

**BigFix Compliance
Client Manager for Endpoint Protection**



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page xxxvi\)](#).

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview.....	5
System requirements.....	5
Dashboards.....	6
Chapter 2. Installation.....	9
Subscribe to the CMEP site.....	9
Activate analyses and tasks.....	9
Chapter 3. Using CMEP.....	12
Overview.....	12
Using the computer filter.....	14
Creating new computer filters.....	15
Updating existing filters.....	15
How to update.....	16
Print to PDF.....	19
Wizards.....	20
Create Update Task Wizard.....	20
Windows Defender Update Wizard.....	23
McAfee On-Demand Scan Wizard.....	26
Chapter 4. Device control.....	30
USB storage.....	32
Appendix A. Support.....	34
Appendix B. Frequently asked questions.....	35
Notices.....	xxxvi

Chapter 1. Overview

BigFix *Client Manager for Endpoint Protection* (CMEP) encompasses Anti-Virus, spyware tools, and device control capabilities.

This application allows the management of endpoint security clients from vendors such as McAfee, Symantec, Windows Defender (also known as Microsoft Defender), Sophos, and Trend Micro. More than just a way to put anti-malware defense under a BigFix umbrella, *CMEP* brings unprecedented scalability, speed, and thoroughness to keep organizations steps ahead of external threats.

The CMEP application includes the following features:

- Real-time visibility into the current health and status of vendor-acquired endpoint security clients
- Management and remediation of unhealthy, vendor-acquired endpoint security clients where possible
- Uninstall tools to enable easy switch-out of incumbent endpoint protection tools
- Web-based reporting to monitor migration progress in real time, with drill-down details
- Closed-loop verification of updates, signature definition files, and more even if endpoints are disconnected from the network
- Unparalleled scalability and speed a single management server can support up to 250,000 endpoints with updates made in minutes

CMEP is intended to supersede the BigFix *Client Manager for Anti-Virus* (CMAV) content site. CMEP contains all of the functions of CMAV, including some additional features:

- New and improved dashboard interface to manage each functional area
- Support for Windows 7 on Symantec, McAfee, and Trend Micro supported products
- Support for Windows 2008 on Symantec, Trend Micro, and Sophos
- Support for Mac on McAfee and Symantec
- Inclusion of device control capability
- Inclusion of the computer filtering feature
- Inclusion of the export to PDF feature

System requirements

This topic describes the requirements before you install and use the BigFix CMEP in console.

Supported products matrix

CMEP offers support for a variety of anti-virus products. The current supported anti-virus products and product versions are listed in the following table:



Important: CMEP only supports the endpoints with Mac and Windows platforms. See the BigFix CMEP Support Matrix for latest information on the supported AV products and functions at <https://bigfix-wiki.hcltechsw.com/wikis/home?lang=en-us#!/wiki/BigFix%20Wiki/page/CMEP%20Support%20Matrix>.

Table 1. Supported products**List of supported anti-virus products for CMEP**

Vendor	Product	Version
McAfee	Endpoint Security	10.x
	Endpoint Security for Mac	10.x
	VirusScan	8.x
	VirusScan for Mac	9.x
	McAfee Security for Microsoft Exchange	8.5
Microsoft	Windows Defender	All known versions
Symantec	Endpoint Protection	12.1, 14
	Endpoint Protection for Macintosh	12, 14
Sophos	Endpoint Security	9.x, 10.x
	Antivirus for Mac	7.x, 8.x (Audit only *)
Trend Micro	OfficeScan	XG
	ServerProtect	5.8
	Trend Micro Security for Mac	1.5, 2.0

**Audit only* Fixlets detect virus definitions that are more than seven days old.

**Notes:**

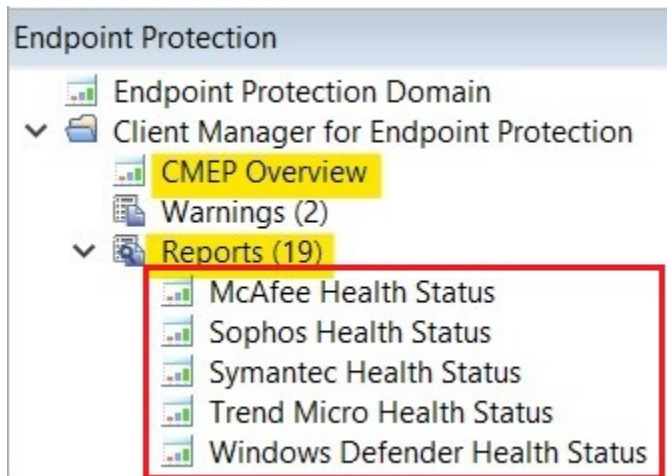
- The vendor defines the supported platform for each anti-virus product. Refer to the vendor website to review the support matrix for a product.
- For each supported anti-virus product, CMEP supports all the platforms that are currently supported by the anti-virus product, as long as the platform is also supported by the BigFix agent. To verify the BigFix support scope, see the [Detailed System Requirement](#).

Dashboards

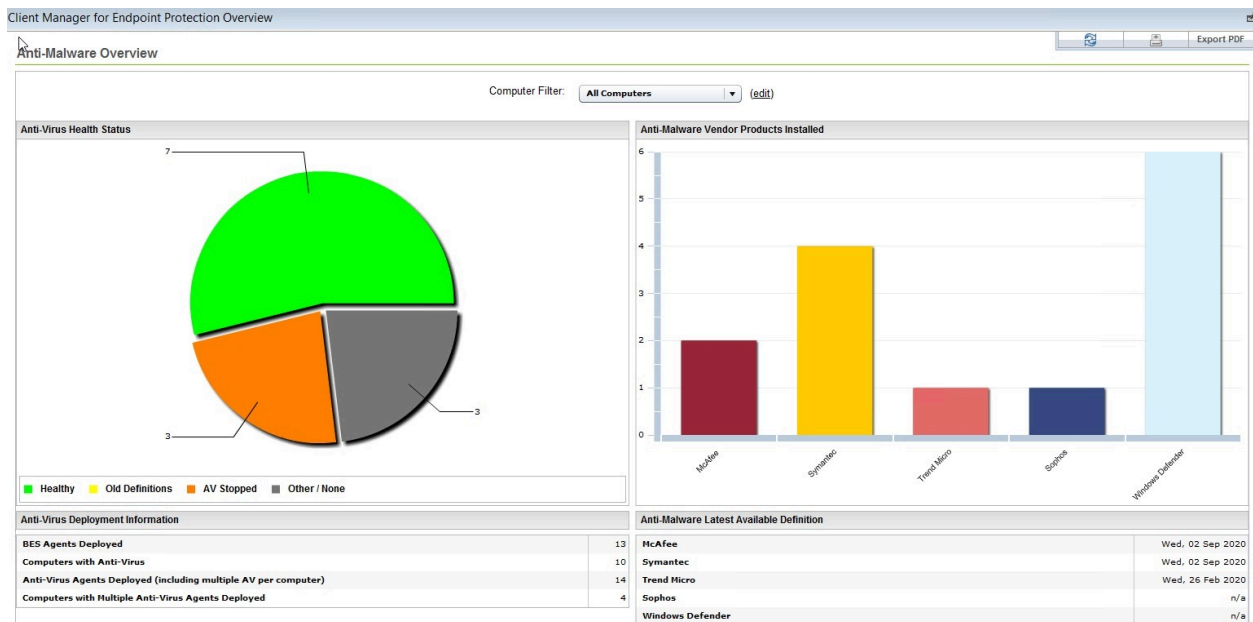
The Dashboards in CMEP include overview pie chart reports that summarize the anti-malware products within your deployment.

You can view an overview of *all* anti-malware products, or view each pie chart individually.

The *CMEP Overview* dashboard is located at the top of the CMEP navigation tree, which is found under the Endpoint Protection Domain. The remaining dashboards are located under the Reports node.



The *CMEP Overview* dashboard contains an Anti-Virus Health Status pie chart, and a graph displaying the vendor products installed in your deployment. Each chart contains a corresponding summary table below it.

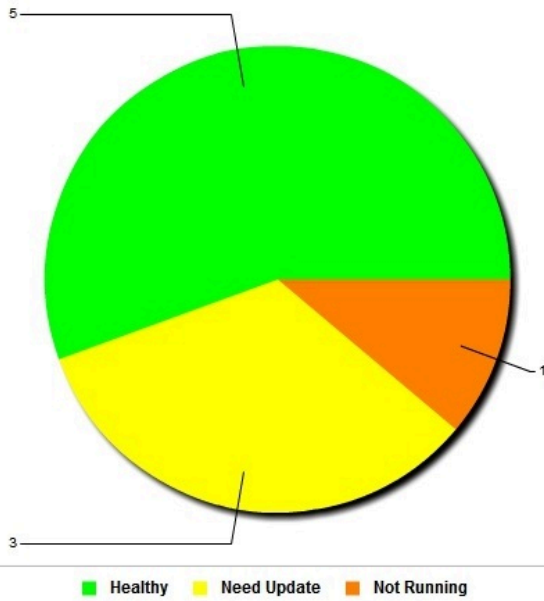


The following image displays individual dashboards by vendor:

McAfee

  Export PDFComputer Filter: **All Computers** [\(edit\)](#)

Agent Status



Latest Available Definition

Wed, 02 Sep 2020

Analyses

McAfee VirusScan Enterprise 8.7/8.8 - Client Information	Activated
McAfee VirusScan: On-Demand Scan - Configuration	Activated
McAfee VirusScan: On-Demand Scan - Configuration	Activated
McAfee Security for Microsoft Exchange v8.5 - Client	Activated
McAfee VirusScan Enterprise 8.7/8.8 - Virus Information	Activated
McAfee VirusScan 9.x for Mac - Client Information	Activated
McAfee Endpoint Security 10.x for Mac - Client	Activated

Chapter 2. Installation

Before beginning the installation, log in to the BigFix console and become familiar with its basic operation. If you have questions about how to use the BigFix console, see the [BigFix Console Operator's Guide \(opens in new window\)](#) before using this publication.

