# Client Manager for Endpoint Protection (CMEP)

User's Guide

July, 2010

All inquiries regarding the foregoing should be addressed to:

BigFix, Inc.
1480 64th Street, Suite 200
Emeryville, California 94608

# Contents

Part One

# Introduction

BigFix *Client Manager for Endpoint Protection* (CMEP) is an application that encompasses Anti-Virus, spyware tools, and device control capabilities. This application enables the management of third-party endpoint security clients from vendors such as McAfee, Symantec, IBM and Trend Micro through the BigFix Unified Management Platform. More than just a way to put anti-malware defense under a BigFix umbrella, BigFix *Client Manger 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 third-party endpoint security clients
- Management and remediation of unhealthy, third-party 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 functionality 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 BigFix device control capability

## System Requirements

BigFix CMEP offers support for a variety of operating systems and products. The table below 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 BigFix support website for the most current CMEP system requirements.

| Vendor | Product | Version | Supported OS |
|---|---|---|---|
| **Computer Associates** | eTrust | 6, 7.1, 8 (Audit only *****) (x86, x64) | Windows NT 4 SP6+, Windows 2000, and Windows XP Professional, Windows Server 2003, Windows Vista |
| **IBM** | ISS Proventia Desktop | (Audit only *****) | Windows 2000 SP3+, Windows XP Professional SP 1+, Windows Vista Enterprise |

| | | | |
|---|---|---|---|
| **McAfee** | VirusScan | 4.03 – 8.7i | Windows 98, Me, Windows NT 4 SP6+, Windows XP, Windows 2000 SP4+, Windows Server 2003 SP1+, Windows Vista, Windows 7 |
| **McAfee** | VirusScan for Mac | 8.x | Mac OS X 10.4.6 or later |
| **McAfee** | NetShield | 4.5 + | Win NT/2000 only |
| **McAfee** | AVERT Stinger | | Windows 98,<br>Windows 2000, Windows XP, Windows Vista, Windows Server 2003 |
| **Microsoft** | Windows Defender | N/A | Windows XP, Windows Vista, Windows Server 2003, Windows 7 |
| **Symantec** | Anti-Virus *Corporate Edition* | 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 |
| **Symantec** | Anti-Virus *Corporate Edition* x64 | All versions | Windows XP 64-Bit Version 2003, Windows Server 2003 64-Bit, Windows Vista, Windows Server 2008 |
| **Symantec** | AntiVirus | 10.2 | Mac OS X 10.3.9+ |
| **Symantec** | Endpoint Protection | 11 | Windows 2000, Windows 2008, Windows Vista, Windows 2000 SP3+, Windows Server 2003, Windows Server 2008, Windows 7 |
| **Sophos** | Anti-Virus | 3.x, 4.1x, 4.6x, 6.x, 7.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 |
| **Trend Micro** | OfficeScan | 7, 8, 10 | 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 |
| **Trend Micro** | ServerProtect | 5.5 | Windows 2000 SP4+, Windows Server 2003 SP1+, Windows Server 2008 |

***** *Audit only* means that CMEP only checks that the definitions are more than 7 days old.

Note: CMEP also requires Flash Player 9 or higher.

Part Two

# Navigating CMEP

The navigation tree in the BigFix Console, which is available for all BigFix products, will serve as your central command for all CMEP functionality. The navigation tree gives you easy access to all reports, wizards, Fixlet messages, analyses and tasks related to the anti-malware tools in your deployment.

## Components

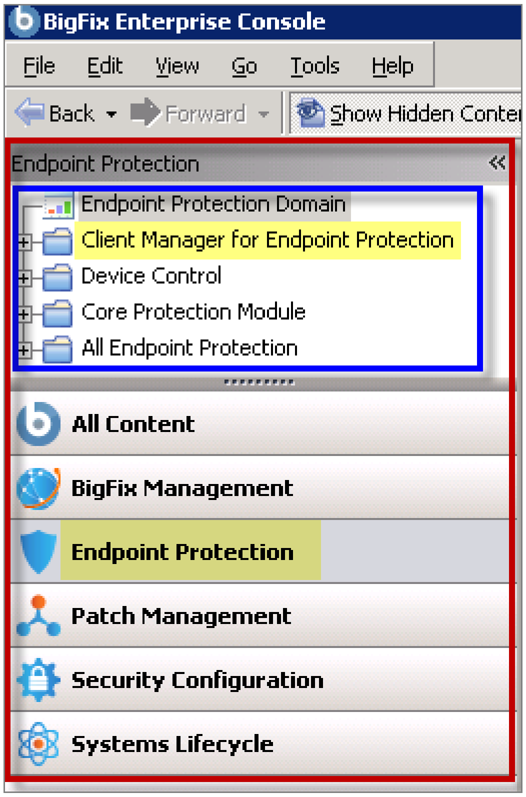
The BigFix Console organizes content into four parts:

- *Domain Panel – Includes navigation tree and list of all domains*
- *Navigation Tree – Includes list of nodes and sub-nodes containing site content*
- *List Panel – Contains listing of tasks and Fixlets*
- *Work Area – Work window where Fixlet and dialogs display*

In the context of the BigFix Console, products or *sites* are grouped by categories or *domains*. For example, CMEP is one of the sites contained within the *Endpoint Protection* domain, along with Device Control and Core Protection Module.

The domain panel is the area on the left side of the Console that includes a navigation tree and a list of all domains. The navigation tree includes a list of nodes and sub-nodes containing site content.

In the image below, you will see a navigation "tree" at the top with expandable and collapsible nodes, and a list of domains at the bottom. By clicking the *Endpoint Protection* domain at the bottom of the domain panel, a list of sites associated with that particular domain will display in the navigation tree at the top.

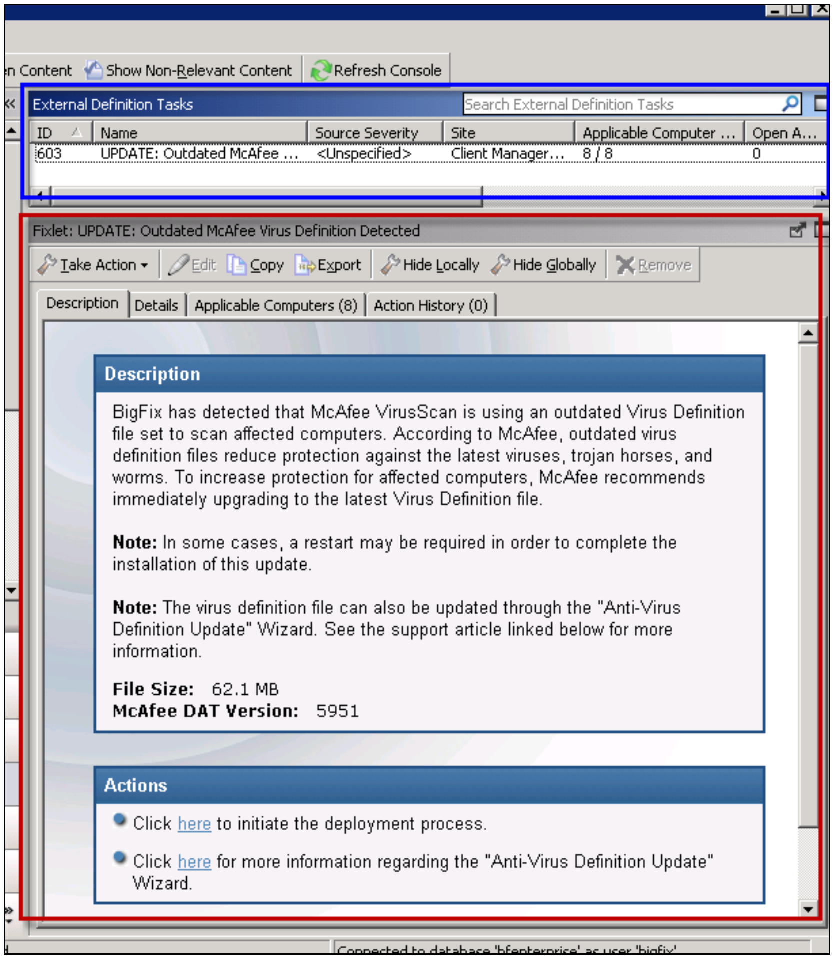


The red-outlined area represents the entire Domain Panel (including the navigation tree and list of domains), and the blue box contains just the Navigation Tree for the *Endpoint Protection* domain.

CMEP tasks are sorted through upper and lower task windows, which are located on the right side of the Console.

