BIGFIX

Core Protection Module *for Mac*

powered by TREND MICRO

User’s Guide

Version 2.0

February, 2010

Contents

CONTENTS

Part 1

Get Started

BigFix Core Protection Module (CPM) uses the highly scalable Unified Management Platform to deliver immediate protection against all types of malware attacks - virus, spyware, rootkit, blended attacks, and malicious website files. By integrating world class Anti-Malware from Trend Micro with multi-vendor management, this solution can simplify endpoint protection, reduce risk, and streamline administrative tasks.

CPM *for Mac* is a version of CPM created specifically for Mac platform users. This Guide will walk you through the upgrading process and describe how CPM *for Mac* differs from CPM.

> **Note:** An existing Trend Micro CPM deployment is required to add on CPM *for Mac*. Before using CPM *for Mac,* you should already be familiar with the CPM application, including product functionality, the dashboard, and navigation. For additional information, refer to the CPM 1.6 User's Guide.

For specific details about differences between CPM and CPM *for Mac,* see Part 3 of this document.

System Requirements

Minimum requirements for CPM *for Mac* endpoints are outlined below:

Supported Operating Systems:

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

Hardware Requirements:

- Macintosh™ computer with PowerPC™ and Intel™ core processor
- RAM: minimum 512 MB. Recommend 1 GB
- Available disk space: 700 MB

Incompatible Software

Trend Micro Software

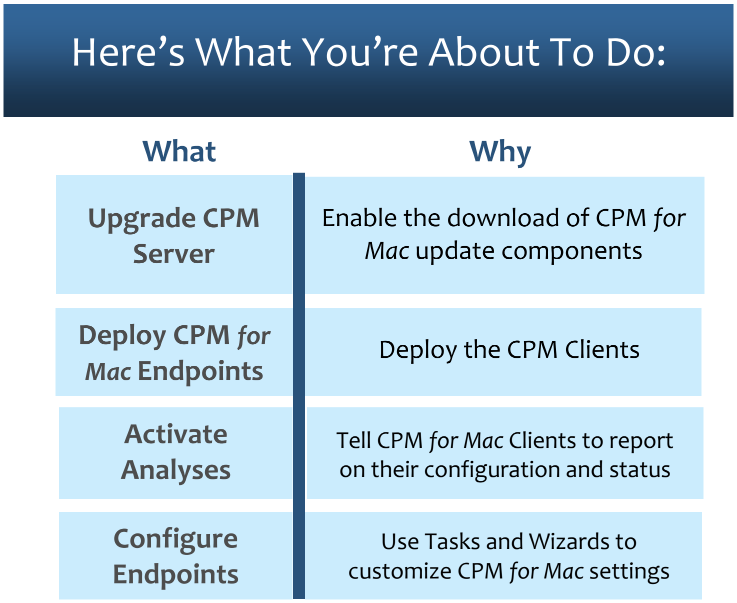
- Trend Micro Security for Macintosh 1.0
- Trend Micro Smart Surfing for Mac 1.0
- Trend Micro Security for Macintosh 1.5
- Trend Micro Smart Surfing for Mac 1.5

Third-Party Software

- Norton AntiVirus for Mac
- Norton Internet Security for Mac
- McAfee VirusScan
- Intego VirusBarrier
- Intego NetBarrier
- Avast! Mac Edition
- Sophos Anti-Virus for Mac OS X
- PC Tools iAntiVirus
- Kaspersky
- MacScan
- ClamXav

Process Overview

The table below displays the four primary steps to using CPM *for Mac:*



Here's What You're About To Do:

What	Why
Upgrade CPM Server	Enable the download of CPM *for Mac* update components
Deploy CPM *for Mac* Endpoints	Deploy the CPM Clients
Activate Analyses	Tell CPM *for Mac* Clients to report on their configuration and status
Configure Endpoints	Use Tasks and Wizards to customize CPM *for Mac* settings

