

IBM Endpoint Manager
Version 9.1

*Client Manager for Endpoint Protection
User's Guide*



IBM Endpoint Manager
Version 9.1

*Client Manager for Endpoint Protection
User's Guide*



Note

Before using this information and the product it supports, read the information in "Notices" on page 37.

This edition applies to version 9, release 1, modification 0 of IBM Endpoint Manager (product number 5725-C44) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2003, 2014.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Overview 1

System requirements. 1

Dashboards. 3

Chapter 2. Installation. 7

Subscribe to the CMEP site 7

Activate analyses and tasks 7

Chapter 3. Using CMEP 11

Reports. 11

 Overview 11

 Using the computer filter. 14

 Creating new computer filters 14

 Updating existing filters 15

 Exporting to PDF 15

How to update 18

Wizards 19

 Create Update Task Wizard 19

 Windows Defender and Microsoft Forefront

 Update Wizards 22

 McAfee On-Demand Scan Wizard 24

Configuration tasks. 27

 Disable and enable system restore. 27

Chapter 4. Device control. 29

USB storage 31

Appendix A. Support. 33

Appendix B. Frequently asked questions 35

Notices 37

Programming interface information 39

Trademarks 39

Terms and conditions for product documentation. . 40

Chapter 1. Overview

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

This application enables the management of endpoint security clients from vendors such as McAfee, Symantec, IBM, and Trend Micro. More than just a way to put anti-malware defense under a Endpoint Manager umbrella, *Client Manager for Endpoint Protection* 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
- Inclusion of the Microsoft Forefront Update Wizard

System requirements

IBM Endpoint Manager Client Manager for Endpoint Protection (CMEP) offers support for a variety of operating systems and products.

The following table highlights each supported product, version, and operating environment. This table includes the most current system requirements for this product. However, as system requirements are likely to change, check the Endpoint Manager support website for the most current CMEP system requirements.

Vendor	Product	Version	Supported OS
--------	---------	---------	--------------

Computer Associates	eTrust (CA Antivirus)	x86	eTrust Antivirus 6, 7.x, 8.x CA Antivirus R12 (Audit only *)	Windows NT 4 SP6+, Windows 2000, Windows XP Professional, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7	
		x64	eTrust Antivirus 7.x, 8.x CA Antivirus R12 (Audit only *)		
	CA Antivirus for MAC	x86	8.x (Audit only *)		Mac OS X 10.2 and later
		x64			
IBM	IBM Proventia Desktop	x86	8.0, 9.0, 10.0 (Audit only *)	Windows 2000 SP3+, Windows XP Professional SP 1+, Windows Vista Enterprise, Windows 7 SP1	
		x64	Not supported	Not supported	
McAfee	VirusScan	x86	4.03 - 8.x	Windows 98, Me, Windows NT 4 SP6+, Windows XP, Windows 2000 SP4+, Windows Server 2003 SP1+, Windows Vista, Windows 7	
		x64	4.03 - 8.x	Windows XP, Windows 2000 SP4+, Windows Server 2003 SP1+, Windows Vista, Windows 7	
	VirusScan for Mac	x86	8.x	Mac OS X 10.4.6 and later	
		x64			
	NetShield	x86	4.5 and later	Win NT/2000	
		x64	Not supported	Not supported	
	McAfee GroupShield for Microsoft Exchange / McAfee Security for Microsoft Exchange	x86	McAfee Group Shield 7.x / McAfee Security for Microsoft Exchange 7.6	Windows 2000 SP1+, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2	
		x64	McAfee Security for Microsoft Exchange 7.6/8.0		
AVERT Stinger	x86	All known versions	Windows 2000, Windows XP Professional, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7		
	x64	All known versions			
Microsoft	Windows Defender	x86	All known versions	Windows XP, Windows Vista, Windows Server 2003, Windows 7, Windows Server 2008	
		x64	Not supported	Not supported	
	Forefront Client Security / Forefront Endpoint Protection 2010	x86	All known versions	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7	
		x64	Not supported	Not supported	

Symantec	Anti-Virus Corporate Edition	x86	7.6, 8, 9, 10, 10.1, 10.2	Windows 95, Windows 98, Windows Me, Windows NT 4 SP6, Windows 2000, Windows XP Professional, Windows Server 2003
		x64	All known versions	Windows XP 64-Bit Version 2003, Windows Server 2003 64-Bit, Windows Vista, Windows Server 2008
	AntiVirus for Macintosh	x86	10.2	Mac OS X 10.3.9 and later
		x64		
	Endpoint Protection	x86	11, 12.1	Windows 2000, Windows 2008, Windows Vista, Windows 2000 SP3+, Windows Server 2003, Windows Server 2008, Windows 7
		x64	Not supported	Not supported
Endpoint Protection for Macintosh	x86	12	Mac OS X 10.5 and later	
	x64			
Sophos	Anti-Virus / Endpoint Protection	x86	Antivirus 3.x, 4.1.x, 4.6.x, 6.x, 7.x, 9.x, 10.x	Windows 95 OSR2, Windows 98 SE, Windows NT 4 SP6+, Windows XP SP1+, Windows Vista, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows 7
		x64	Not supported	Not supported
	Antivirus for Mac	x86	7.x, 8.x (Audit only *)	Mac OS X 10.4 and later
	x64			
Trend Micro	OfficeScan	x86	7, 8, 10, 10.5, 10.6	Windows 2000, Windows XP Pro SP2+, Windows XP Home SP3+, Windows Server 2003 SP2+ Windows Server 2003 R2 SP2+, Windows Vista SP1+, Windows Server 2008 SP1+, Windows 7
		x64		
	ServerProtect	x86	5.5, 5.8	Windows 2000 SP4+, Windows Server 2003 SP1+, Windows Server 2008
		x64	5.8	
	Trend Micro Security for Mac	x86	1.5	Mac OS X 10 and later
x64				

**Audit only* means that CMED detects when virus definitions are more than seven days old.

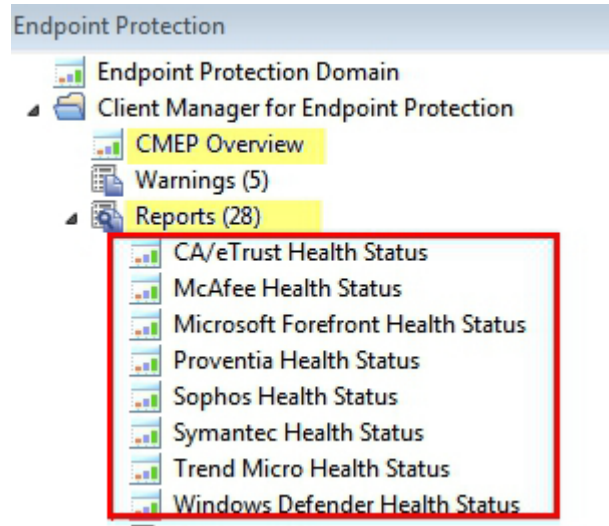
Note: CMED also requires Flash Player 9 or later.

Dashboards

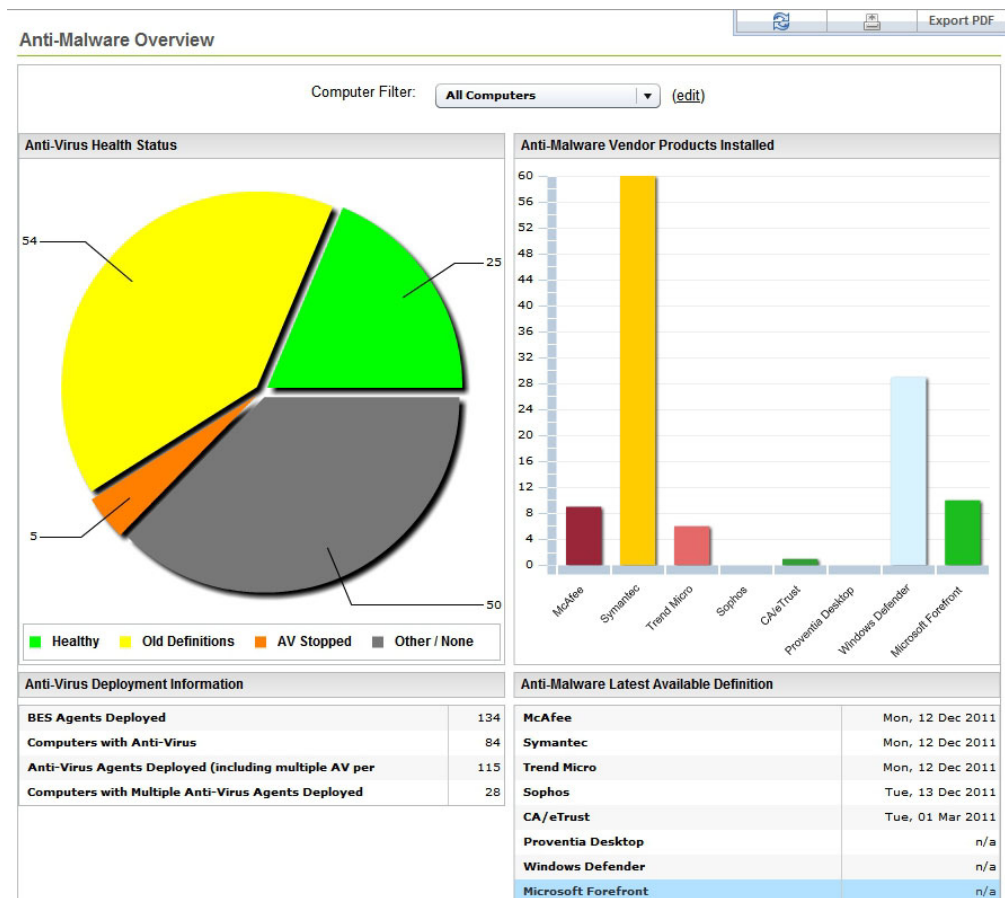
The Dashboards in CMED include overview pie chart reports that summarize the anti-malware products within your deployment.