The upper panel, called the *List Panel* (blue), contains columns that sort data according to type, such as ID, Name, Site, Applicable Computer Count, etc.

The lower panel or *Work Area* (red) presents the Fixlet, task screen or Wizard from which you will be directed to take specific actions to customize the content in your deployment.



| ID | Name | Source Severity | Site | Applicable Computer ... | Open A... |
|---|---|---|---|---|---|
| 603 | UPDATE: Outdated McAfee ... | <Unspecified> | Client Manager... | 8 / 8 | 0 |

Fixlet: UPDATE: Outdated McAfee Virus Definition Detected

**Description**

BigFix has detected that McAfee VirusScan is using an outdated Virus Definition file set to scan affected computers. According to McAfee, outdated virus definition files reduce protection against the latest viruses, trojan horses, and worms. To increase protection for affected computers, McAfee recommends immediately upgrading to the latest Virus Definition file.

**Note:** In some cases, a restart may be required in order to complete the installation of this update.

**Note:** The virus definition file can also be updated through the "Anti-Virus Definition Update" Wizard. See the support article linked below for more information.

**File Size:** 62.1 MB
**McAfee DAT Version:** 5951

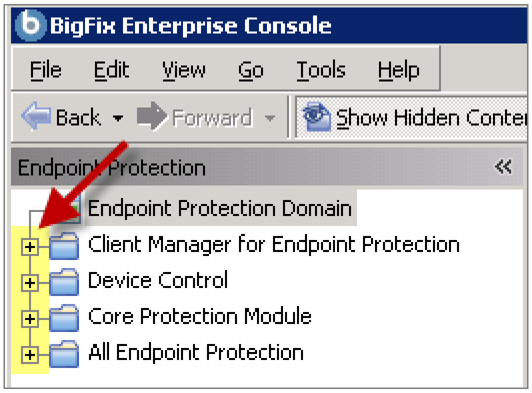
**Actions**

- Click here to initiate the deployment process.
- Click here for more information regarding the "Anti-Virus Definition Update" Wizard.

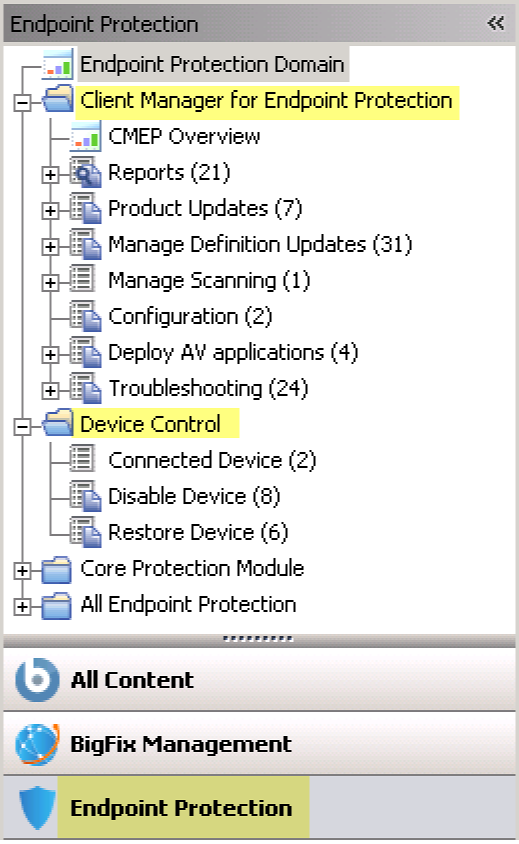
Connected to database 'bfenterprise' as user 'bigfix'

## Working with Content

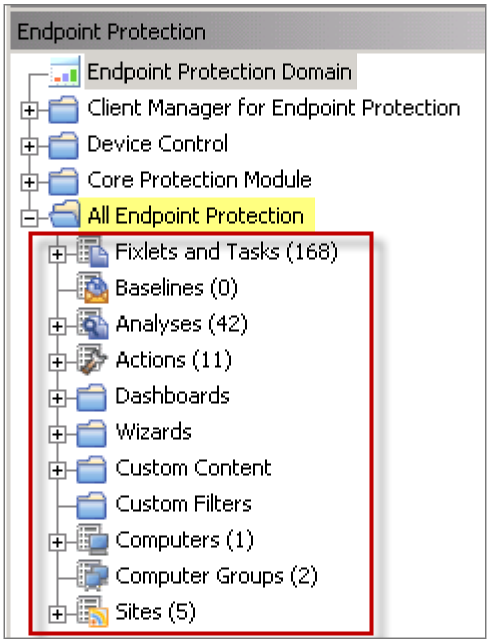
The navigation tree organizes CMEP content into expandable and collapsible folders that enable you to easily navigate and manage relevant components in your deployment. Click the plus sign (+) to expand the navigation tree nodes and the minus sign (-) to collapse them.



When you click on the Endpoint Protection domain at the bottom of your screen, you will see content related to the CMEP and Device Control “sites” organized into expandable nodes.



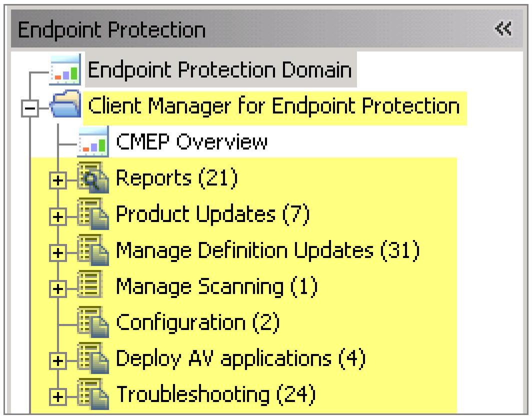
The *All Endpoint Protection* node includes content (analyses, dashboards, wizards, etc.) related to the entire Endpoint Protection domain as a whole, including all of its related “sites”.



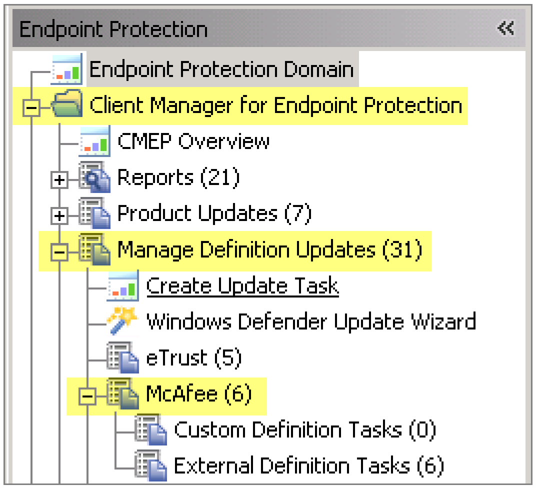
Note: Depending on your operating system, your system may display the "+" and "-" buttons in the navigation tree as triangles. Specifically, the "+" and "-" icons will display on Windows XP/2003/2008/2008R2 machines, and triangles will display on Windows Vista/7. This feature was designed so that the Console matches the standards and conventions of your specific operating system. Regardless of the particular icon, the functionality of these buttons works the same way to either expand or collapse content.

You will use this same expand/collapse method to move through the entire navigation tree.

The CMEP site is organized into 6 primary nodes: *Reports, Product Updates, Manage Definitive Updates, Manage Scanning, Deploy AV Applications,* and *Troubleshooting.*


Endpoint Protection
Endpoint Protection Domain
Client Manager for Endpoint Protection
CMEP Overview
Reports (21)
Product Updates (7)
Manage Definition Updates (31)
Manage Scanning (1)
Configuration (2)
Deploy AV applications (4)
Troubleshooting (24)

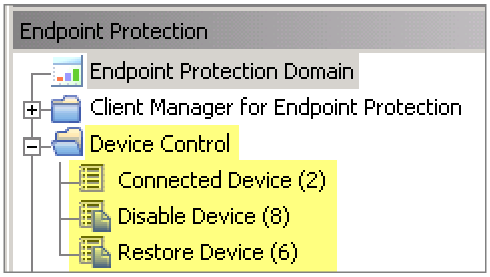
Some of these nodes expand into sub-nodes that contain additional content:



Endpoint Protection

- Endpoint Protection Domain
- Client Manager for Endpoint Protection
  - CMEP Overview
  - Reports (21)
  - Product Updates (7)
  - Manage Definition Updates (31)
    - Create Update Task
    - Windows Defender Update Wizard
    - eTrust (5)
    - McAfee (6)
      - Custom Definition Tasks (0)
      - External Definition Tasks (6)

The Device Control node includes tasks for monitoring connected devices and disabling / restoring devices.