Part 2

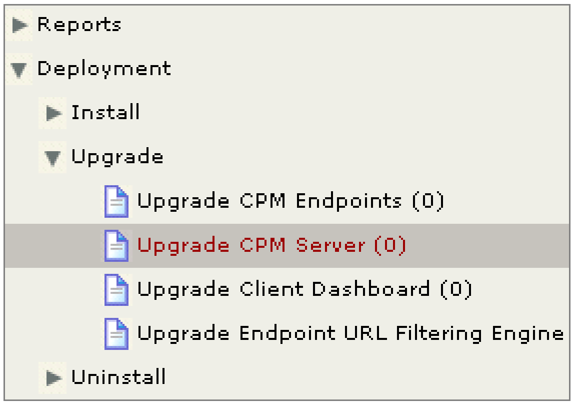
Upgrade

Before using CPM *for Mac,* you should have already installed the BigFix Unified Management Platform and be familiar with the operation of the BigFix Console. Detailed information on the Console can be found in the BigFix Console Operators Guide available on the BigFix support website.

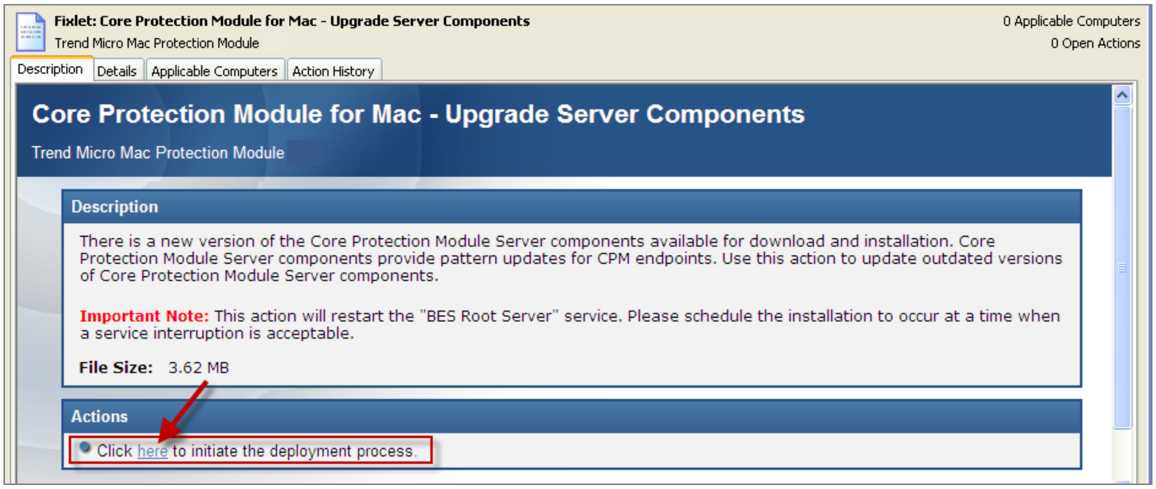
Upgrading Server Components

CPM *for Mac* is added to existing Core Protection Module deployments. To enable pattern and component updates for Mac endpoints, the server components must be upgraded to enable the download of Mac-specific update components.

To upgrade the server components, click the *Deployment* node of the navigation tree, then select the *Upgrade* sub-node. Click the *Upgrade CPM Server* task.


Reports
Deployment
Install
Upgrade
Upgrade CPM Endpoints (0)
Upgrade CPM Server (0)
Upgrade Client Dashboard (0)
Upgrade Endpoint URL Filtering Engine
Uninstall

At the CPM *for Mac* Upgrade Server Components window, review the text in the *Description* box and click where indicated in the *Actions* box to initiate the deployment process.



Fixlet: Core Protection Module for Mac - Upgrade Server Components
Trend Micro Mac Protection Module

0 Applicable Computers
0 Open Actions

Core Protection Module for Mac - Upgrade Server Components

Trend Micro Mac Protection Module

Description

There is a new version of the Core Protection Module Server components available for download and installation. Core Protection Module Server components provide pattern updates for CPM endpoints. Use this action to update outdated versions of Core Protection Module Server components.

Important Note: This action will restart the "BES Root Server" service. Please schedule the installation to occur at a time when a service interruption is acceptable.