Installation and setup of CMEP involves two basic steps:

- *Site subscription*
- *Activating tasks and analyses*

Subscribe to the CMEP site

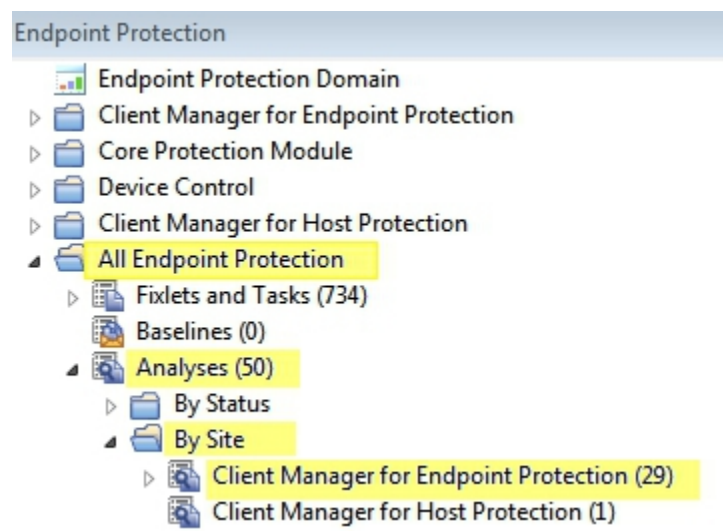
The process for site subscription depends on the version of the BigFix console that you have.

The CMEP site contains tasks, analyses, wizards and Fixlets for protecting your deployment from malware. You must be subscribed to the CMEP site to collect data from the BigFix clients. This data is used for reporting and analysis.

Activate analyses and tasks

On successful gathering of the applicable tasks and analyses from the content server, you must deploy those tasks and activate those analyses to make them visible in the BigFix console.

Start by viewing the *All Endpoint Protection* node in the navigation tree. Click *Analyses*, and then click *By Site* and select *Client Manager for Endpoint Protection*. The corresponding number in parentheses indicates how many analyses are available and applicable to the CMEP site.



Click *Client Manager for Endpoint Protection* to display the list of related Analyses in the window.

Analyses	
Status	Name
Not Activated	CA Anti-Virus/Total Defense R12 Client Information
Activated Globally	eTrust (CA) Anti-Virus Client Information - 6.0/7.x
Activated Globally	eTrust (CA) Anti-Virus Client Information - 8.x
Not Activated	eTrust (CA) Anti-Virus Client Information - 8.x for MAC
Not Activated	Forefront Client Security - Client Information
Not Activated	Forefront Endpoint Protection - Client Information
Not Activated	ISS Proventia Desktop
Not Activated	McAfee AVERT Stinger Information
Activated Globally	McAfee GroupShield / Security - Client Information
Activated Globally	McAfee VirusScan - Client Information

This is a composite view:

Endpoint Protection << Analyses	
Status	Name
Not Activated	CA Anti-Virus/Total Defense R12 Client Information
Activated Globally	eTrust (CA) Anti-Virus Client Information - 6.0/7.x
Activated Globally	eTrust (CA) Anti-Virus Client Information - 8.x
Not Activated	eTrust (CA) Anti-Virus Client Information - 8.x for MAC
Not Activated	Forefront Client Security - Client Information
Not Activated	Forefront Endpoint Protection - Client Information
Not Activated	ISS Proventia Desktop
Not Activated	McAfee AVERT Stinger Information
Activated Globally	McAfee GroupShield / Security - Client Information
Activated Globally	McAfee VirusScan - Client Information
Activated Globally	McAfee VirusScan - Client Information - NetShield 4.5
Not Activated	McAfee VirusScan 8.x/9.x for Mac - Client Information

To activate a number of analyses at the same time, highlight the list of analyses and select *Activate* from the right-click menu. Enter your Private Key Password.

After all analyses have been activated, they display with an *Activated* status in the window:

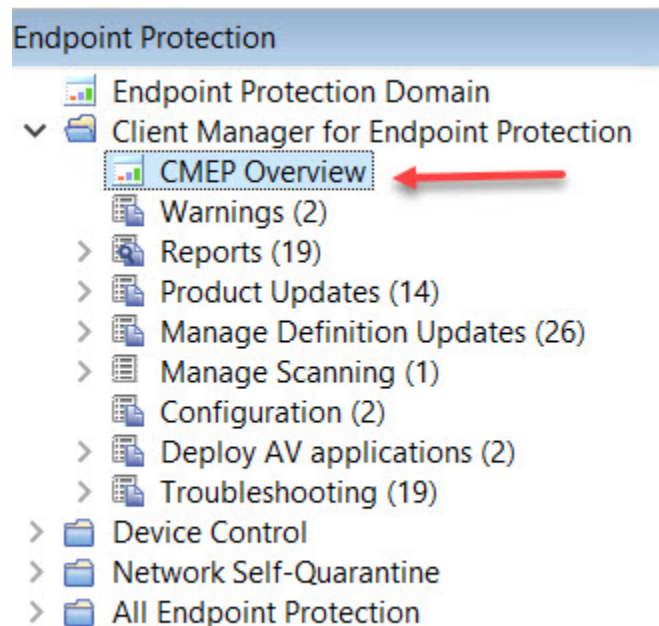
Analyses	
Status	Name
Activated Globally	eTrust (CA) Anti-Virus Client Information - 6.0/7.x
Activated Globally	eTrust (CA) Anti-Virus Client Information - 8.x
Activated Globally	McAfee GroupShield / Security - Client Information
Activated Globally	McAfee VirusScan - Client Information
Activated Globally	McAfee VirusScan - Client Information - NetShield 4.5
Activated Globally	McAfee VirusScan Enterprise 8.5/8.7/8.8 - Virus Information
Activated Globally	McAfee VirusScan: On-Demand Scan - Configuration Information (P
Activated Globally	Sophos Anti-Virus Client Information - 7.x
Activated Globally	Symantec AntiVirus - Client Information - Windows NT/2000/XP/200
Activated Globally	Symantec AntiVirus - Virus Information
Activated Globally	Symantec Endpoint Protection - Client Information - Windows NT/2
Activated Globally	Windows Defender - Configuration Information

For more detailed information about deploying tasks and activating analyses, see the [BigFix Console Operator's Guide](#).

Chapter 3. Using CMEP

Use the **Client Manager Endpoint Manager Overview** window to view and manage the Anti-virus updates of your organization.

You can access the window from **Client Manager for Endpoint Protection** navigation tree of Endpoint Protection domain.

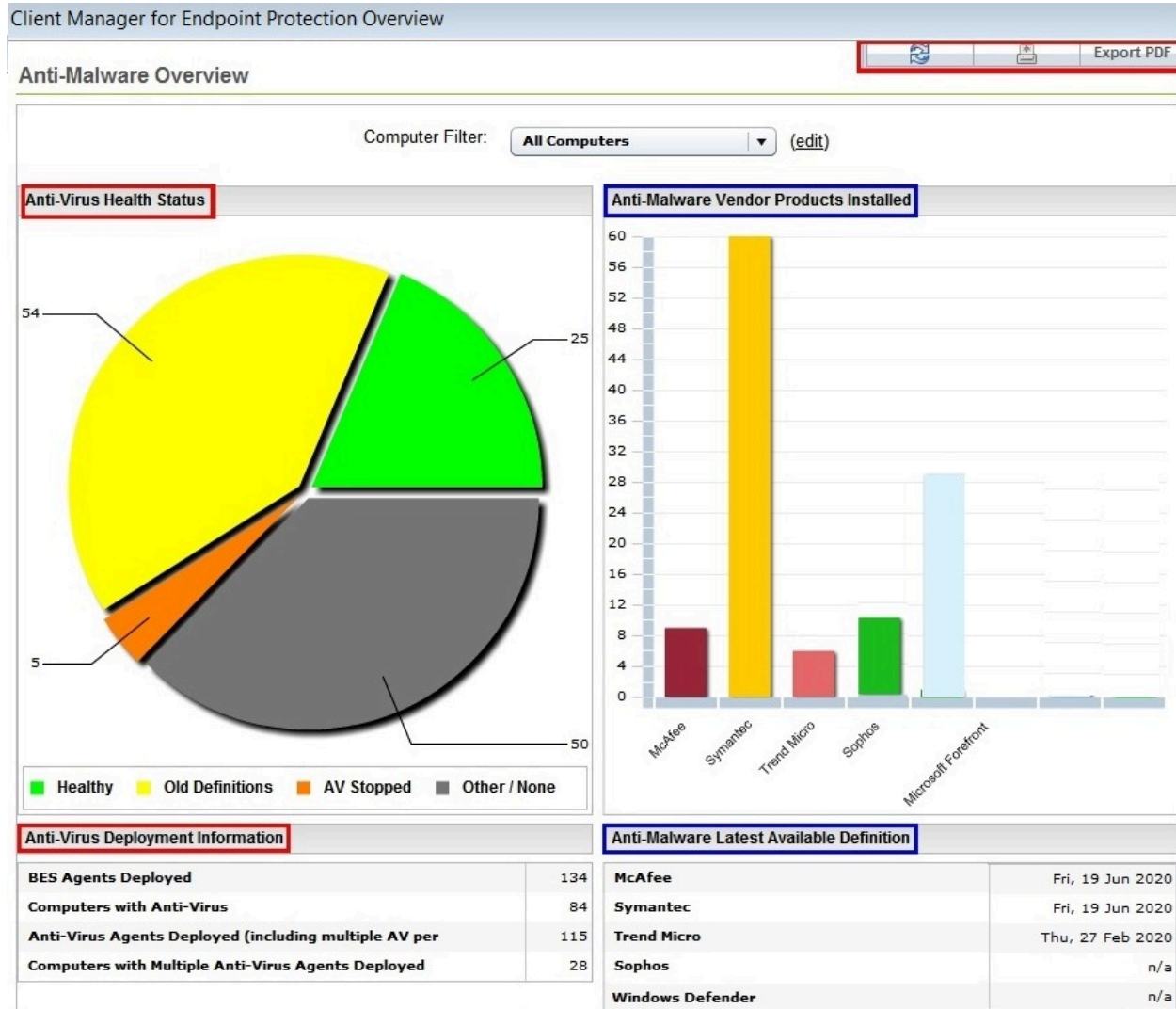


Overview

The **Client Manager for Endpoint Protection Overview** window provides a summary of Anti-Virus health and Anti-Malware products in your deployment.

The left side of the Overview window contains an Anti-Virus Health Status pie chart and Anti-Virus Deployment Information statistics. The right side contains an Anti-Malware Vendor Products bar graph with dates of the latest available Anti-Malware definitions.

The top of the report shows the Computer Filter, which sets the criteria of what is shown in the Overview Report. The upper-right corner includes the Refresh, Printer, and the Export PDF buttons.



The following table illustrates the color-coding used for the Anti-Virus Health Status pie chart, as well as a brief description of each category:

Category	Definition
Healthy	This machine is adequately protected from Malware
Old Definitions	Virus definitions need to be updated on this machine
AV Stopped	The required Anti-Virus application or service(s) are not running
Other / None	This machine uses an unsupported Anti-Virus product, or no Anti-Virus has been installed.