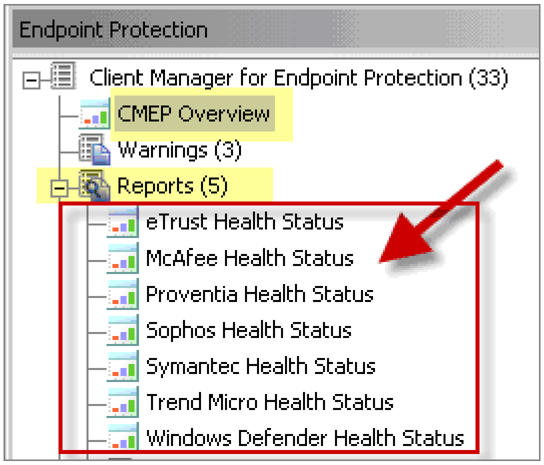
Endpoint Protection

- Endpoint Protection Domain
- Client Manager for Endpoint Protection
- Device Control
  - Connected Device (2)
  - Disable Device (8)
  - Restore Device (6)

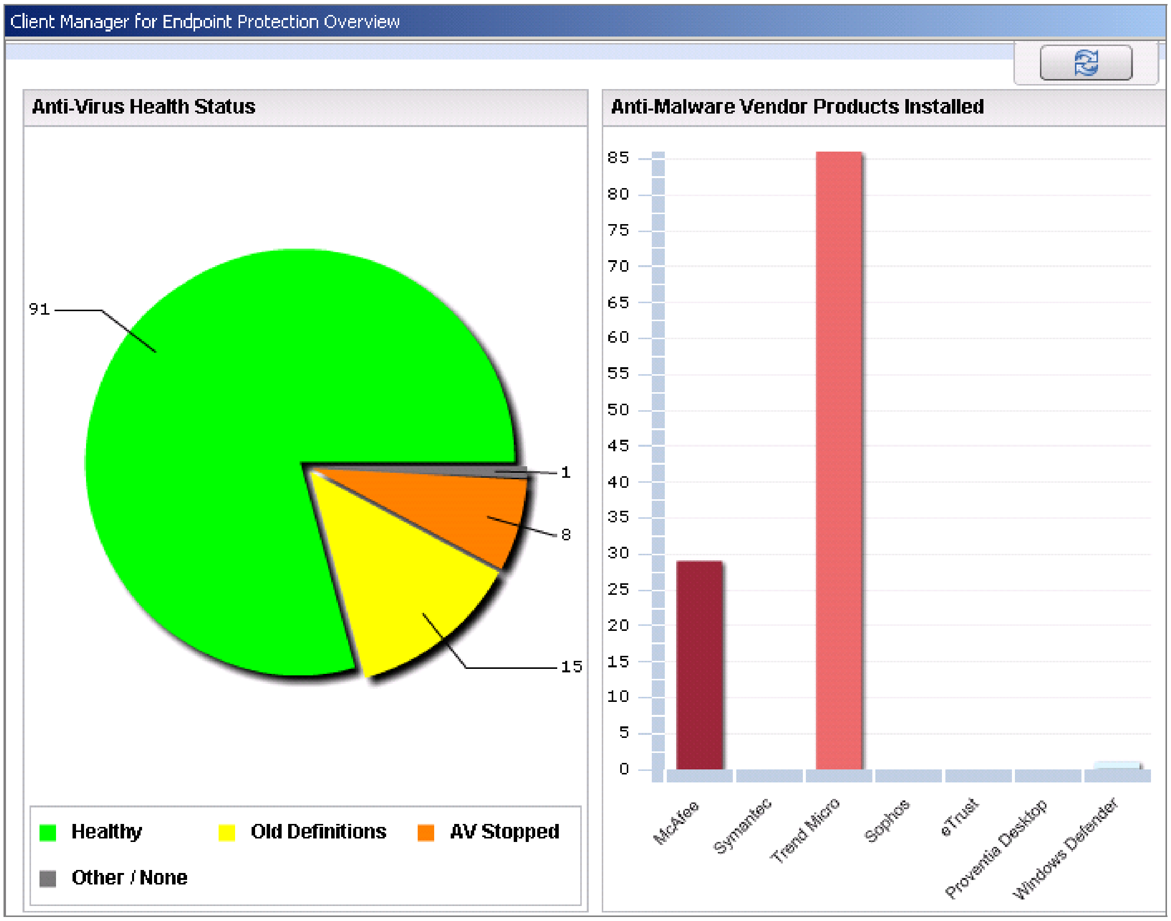
## Dashboards

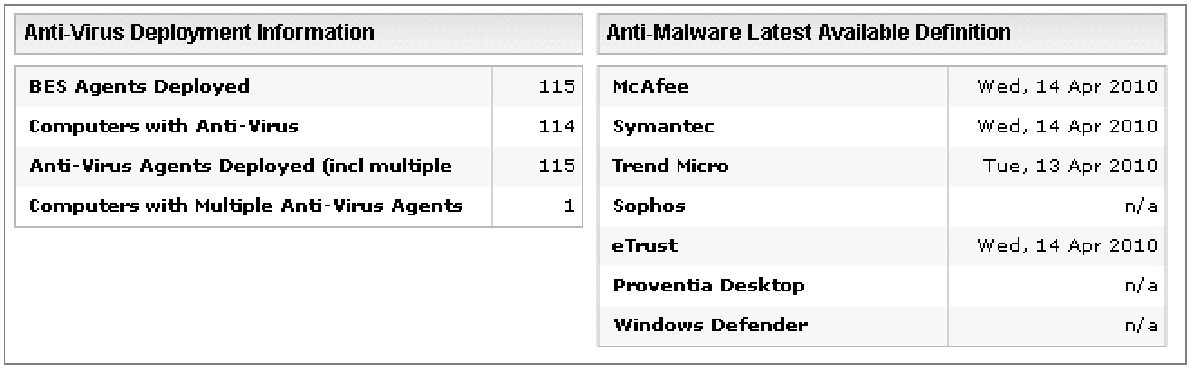
The Dashboards in CMEP include overview pie chart reports that summarize the anti-malware products within your deployment. You can view an overview of *all* anti-malware products, or view each pie chart individually.

The *CMEP Overview* dashboard is located at the top of the CMEP navigation tree. 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.





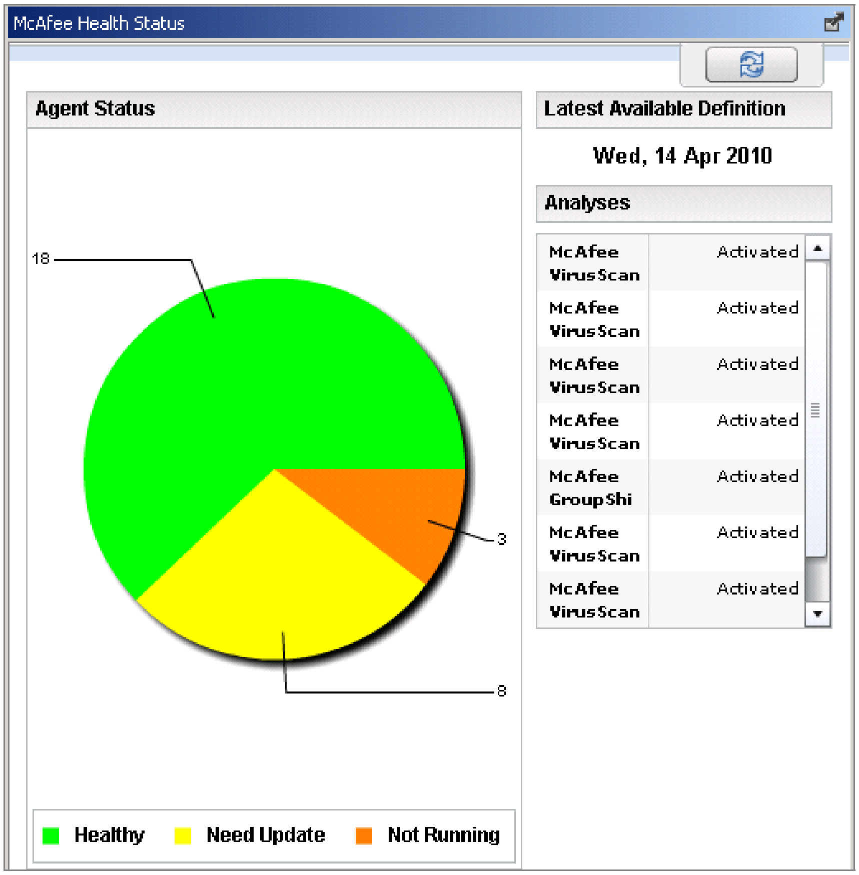
**Anti-Virus Deployment Information**

| | |
|---|---|
| BES Agents Deployed | 115 |
| Computers with Anti-Virus | 114 |
| Anti-Virus Agents Deployed (incl multiple | 115 |
| Computers with Multiple Anti-Virus Agents | 1 |