File Size: 3.62 MB

Actions

- Click here to initiate the deployment process.

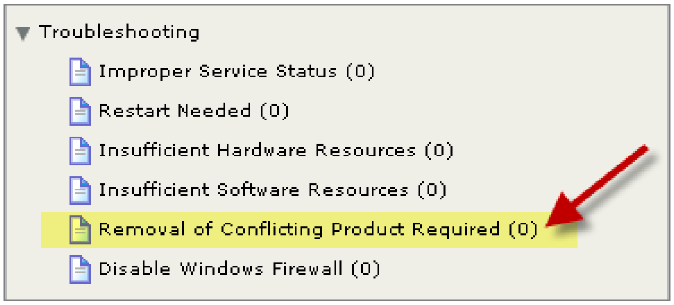
When the Take Action dialog opens, go through the tabs (Target, Execution, etc.) to customize this action within your system, then click *OK*. Check the BigFix Console Operators Guide for specific details about how to set parameters with the Take Action dialog.

Note: The *Upgrade Server Components* task automatically restarts the BES root server service.

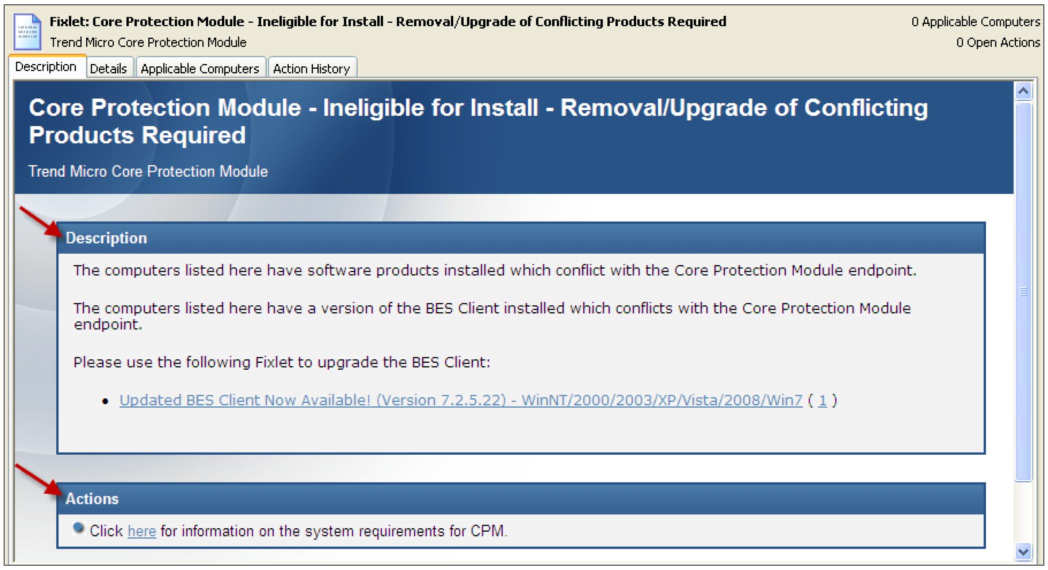
Removing Conflicting Products

If you are unable to install CPM *for Mac* on a particular endpoint, this could mean that the computer is "relevant" to the *Removal of Conflicting Product* Fixlet. To resolve this issue, you should remove the conflicting product before proceeding.

Click the *Removal of Conflicting Product Required* Fixlet located in the Troubleshooting node of the navigation tree.


Troubleshooting
Improper Service Status (0)
Restart Needed (0)
Insufficient Hardware Resources (0)
Insufficient Software Resources (0)
Removal of Conflicting Product Required (0)
Disable Windows Firewall (0)

Follow the directions listed in the Description box, or click where indicated in the Actions box to review CPM system requirements.


Fixlet: Core Protection Module - Ineligible for Install - Removal/Upgrade of Conflicting Products Required
Trend Micro Core Protection Module
0 Applicable Computers
0 Open Actions
Description
Details
Applicable Computers
Action History

Core Protection Module - Ineligible for Install - Removal/Upgrade of Conflicting Products Required

Trend Micro Core Protection Module

Description

The computers listed here have software products installed which conflict with the Core Protection Module endpoint.