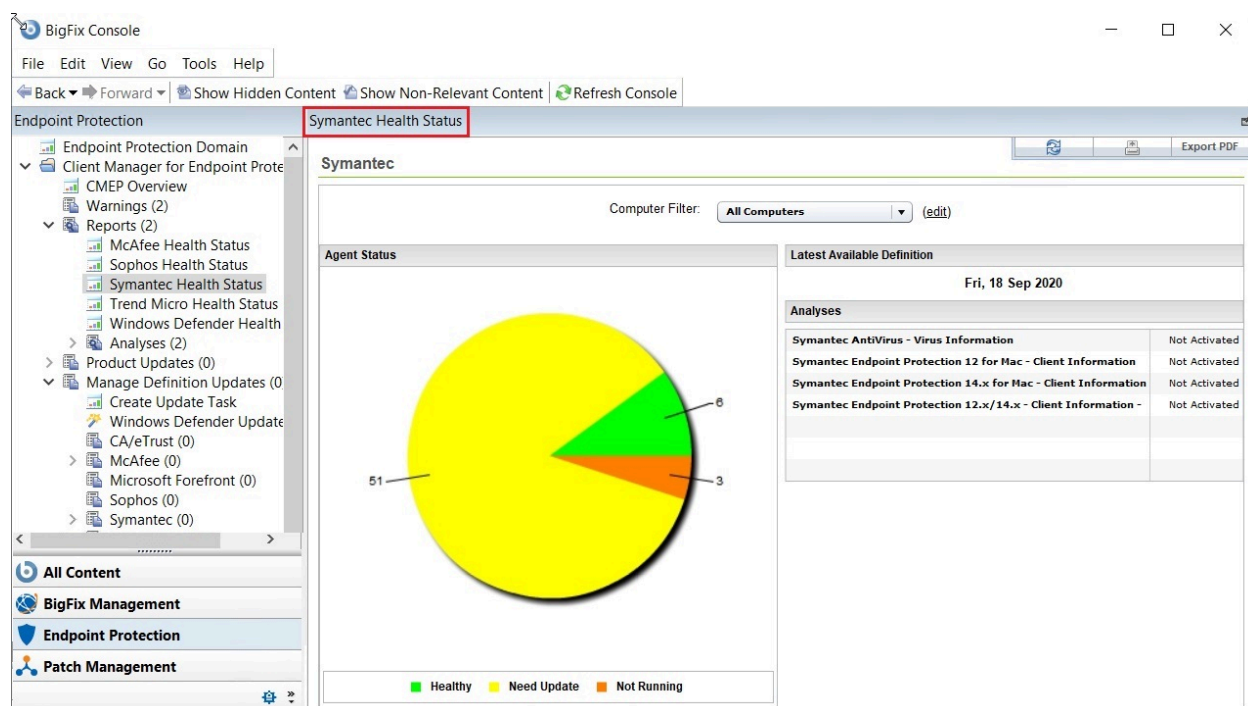


Note: For detailed information about how CMEP defines healthy in the Health Status pie chart, see the related [article](#) on the BigFix support website.

The *Anti-Malware Vendor Products* bar graph is color-coded according to vendor, as shown in the previous image.

McAfee
Symantec
Trend Micro
Sophos
Windows Defender

You can select individual vendors to display a customized pie chart and summary. For example, by selecting to view the Symantec Health Status report, the dashboard displays the Symantec health status pie chart, the date of the latest definition release, and a list of related analyses with either *Activated* or *Not Activated* status.



The **Agent Status** section displays pie charts representing the health and status of your Anti-Virus according to each vendor. Status is measured by the following criteria:

Healthy Anti-Virus applications are running correctly on this machine.

Need Update Virus definitions need to be updated on this machine.

Not Running The required Anti-Virus application or service is not running.

Using the computer filter

Use the computer filter feature to set the criteria of what to include in the Overview window.

The *Computer Filter* section can be found above the *Agent Status* section. From this section, you can select, apply, create, and update filters.

Anti-Malware Overview

Computer Filter: **All Computers** (edit)

By default, the computer filter is set to *All Computers*.

Creating new computer filters

Use this option to create and customize a filter according to your preference.

To create a new computer filter, click *(edit)*, next to the *Computer Filter* pull-down list. The **Create Filter** window opens.

Enter a name for the filter criteria in the **Name** field. Select the **Visibility** checkbox to make the filter criteria available to all operators.

Computer Filter: **All Computers** (edit)

From the first pull-down list in the **Include computers with the following property** section, select the computer properties that will apply the filter criteria you are creating.

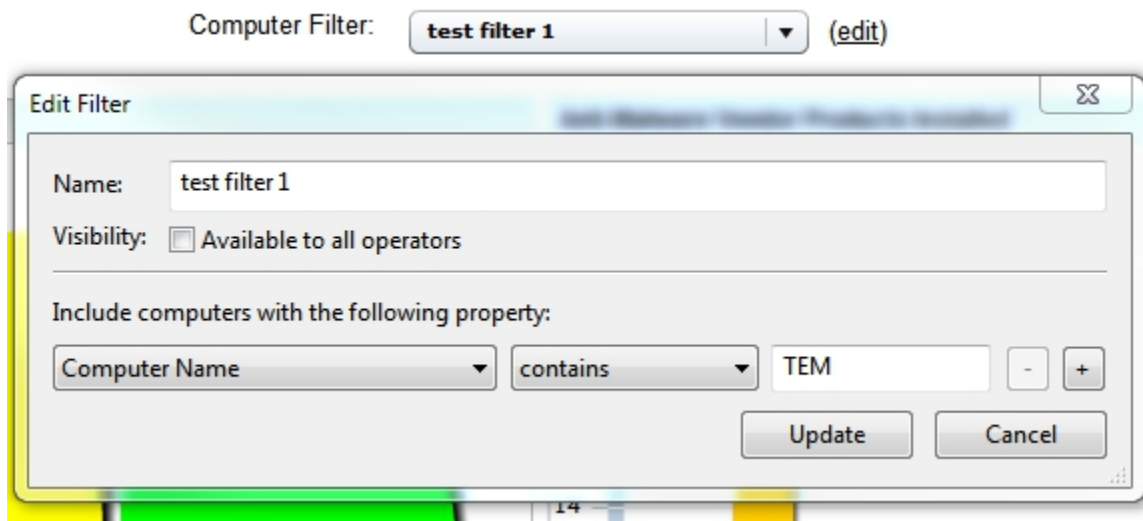
From the next pull-down list, select either *contains* or *does not contain*. Enter the string in the next field. To add more filtering criteria, select **Available to all operators** check box. A new row is added. Follow the same steps to create a new filter criteria.

Click **Create**. The Overview report updates to show the set computer filter settings.

Updating existing filters

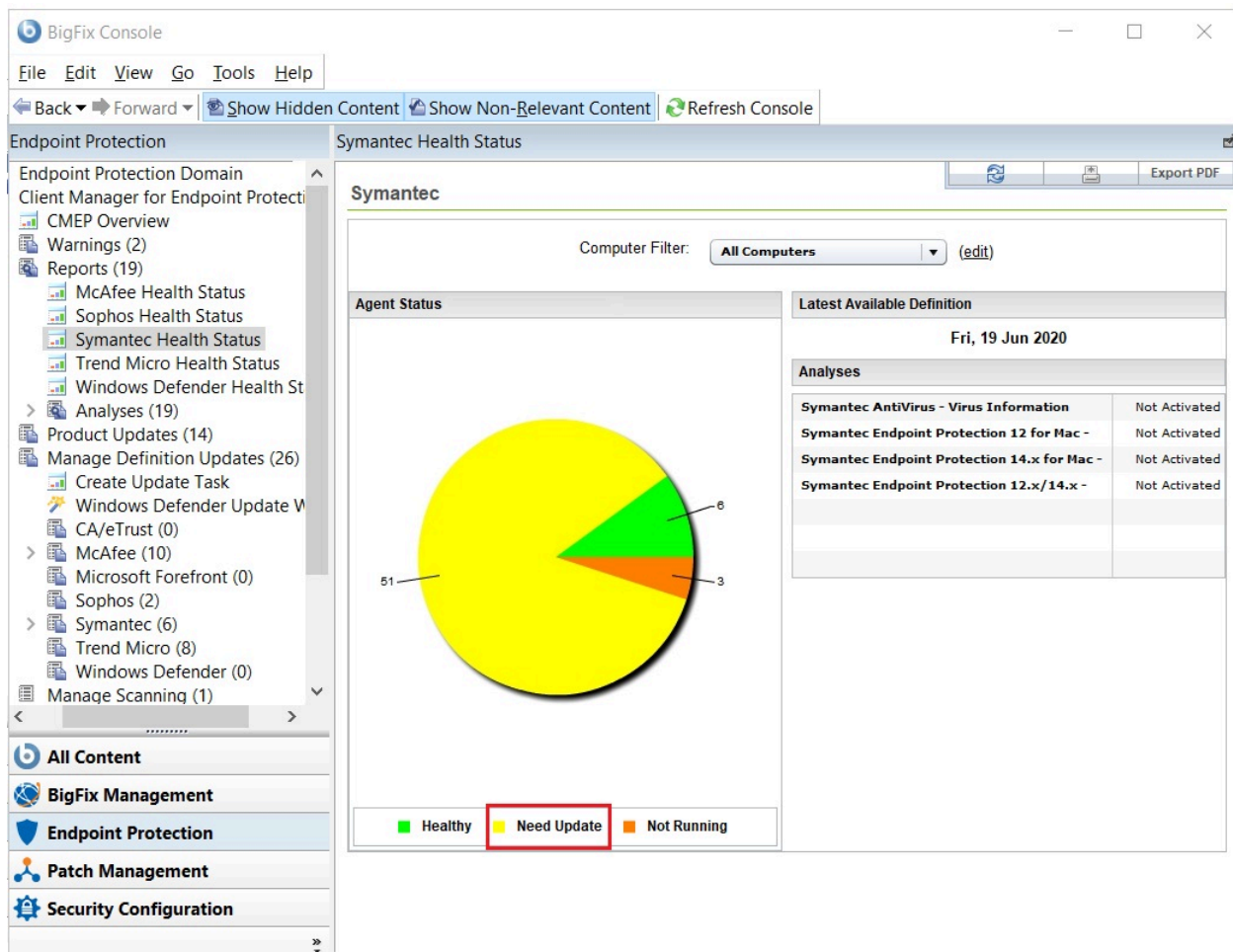
Use this option to update an existing Filter.