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

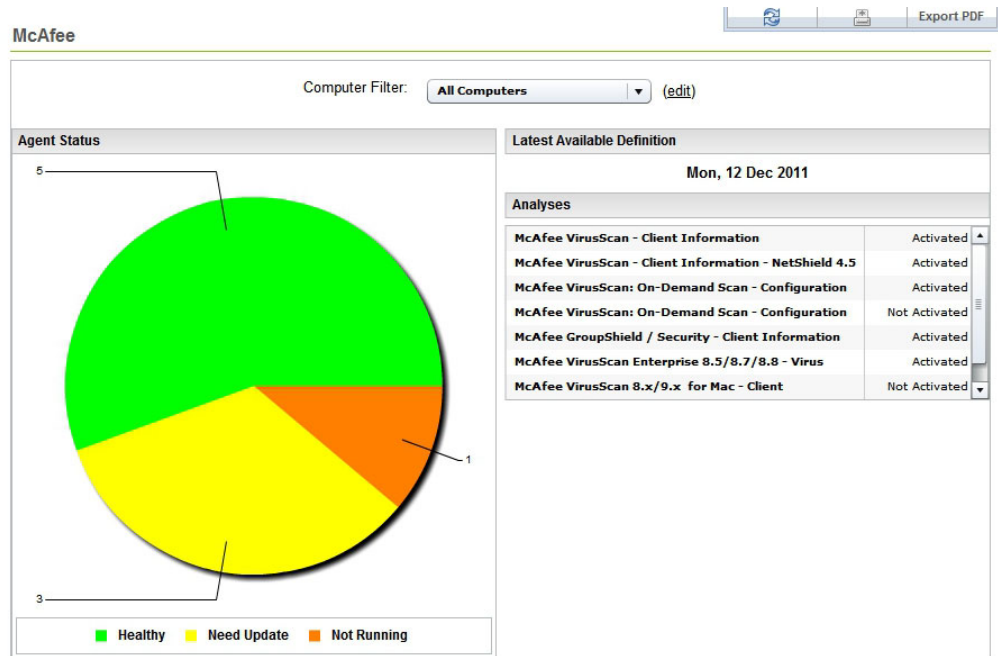
The *CMEP Overview* dashboard is located at the top of the CMEP navigation tree, which is found under the Endpoint Protection Domain. The remaining dashboards are located under the Reports node.



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:



Chapter 2. Installation

Before beginning the installation, log in to the Endpoint Manager console and become familiar with its basic operation. If you have questions about how to use the Endpoint Manager console, see the *IBM® Endpoint Manager Console Operator's Guide* 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 CMEP site contains tasks, analyses, wizards and Fixlets for protecting your deployment from malware.

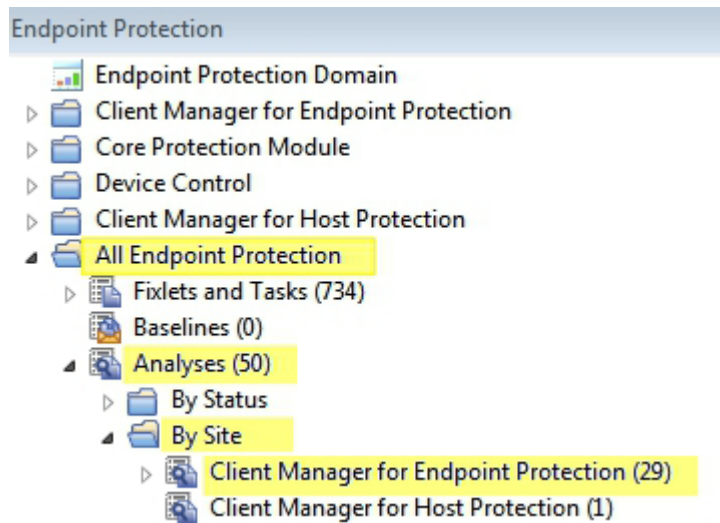
You must be subscribed to the CMEP site to collect data from the Tivoli Endpoint Manager clients. This data is used for reporting and analysis.

The process for site subscription depends on the version of the Tivoli Endpoint Manager Console that you have. Click [here](#) to get specific site subscription directions from the Knowledge Base.

Activate analyses and tasks

After the applicable tasks and analyses have been gathered from the content server, you must deploy those tasks and activate those analyses to make them visible in the Tivoli Endpoint Manager 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.



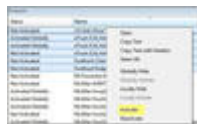
Click *Client Manager for Endpoint Protection* to display the list of related Analyses in the window on the right.

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
Endpoint Protection Domain		Not Activated	CA Anti-Virus/Total Defense R12 Client Information
Client Manager for Endpoint Protection		Activated Globally	eTrust (CA) Anti-Virus Client Information - 6.0/7.x
Core Protection Module		Activated Globally	eTrust (CA) Anti-Virus Client Information - 8.x
Device Control		Not Activated	eTrust (CA) Anti-Virus Client Information - 8.x for MAC
Client Manager for Host Protection		Not Activated	Forefront Client Security - Client Information
All Endpoint Protection		Not Activated	Forefront Endpoint Protection - Client Information
Fixlets and Tasks (734)		Not Activated	ISS Proventia Desktop
Baselines (0)		Not Activated	McAfee AVERT Stinger Information
Analyses (50)		Activated Globally	McAfee GroupShield / Security - Client Information
By Status		Activated Globally	McAfee VirusScan - Client Information
By Site		Activated Globally	McAfee VirusScan - Client Information - NetShield 4.5
Client Manager for Endpoint Protection (29)		Not Activated	McAfee VirusScan 8.x/9.x for Mac - Client Information
Client Manager for Host Protection (1)			
Trend Micro Core Protection Module (20)			

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 Tivoli Endpoint Manager Console Operator's Guide.

