrograms_Test_File< />2< />1< />0< />20090108114038075460_JokePrograms_Test_File< />
```
- Spyware\_detail.log  

```
[20090108114038075460_JokePrograms_Test_File]
Timestamp=1231443630
ScanType=1
ActionResult=2
ItemCount=1
ItemLocation#0=C:\Documents and Settings\Administrator\Desktop\JOKE_Test_File.exe
ItemScannerType#0=10
ItemThreatType#0=6
ItemRiskLevel#0=0
ItemActionResult#0=257
```

## 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:

```
%ProgramFiles%\Trend Micro\Core Protection  
Module\Bin\AU_Log\TmuDump.txt
```

#### 4. CPM AU Server Logs:

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

## Components Installation Debug Logs (CPM Server)

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

Directory = %WINDOWS%

- CPMInstallResult.log
- CPMsrvInstall.log
- ClnExtor.log
- CPMsrvISSetup.log

## Components Installation Debug Logs (CPM Client)

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

Directory = %WINDOWS%

- ClnExtor.log\*
- CPMInstall.log\*
- CPMInstallResult.log\*
- CPMISSetup.log\*
- ofcdebug.log
- OFCNT.log
- setupapi.log
- OFCISSetup.log

Log file names followed by an asterisk (\*) also serve as CPM Client upgrade debug logs. All logs files can be collected by CDT.

## CPM Clients

### To enable debugging on the CPM clients:

1. Create the following directory:

```
c:\logserver
```

2. Change to this directory and then create a text file with name and content shown below:

```
File name = ofcdebug.ini  
  
[debug]  
Debuglog = c:\logserver\ofcdebug.log  
Debuglevel = 9  
Debuglevel_new = D
```

3. Save and close the file.
4. Run the following program from a command prompt:

```
Logserver.exe
```

#### **To collect information by CDT:**

1. Run the following program on the endpoint in question:  

```
%ProgramFiles%\Trend Micro\Core Protection  
Module\CDT\CaseDiagnosticTool.exe
```
2. Copy the output file from its location at C:\CDT\_Data\  
The file name will be similar to: CDT-20091003-030750.zip
3. Send the compressed 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 server components include:
  - Proxy Settings
  - TMCPMAuHelper.exe
  - TrendMirrorScript.exe
- CPM console components include:
  - Pattern Update Wizard
  - Pattern-set Loading via Manifest.json
- CPM client components include:

- BESClient.exe (for dynamic download requests for pattern-sets)
- TMCPCMAuUpdater.exe (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 version 1.6:
 

```
http://cpm15-p.activeupdate.trendmicro.com/activeupdate
```
- **CPM server:** Check that the server exists in the Windows Registry:
 

```
HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\CPM\server
```
- **CPM server:** If the automatic update Task is successful, the CPM site will exist in the 'bfsites' directory:
 

```
<%Program Files%>\BigFix Enterprise\BES
Server\wwwrootbes\bfsites\CustomSite_FileOnlyCustomSite_CPMAuto
Update_1
```
- **CPM client:** After automatic updates have been enabled on the client, the CPM site will exist 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 – 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\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 - 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 a 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 clients that have been enabled for automatic updates, the EnableAutoUpdate registry key must be set to 1:

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

## 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 server component proxy authentication settings** (used by the update program, TMCPCMAuHelper.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:  
`%TMCPMAuHelper_install_path%\bin\AU_Data`
2. Delete all files and any subfolders from this directory (but not the folder itself):  
`%TMCPMAuHelper_install_path%\download`
3. From the CPM Dashboard, run the **Check Server for Pattern Updates** Task.

## Client-Side Logging: ActiveUpdate

1. On the CPM server, create/locate and open the following text file:  
`%CPM_SERVER_INSTALL_FOLDER%\bin\aucfg.ini`
2. Add or change the following parameter:  