To make changes to existing filters, select the filter from the *Computer Filter*: pull-down list, then click **(edit)**. The **Edit Filter** window opens. Edit the filter criteria settings, and click **Update**.



How to update

This section describes if one of your Anti-Malware vendors displays a yellow **Need Update status** in the Agent Status pie chart, you must update your virus definitions to ensure that all applicable computers are adequately protected.



Start by clicking directly on the pie chart to open a new window where you can update the related Fixlets. Click the applicable computer listed under the *Computer Name* column on the right side of the window.

Agent: Symantec Status: Need Update

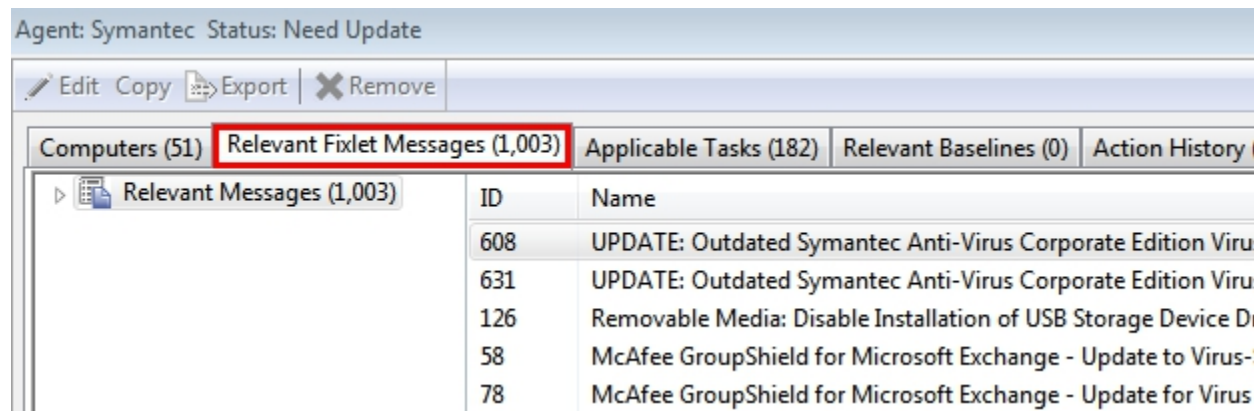
EditCopyExportRemove

Computers (51)Relevant Fixlet Messages (1,003)Applicable Tasks (182)Relevant Baselines (0)Action H

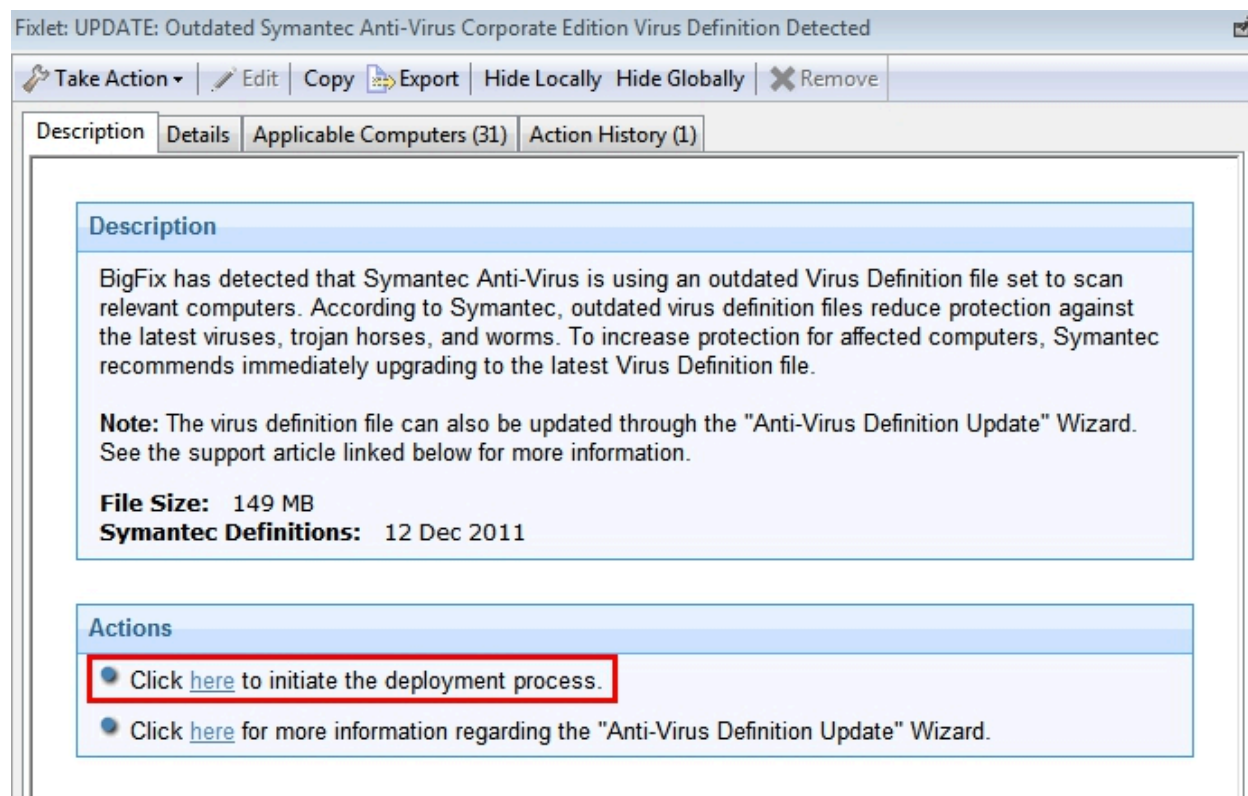
Computers (51)

Computer Na...	OS	CPU
BITLOCKER1	WinVista 6.0.6...	3100 MHz Inte
BITLOCKER3	Win7 6.1.7601	3000 MHz Per
TEMBESSER...	Win2008 6.0.6...	3100 MHz Xec
TEMWIN2K...	Win2003 5.2.3...	3100 MHz Inte
TEMWIN2K...	Win2003 5.2.3...	3100 MHz Inte
TEMWIN2K...	Win2003 5.2.3...	3100 MHz Inte
TEMWIN2K...	Win2003 5.2.3...	3100 MHz Inte
TEMWIN2K...	Win2003 5.2.3...	3100 MHz Inte

Next, click the **Relevant Fixlet Messages** tab to display a list of all applicable Fixlets associated with this computer. Scan the list to find the relevant *update* Fixlet.



Double-click the Fixlet name in the displayed list to open the Fixlet window. Review the description, and click where indicated in the Actions box to start the deployment process.



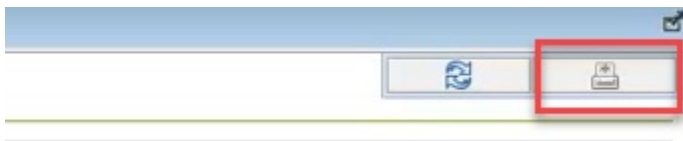
The Take Action dialog opens, where you can set specific parameters for this action. As an alternative, you can also click the *Take Action* pull-down in the top-left corner of the panel. For detailed information about the Take Action dialog, see the [BigFix Console Operator's Guide \(opens in new window\)](#).

Print to PDF

You can export the Overview reports to PDF format.

To print a report, perform the following steps:

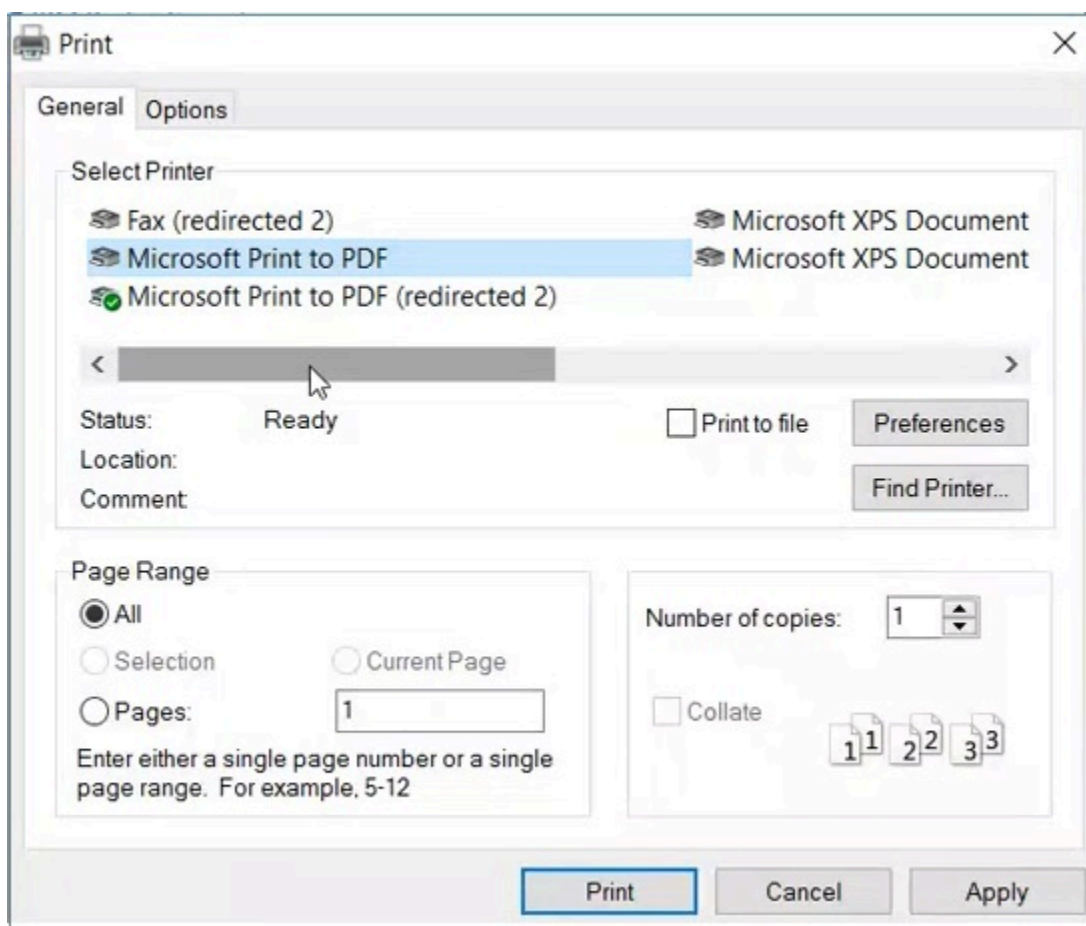
1. At the upper-right corner of the **Overview** window, click **Print** button.