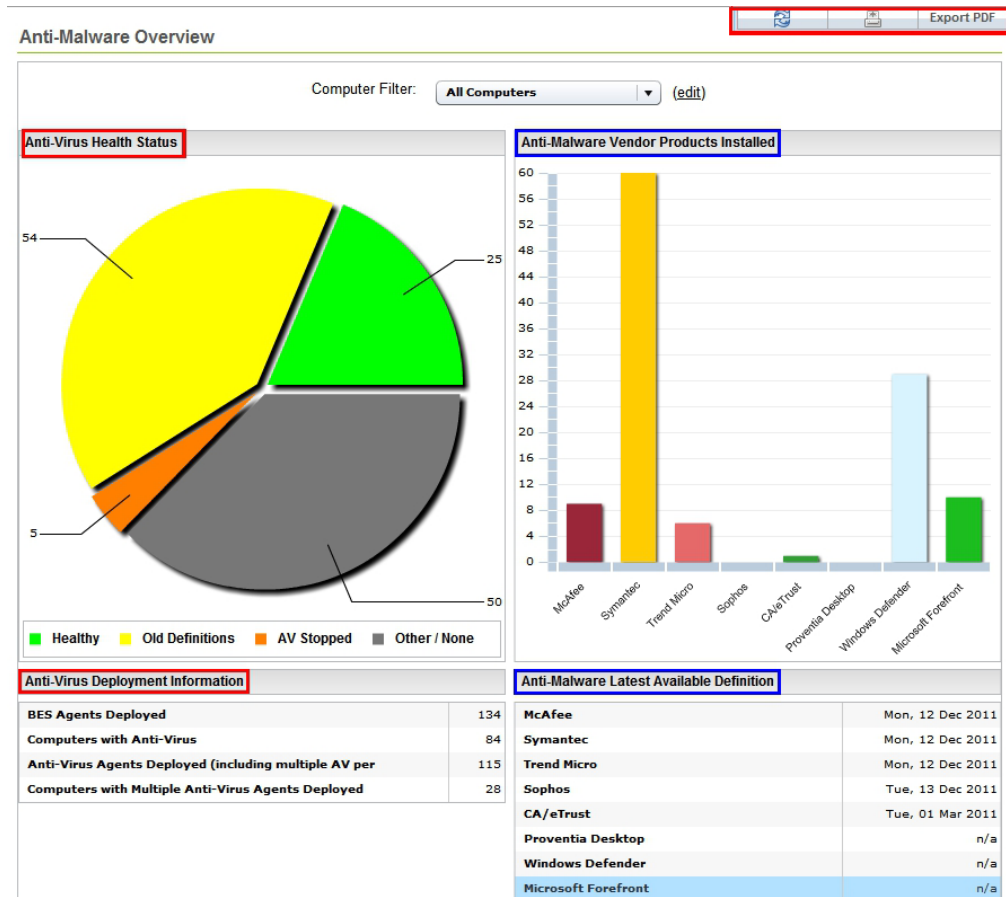
Chapter 3. Using CMEP

Reports

Overview

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

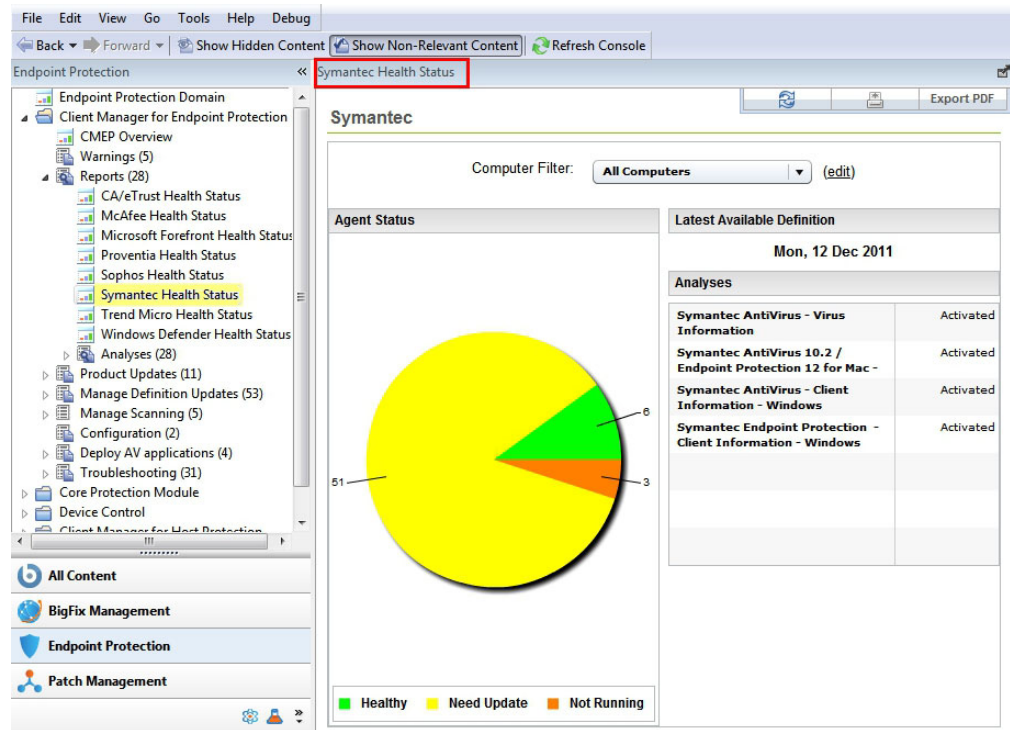
Category	Definition
Healthy	This machine is adequately protected from Malware
Old Definitions	Virus definitions need to be updated on this machine
AV Stopped	The required Anti-Virus application or service(s) are not running
Other / None	This machine uses an unsupported Anti-Virus product, or no Anti-Virus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

Note: For detailed information about how CMEP defines healthy in the Health Status pie chart, see the related Knowledge Base article on the Endpoint Manager support website.

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

McAfee
Symantec
Trend Micro
Sophos
eTrust
Proventia Desktop
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.

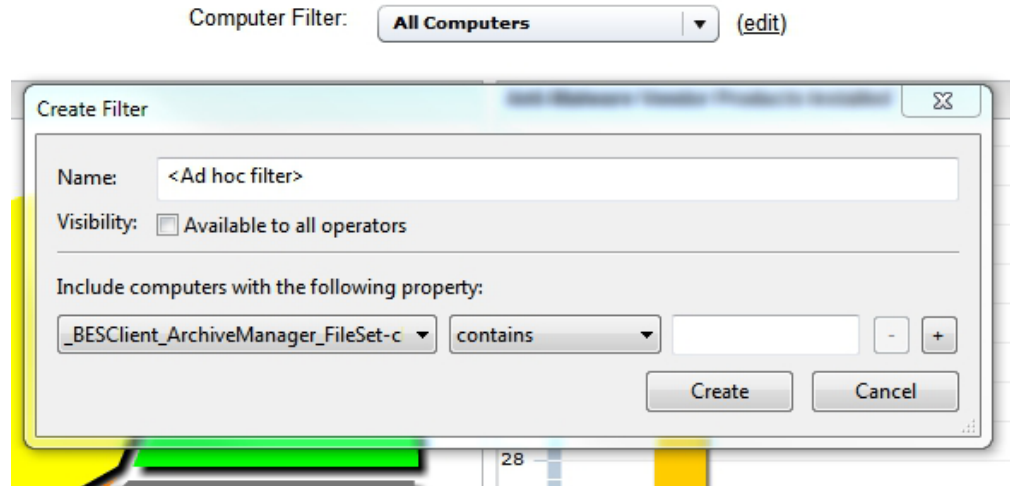


The *Agent Status* section displays pie charts representing the health and status of your Anti-Virus according to each vendor. Status is measured by the following criteria:

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.



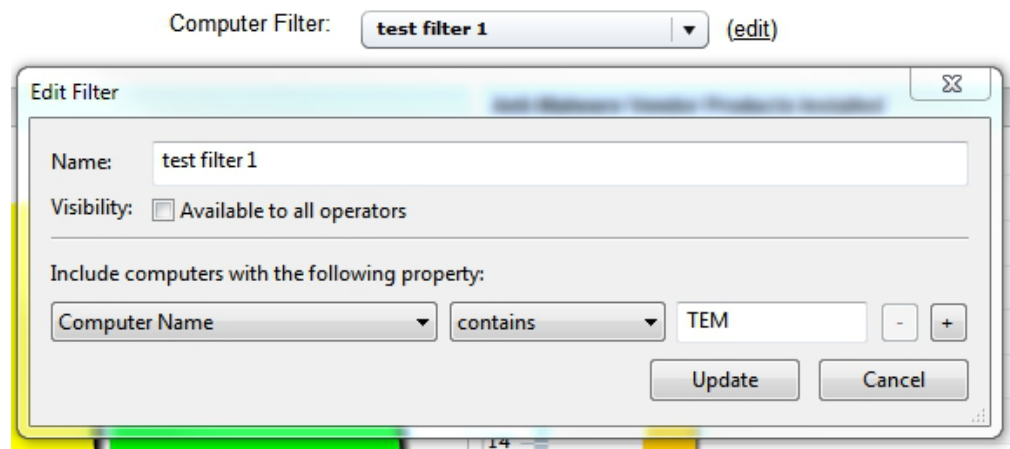
From the first pull-down list in the **Include computers with the following property** section, select the computer properties that will apply the filter criteria you are creating.

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, click the “+” button. 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.

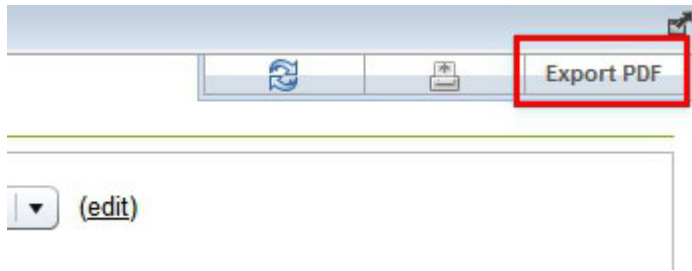
Updating existing filters

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**.

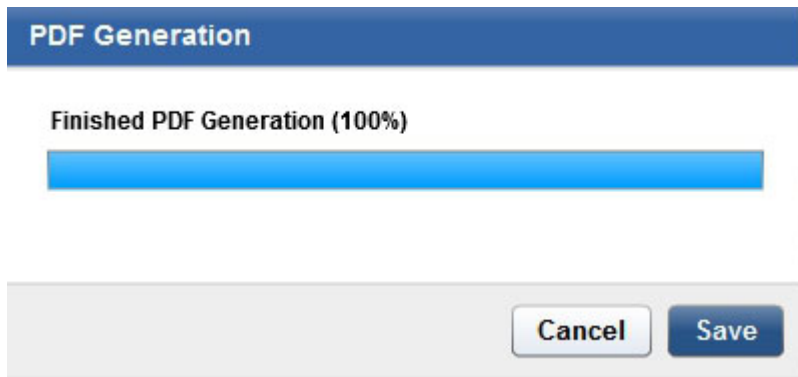


Exporting to PDF

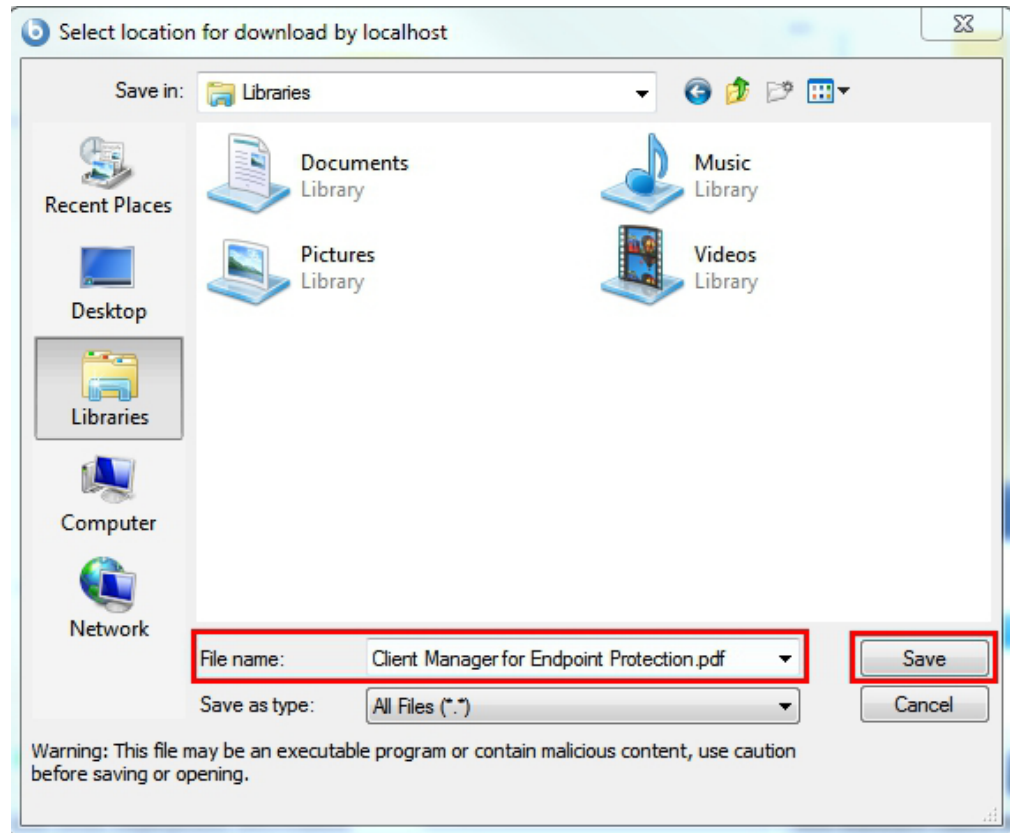
You can export Overview reports to PDF format. At the upper right corner of the Overview reports dashboard, click *Export to PDF*.