```
[debug]
level=-1
```
3. Save and close the file.
4. Log output will be saved here:  
`%CPM_SERVER_INSTALL_FOLDER%\Bin\AU_Data\AU_Log\TmuDump.txt`

## Additional Files

- Create a manifest file and list of URLs by typing the following at a command prompt:  
`TMCPMAuUpdater -pu -m Manifest -f urlist`
- Check the file, server.ini in the following location:  
`%CPM_INSTALL_FOLDER%\Web\officescan\download`

## Firewall Troubleshooting

The best tool for understanding and troubleshooting the Trend Micro Common Firewall in CPM is a port scanner. Many are available. Use your favorite, or try Nmap, from [nmap.org](http://nmap.org).

## General

1. Disable third-party firewalls or other conflicting products.
2. Check that you are running CPM version 1.6.
  - In the ESP Console, select the Analysis: **Core Protection Module – Endpoint Information**.
  - Upgrade endpoints as necessary by running the Task, **Core Protection Module - Update Endpoint**.
3. Confirm that the firewall is enabled.
  - In the ESP Console, select the Analysis: **Common Firewall – Endpoint Firewall Setting**.
4. Check the **Action History** for Tasks already run, especially if you are using a location property ([Creating Location-Specific Tasks on page 8-5](#)) with your firewall Tasks. Be sure that conflicting policies have not been deployed to the same endpoint(s).
  - a. From the ESP Console, select a target computer and open its **Action History**.
  - b. If you see in History that multiple firewall Tasks are overwriting one another, chances are that multiple policies are claiming relevance and updating the policy on the endpoint. In this case, delete all your Actions and re-apply the Tasks.
5. Confirm that the firewall services are running on the computers in question.
  - From the CPM Dashboard, click **Troubleshooting > Improper Service Status** to run the **Improper Service Status** Fixlet.
  - At the endpoint(s) in question check that the following Windows Services are running:  
  
`OfficeScan NT Listener`  
`OfficeScan NT RealTime Scan`  
`OfficeScan NT Firewall`

## Client is not Connecting to the ESP Server or Relays

By default, ESP Server-Agent and CPM server-client communication occur using port 52311. This port is automatically allowed by the Trend Micro Common Firewall.

If you have installed ESP using a different port, the firewall will automatically recognize that port. However, if you have re-installed the ESP Server and in that installation designated a different port, the firewall will not pick up that change. Add an exception in your firewall policies.





## Contacting Trend Micro

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

Topics in this chapter include:

- [Technical Support on page 11-2](#)
- [Contact Information on page 11-2](#)
- [Sending Suspicious Files to Trend Micro on page 11-3](#)
- [Documentation Feedback on page 11-3](#)
- [The Trend Micro Knowledge Base on page 11-3](#)
- [TrendLabs on page 11-4](#)
- [Security Information Center on page 11-4](#)
- [Security Risks on page 11-4](#)

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

Email: [support@trendmicro.com](mailto:support@trendmicro.com)

## Speeding Up Your Support Call

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

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

- Steps to reproduce the problem

## 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 spyware and viruses).

- Send an email to: [virusresponse@trendmicro.com](mailto: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 will investigate the issue and respond as soon as possible.

## TrendLabs

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

You can rely on the following post-sales service:

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

TrendLabs has achieved ISO 9002 quality assurance certification.

## Security Information Center

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

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

## Security Risks

This section describes common security risks (viruses/malware, spyware/grayware, and Web threats). CPM protects computers from each of the security risks described below.



## 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 will include a URL to a Web site that looks exactly like the real thing (it is simple to copy a legitimate email and a legitimate Web site but then change the so-called 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.

## Spyware and Grayware

Client computers are at risk from potential threats other than viruses/malware. Spyware/Grayware 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 spyware/grayware 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 cannot detect as grayware but you think is a type of grayware, send it to Trend Micro for analysis:

<http://subwiz.trendmicro.com/SubWiz>

### How Spyware/Grayware Gets into the Network

Spyware/Grayware often gets into a corporate network when users download legitimate software that have grayware 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 to collect personal data; however, users often overlook this information or do not understand the legal jargon.

## Types of Spyware/Grayware

- **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 are often pay-per-call or international numbers that 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.

## Viruses and Malware

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