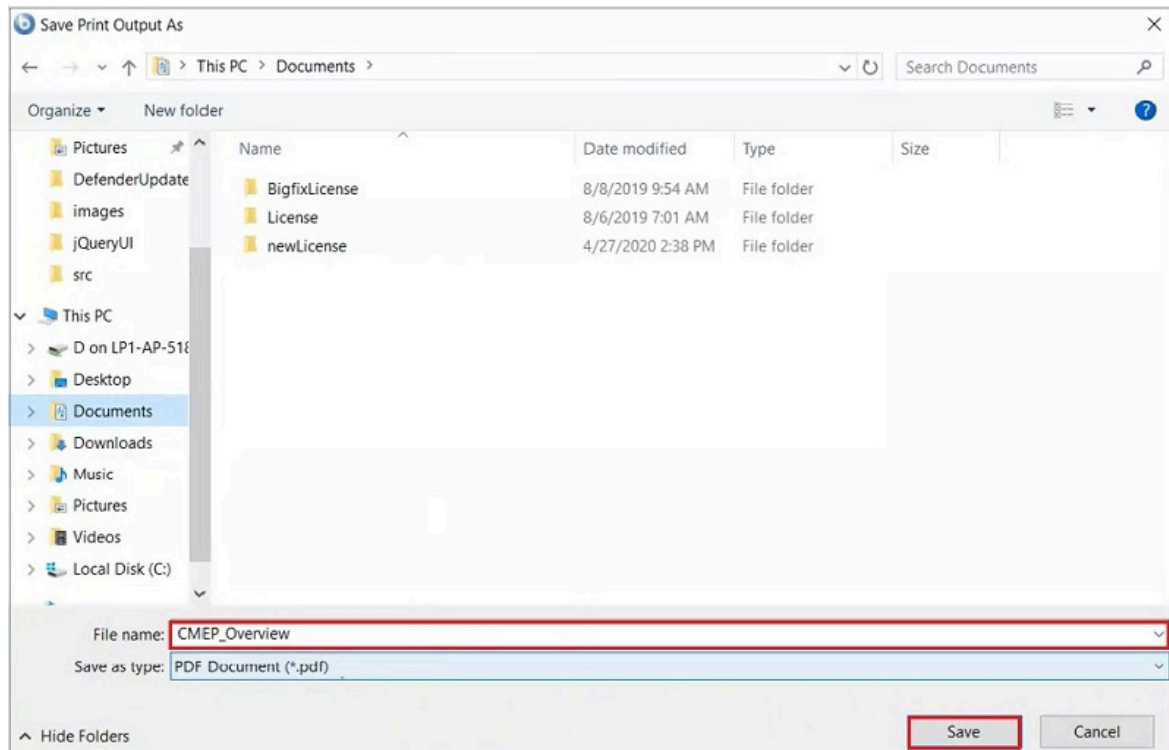
2. The **Print** window opens. Select the **Print to PDF** option and then click **Print**.



Note: All latest operating systems support *Print to PDF* functionality.



3. The **Save Print Output As** window appears.



4. Navigate to the location where you want to save the PDF file. In the **File name** field, provide the file name and click **Save**.

The report is saved in PDF format in the desired location.

Wizards

CMEP Anti-Malware wizards offer an easy, step-by-step guided process for updating virus definitions and setting up on-demand virus scans on your endpoints.

Create Update Task Wizard

The Create Update Task wizard allows you to create anti-virus definition updates for a number of McAfee and Symantec applications.

Access the wizard by expanding the *Manage Definition Updates* sub-node in the navigation tree. Click *Create Update Task*. This action opens the wizard.

Endpoint Protection

- Endpoint Protection Domain
 - Client Manager for Endpoint Protection
 - CMEP Overview
 - Warnings (5)
 - Reports (28)
 - Product Updates (11)
 - Manage Definition Updates (53)
 - Create Update Task
 - Windows Defender Update Wizard
 - CA/eTrust (8)
 - McAfee (11)

Create Update Task

Anti-Virus Definition Update Task Wizard

Welcome to the Anti-Virus Definition Update Wizard!

Please select an Anti-Virus application from the list below:

- ☐ McAfee VirusScan 4.0.3 ~ 7.0
- ☐ McAfee VirusScan 8i
- ☐ McAfee VirusScan 8.5i / 8.7i / 8.8i
- ☐ McAfee VirusScan 8.x/9.x for Mac
- ☐ Symantec Anti-Virus Corporate Edition
- ☐ Symantec Endpoint Protection 11.x/12.x
- ☐ Symantec Anti-Virus 10.2 for Mac (PowerPC)
- ☐ Symantec Anti-Virus 10.2 / Endpoint Protection 12 for Mac (Intel)

Selecting any anti-virus product from the list displays more information at the bottom section of the panel. You can either retrieve the package from a URL or browse to locate the package from your computer.

The box in the lower-left corner of the window allows you to either create a reusable Fixlet or a one-time action. Click *Finish*.

☐ Symantec Endpoint Protection 11.x/12.x

☐ Symantec Anti-Virus 10.2 for Mac (PowerPC)

☒ Symantec Anti-Virus 10.2 / Endpoint Protection 12 for Mac (Intel)

☒ Download from URL - Retrieve the package from a URL

☐ File - Select the package on this computer.

Note: Uploading the definition file may take considerable time.

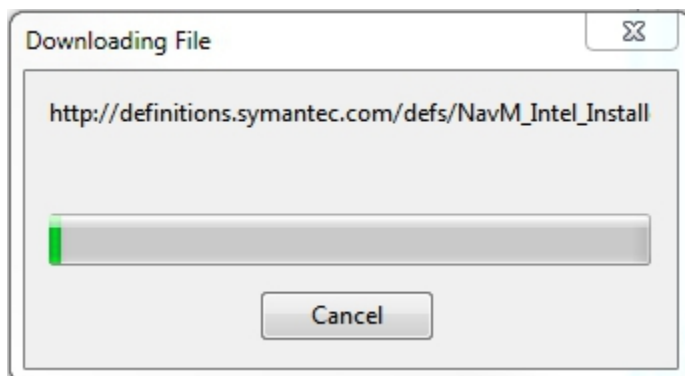
Note: The file you select will be placed on the BES Server and a SHA1 checksum will be calculated and stored in the action for security and caching purposes. If you would like to change the file later, you will need to run this wizard again.

☐ Create a one-time action. Leave this unchecked to create a Fixlet you can reuse.

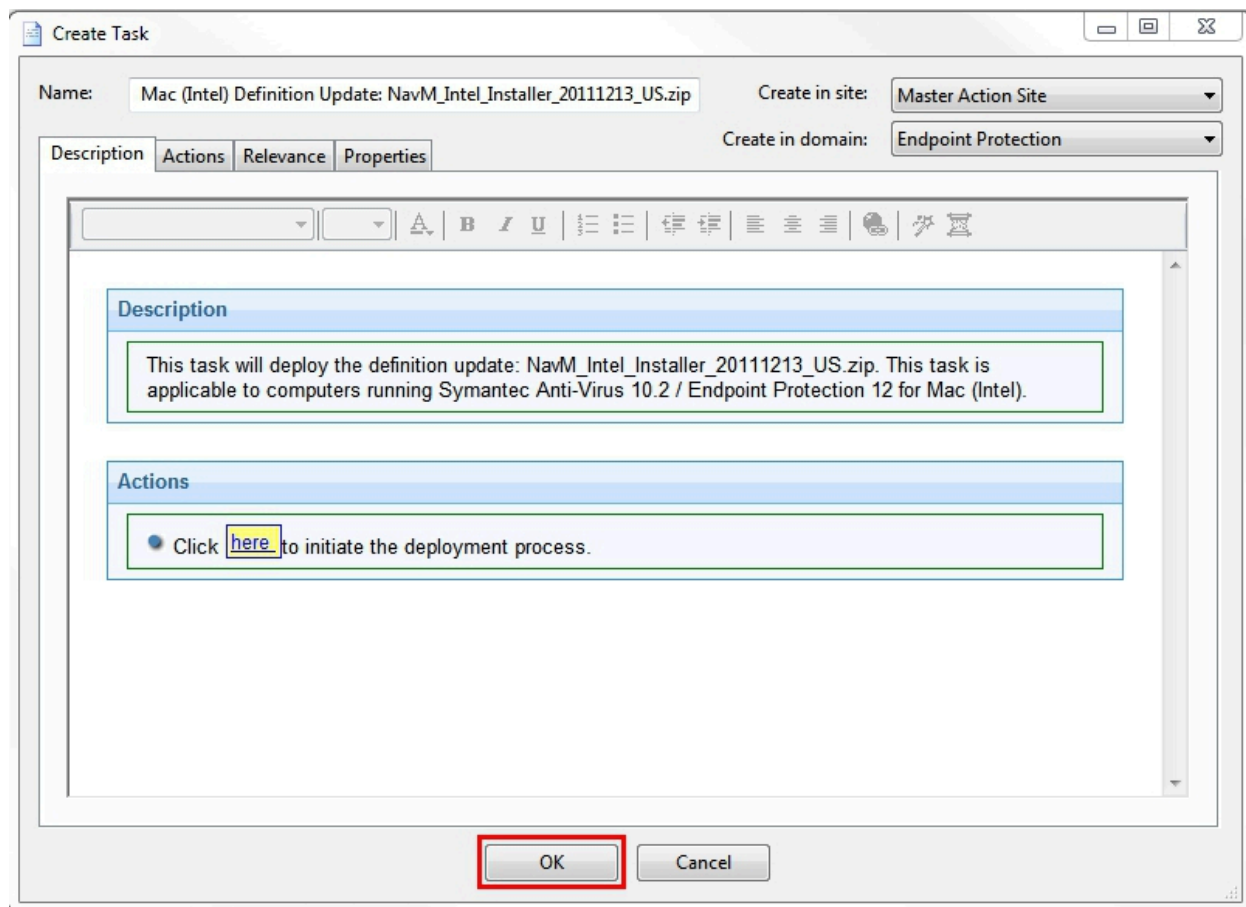


Note: To enter the correct URL, go to the virus definitions page on the McAfee or Symantec website and paste the link into the dialog field. You can also download the virus definition to your computer and browse to its location by selecting the second button.

You see the following screen as the virus definitions are downloaded to your system:



The Create Task window opens. Review the content in the Description, Actions, Relevance, and Properties tabs, click **OK**, and enter your Private Key Password.