The *PDF Generation* status window opens. When the status shows *Finished Generation (100%)*, click **Save**.



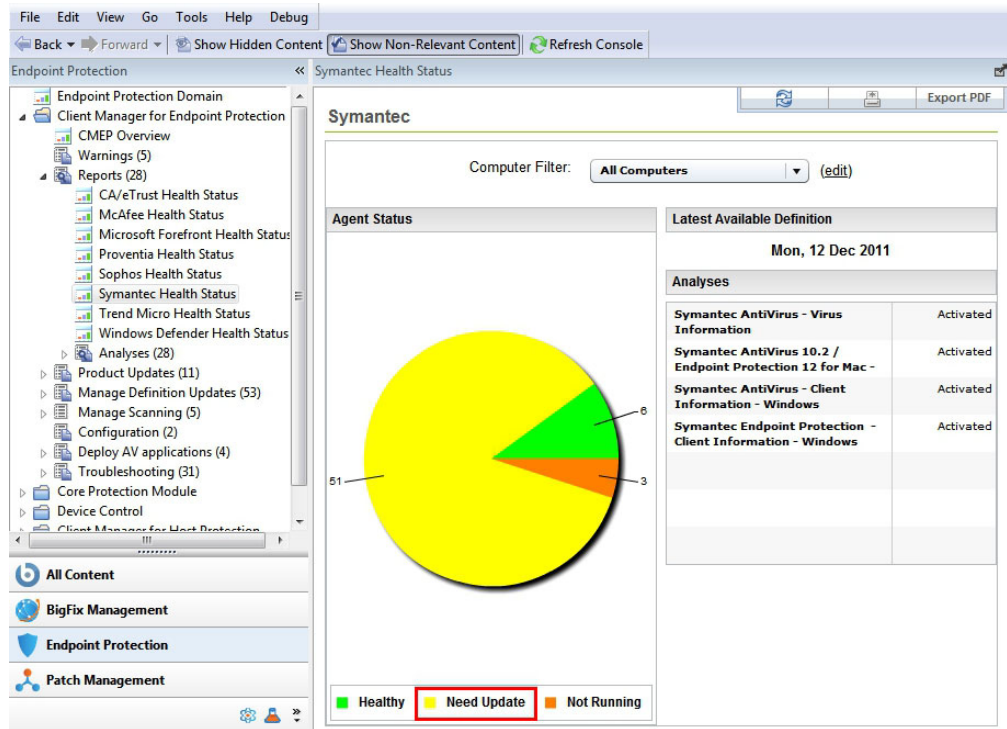
The *Select location for download by localhost* window opens.



In the *Save in* pull-down list, navigate to the location where the PDF file will be saved. Fill in the *File name* field and click *Save*.

How to update

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.

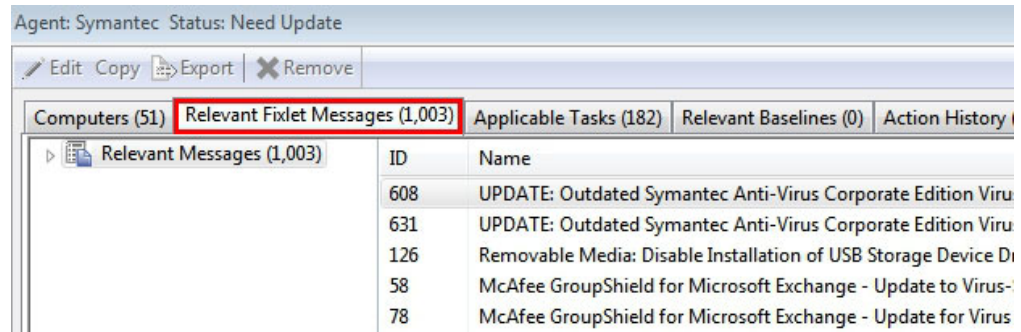


Start by clicking directly on the pie chart to open a new window where you can update the related Fixlets. Click the applicable computer listed under the *Computer Name* column on the right side of the window.

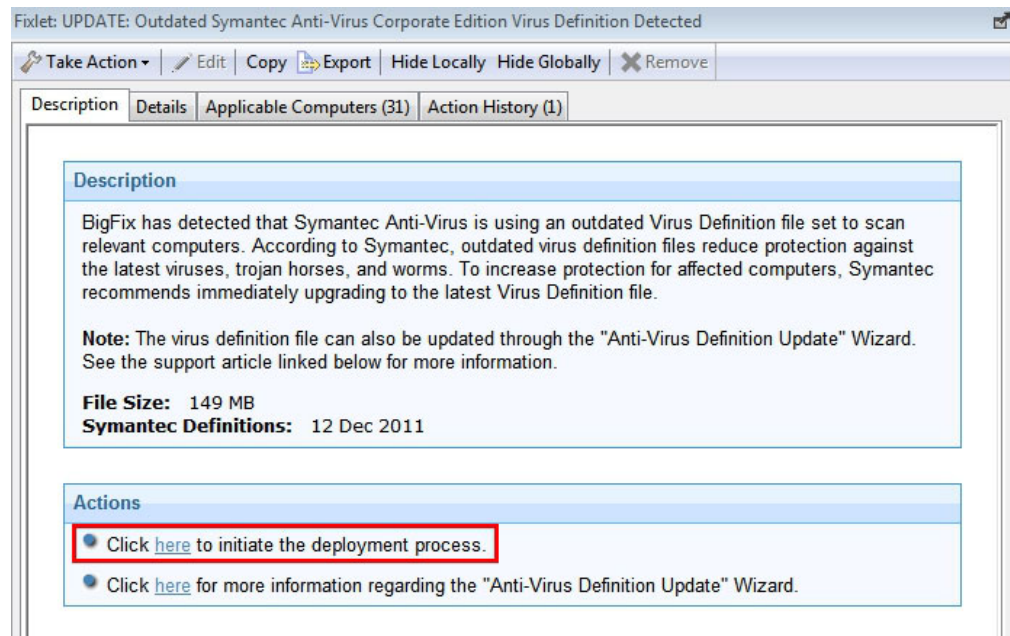
The screenshot shows the 'Agent: Symantec Status: Need Update' window. The 'Computers (51)' tab is selected, displaying a list of computers. A red box highlights the first few rows of the list.

Computer Name	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

Next, click the *Relevant Fixlet Messages* tab on the left 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 of the panel. For detailed information about the Take Action dialog, see the Tivoli Endpoint Manager Console Operator's Guide.