**Anti-Malware Latest Available Definition**

| | |
|---|---|
| McAfee | Wed, 14 Apr 2010 |
| Symantec | Wed, 14 Apr 2010 |
| Trend Micro | Tue, 13 Apr 2010 |
| Sophos | n/a |
| eTrust | Wed, 14 Apr 2010 |
| Proventia Desktop | n/a |
| Windows Defender | n/a |

Individual dashboards look like this:



**Latest Available Definition**

Wed, 14 Apr 2010

**Analyses**

| | |
|---|---|
| McAfee VirusScan | Activated |
| McAfee VirusScan | Activated |
| McAfee VirusScan | Activated |
| McAfee VirusScan | Activated |
| McAfee GroupShi | Activated |
| McAfee VirusScan | Activated |
| McAfee VirusScan | Activated |

Part Three

# Installation

Prior to beginning installation, you should be logged into the BigFix Console and be familiar with its basic operation. If you have questions about how to use the BigFix Console, we recommend that you review the BigFix Console Operator's Guide prior to using this document.

Installation and setup of CMEP involves two basic steps:

- *Site Subscription*
- *Activating tasks and analyses*

## Subscribing to the CMEP Site

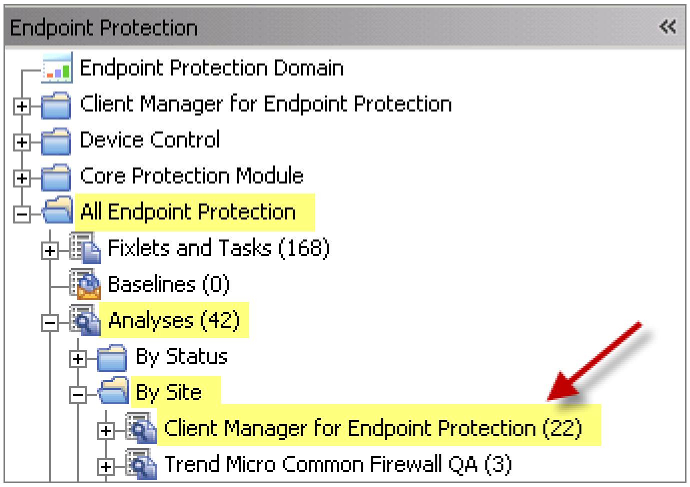
The CMEP Masthead contains information about BigFix content that performs certain tasks and analyses within your deployment. You must be subscribed to the CMEP site in order to collect data from the BigFix Clients. This data will be utilized for reporting and analysis.

The process for site subscription depends on the version of the BigFix Console that you have. Click **here** to get specific site subscription directions from the BigFix Knowledge Base.

## Activating Analyses and Tasks

Once the Masthead file has been downloaded and applicable tasks and analyses have been gathered from the content server, you will then need to deploy those tasks and activate those analyses to make them visible in the BigFix Console.

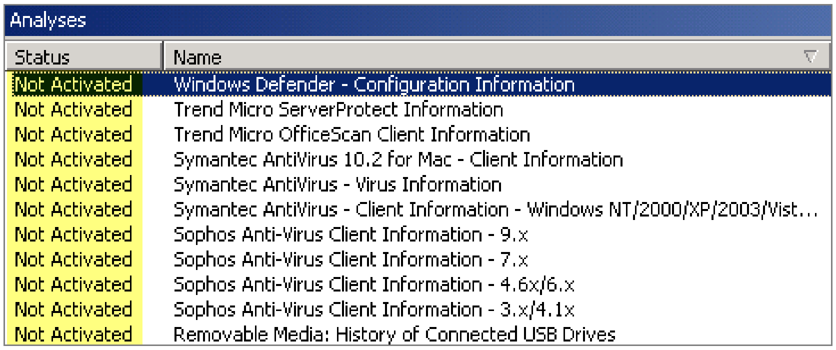
Start by viewing the *All Endpoint Protection* node in the navigation tree. Click on *Analyses,* then click *By Site* and select *Client Manager for Endpoint Protection.* The corresponding number in parentheses indicates how many analyses are available and applicable to the CMEP site.



Endpoint Protection

- Endpoint Protection Domain
- Client Manager for Endpoint Protection
- Device Control
- Core Protection Module
- All Endpoint Protection
  - Fixlets and Tasks (168)
  - Baselines (0)
  - Analyses (42)
    - By Status
    - By Site
      - Client Manager for Endpoint Protection (22)
      - Trend Micro Common Firewall QA (3)

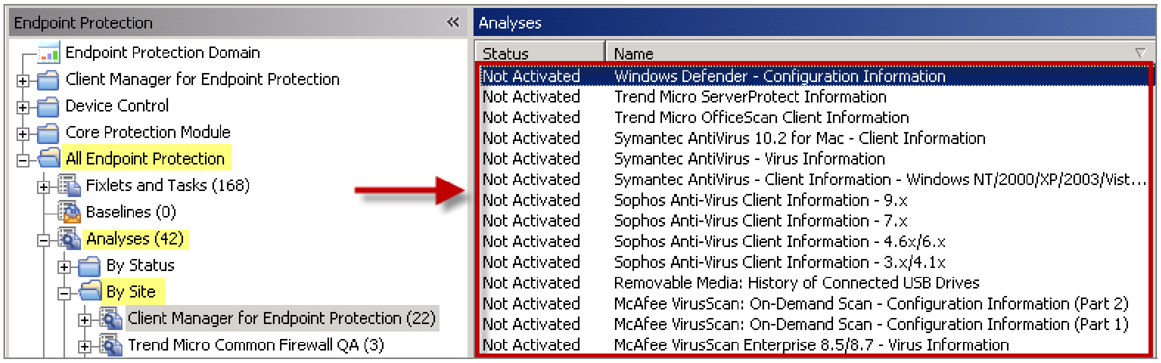
Click *Client Manager for Endpoint Protection.* This will display the list of related Analyses in the window on the right.



Analyses

| Status | Name |
|---|---|
| Not Activated | Windows Defender - Configuration Information |
| Not Activated | Trend Micro ServerProtect Information |
| Not Activated | Trend Micro OfficeScan Client Information |
| Not Activated | Symantec AntiVirus 10.2 for Mac - Client Information |
| Not Activated | Symantec AntiVirus - Virus Information |
| Not Activated | Symantec AntiVirus - Client Information - Windows NT/2000/XP/2003/Vist… |
| Not Activated | Sophos Anti-Virus Client Information - 9.x |
| Not Activated | Sophos Anti-Virus Client Information - 7.x |
| Not Activated | Sophos Anti-Virus Client Information - 4.6x/6.x |
| Not Activated | Sophos Anti-Virus Client Information - 3.x/4.1x |
| Not Activated | Removable Media: History of Connected USB Drives |

Below is a composite view:



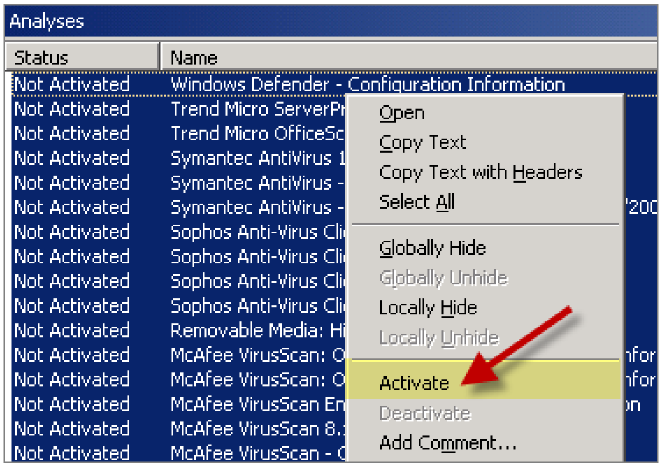
Endpoint Protection

- Endpoint Protection Domain
- Client Manager for Endpoint Protection
- Device Control
- Core Protection Module
- All Endpoint Protection
  - Fixlets and Tasks (168)
  - Baselines (0)
  - Analyses (42)
    - By Status
    - By Site
      - Client Manager for Endpoint Protection (22)
      - Trend Micro Common Firewall QA (3)