In the next task window, click in the Actions box to initiate deployment to open the Take Action dialog.

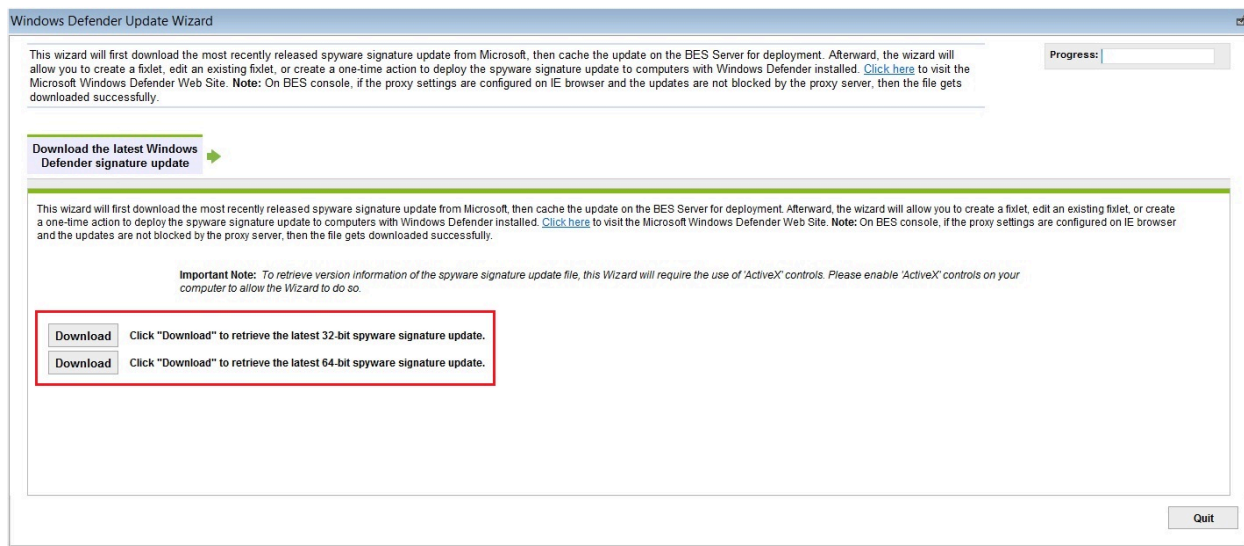
Windows Defender Update Wizard

The Windows Defender Update wizard allows you to create and update the spyware signature update from Microsoft application.

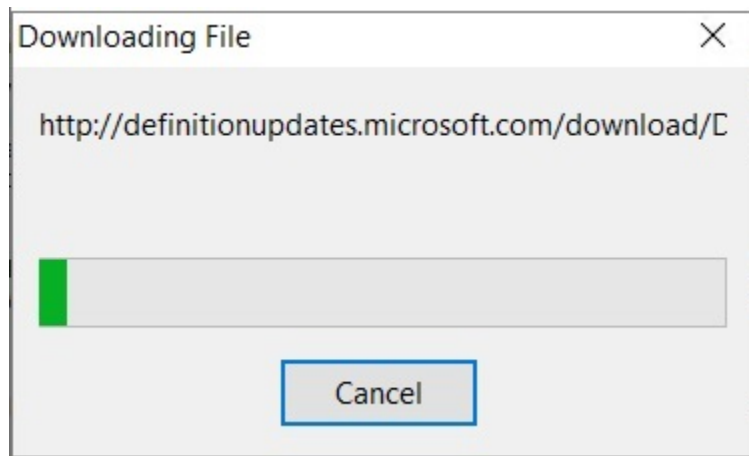
To access the Windows Defender Update Wizard, click the *Manage Definition Updates Wizard* subnode in the navigation tree.



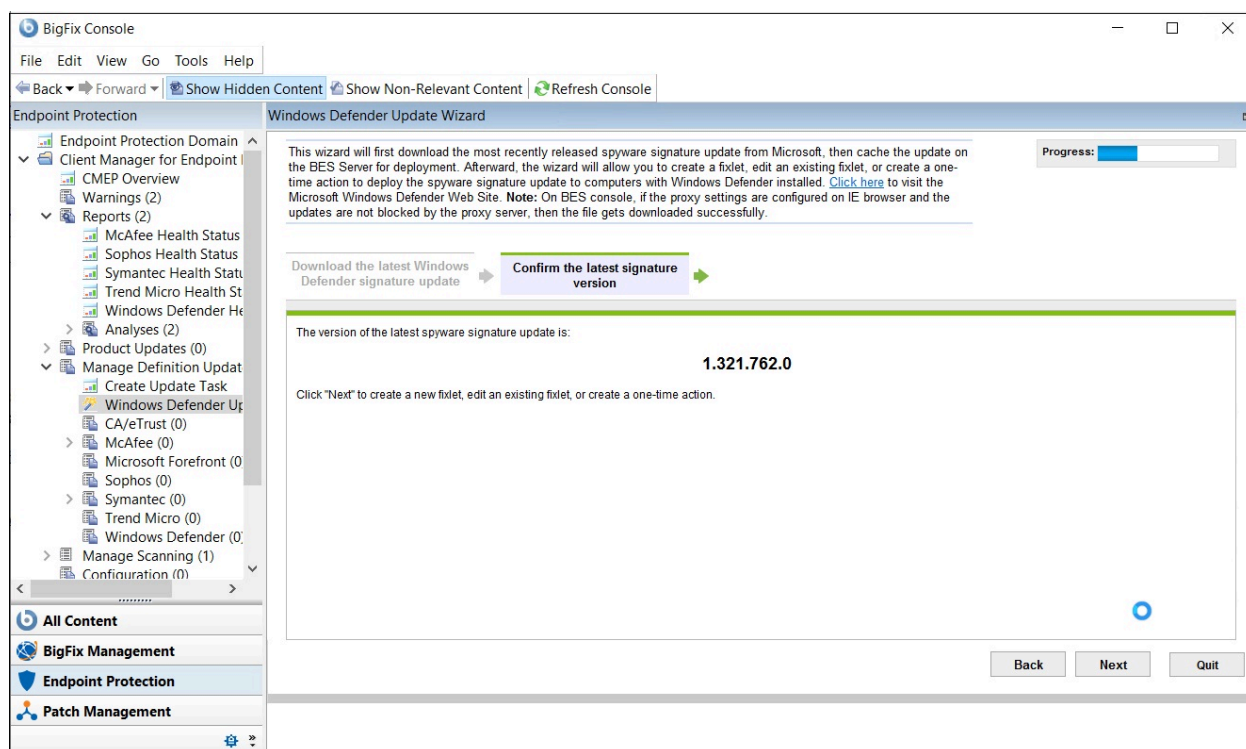
The Windows Defender Update Wizard opens in the Work Panel.



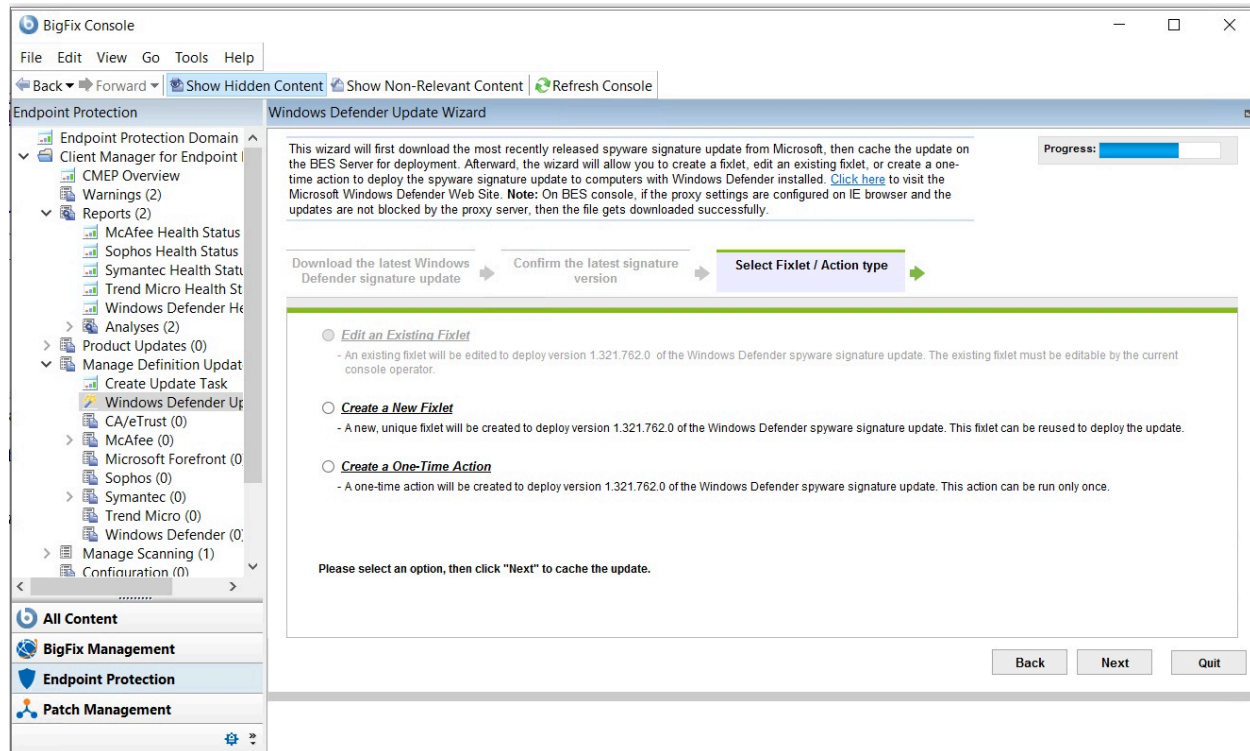
Click **Download** to see a progress window while the wizard retrieves spyware updates.



After spyware signatures have been downloaded, you see a window displaying the version number of the latest update. Click **Next** to take additional actions.



From this window, you can choose to edit or create a Fixlet, or create a one-time action.

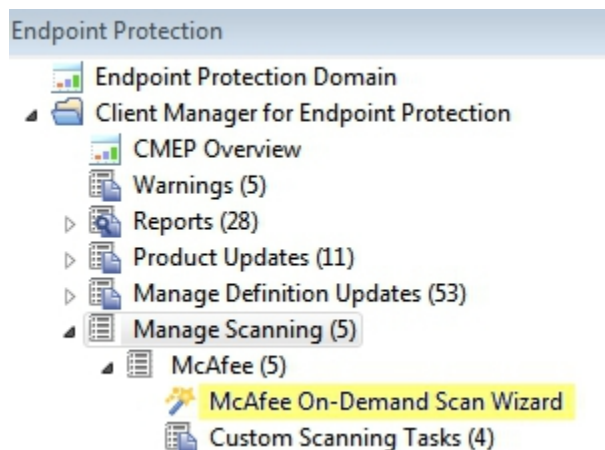


Click **Next** to proceed through the Wizard.