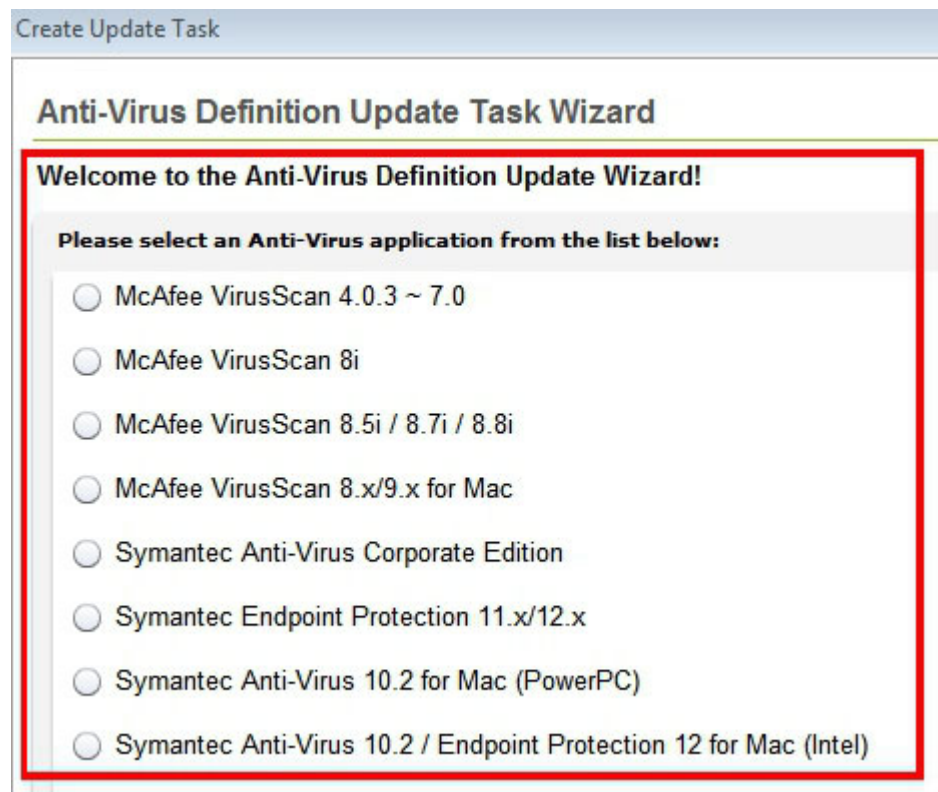
Wizards

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

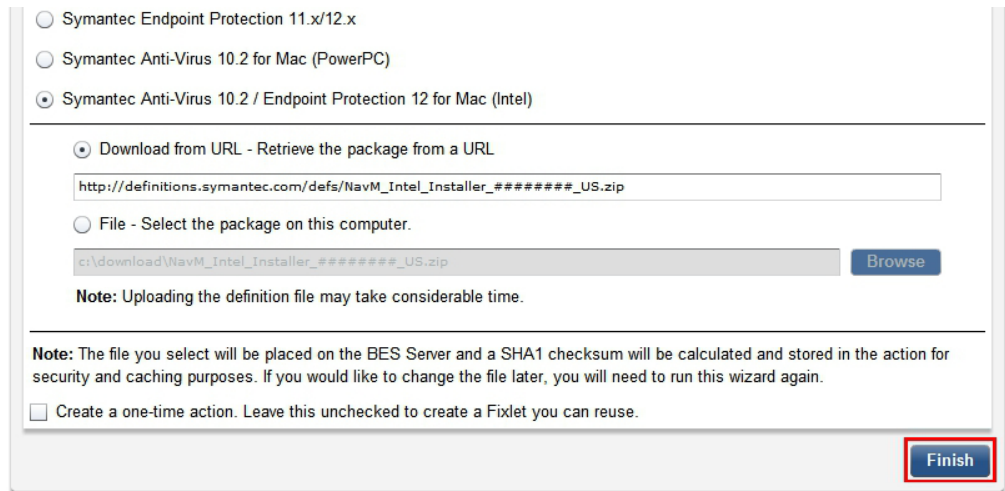
The Create Update Task wizard allows you to create anti-virus definition updates for a number of McAfee and Symantec applications.

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



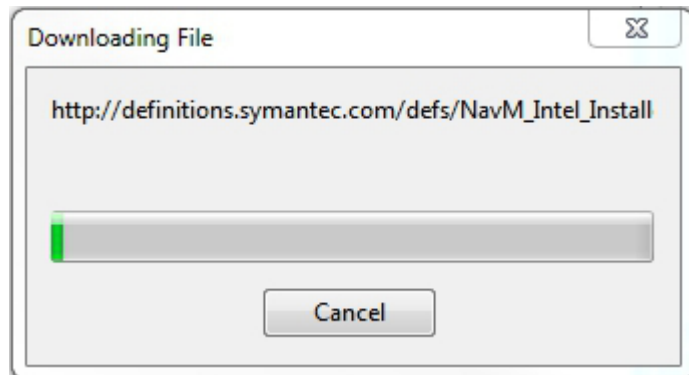
Selecting any anti-virus product from the list displays more information at the bottom of the panel. You can either retrieve the package from a URL or browse to locate the package from your computer.

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

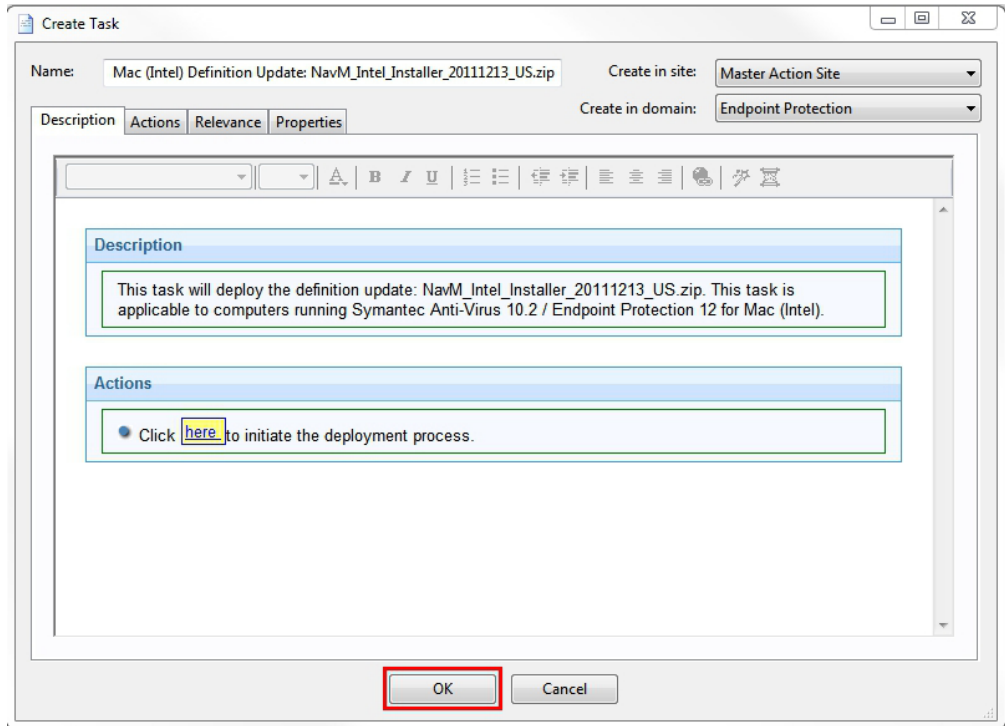


Note: To enter the correct URL, go to the virus definitions page on the McAfee or Symantec website and paste the link into the dialog field. You can also download the virus definition to your computer and browse to its location by selecting the second button.

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



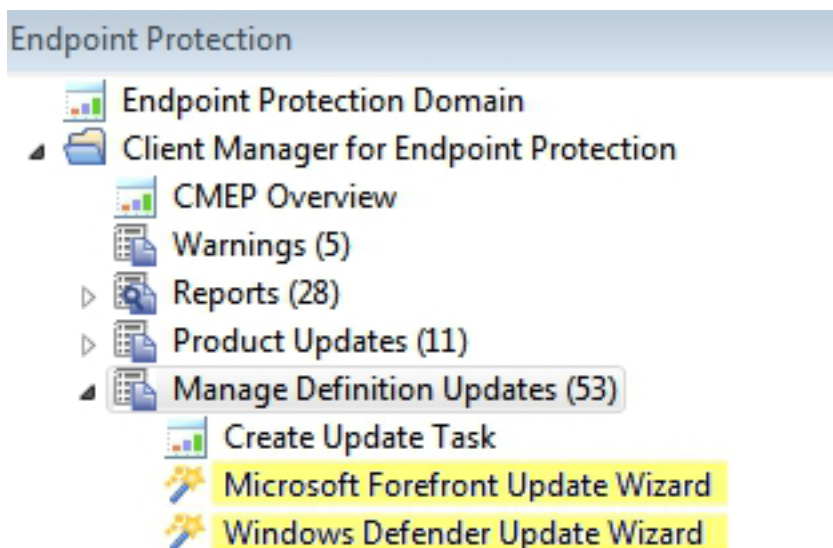
The Create Task window opens. Review the content in the Description, Actions, Relevance, and Properties tabs, click **OK**, and enter your Private Key Password.



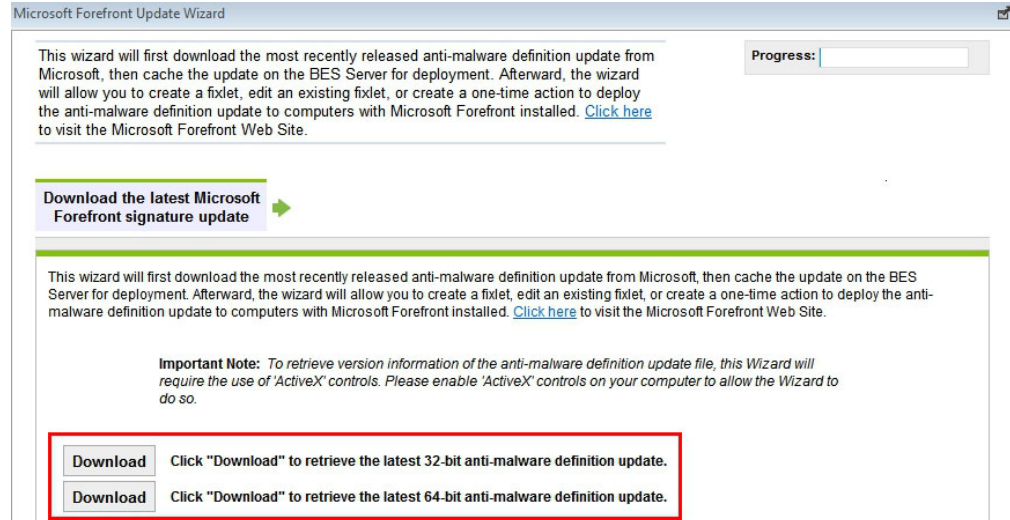
In the next task window, click in the Actions box to initiate deployment to open the Take Action dialog.

