



# Core Protection Module 1.6 for Mac

*powered by*  **TREND  
MICRO**

---

User's Guide

July, 2010

Copyright © 2010 BigFix, Inc. All rights reserved.

Copyright © 1998-2010 Trend Micro Incorporated.

BigFix®, Fixlet®, Relevance Engine®, Powered by BigFix™ and related BigFix logos are trademarks of BigFix, Inc.

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, Damage Cleanup Services, ScanMail, ServerProtect, and TrendLabs are trademarks or registered trademarks of Trend Micro, Inc. or its affiliated entities. All other product or company names may be trademarks or registered trademarks of their respective owners. BigFix and Trend Micro use of any other company's trademarks, trade names, product names and logos or images of the same does not necessarily constitute: (1) an endorsement by such company of BigFix, Trend Micro, or their products, or (2) an endorsement of such company or its products by either BigFix or Trend Micro.

No part of this documentation or any related software may be reproduced, transmitted, or otherwise distributed in any form or by any means (electronic or otherwise) without the prior written consent of BigFix, Inc. or Trend Micro, Inc. You may not use, modify, perform or display this documentation or any related software for any purpose except in connection with your use or evaluation of the BigFix/Trend Micro software delivered herewith as expressly set forth in a separate written agreement executed by BigFix, Inc. or Trend Micro, Inc. and any other use, including the reverse engineering of such software or creating compatible software or derivative works, is prohibited. If the license to the software that this documentation accompanies is terminated, you must immediately return this documentation and any related software to BigFix, Inc. or Trend Micro, Inc., or destroy all copies thereof that you may have and so certify upon request by BigFix, Inc. or Trend Micro Incorporated.

Both BigFix, Inc. and Trend Micro, Inc. reserve the right to make changes to this document and to the products described herein without notice.

All rights reserved.

# Contents

<b>PART 1</b> .....	<b>4</b>
<b>Get Started</b> 4	
System Requirements .....	4
Incompatible Software.....	4
Process Overview .....	5
<b>PART 2</b> .....	<b>6</b>
<b>Upgrade</b> 6	
Upgrading Server Components .....	6
Removing Conflicting Products .....	7
Installing Endpoints.....	8
Automatic Updates to CPM for Mac Endpoints.....	9
<b>PART 3</b> .....	<b>11</b>
<b>What's Different about CPM for Mac</b> 11	
Reports.....	11
Wizards.....	12
Tasks.....	12
<b>PART 4</b> .....	<b>13</b>
<b>Appendix</b> 13	
Troubleshooting .....	13
Uninstalling CPM for Mac .....	13
Technical Support.....	14

## 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 <i>for Mac</i> update components
Deploy CPM <i>for Mac</i> Endpoints	Deploy the CPM Clients
Activate Analyses	Tell CPM <i>for Mac</i> Clients to report on their configuration and status
Configure Endpoints	Use Tasks and Wizards to customize CPM <i>for Mac</i> settings

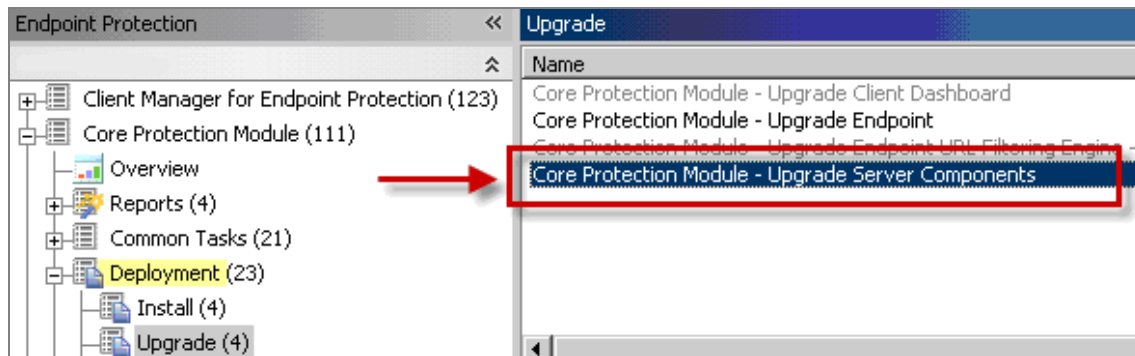
## Upgrade

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.