The computers listed here have a version of the BES Client installed which conflicts with the Core Protection Module endpoint.

Please use the following Fixlet to upgrade the BES Client:

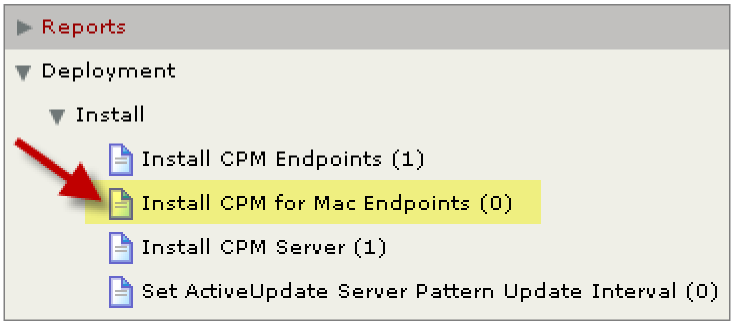
- Updated BES Client Now Available! (Version 7.2.5.22) - WinNT/2000/2003/XP/Vista/2008/Win7 (1)

Actions

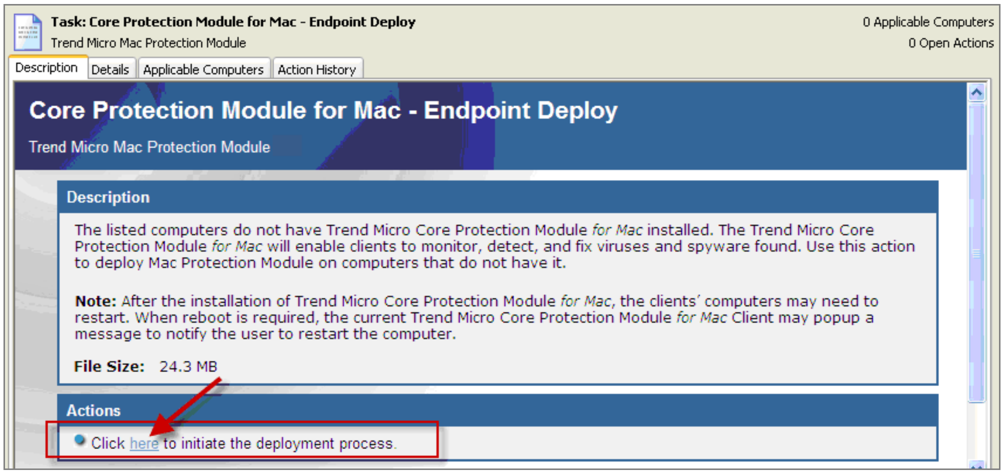
- Click here for information on the system requirements for CPM.

Installing Endpoints

To install endpoints, go to the Deployment node of the navigation tree, select *Install,* then click on the *Install CPM for Mac Endpoints* task to target and deploy CPM to relevant computers.


Reports
Deployment
Install
Install CPM Endpoints (1)
Install CPM for Mac Endpoints (0)
Install CPM Server (1)
Set ActiveUpdate Server Pattern Update Interval (0)

At the Endpoint Deploy Task window, go to the Actions box and click where indicated to initiate the deployment process.



Core Protection Module for Mac - Endpoint Deploy

Trend Micro Mac Protection Module

Description

The listed computers do not have Trend Micro Core Protection Module *for Mac* installed. The Trend Micro Core Protection Module *for Mac* will enable clients to monitor, detect, and fix viruses and spyware found. Use this action to deploy Mac Protection Module on computers that do not have it.