- **Probable virus/malware:** Suspicious files that have some of the characteristics of virus/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 computers.executable program. Trojan horse programs do not replicate but instead resides on systems to perform malicious acts, such as opening ports for hackers to enter. A Traditional antivirus solutions can detect and remove viruses 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 virus:** An inert file that acts like a real virus and is detectable by virus-scanning software. Use test viruses, such as the EICAR test script, to verify that your antivirus 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 antivirus products to detect.
  - **Others:** Virus/Malware not categorized under any of the other virus/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 Spyware/Grayware and Other Threats

There are many steps you can take to prevent the installation of spyware/grayware onto your computer. Trend Micro suggests the following:

- Configure On-Demand, Real-time, and Scheduled On-Demand Scans to find and remove spyware/grayware 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, 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 grayware applications may be masked as other types of files your users may want to download, such as MP3 music files.
- Periodically examine the installed software on your agent computers and look for applications that may be spyware or other grayware.
- Keep your Windows operating systems updated with the latest patches from Microsoft. See the Microsoft Web site for details.



# Appendix A

## Routine CPM 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 on page A-2](#)
- [Spyware Handling and Correction on page A-4](#)
- [CPM Server Management on page A-4](#)
- [CPM Client Management on page A-5](#)
- [Pattern File Management on page A-8](#)
- [Web Reputation on page A-10](#)
- [CPM Firewall on page A-10](#)

## Scan Management

Scan management procedures included in this section include:

For General Scan Configurations:

- [To change or configure scan settings: on page A-2](#)

For Real-time and On-Demand Scans:

- [To configure the Scan Now scan: on page A-3](#)
- [To start scanning with the default settings: on page A-3](#)
- [To create and run a custom On-Demand Scan Task: on page A-3](#)
- [To run an On-Demand Scan: on page A-3](#)
- [To schedule an On-Demand Scan: on page A-3](#)

## General Scan Configurations

The steps below are for experienced ESP administrators who just need a reminder list of tasks involving the CPM scan configurations.

- Embedded OLE objects (how to handle)
- Microsoft Exchange folders (prevent scanning)
- Compressed file scanning (how to handle)
- Compressed file scanning (large)
- Action to take on spyware and malware
- Cookie scanning
- Disk space available for pattern files and updates

### To change or configure scan settings:

1. In the CPM Dashboard, click **Configuration > Global Settings > New Global Settings Task**.
2. Deploy the Global Settings by clicking **Configuration > Global Settings > [scan name]** in the CPM Dashboard.

## 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 > 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, 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 time period suits you).

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

- Client performance (CPU throttling)
- Virus and malware scanning
- Spyware and grayware 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)
- Boot sector scanning
- Floppy disk scanning (real-time)

- 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]**.

## Spyware Handling and Correction

### To exempt files from detection:

1. Click **Configuration > New Spyware White List Task**.
2. Identify the file(s) you want to prevent from being detected as spyware.
3. Click the **Create Spyware White List Configuration Task...** button.

### To recover “spyware” files:

In the CPM Dashboard, click **Tasks > Core Protection Module > Restore Spyware/Grayware....** The Spyware/Grayware Restore Wizard appears.

## CPM Server Management

The steps below 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-5](#)
- [To update or remove CPM server components: on page A-5](#)



- [To remove the Core Protection Module site: on page A-5](#)
- [To display the CPM icon on endpoints: on page A-6](#)
- [To view CPM hidden client statistics for a given endpoint: on page A-6](#)
- [To decrypt quarantined files: on page A-6](#)

**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** 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 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 site:**

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

## CPM Client Management

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

- [To display the CPM icon on endpoints: on page A-6](#)
- [To view CPM hidden client statistics for a given endpoint: on page A-6](#)
- [To decrypt quarantined files: on page A-6](#)
- [To deploy CPM clients: on page A-6](#)
- [To remove CPM clients: on page A-7](#)
- [To enable the Client Console: on page A-7](#)
- [To enable notifications on the client: on page A-7](#)

### To display the CPM icon on endpoints:

- In the CPM Dashboard, click **Tasks > Enable Client Dashboard**. The **Task Description** opens.

### To view CPM 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 may spread the virus/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 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.

Required the following files:

- 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}
```