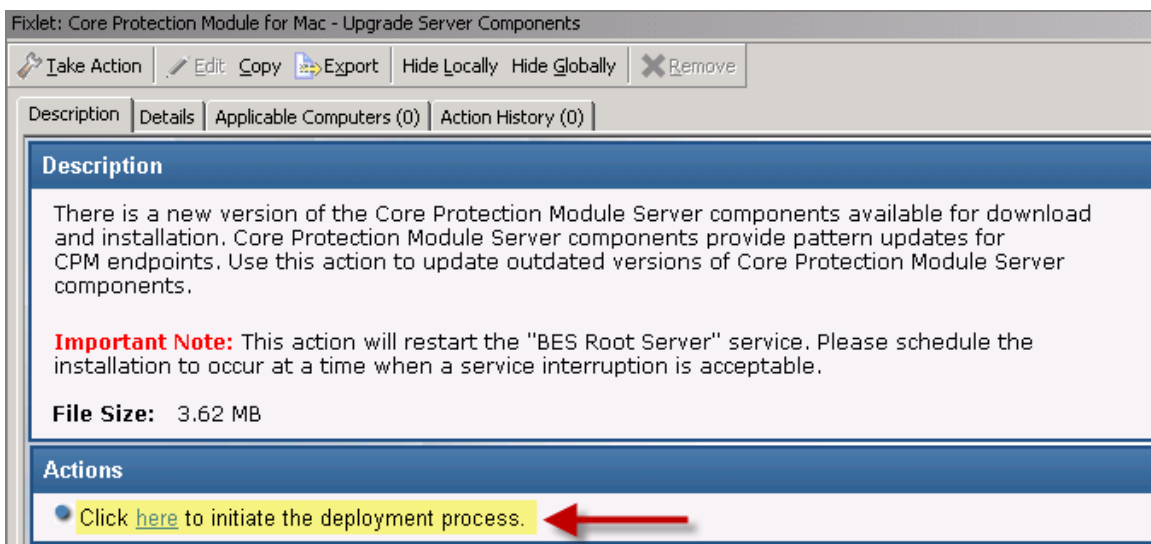
### Upgrading Server Components

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 Server Components* task in the list panel on the right.



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.



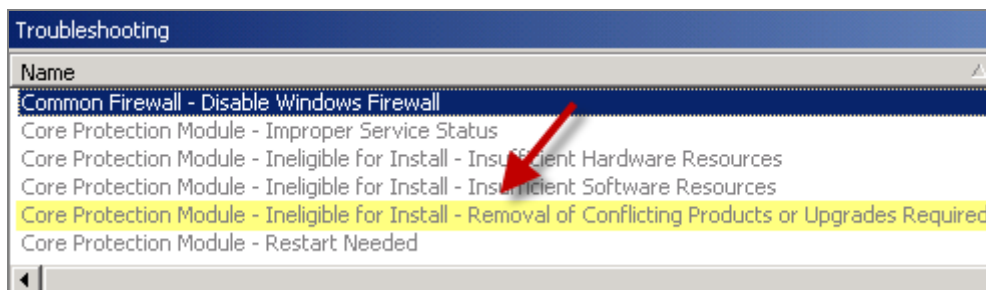
When the Take Action dialog opens, go through the tabs (Target, Execution, etc.) to customize this action within your system, then click *OK*. Check the [BigFix Console Operators Guide](#) for specific details about how to set parameters with the Take Action dialog.