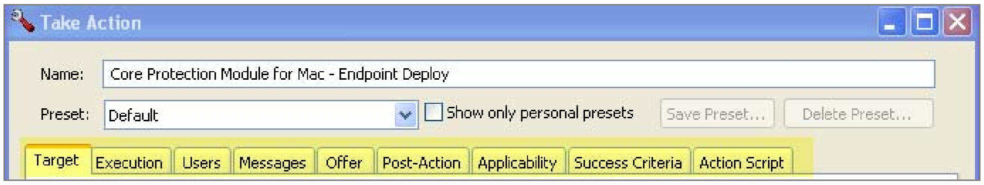
Note: After the installation of Trend Micro Core Protection Module *for Mac*, the clients' computers may need to restart. When reboot is required, the current Trend Micro Core Protection Module *for Mac* Client may popup a message to notify the user to restart the computer.

File Size: 24.3 MB

Actions

- Click here to initiate the deployment process.

Set your desired parameters for this task by using the "tabs" presented in the Take Action dialog. Then click *OK*.



Name: Core Protection Module for Mac - Endpoint Deploy

Preset: Default ☐ Show only personal presets

For questions regarding Configuration, Reports or Tasks in CPM, please refer to the CPM 1.6 User's Guide.

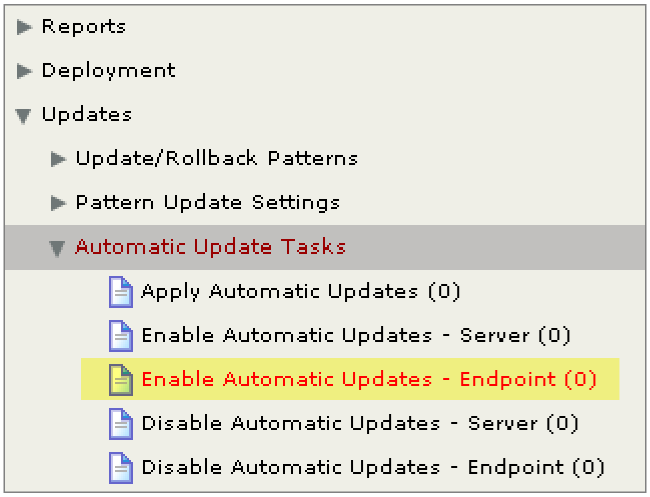
Automatic Updates to CPM *for Mac* Endpoints

After deploying CPM *for Mac* endpoints, you may want to configure the Automatic Updates feature. If this feature has not been configured before, please refer to the Core Protection Module Users Guide for specific information. You may also review the CPM Automatic Update knowledge base article available on the BigFix support website.

If the Automatic Updates feature was previously configured, you will only need to enable and apply Automatic Updates to the newly deployed CPM *for Mac* endpoints.

The following tasks are located in the CPM Dashboard under Updates/Automatic Update Tasks:

1. Run the *Core Protection Module - Enable Automatic Updates – Endpoint* task on CPM *for Mac* endpoints. When the Fixlet window opens, click where indicated in the Actions box to enable Automatic Updates.


▶ Reports
▶ Deployment
▼ Updates
▶ Update/Rollback Patterns
▶ Pattern Update Settings
▼ Automatic Update Tasks
Apply Automatic Updates (0)
Enable Automatic Updates - Server (0)
Enable Automatic Updates - Endpoint (0)
Disable Automatic Updates - Server (0)
Disable Automatic Updates - Endpoint (0)

Note: There is a corresponding *Disable Automatic Updates – Endpoint* task. If you want to stop selected endpoints from automatically updating pattern files, target them with this disable task.

2. Issue a policy action using the *Core Protection Module - Apply Automatic Updates* task (as shown in the image above). You may already have a policy action previously deployed for CPM for Windows endpoints. You will need to issue an additional policy action for new CPM *for Mac* endpoints.This policy action monitors the latest pattern file versions and applies them to endpoints with Automatic Updates enabled. The action should be targeted at all CPM *for Mac* endpoints and set with the following parameters:

   - Never expire
   - Re-apply whenever relevant
   - Retry up to 99 times on failure
   - Re-apply an unlimited number of times

Part 3

What’s Different about CPM *for Mac*

CPM *for Mac* includes most of the functionality of CPM plus additional features, such as Fixlets, tasks, charts and procedures. The tables below display a description of these changes or features and where they are located in the CPM Dashboard.