Windows Defender and Microsoft Forefront Update Wizards

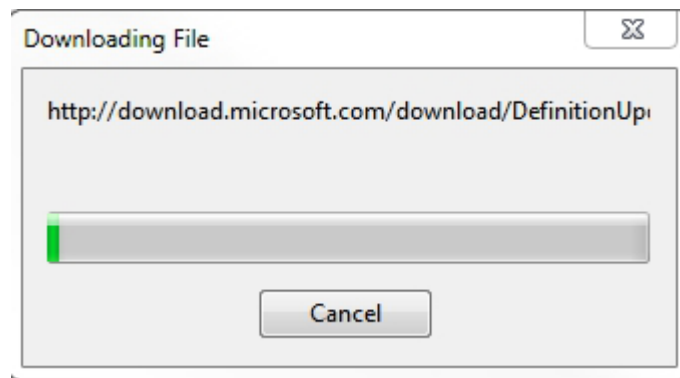
To access the Windows Defender Update Wizard or the Microsoft Forefront Update Wizard, click the Wizard from the *Manage Definition Updates* subnode in the navigation tree. In this example, we are using Microsoft Forefront Update Wizard.



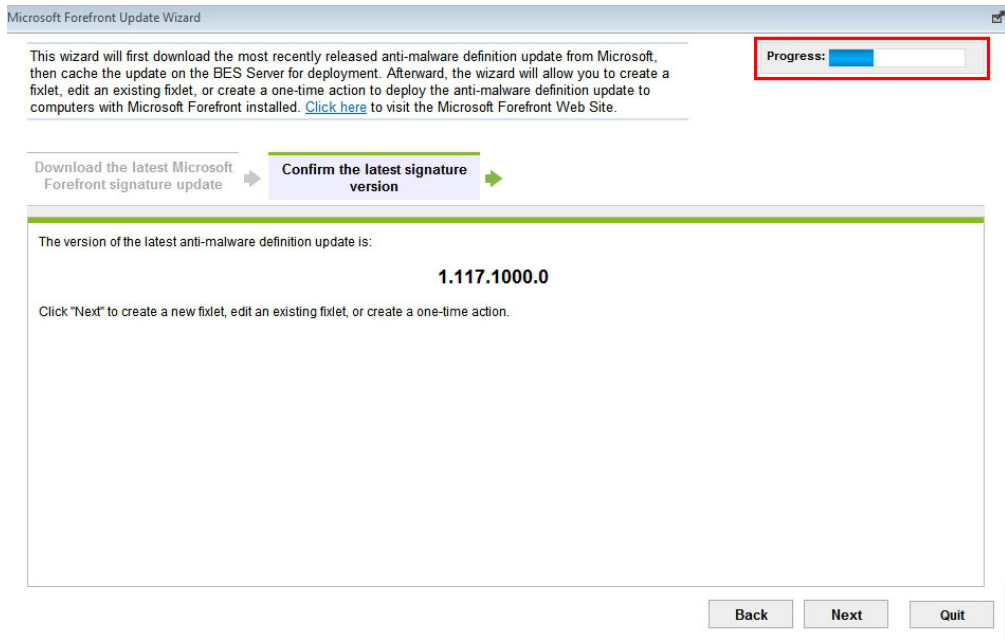
The Wizard opens in the Work Panel on the right. In this example, the Microsoft Forefront Update Wizard opens.



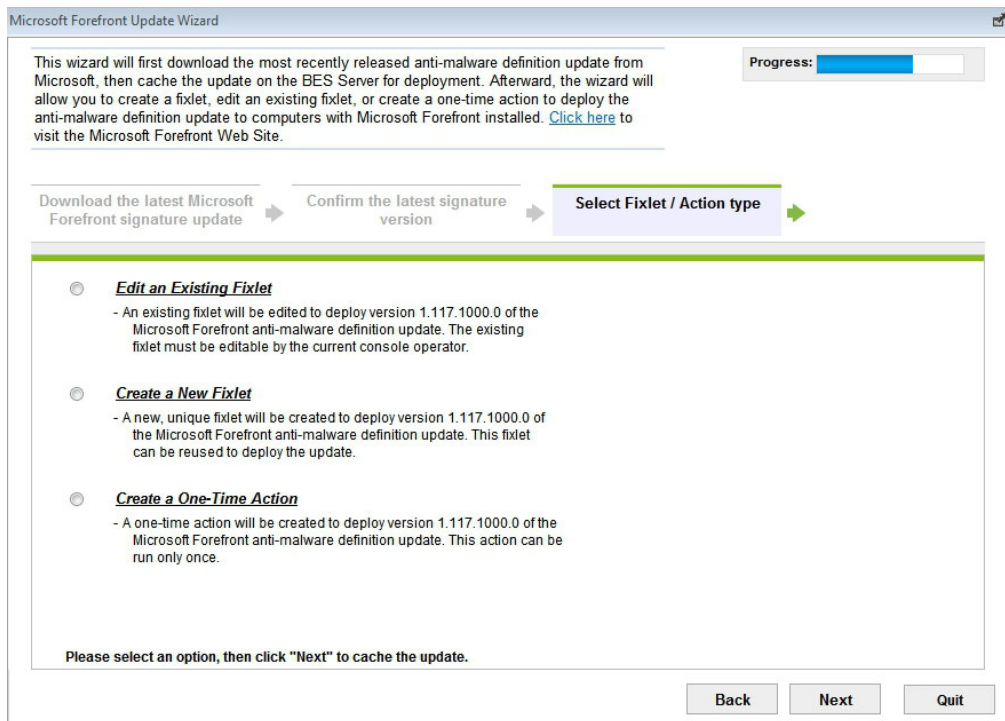
Click *Download* to see a progress window while the wizard retrieves spyware updates.



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



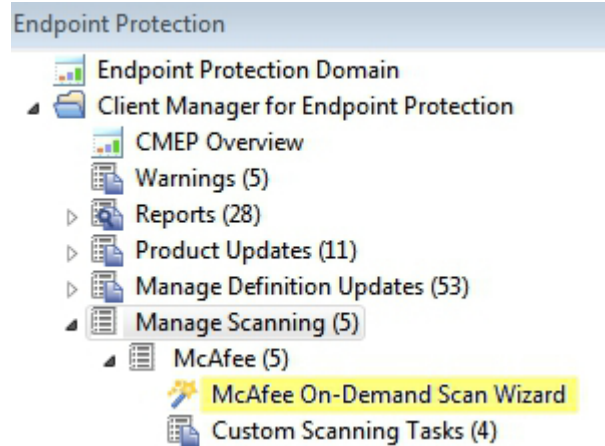
From this window, you can choose to edit or create a Fixlet, or create a one-time action.



Click *Next* to proceed through the Wizard.