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

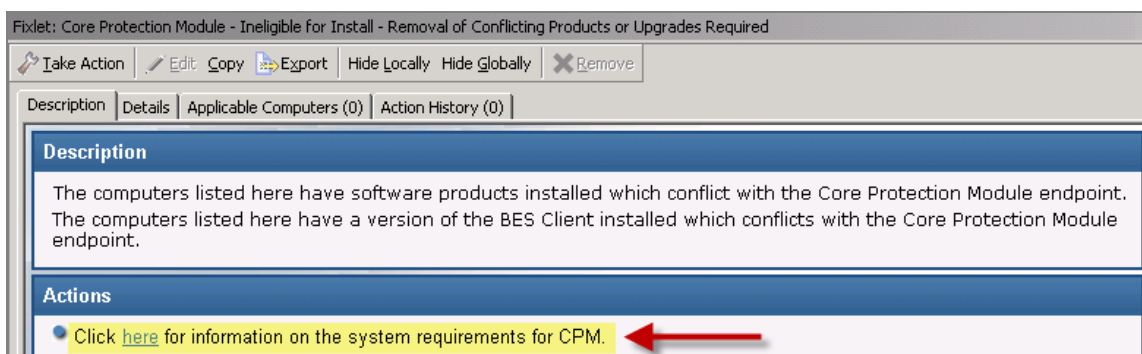
## Removing Conflicting Products

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.

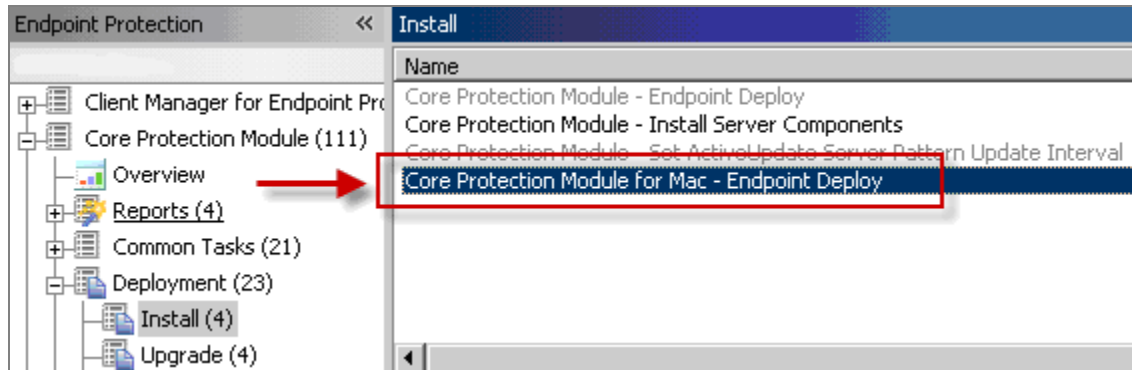


Follow the directions listed in the Description box, or click where indicated in the Actions box to review CPM system requirements.

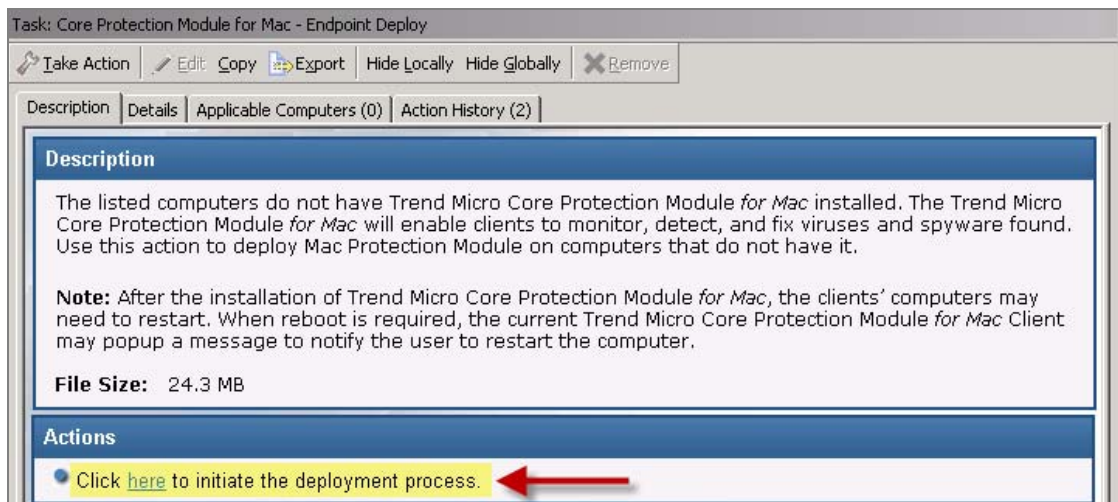


## Installing Endpoints

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



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

For questions regarding Configuration, Reports or Tasks in CPM, please refer to the [CPM Version 1.6 User's Guide](#) on the BigFix support website.