Reports

Report	*Description*	*Location*
Overview Report	Includes health status of both Windows and Mac endpoints	Reports > Overview
Version Report	New Anti-Virus Engine Version (*for Mac*) pie chart	Reports > Versions
	New CPM *for Mac* Program Version pie chart added	Reports > Versions
	Anti-Virus Pattern Versions pie chart supports Windows *and* Mac endpoints	Reports > Versions
	Spyware Active-Monitor Pattern Version pie chart supports Windows *and* Mac endpoints	Reports > Versions
Infection Report	New Top Mac Malware Infections pie chart	Reports > Infections
	New Mac Malware Infections data chart	Reports > Infections
	Infected Computers Report now supports Mac clients	Reports > Infections
Web Reputation	Blocked Sites Report now supports Mac clients	Reports > Web Reputation

Wizards

All wizards are located under Configuration and their respective sub-nodes of the navigation tree.

Wizard	*Change Summary*	*Change Detail*
Pattern Update Rollback Wizard	Change in available pattern updates displayed – Virus Scan engine for Mac is included	After server components upgrade, the wizard will show pattern updates for both CPM and CPM *for Mac* clients. The rollback feature is supported for CPM but not CPM *for Mac.*
Pattern Update Settings Wizard	Virus Scan Engine for Mac	After server components are upgraded, the setting to enable/disable update of Virus Scan Engine for Mac is available for configuration.
On-Demand Scan Settings Wizard	Spyware/Grayware actions/options	Not supported in CPM *for Mac.* Virus/Malware settings are used instead.
	Files to Scan	Not supported in CPM *for Mac.* Windows client filters by extension, whereas Mac takes lists of file names. There are different target options for CPM and CPM *for Mac.*
	Scan Compressed files max layers	Not supported on CPM *for Mac.*
	Scan Boot Area	Not supported on CPM *for Mac.*
	Enable IntelliTrap	Not supported on CPM *for Mac.*
	CPU Setting "Medium"	Mapped to "Low" in CPM *for Mac.*
	Scan Exclusion options	Not supported on CPM *for Mac.*
	"Rename" action option	Not supported on CPM *for Mac.*
	Specific action for virus type	Use defaults (Clean/Quarantine).
	Back up files before cleaning	Not supported on CPM *for Mac.*
	Display notification message	Not supported on CPM *for Mac.*
	Scan Now option	CPM *for Mac* does not support specifying alternate configuration files for running custom scans, so this option is only available in CPM.

Tasks

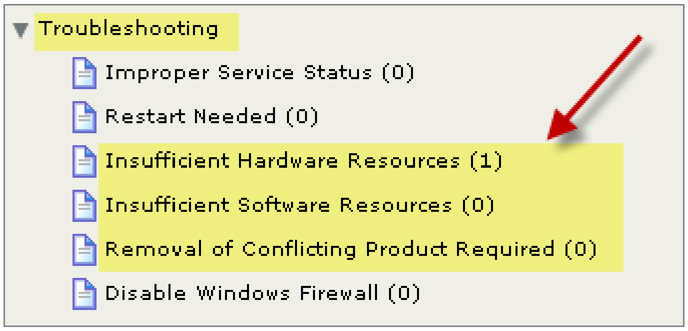
Task	*Description*	*Location*
Install CPM *for Mac* Endpoints	Enables you to install CPM on your Mac endpoints	Deployment > Install
Four new CPM *for Mac* Endpoint analyses	Includes analyses that report on configuration and infection information	Analyses > CPM *for Mac* Endpoints
Two new Web Reputation *for Mac* analyses	Enables you to view site statistics and client information on endpoints	Analyses > Web Reputation *for Mac*