McAfee On-Demand Scan Wizard

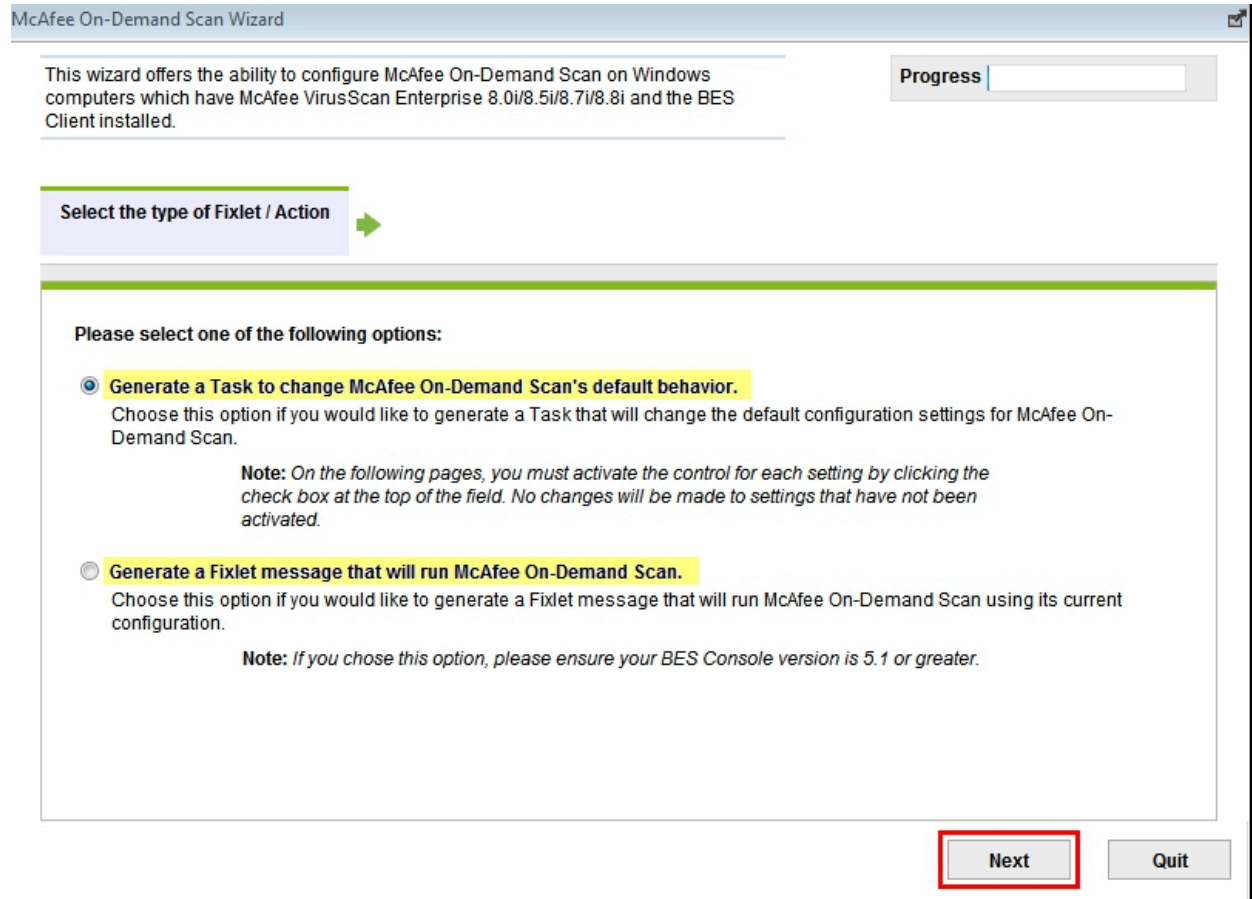
This wizard allows you to configure the McAfee On-Demand Scan on Windows computers which have McAfee VirusScan Enterprise 8.0 and above and the BES Client installed.

Access the *McAfee On-Demand Scan Wizard* from the *Manage Scanning* node in the navigation tree.



The Wizard allows you to configure McAfee On-Demand scan on Windows computers that have McAfee VirusScan Enterprise 8.0i and the BigFix client installed.

When you click to open the Wizard, you can either generate a task to change the default behavior, or generate a Fixlet to run the scan. Make a selection and click *Next*.



The image shows the 'McAfee On-Demand Scan Wizard' dialog box. At the top, it states: 'This wizard offers the ability to configure McAfee On-Demand Scan on Windows computers which have McAfee VirusScan Enterprise 8.0i/8.5i/8.7i/8.8i and the BES Client installed.' To the right of this text is a 'Progress' bar. Below the introductory text is a section titled 'Select the type of Fixlet / Action' with a green arrow pointing right. The main area of the wizard contains the instruction 'Please select one of the following options:' followed by two radio button options. The first option, 'Generate a Task to change McAfee On-Demand Scan's default behavior.', is selected and highlighted with a yellow background. It includes a note: 'Note: On the following pages, you must activate the control for each setting by clicking the check box at the top of the field. No changes will be made to settings that have not been activated.' The second option, 'Generate a Fixlet message that will run McAfee On-Demand Scan.', is also highlighted with a yellow background and includes a note: 'Note: If you chose this option, please ensure your BES Console version is 5.1 or greater.' At the bottom right of the dialog are two buttons: 'Next' (which is highlighted with a red rectangle) and 'Quit'.

McAfee On-Demand Scan Wizard

This wizard offers the ability to configure McAfee On-Demand Scan on Windows computers which have McAfee VirusScan Enterprise 8.0i/8.5i/8.7i/8.8i and the BES Client installed.

Progress

Select the type of Fixlet / Action

Please select one of the following options:


- ☒ **Generate a Task to change McAfee On-Demand Scan's default behavior.**
Choose this option if you would like to generate a Task that will change the default configuration settings for McAfee On-Demand Scan.
Note: On the following pages, you must activate the control for each setting by clicking the check box at the top of the field. No changes will be made to settings that have not been activated.
- ☐ **Generate a Fixlet message that will run McAfee On-Demand Scan.**
Choose this option if you would like to generate a Fixlet message that will run McAfee On-Demand Scan using its current configuration.
Note: If you chose this option, please ensure your BES Console version is 5.1 or greater.

Next Quit

If you click *Generate a Task* to change default behavior, you will see the following screen. Select a scan location, and then make a drive selection from the pull-down list. You can select multiple drives by using the Add and Remove buttons.

McAfee On-Demand Scan Wizard

This wizard offers the ability to configure McAfee On-Demand Scan on Windows computers which have McAfee VirusScan Enterprise 8.0i/8.5i/8.7i/8.8i and the BES Client installed.

Progress 

Select the type of Fixlet / Action → Specify scan location options →

☒ Scan Locations

All local drives
Running processes

My computer (all drives) ▼ Add Remove

My computer (all drives)
All local drives
All fixed drives
All removable drives
All mapped network drives
Running processes
Home folder
User profile folder
Recycle bin
Drive or folder
File


Browse...

Back Next Quit

You can also choose to select additional scan options, and then click *Next*.

McAfee On-Demand Scan Wizard

This wizard offers the ability to configure McAfee On-Demand Scan on Windows computers which have McAfee VirusScan Enterprise 8.0i/8.5i/8.7i/8.8i and the BES Client installed.

Progress 

Select the type of Fixlet / Action → Specify scan location options →

☒ Scan Locations

All local drives
Running processes

My computer (all drives) Add Remove

C:\ Browse...

☐ Additional Scan Options

☒ Include subfolders
☒ Scan boot sectors

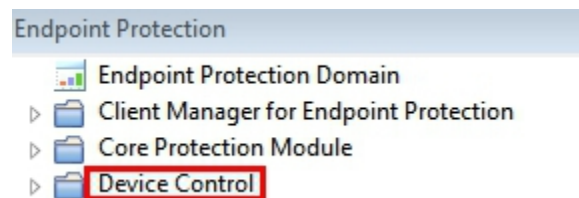
Back Next Quit

Use the *Next*, *Back*, and *Quit* navigation buttons at the bottom of each window to proceed through the Wizard. The remaining windows allow you to select scan inclusions and exclusions, specify advanced scan options, specify virus detection options, specify destination options for unwanted programs, and specify log file options.

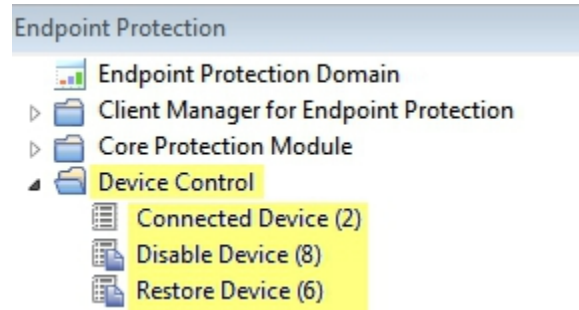
Chapter 4. Device control

Device Control manages and controls various devices in your deployment, including USB storage devices and CD-ROM drives.

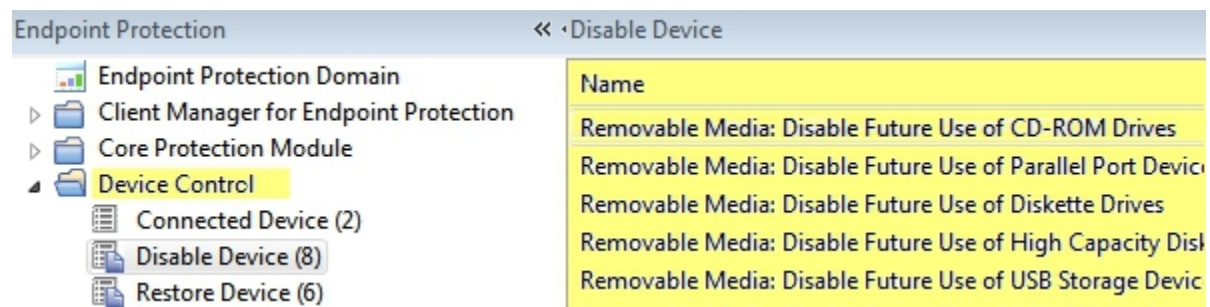
To view applicable tasks related to Device Control, click the *Device Control* site located under the *Client Manager for Endpoint Protection* site within the Endpoint Protection domain.