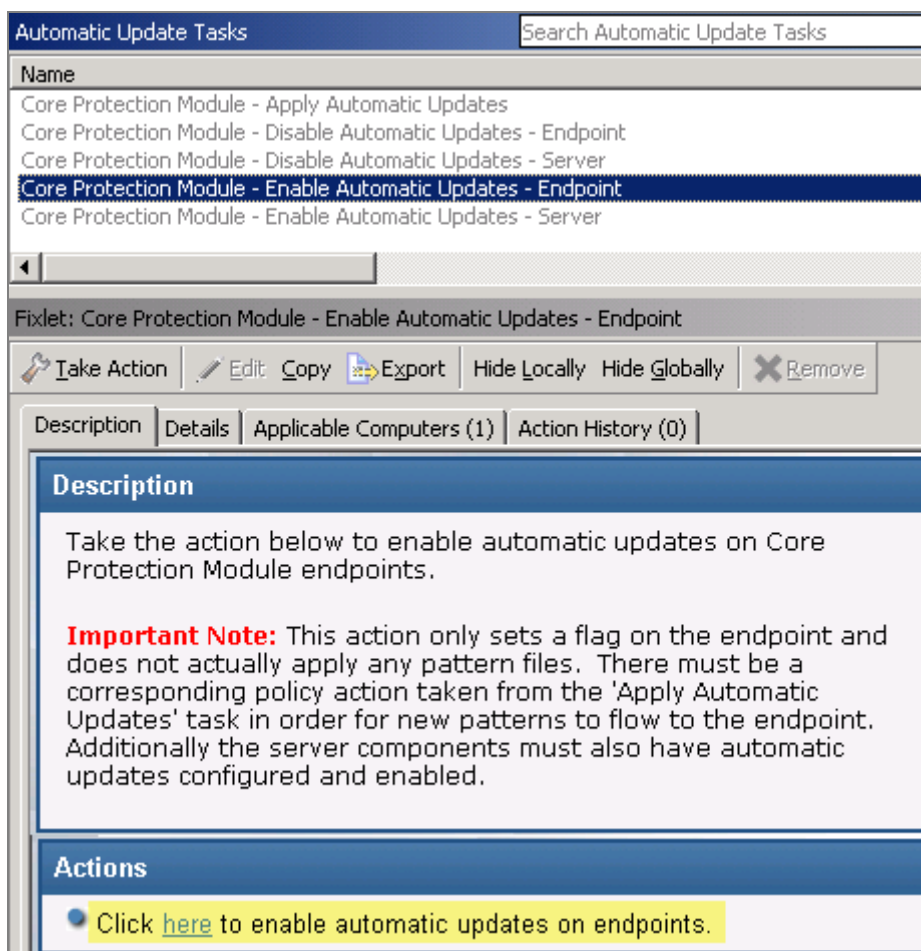
## Automatic Updates to CPM for Mac Endpoints

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 navigation tree 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.



**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

## 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

<i>Report</i>	<i>Description</i>	<i>Location</i>
<b>Overview Report</b>	Includes health status of both Windows and Mac endpoints	Reports > Overview
<b>Version Report</b>	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
<b>Infection Report</b>	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
<b>Web Reputation</b>	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.