### To deploy CPM clients:

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

**To remove CPM clients:**

To uninstall CPM, you first remove all the CPM clients installed on the endpoint, and then the CPM 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**.
2. Locate **Core Protection Module - Endpoint Uninstall** in the list of Actions that appears and double click it to open the Description.

**To enable the Client Console:**

1. Go to **Configuration > Global Settings > New Global Settings Task**.
2. Scroll down to the Client Console Settings.
3. Check the appropriate check boxes:
  - Click **Enable system tray icon** to display the icon used to access the client console on the relevant endpoints
  - Click **Enable the manual scan in the Windows Explorer context menu** to allow initiating a manual scan from Windows Explorer.
4. Click the **Create Global Scan Settings Configure Task** button.  
The Edit Task window opens.
5. Type a descriptive (or memorable) name for the Task such as “Enable Client Console.”
6. Click **OK** to close the Windows, and when prompted type your private key password and click **OK** to create the new global policy.
7. The new settings now appears in the **Configuration > Global Settings Dashboard**.

**To enable notifications on the client:**

Use the On-Demand or Real-Time Scan Settings Wizards to display notifications on the client computer about virus/malware or spyware/grayware detections.

See [If you are running Trend Micro ScanMail for Exchange, you can configure CPM to exclude Microsoft Exchange 2000/2003 directories from On-Demand and Real-time Scans. For Microsoft Exchange 2007, you need to manually add the directory to the scan](#)

exclusion list. For more information, see:  
<http://technet.microsoft.com/en-us/library/bb332342>. on page 5-9 for details.

## Pattern File Management

The steps below 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-8](#)
- [To deploy selected pattern files: on page A-8](#)
- [To revert to a previous version of the pattern files: on page A-8](#)
- [To re-enable updates following a rollback: on page A-9](#)
- [To update pattern files on the CPM server: on page A-9](#)
- [To update pattern files on the CPM clients: on page A-9](#)

### **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 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 revert to a previous version of the pattern files:**

In the CPM Dashboard, click **Updates > Update/Rollback Patterns > New Pattern Update/Rollback Task...**

**To re-enable updates following a rollback:**

After a rollback, you must clear the rollback flag setting attached to patterns on your CPM clients to re-enable manual, cloud, and/or automatic pattern updates. The same holds true even for pattern files that were not included in the rollback.

1. In the CPM Dashboard, click **Updates > Other Update Tasks > Clear Rollback Flag**. The Task **Description** window opens.
2. Below **Actions**, click the hyperlink to open the **Take Action** window.
  - In the **Target** tab, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
  - Click **OK**, and then when prompted, type your private key password and click **OK**.

**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 Server updates: Open the **Fixlet Messages** tab > **All Fixlet Messages > Core Protection Module - Enable Automatic Updates - Server**.
3. Update the pattern file on the CPM server: In the CPM Dashboard, click **Deployment > Install > Set ActiveUpdate Server Pattern Update Interval...**

**To update pattern files on the CPM clients:**

1. Enable CPM 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 clients with the latest pattern files: Click **Updates > Update/Rollback Patterns > New Pattern Update/Rollback Task...**

## Web Reputation

The steps below 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.

## CPM Firewall

The steps below are for experienced ESP administrators who just need a list for tasks involving the CPM Common Firewall. Procedures include:

- [To create a firewall policy: on page A-10](#)
- [To deploy a firewall policy: on page A-10](#)
- [To disable the firewall on all or selected endpoints: on page A-11](#)

### To create a firewall policy:

1. In the ESP Console menu, click **Common Firewall Settings > New Policy Task...**
2. Click the **Add** button.
3. Choose the following:
  - **Firewall Enabled**
  - **Security Level**
  - **Apply to All Possible IP Addresses**
4. Add any exceptions (relative to the Security Level).

### To deploy a firewall policy:

1. Click **Common Firewall Settings > New Policy Task...** and select the policies you want in the Policy List.
2. Move your policy to the top of the list and click the **Save Order** button.

3. Click the **Create Firewall Policy Task...** button at the top of the screen.

**To disable the firewall on all or selected endpoints:**

1. Click **Common Firewall Settings > New Policy Task...**
2. Click the **Add** button.
3. Remove the check from **Firewall Enabled**
4. Click **Save**.
5. Select the policy you just created in the Policy List and clear the check from any other policies if necessary.
6. Click the **Create Firewall Policy Task...** button at the top of the screen.