Analyses

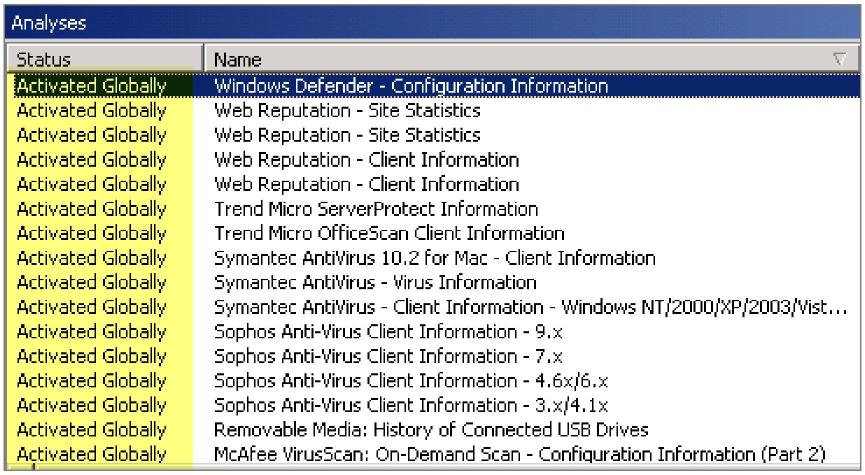
| Status | Name |
|---|---|
| Not Activated | Windows Defender - Configuration Information |
| Not Activated | Trend Micro ServerProtect Information |
| Not Activated | Trend Micro OfficeScan Client Information |
| Not Activated | Symantec AntiVirus 10.2 for Mac - Client Information |
| Not Activated | Symantec AntiVirus - Virus Information |
| Not Activated | Symantec AntiVirus - Client Information - Windows NT/2000/XP/2003/Vist… |
| Not Activated | Sophos Anti-Virus Client Information - 9.x |
| Not Activated | Sophos Anti-Virus Client Information - 7.x |
| Not Activated | Sophos Anti-Virus Client Information - 4.6x/6.x |
| Not Activated | Sophos Anti-Virus Client Information - 3.x/4.1x |
| Not Activated | Removable Media: History of Connected USB Drives |
| Not Activated | McAfee VirusScan: On-Demand Scan - Configuration Information (Part 2) |
| Not Activated | McAfee VirusScan: On-Demand Scan - Configuration Information (Part 1) |
| Not Activated | McAfee VirusScan Enterprise 8.5/8.7 - Virus Information |

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


Analyses

| Status | Name |
|---|---|
| Not Activated | Windows Defender - Configuration Information |
| Not Activated | Trend Micro ServerPr |
| Not Activated | Trend Micro OfficeSc |
| Not Activated | Symantec AntiVirus 1 |
| Not Activated | Symantec AntiVirus - |
| Not Activated | Symantec AntiVirus - |
| Not Activated | Sophos Anti-Virus Cli |
| Not Activated | Sophos Anti-Virus Cli |
| Not Activated | Sophos Anti-Virus Cli |
| Not Activated | Sophos Anti-Virus Cli |
| Not Activated | Removable Media: Hi |
| Not Activated | McAfee VirusScan: O |
| Not Activated | McAfee VirusScan: O |
| Not Activated | McAfee VirusScan En |
| Not Activated | McAfee VirusScan 8. |
| Not Activated | McAfee VirusScan - C |

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


Analyses

| Status | Name |
|---|---|
| Activated Globally | Windows Defender - Configuration Information |
| Activated Globally | Web Reputation - Site Statistics |
| Activated Globally | Web Reputation - Site Statistics |
| Activated Globally | Web Reputation - Client Information |
| Activated Globally | Web Reputation - Client Information |
| Activated Globally | Trend Micro ServerProtect Information |
| Activated Globally | Trend Micro OfficeScan Client Information |
| Activated Globally | Symantec AntiVirus 10.2 for Mac - Client Information |
| Activated Globally | Symantec AntiVirus - Virus Information |
| Activated Globally | Symantec AntiVirus - Client Information - Windows NT/2000/XP/2003/Vist... |
| Activated Globally | Sophos Anti-Virus Client Information - 9.x |
| Activated Globally | Sophos Anti-Virus Client Information - 7.x |
| Activated Globally | Sophos Anti-Virus Client Information - 4.6x/6.x |
| Activated Globally | Sophos Anti-Virus Client Information - 3.x/4.1x |
| Activated Globally | Removable Media: History of Connected USB Drives |
| Activated Globally | McAfee VirusScan: On-Demand Scan - Configuration Information (Part 2) |

For more detailed information on deploying tasks and activating analyses, review the BigFix Console Operator's Guide available on the BigFix support website.

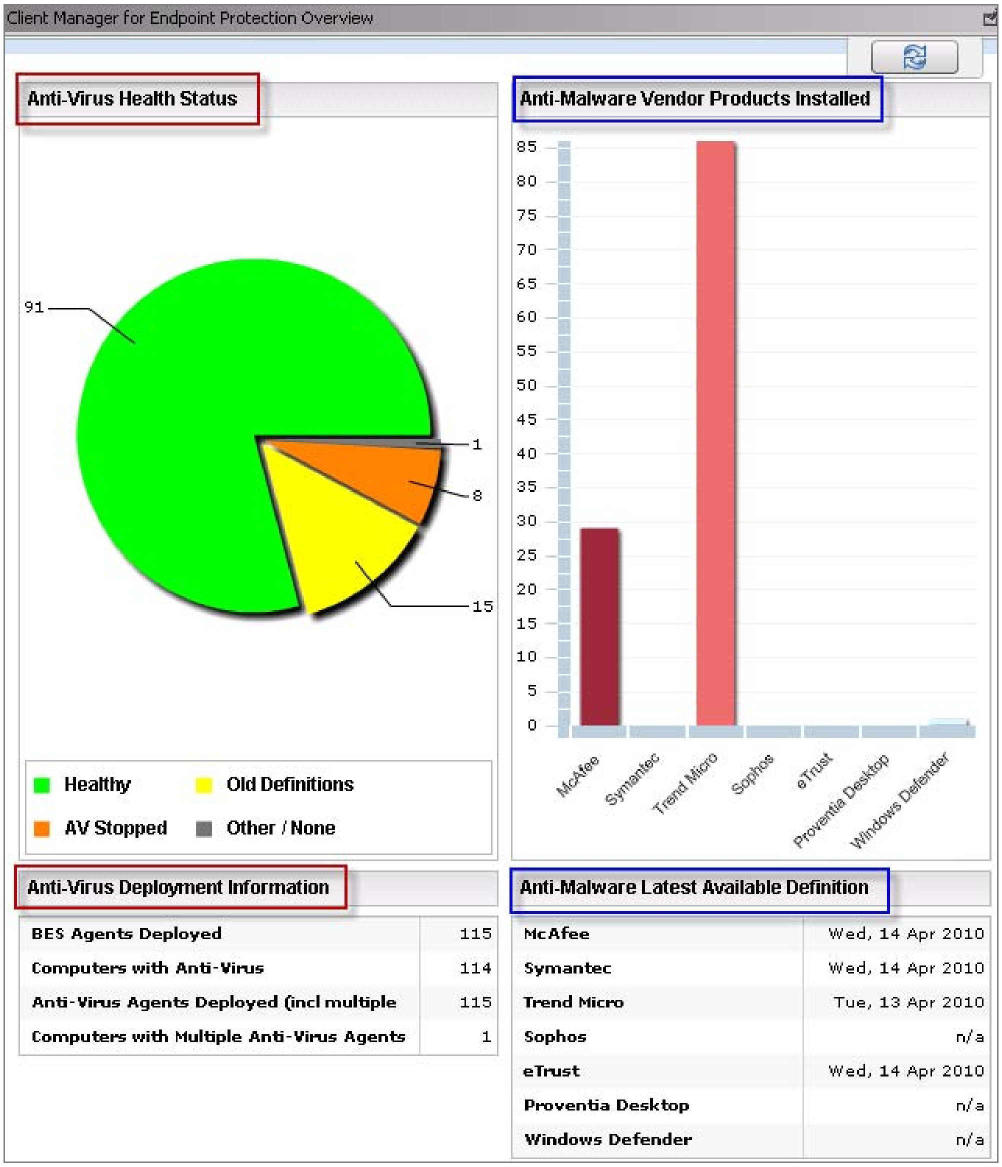
Part Four

# 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 screen 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.



Anti-Virus Deployment Information

| | |
|---|---|
| BES Agents Deployed | 115 |
| Computers with Anti-Virus | 114 |
| Anti-Virus Agents Deployed (incl multiple | 115 |
| Computers with Multiple Anti-Virus Agents | 1 |