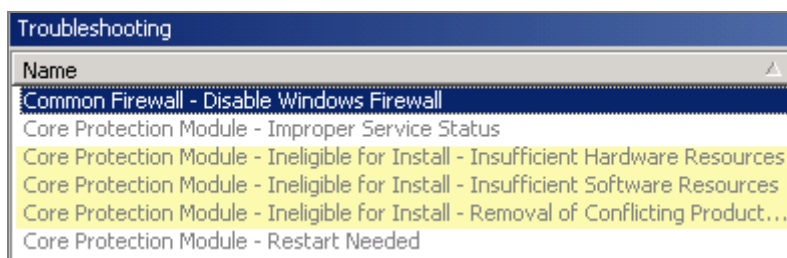
<i>Wizard</i>	<i>Change Summary</i>	<i>Change Detail</i>
<b>Pattern Update Rollback Wizard</b>	Change in available pattern updates displayed – Virus Scan engine for Mac is included	After server components upgrade, the wizard will show pattern updates for both CPM and CPM for Mac clients. The rollback feature is supported for CPM but not CPM for Mac.
<b>Pattern Update Settings Wizard</b>	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.
<b>On-Demand Scan Settings Wizard</b>	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

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

## Troubleshooting

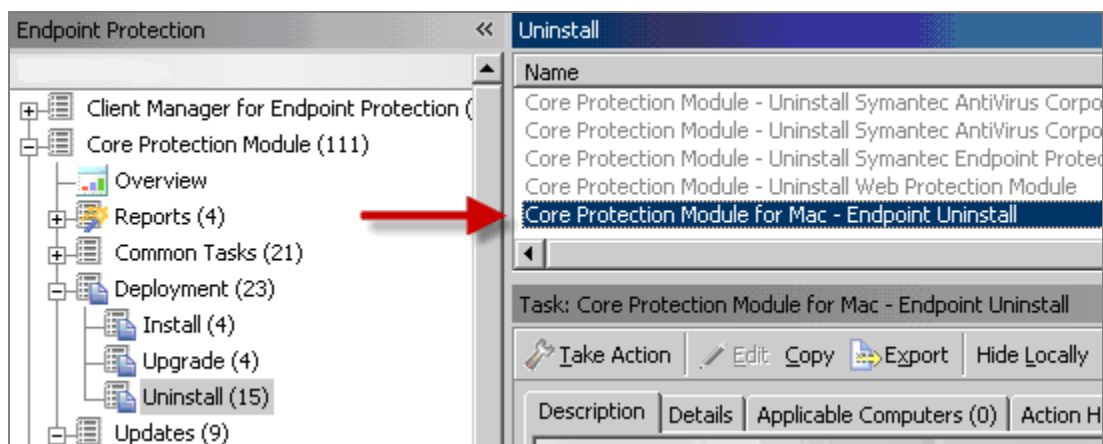
Five of the Fixlets listed in the Troubleshooting node of the navigation tree enable you to resolve issues identified in the Health Status Chart under Deployment/Overview. Three audit Fixlets, shown below, specifically detect machines that are ineligible for a CPM installation:

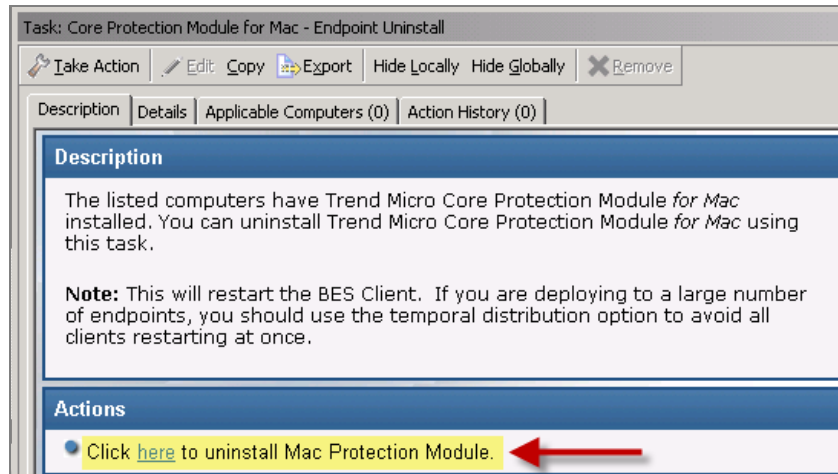


The remaining Fixlets identify machines with improper service status or machines that require a restart.

## 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.





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](mailto:enterprisesupport@bigfix.com)