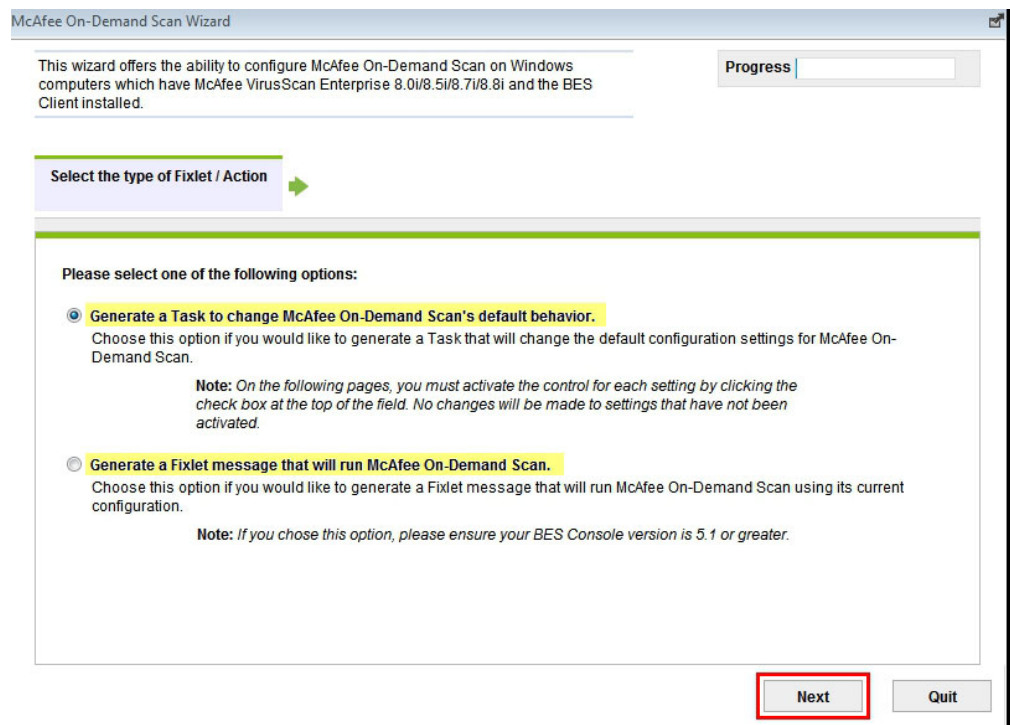
McAfee On-Demand Scan Wizard

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

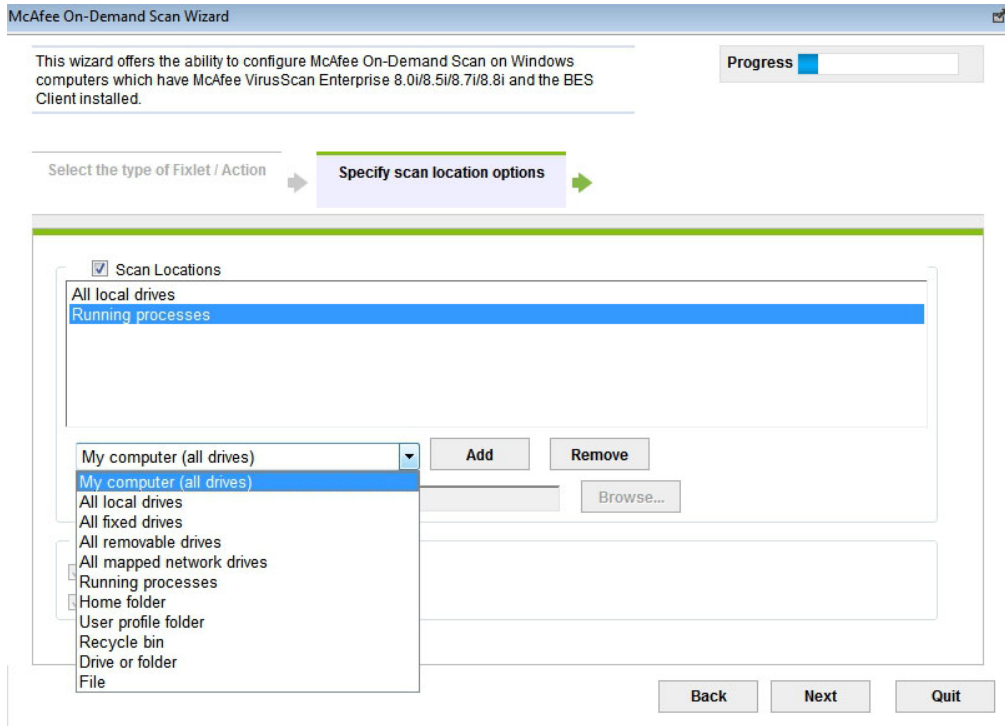


The Wizard allows you to configure McAfee On-Demand scan on Windows computers that have McAfee VirusScan Enterprise 8.0i and the Endpoint Manager client installed.

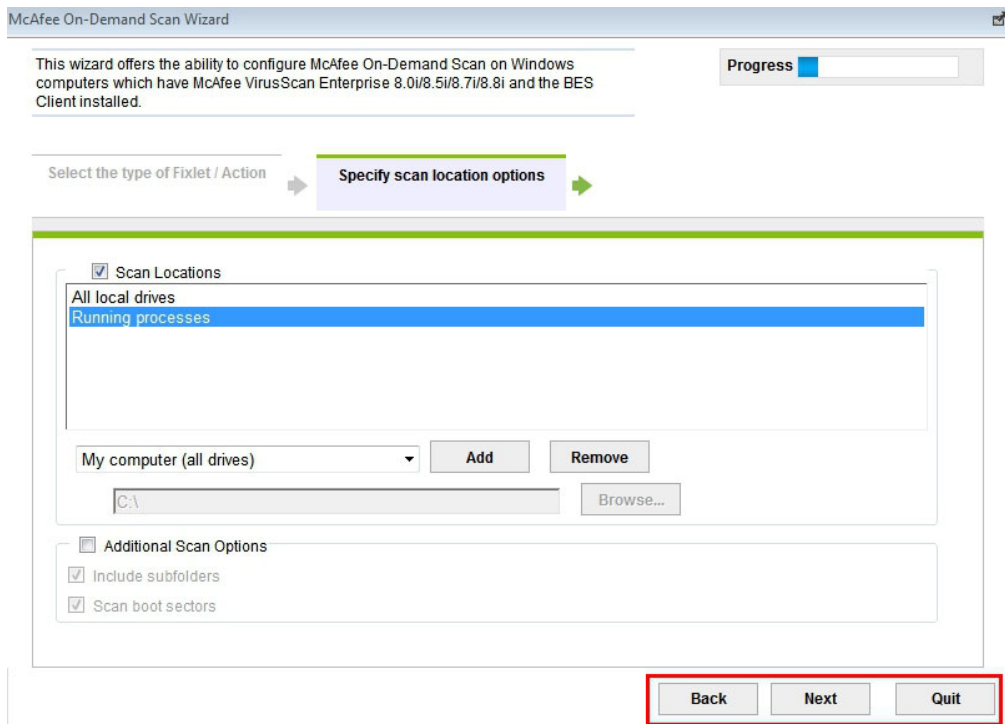
When you click to open the Wizard, you can either generate a task to change the default behavior, or generate a Fixlet to run the scan. Make a selection and click *Next*.



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.



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



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.

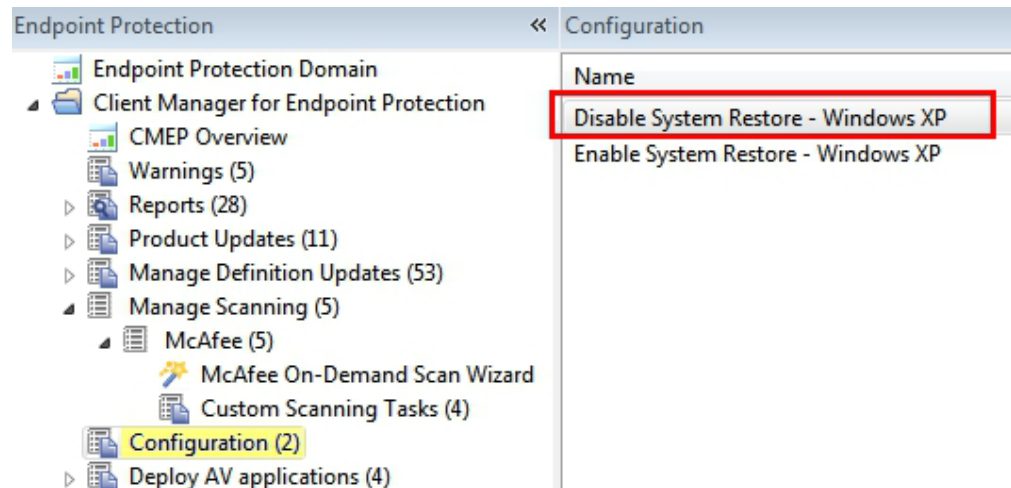
Configuration tasks

Use Anti-Malware configuration tasks to manage aspects of McAfee AVERT Stinger, Symantec UPX Parsing Engine, and Windows Defender.

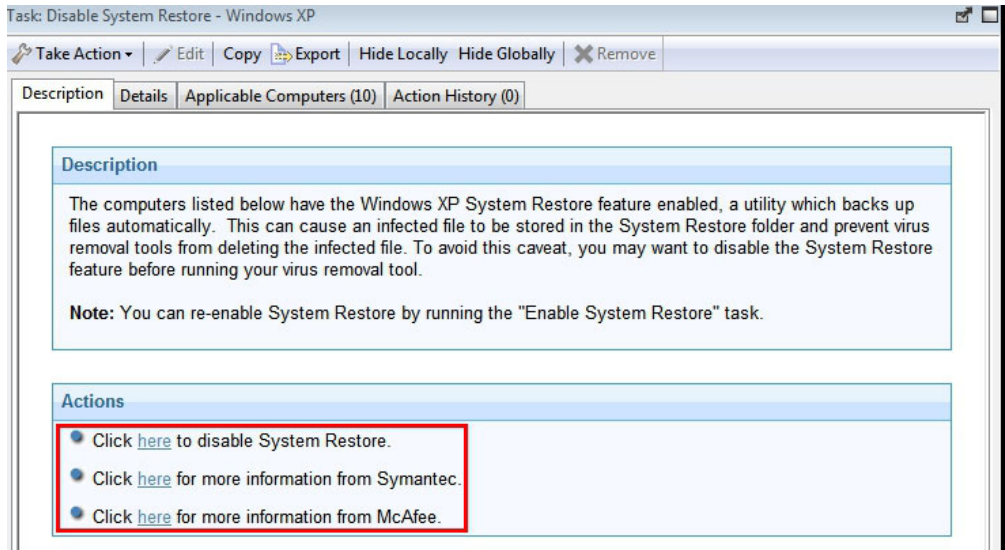
Click any title in the list of Anti-Malware tasks to display the related Fixlet window.

Disable and enable system restore

Access the Disable/Enable System Restore task from the Configuration node of the navigation tree.



Click the task to display the task window in the lower panel. If System Restore is currently enabled, using this task allows you to disable it, and vice versa. Review the text in the Description, and then click the applicable link in the Actions box to disable System Restore. You can also select an Action from the *Take Action* menu at the top of the panel.

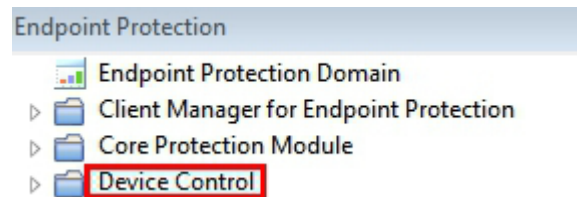


You can also click the bottom two links in the Actions box to read about how Microsoft System Restore affects other anti-virus products.