Anti-Malware Latest Available Definition

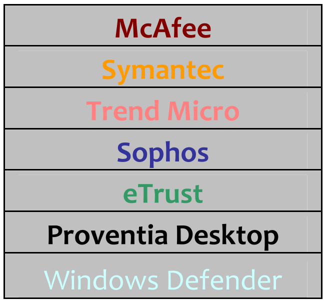
| | |
|---|---|
| McAfee | Wed, 14 Apr 2010 |
| Symantec | Wed, 14 Apr 2010 |
| Trend Micro | Tue, 13 Apr 2010 |
| Sophos | n/a |
| eTrust | Wed, 14 Apr 2010 |
| Proventia Desktop | n/a |
| Windows Defender | n/a |

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. |

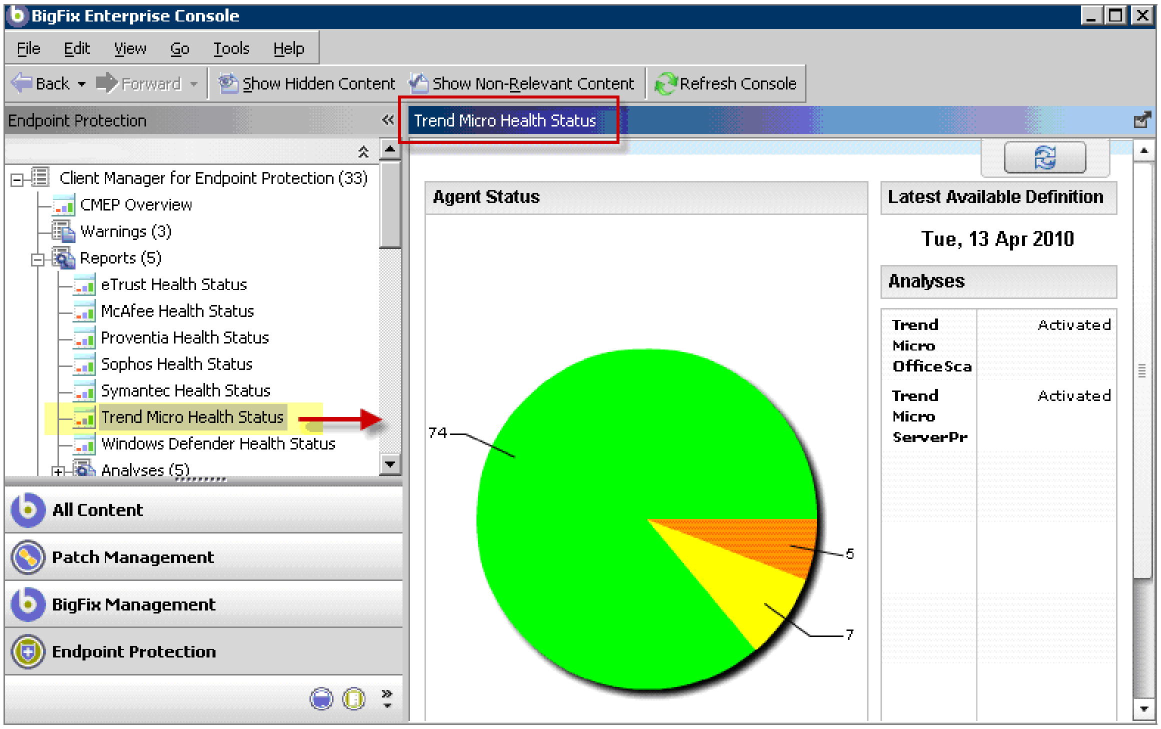
* **Special Note**: For detailed information on how CMEP defines the "healthy" category in the Health Status pie chart, see the related Knowledge Base article on the BigFix support website.

The *Anti-Malware Vendor Products* bar graph is color-coded according to vendor, as shown in the image on page 12 above.



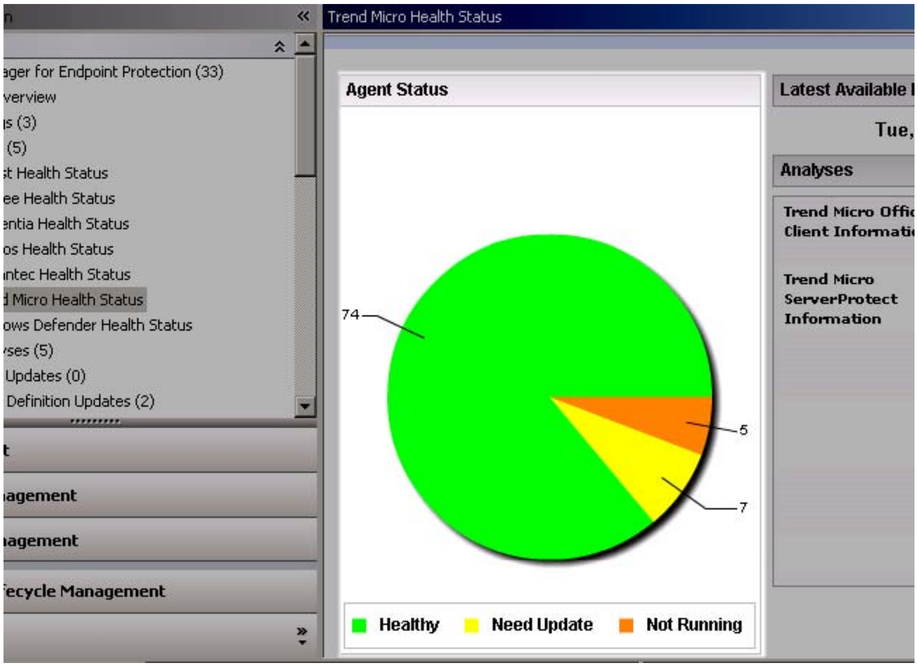
| |
|---|
| McAfee |
| Symantec |
| Trend Micro |
| Sophos |
| eTrust |
| Proventia Desktop |
| Windows Defender |

You may also select individual vendors to display a customized pie chart and summary. For example, by selecting to view the Trend Micro report, the dashboard will display the Trend Micro health status pie chart, the date of the latest definition release, and a list of related Analyses with either *Activated* or *Not Activated* status.



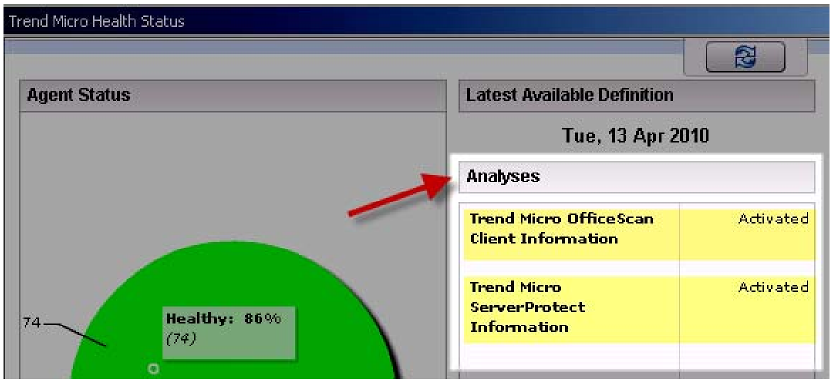
The ***Agent Status*** section displays pie charts representing the health and status of your Anti-Virus according to each vendor. Status is measured by the following criteria:

- 🟩 **Healthy –** Anti-Virus applications are running properly on this machine.
- 🟨 **Need Update –** Virus definitions need to be updated on this machine.
- 🟧 **Not Running –** The required Anti-Virus application or service(s) is not running.