Part 4

Appendix

Troubleshooting

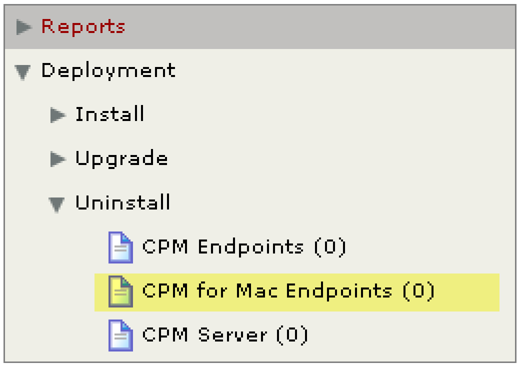
Five of the Fixlets listed in the Troubleshooting node of the navigation tree enable you to resolve issues identified in the Health Status Chart under Deployment/Overview. Three audit Fixlets, shown below, specifically detect machines that are ineligible for a CPM installation:

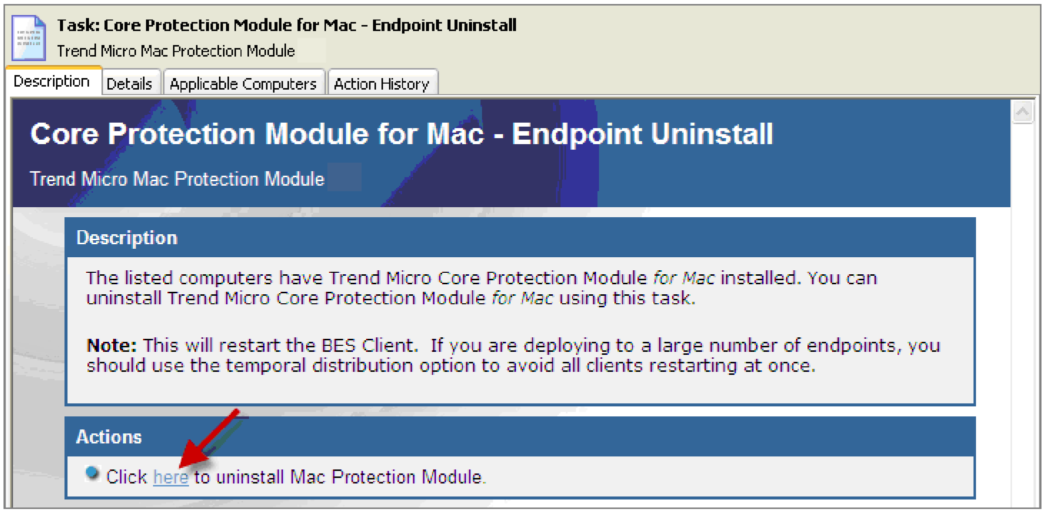

Troubleshooting
Improper Service Status (0)
Restart Needed (0)
Insufficient Hardware Resources (1)
Insufficient Software Resources (0)
Removal of Conflicting Product Required (0)
Disable Windows Firewall (0)

The remaining Fixlets identify machines with improper service status or machines that require a restart.

Uninstalling CPM *for Mac*

To uninstall CPM *for Mac* from your environment, click *Uninstall* under the *Deployment* node of the navigation tree to find the *CPM for Mac Endpoints* uninstall tool.





Task: Core Protection Module for Mac - Endpoint Uninstall
Trend Micro Mac Protection Module

Core Protection Module for Mac - Endpoint Uninstall

Trend Micro Mac Protection Module

Description

The listed computers have Trend Micro Core Protection Module *for Mac* installed. You can uninstall Trend Micro Core Protection Module *for Mac* using this task.

Note: This will restart the BES Client. If you are deploying to a large number of endpoints, you should use the temporal distribution option to avoid all clients restarting at once.

Actions

Click here to uninstall Mac Protection Module.

After removing all of the binary components, you should also stop any open CPM policy actions, such as actions taken from the *Set ActiveUpdate Pattern Update Interval* or *Apply Automatic Updates* tasks, as well as any client offers you may have issued.

Technical Support

BigFix offers a suite of support options to help optimize your user-experience and success with this product. Here's how it works:

- First, check the BigFix website Documentation page:
- Next, search the BigFix Knowledge Base for applicable articles on your topic:
- Then check the User Forum for discussion threads and community-based support:

If you still can't find the answer you need, contact BigFix's support team for technical assistance:

Phone/US:	866 752-6208 (United States)
Phone/International:	661 367-2202 (International)
Email:	enterprisesupport@bigfix.com