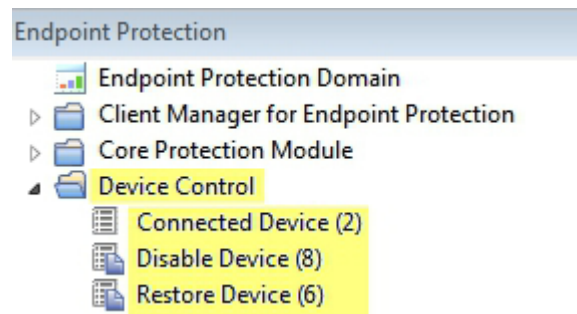
Chapter 4. Device control

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

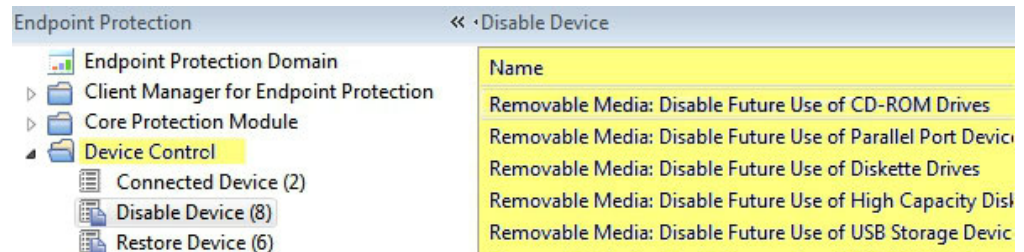
To view applicable tasks related to Device Control, click the *Device Control* site located below the *Client Manager for Endpoint Protection* site within the Endpoint Protection domain.



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.

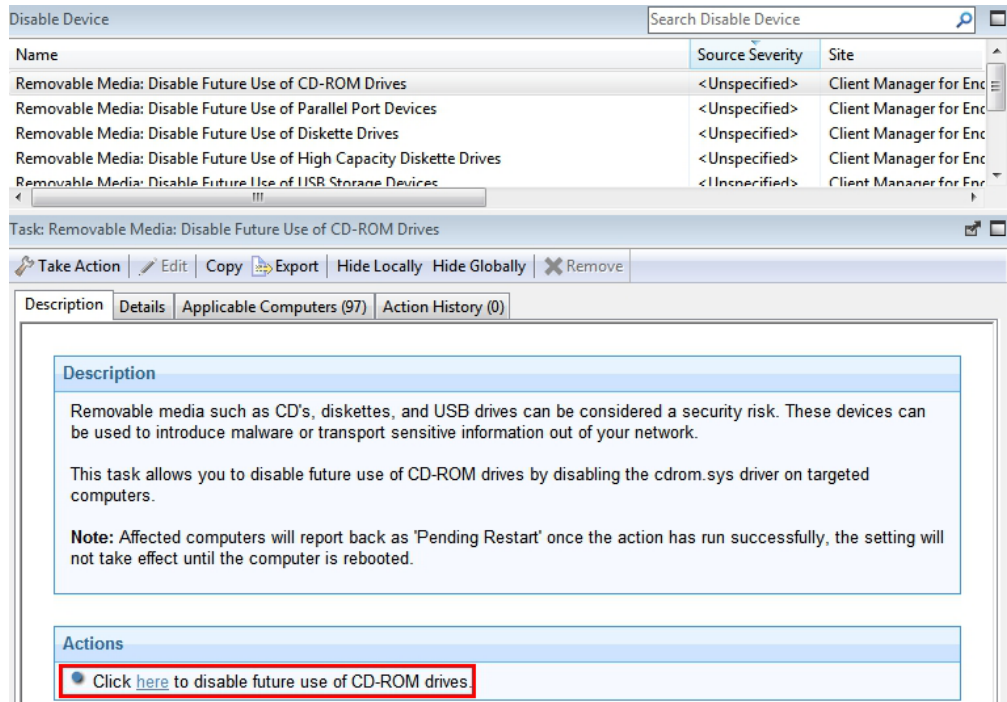


The tasks listed in the Device Control node allow you to control removable media devices by either *disabling* or *restoring* future use of the devices. These devices include:

- USB Storage
- CD-ROMs
- Floppy Disk drives

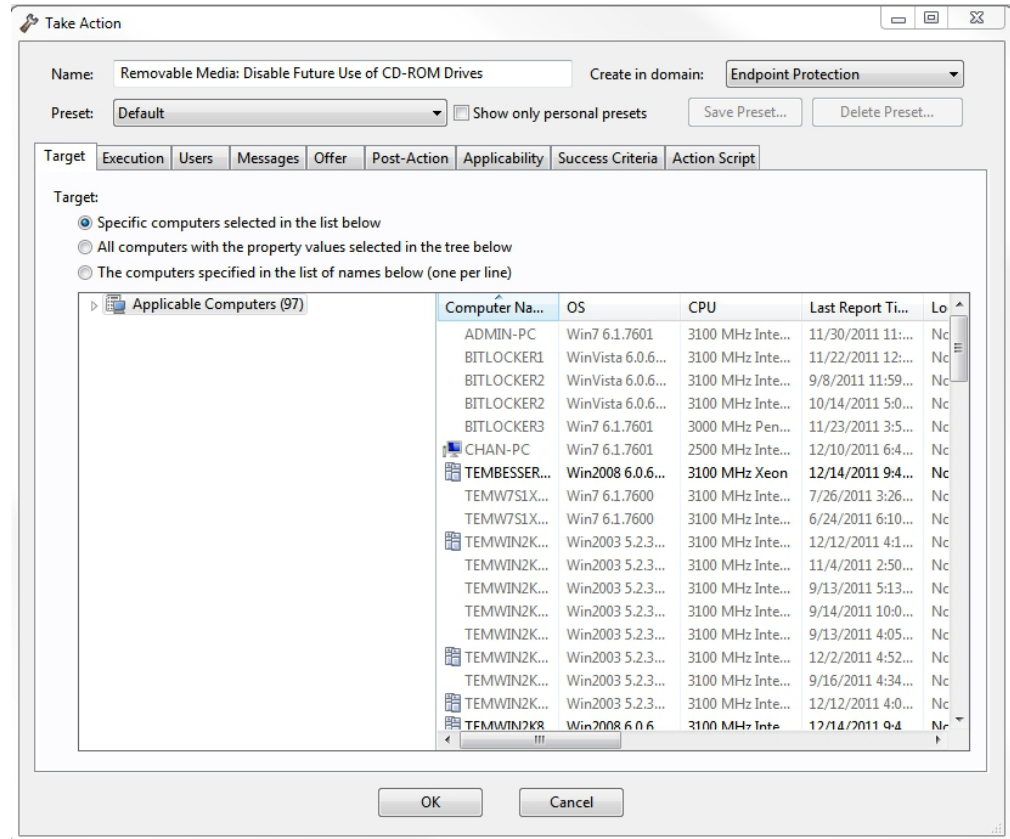
- High Capacity Floppy Disk Drives
- Parallel Port Devices
- PCMCIA Devices

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



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 *IBM Endpoint Manager Console Operator's Guide*.



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

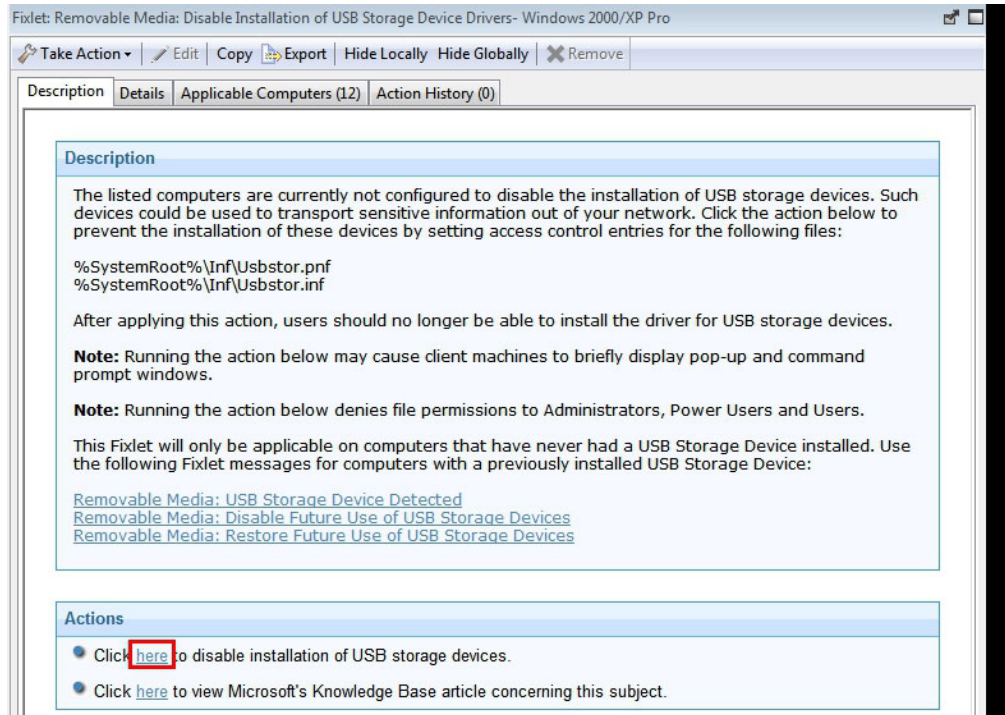
USB storage

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.



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.



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:

- http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Appendix B. Frequently asked questions

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 BES 7.2.4 (or an earlier version) installed, Windows 7 and Windows 2008 are not supported. If you upgrade to BES 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 bottom of 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:



Client Manager for Anti-Virus Overview

This dashboard has been superseded by the "Client Manager for Endpoint Protection Overview" dashboard. Please click [here](#) to open the Client Manager for Endpoint Protection 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 Endpoint Manager 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 that are offered in the USA.

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

IBM 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:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America*

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

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION 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 states 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. IBM 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-IBM 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 IBM product and use of those websites is at your own risk.

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

Licenses 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:

*IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.*

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 IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 the names and addresses used by an actual business enterprise 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 IBM, 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. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM 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:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_. All rights reserved.

Programming interface information

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

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

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

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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 IBM 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 IBM.

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 IBM.

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.

IBM 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 IBM, 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.

IBM 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.



Product Number: 5725-C44

Printed in USA