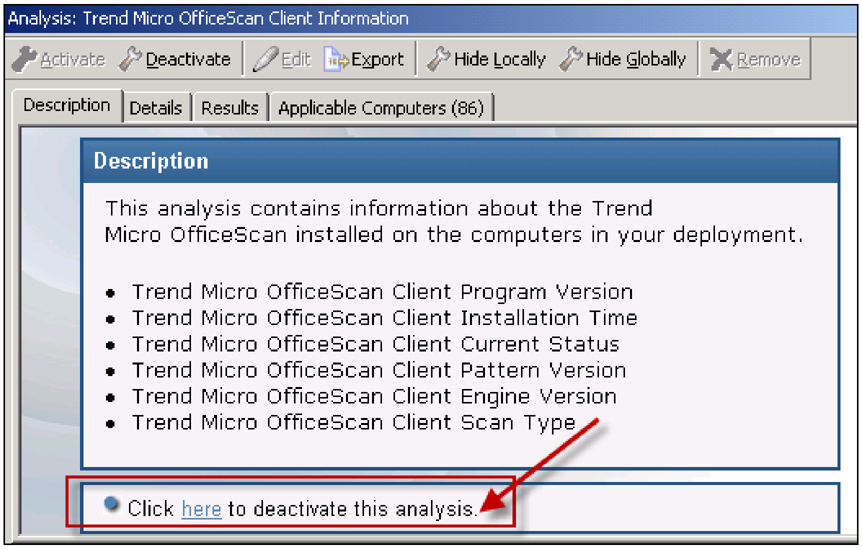


## Analyses

For each of the vendors represented in the Anti-Malware reports, there are corresponding analyses listed in the **Latest Available Definition** section on the right of each pie chart.


Trend Micro Health Status
Agent Status
Latest Available Definition
Tue, 13 Apr 2010
Analyses
Trend Micro OfficeScan Client Information
Activated
Trend Micro ServerProtect Information
Activated
74
Healthy: 86% (74)

When clicked, each item will display a Fixlet that allows you to either activate or de-activate that particular analysis.



Description

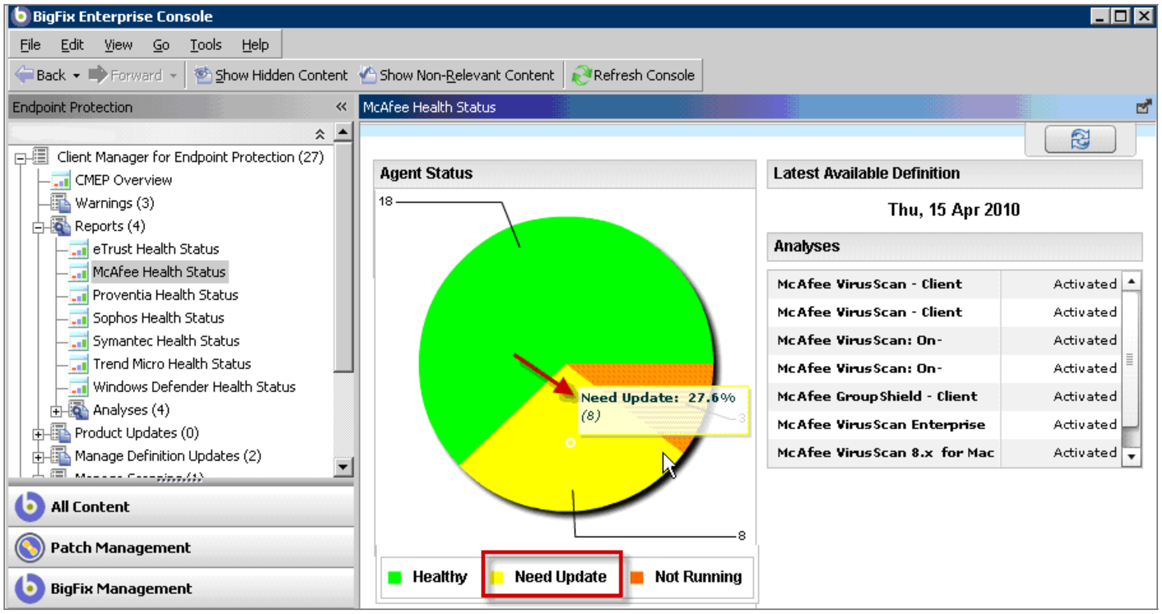
This analysis contains information about the Trend Micro OfficeScan installed on the computers in your deployment.

- Trend Micro OfficeScan Client Program Version
- Trend Micro OfficeScan Client Installation Time
- Trend Micro OfficeScan Client Current Status
- Trend Micro OfficeScan Client Pattern Version
- Trend Micro OfficeScan Client Engine Version
- Trend Micro OfficeScan Client Scan Type

● Click here to deactivate this analysis.

# How to Update

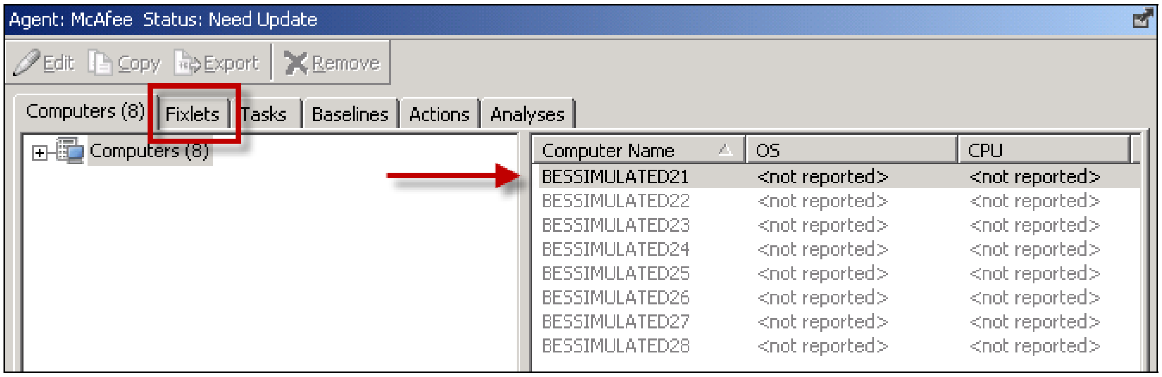
If one of your Anti-Malware vendors displays a yellow “Need Update” status in the Agent Status pie chart, you need to update your virus definitions to ensure that all applicable computers are adequately protected.



Thu, 15 Apr 2010

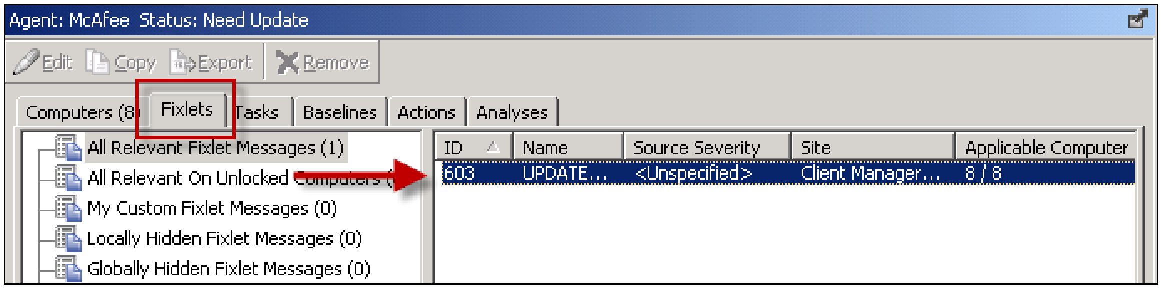
| | |
|---|---|
| McAfee VirusScan - Client | Activated |
| McAfee VirusScan - Client | Activated |
| McAfee VirusScan: On- | Activated |
| McAfee VirusScan: On- | Activated |
| McAfee GroupShield - Client | Activated |
| McAfee VirusScan Enterprise | Activated |
| McAfee VirusScan 8.x for Mac | Activated |

Start by clicking directly on the pie chart. This will open a new window where you can update the related Fixlets. When the window opens, click on the applicable computer listed under the Computers column on the right side of the screen.