# Appendix B

## Reference Tables

The reference tables included in this appendix include:

- [Default ActiveAction Behaviors on page B-2](#)
- [Available Virus/Malware Scan Actions on page B-3](#)
- [Pattern and Scan Engine Files on page B-4](#)
- [Scan Action Results for Compressed Files on page B-6](#)
- [Default Firewall Global Exceptions on page B-7](#)

## Default ActiveAction Behaviors

VIRUS/MALWARE TYPE	REAL-TIME SCAN		ON-DEMAND SCAN	
	FIRST ACTION	SECOND ACTION	FIRST ACTION	SECOND ACTION
Joke program	*Quarantine	N/A	Quarantine	N/A
Trojan horse	Quarantine	N/A	Quarantine	N/A
Virus	Clean	Quarantine	Clean	Quarantine
Test virus	Deny Access	N/A	Pass	N/A
Packer	Quarantine	N/A	Quarantine	N/A
Others	Clean	Quarantine	Clean	Quarantine
Probable virus/malware	Pass	N/A	Pass	N/A

\* CPM renames and then moves infected files to the following, non-configurable, directory on the client's computer:

```
c:\Program Files\Trend Micro\Core Protection
Module\Quarantine
```

If you need to access any of the quarantined files, you can access the directory using system administrator credentials and restore it using the VSEncrypt tool.

## Available Virus/Malware Scan Actions

SCAN ACTION	DESCRIPTION
Delete	CPM deletes the infected file.
Quarantine	<p>CPM renames and then moves infected files to the following, non-configurable, directory on the client's computer:</p> <pre>c:\Program Files\Trend Micro\Core Protection Module\Quarantine</pre> <p>If you need to access any of the quarantined files, you can access the directory using system administrator credentials and restore it using the VSEncrypt tool (see <a href="#">Scan Action Results for Compressed Files on page B-6</a>).</p>
Clean	CPM cleans the infected file before allowing full access to the file. If the file is uncleanable, CPM performs a second action, which can be one of the following actions: Quarantine (typical), Delete, Rename or Pass.
Rename	<p>CPM changes the infected file's extension to "vir". Users cannot open the renamed file initially, but can do so if they associate the file with a certain application.</p> <p><b>Warning!</b> Renaming the file will not prevent the virus/malware from executing. Consider using Quarantine or Delete, instead.</p>
Pass	<p>CPM performs no action on the infected file but records the virus/malware detection in the logs. The file stays where it is located.</p> <p>CPM 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 virus/malware to execute. All the other scan actions can be used during Real-time Scan.</p> <p>For the "probable virus/malware" type, CPM always performs no action on detected files (regardless of the scan type) to mitigate false positives. If further analysis confirms that the probable virus/malware is indeed a security risk, a new pattern will be released to allow CPM to take the appropriate scan action. If actually harmless, the probable virus/malware will no longer be detected.</p>
Deny Access	This scan action can only be performed during Real-time Scan. When CPM detects an attempt to open or execute an infected file, it immediately blocks the operation. Users receive no CPM-specific notification of the action, only a message from the operating system. Users can manually delete the infected file.

## Pattern and Scan Engine Files

COMPONENT	DESCRIPTION
<b>Antivirus</b>	
Virus Pattern	A file that helps CPM identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.
IntelliTrap Pattern	The file for detecting real-time compression files packed as executable files
IntelliTrap Exception Pattern	The file containing a list of "approved" compression files
Virus Scan Engine	The engine that scans for and takes appropriate action on viruses/malware; supports 32-bit and 64-bit platforms
<b>Anti-spyware</b>	
Spyware Pattern	The file that identifies spyware/grayware in files and programs, modules in memory, Windows registry and URL shortcuts
Spyware Active-monitoring Pattern	File used for real-time spyware/grayware scanning
Spyware Scan Engine	The engine that scans for and takes appropriate action on spyware/grayware; supports 32-bit and 64-bit platforms
<b>Firewall</b>	
Common Firewall Pattern	Required for the optional CPM firewall; available in version CPM 1.6 (not found in CPM 1.0)
<b>Damage Cleanup Services</b>	
Virus Cleanup Template	Used by the Virus Cleanup Engine, this template helps identify Trojan files and processes so the engine can eliminate them
Virus Cleanup Engine	The engine Damage Cleanup Services uses to scan for and remove Trojans and Trojan processes; supports 32-bit and 64-bit platforms
<b>Common component</b>	