Click **Device Control** to display a list of tasks, analyses, or Fixlets related to Device Control.



Click each category to display the related tasks, or use the top-right panel in the console to deploy these actions from a single list. Any tasks beginning with *Removable Media* are related to the Device Control component of CMEP.



The tasks listed in the Device Control node allow you to control removable media devices by either *disabling* or *restoring* future use of the devices. These devices include:

- USB Storage
- CD-ROMs
- Floppy Disk drives
- High Capacity Floppy Disk Drives

- Parallel Port Devices
- PCMCIA Devices

Click each name in the list to display the related Fixlet in the following window:

The screenshot shows the 'Disable Device' window. At the top, there is a search bar labeled 'Search Disable Device'. Below it is a table with columns 'Name', 'Source Severity', and 'Site'. The table lists several tasks related to disabling future use of various storage devices. The task 'Removable Media: Disable Future Use of CD-ROM Drives' is selected. Below the table, there is a toolbar with buttons: 'Take Action', 'Edit', 'Copy', 'Export', 'Hide Locally', 'Hide Globally', and 'Remove'. Below the toolbar, there are tabs: 'Description', 'Details', 'Applicable Computers (97)', and 'Action History (0)'. The 'Description' tab is active, showing a description of the task and a note. Below the description, there is an 'Actions' section with a link 'Click here to disable future use of CD-ROM drives' highlighted by a red box.

Name	Source Severity	Site
Removable Media: Disable Future Use of CD-ROM Drives	<Unspecified>	Client Manager for Enc
Removable Media: Disable Future Use of Parallel Port Devices	<Unspecified>	Client Manager for Enc
Removable Media: Disable Future Use of Diskette Drives	<Unspecified>	Client Manager for Enc
Removable Media: Disable Future Use of High Capacity Diskette Drives	<Unspecified>	Client Manager for Enc
Removable Media: Disable Future Use of USB Storage Devices	<Unspecified>	Client Manager for Enc

Task: Removable Media: Disable Future Use of CD-ROM Drives

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (97) | Action History (0)

Description

Removable media such as CD's, diskettes, and USB drives can be considered a security risk. These devices can be used to introduce malware or transport sensitive information out of your network.

This task allows you to disable future use of CD-ROM drives by disabling the cdrom.sys driver on targeted computers.

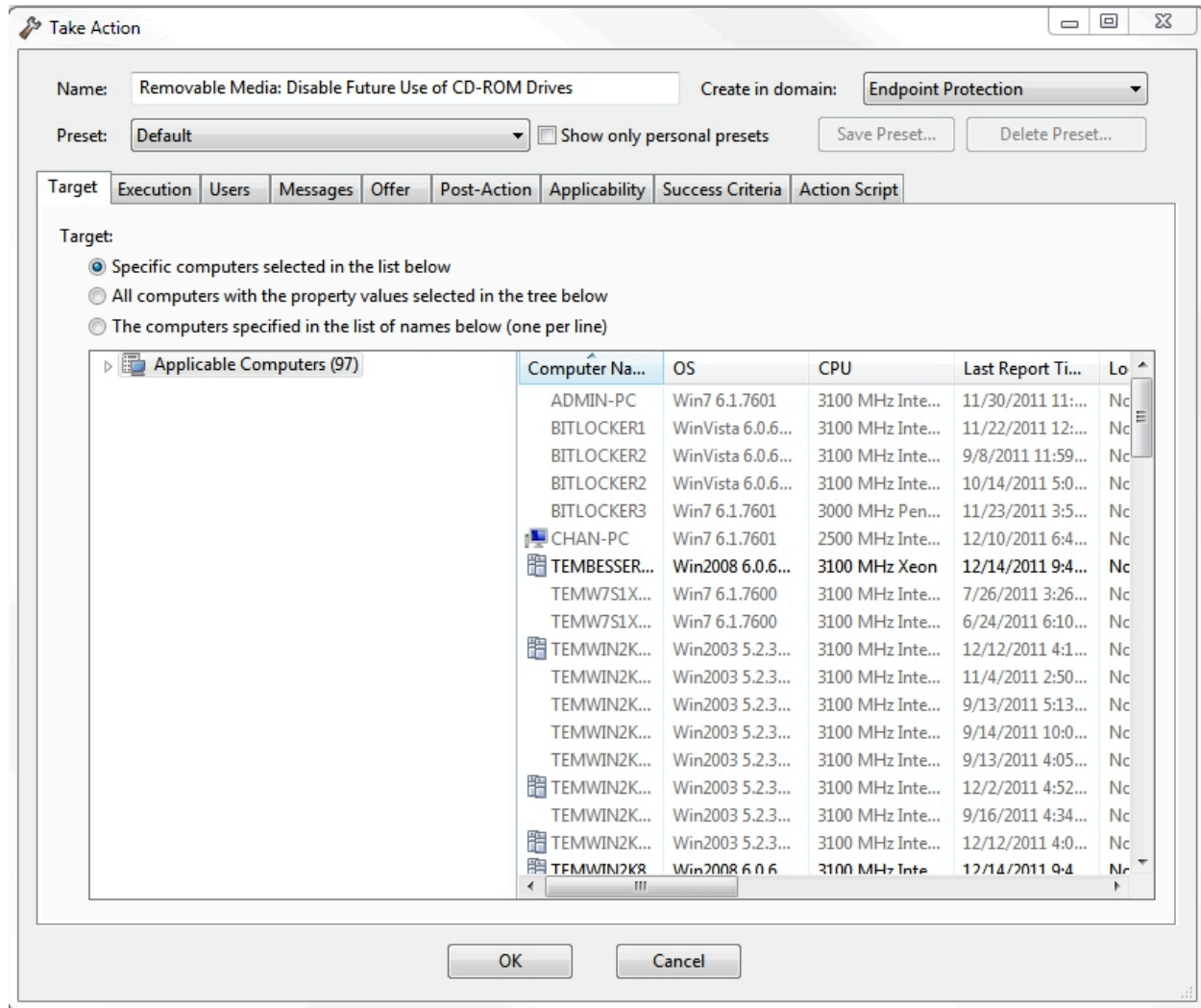
Note: Affected computers will report back as 'Pending Restart' once the action has run successfully, the setting will not take effect until the computer is rebooted.

Actions

Click [here](#) to disable future use of CD-ROM drives.

After reviewing the information displayed in the Description box, click in the Actions box to deploy the task and enter your Private Key Password.

This link displays the Take Action dialog, where you can set specific parameters of the task. For more information about using the Take Action dialog, see the [BigFix Console Operator's Guide](#).



Use this same method to work with all existing content in Device Control, including analyses, Fixlets, and tasks.

USB storage

Removable media, such as CDs, USB drives, and memory sticks can be considered a security risk, because they can potentially introduce malware or transport sensitive information out of your network. The Device Control configuration tasks control future use of USB storage devices by disabling the ***usbstor.sys*** driver on targeted computers.

To disable the future use of a USB Storage device, click the applicable task displayed under the Device Control node in the navigation tree.

Disable Device		Search
Name		
Removable Media: Disable Future Use of USB Storage Devices		
Removable Media: Disable Future Use of PCMCIA Devices		
Removable Media: Disable Installation of USB Storage Device Drivers- Windows 2000/XP Pro		
Removable Media: Disable Installation of USB Storage Device Drivers - Windows XP Home		

A Fixlet opens in the following window. Click where indicated in the Actions box to either start this task or to view the related article on the Microsoft website.

Fixlet: Removable Media: Disable Installation of USB Storage Device Drivers- Windows 2000/XP Pro

Take Action Edit Copy Export Hide Locally Hide Globally Remove

Description Details Applicable Computers (12) Action History (0)

Description

The listed computers are currently not configured to disable the installation of USB storage devices. Such devices could be used to transport sensitive information out of your network. Click the action below to prevent the installation of these devices by setting access control entries for the following files:

```
%SystemRoot%\Inf\Usbstor.pnf
%SystemRoot%\Inf\Usbstor.inf
```

After applying this action, users should no longer be able to install the driver for USB storage devices.

Note: Running the action below may cause client machines to briefly display pop-up and command prompt windows.

Note: Running the action below denies file permissions to Administrators, Power Users and Users.

This Fixlet will only be applicable on computers that have never had a USB Storage Device installed. Use the following Fixlet messages for computers with a previously installed USB Storage Device:

[Removable Media: USB Storage Device Detected](#)
[Removable Media: Disable Future Use of USB Storage Devices](#)
[Removable Media: Restore Future Use of USB Storage Devices](#)

Actions

- Click [here](#) to disable installation of USB storage devices.
- Click [here](#) to view Microsoft's Knowledge Base article concerning this subject.



Note: Affected computers might report back as Pending Restart after the Action has run successfully. The setting might not take effect until the computer is rebooted.

Use this same method for restoring or disabling CD-ROM drives, Floppy Disk drives, High Capacity Floppy Disk drives, Parallel Port Devices, or PCMCIA Devices.

Appendix A. Support

For more information about this product, see the following resources:

- [BigFix Support Portal](#)
- [BigFix Developer](#)
- [BigFix Playlist on YouTube](#)
- [BigFix Tech Advisors channel on YouTube](#)
- [BigFix Forum](#)

Appendix B. Frequently asked questions

This section is designed to help you better understand BigFix CMEP through questions and answers.

Why are my Windows 7 and Windows 2008 machines, which have a supported Anti-Virus installed, showing up as *Other/None* in the Health Status overview pie chart?

If you have BigFix 7.2.4 (or an earlier version) installed, Windows 7 and Windows 2008 are not supported. If you upgrade to BigFix 7.2.5 or later, those operating systems will display as expected in the pie chart.

If I already have *Client Manager for Anti-Virus*, how do I get the new dashboard for *Client Manager for Endpoint Protection*?

You can get to the new CMEP dashboard in two ways:

- In the Domain Panel, click the *Endpoint Protection* domain. This will display the *Client Manager for Endpoint Protection* site at the top of the navigation bar.
- The *Client Manager for Anti-Virus* dashboard contains a note with a link to the current CMEP dashboard:



Note: If your console is open and displaying the old dashboard, you must close and then re-open the old dashboard for the “*This dashboard has been superseded*” message to display.

How do I get back to the CMEP navigation tree from within the wizards?

The domain panel, which contains the navigation tree for all BigFix products, is always visible on the left side of your window. When Fixlets or tasks display, they open in a window on the lower-right part of your screen.

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.