---

<b>COMPONENT</b>	<b>DESCRIPTION</b>
Anti-rootkit Driver	A kernel mode driver used by the Spyware Scan Engine that provides functionality to bypass any potential redirection by rootkits; supports 32-bit platforms

---

## Scan Action Results for Compressed Files

STATUS OF CLEAN/DELETE INFECTED FILES IN COMPRESSED FILES	CPM ACTION	COMPRESSED FILE FORMAT	RESULT
Enabled	Clean or Delete	Not supported Example: <i>def.rar</i> contains an infected file <i>123.doc</i> .	CPM encrypts <i>def.rar</i> but does not clean, delete, or perform any other action on <i>123.doc</i> .
Disabled	Clean or Delete	Supported/Not supported Example: <i>abc.zip</i> contains an infected file <i>123.doc</i> .	CPM does not clean, delete, or perform any other action on both <i>abc.zip</i> and <i>123.doc</i> .
Enabled/Disabled	Not Clean or Delete (in other words, any of the following: Rename, Quarantine, Deny Access or Pass)	Supported/Not supported Example: <i>abc.zip</i> contains an infected file <i>123.doc</i> .	<p>CPM performs the configured action (Rename, Quarantine, Deny Access or Pass) on <i>abc.zip</i>, not <i>123.doc</i>.</p> <p>If the action is:</p> <p><b>Rename:</b> CPM renames <i>abc.zip</i> to <i>abc.vir</i>, but does not rename <i>123.doc</i>.</p> <p><b>Quarantine:</b> CPM quarantines <i>abc.zip</i> (<i>123.doc</i> and all non-infected files are quarantined).</p> <p><b>Pass:</b> CPM performs no action on both <i>abc.zip</i> and <i>123.doc</i> but logs the virus detection.</p> <p><b>Deny Access:</b> CPM denies access to <i>abc.zip</i> when it is opened (<i>123.doc</i> and all non-infected files cannot be opened).</p>

## Default Firewall Global Exceptions

<b>RULE NAME</b>	<b>ACTION</b>	<b>PROTOCOL</b>	<b>PORT</b>	<b>DIRECTION</b>
FTP Data	Allow	TCP	20	Bidirectional
FTP	Allow	TCP	21	Bidirectional
SSH	Allow	TCP	22	Bidirectional
Telnet	Allow	TCP	23	Bidirectional
SMTP	Allow	TCP	25	Bidirectional
DNS (TCP)	Allow	TCP	53	Bidirectional
DNS (UDP)	Allow	UDP	53	Bidirectional
TFTP	Allow	UDP	69	Bidirectional
HTTP	Allow	TCP	80	Bidirectional
Kerberos (TCP)	Allow	TCP	88	Bidirectional
Kerberos (UDP)	Allow	UDP	88	Bidirectional
POP3	Allow	TCP	110	Bidirectional
AUTH (TCP)	Allow	TCP	113	Bidirectional
AUTH (UDP)	Allow	UDP	113	Bidirectional
NTP (TCP)	Allow	TCP	123	Bidirectional
NTP (UDP)	Allow	UDP	123	Bidirectional
NETBIOS Name Service (TCP)	Allow	TCP	137	Bidirectional
NETBIOS Name Service (UDP)	Allow	UDP	137	Bidirectional
NETBIOS Datagram Service (TCP)	Allow	TCP	138	Bidirectional
NETBIOS Datagram Service (UDP)	Allow	UDP	138	Bidirectional

<b>RULE NAME</b>	<b>ACTION</b>	<b>PROTOCOL</b>	<b>PORT</b>	<b>DIRECTION</b>
NETBIOS Sessions Service (TCP)	Allow	TCP	139	Bidirectional
NETBIOS Sessions Service (UDP)	Allow	UDP	139	Bidirectional
SNMP	Allow	UDP	161	Bidirectional
SNMP-TRAP	Allow	UDP	162	Bidirectional
HTTPS	Allow	TCP	443	Bidirectional
SMB (TCP)	Allow	TCP	445	Bidirectional
SMB (UDP)	Allow	UDP	445	Bidirectional
IPsec (TCP)	Allow	TCP	500	Bidirectional
IPsec (UDP)	Allow	UDP	500	Bidirectional