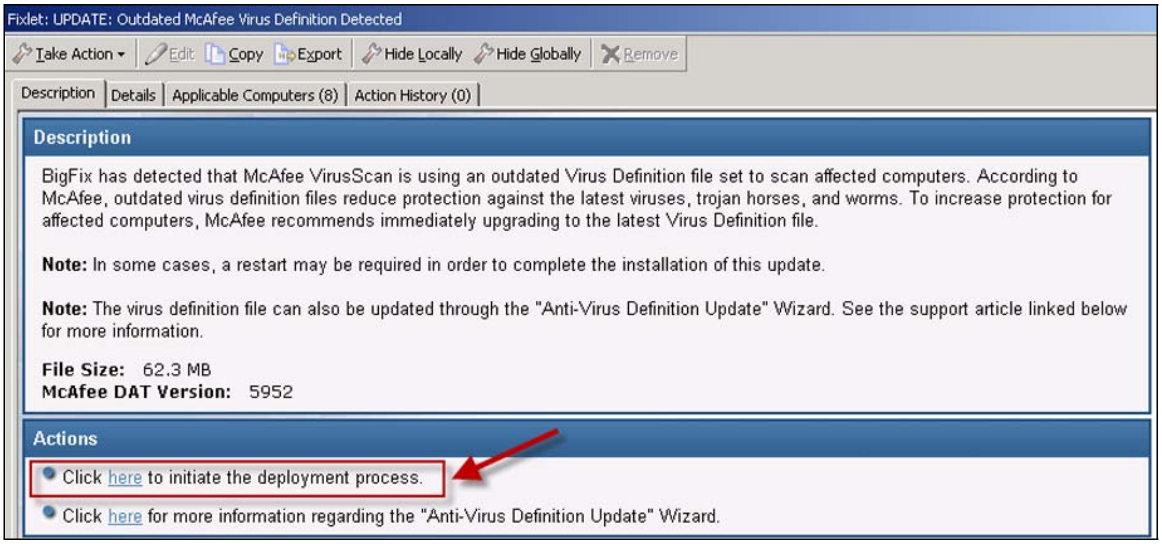
| Computer Name | OS | CPU |
|---|---|---|
| BESSIMULATED21 | <not reported> | <not reported> |
| BESSIMULATED22 | <not reported> | <not reported> |
| BESSIMULATED23 | <not reported> | <not reported> |
| BESSIMULATED24 | <not reported> | <not reported> |
| BESSIMULATED25 | <not reported> | <not reported> |
| BESSIMULATED26 | <not reported> | <not reported> |
| BESSIMULATED27 | <not reported> | <not reported> |
| BESSIMULATED28 | <not reported> | <not reported> |

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


Agent: McAfee Status: Need Update
Edit
Copy
Export
Remove
Computers (8)
Fixlets
Tasks
Baselines
Actions
Analyses
All Relevant Fixlet Messages (1)
All Relevant On Unlocked Computers (
My Custom Fixlet Messages (0)
Locally Hidden Fixlet Messages (0)
Globally Hidden Fixlet Messages (0)

| ID | Name | Source Severity | Site | Applicable Computer |
|---|---|---|---|---|
| 603 | UPDATE... | <Unspecified> | Client Manager... | 8 / 8 |

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



Description

BigFix has detected that McAfee VirusScan is using an outdated Virus Definition file set to scan affected computers. According to McAfee, outdated virus definition files reduce protection against the latest viruses, trojan horses, and worms. To increase protection for affected computers, McAfee recommends immediately upgrading to the latest Virus Definition file.

**Note:** In some cases, a restart may be required in order to complete the installation of this update.

**Note:** The virus definition file can also be updated through the "Anti-Virus Definition Update" Wizard. See the support article linked below for more information.

**File Size:** 62.3 MB
**McAfee DAT Version:** 5952

Actions

- Click here to initiate the deployment process.
- Click here for more information regarding the "Anti-Virus Definition Update" Wizard.

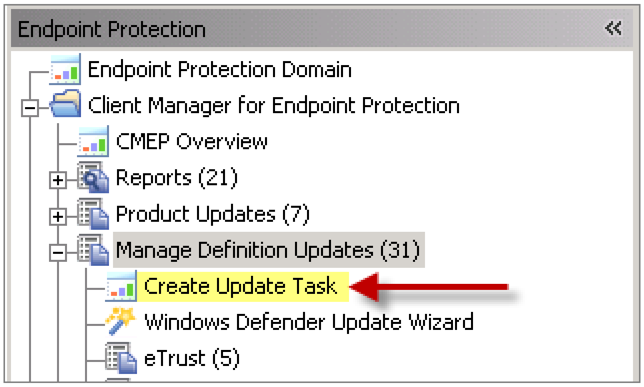
This will open the Take Action dialog, where you can set specific parameters for this action. As an alternative, you may also click the *Take Action* pull-down in the top left of the panel. For detailed information about the Take Action dialog, review the BigFix Console Operator's Guide.

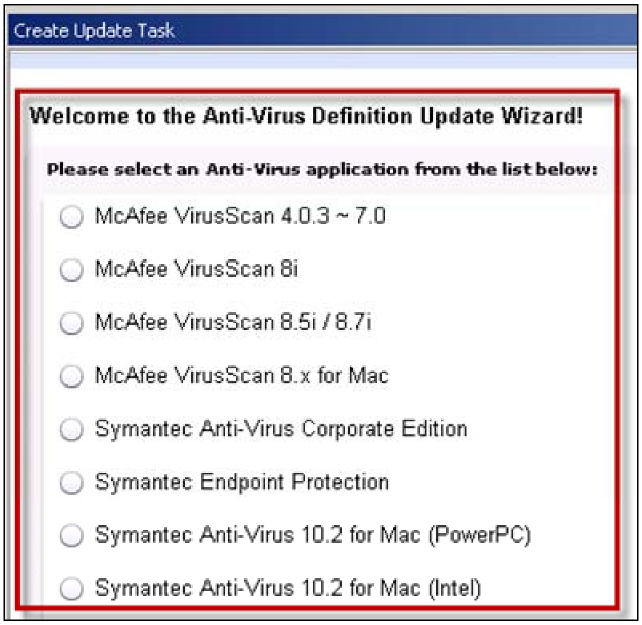
## Wizards

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,* as shown below. This will open the wizard in the lower panel.


Endpoint Protection
Endpoint Protection Domain
Client Manager for Endpoint Protection
CMEP Overview
Reports (21)
Product Updates (7)
Manage Definition Updates (31)
Create Update Task
Windows Defender Update Wizard
eTrust (5)



**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

○ McAfee VirusScan 8.x for Mac

○ Symantec Anti-Virus Corporate Edition

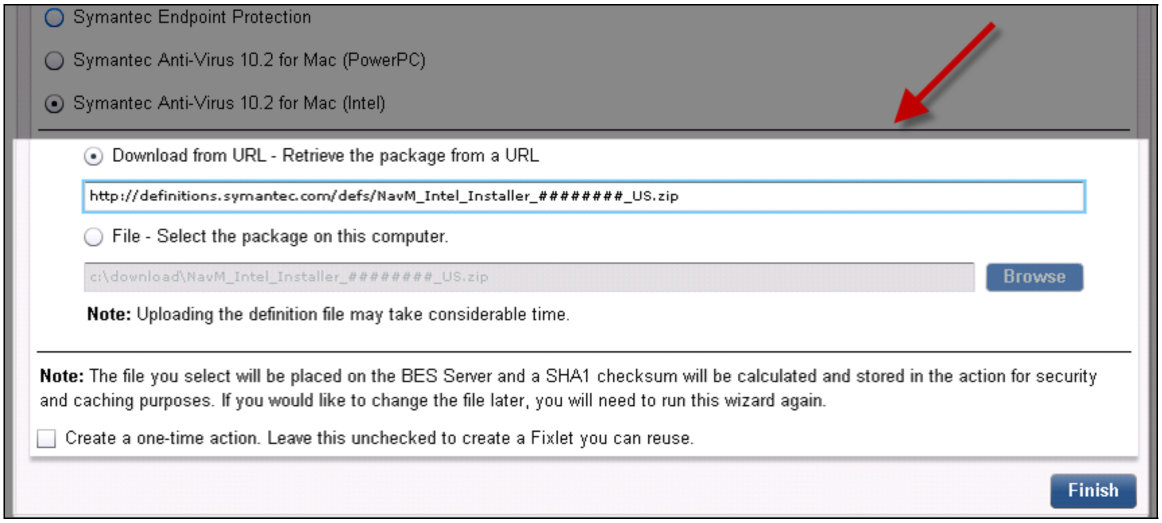
○ Symantec Endpoint Protection

○ Symantec Anti-Virus 10.2 for Mac (PowerPC)

○ Symantec Anti-Virus 10.2 for Mac (Intel)

Selecting any anti-virus product from the list will display more information at the bottom of the panel. You may 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.*



○ Symantec Endpoint Protection

○ Symantec Anti-Virus 10.2 for Mac (PowerPC)

● Symantec Anti-Virus 10.2 for Mac (Intel)

● Download from URL - Retrieve the package from a URL

http://definitions.symantec.com/defs/NavM_Intel_Installer_########_US.zip

○ File - Select the package on this computer.

c:\download\NavM_Intel_Installer_########_US.zip

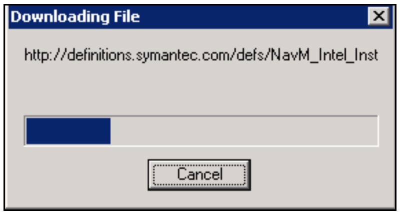
**Note:** Uploading the definition file may take considerable time.

**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: In order to enter the correct URL, go to the virus definitions page on the McAfee or Symantec website copy/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.

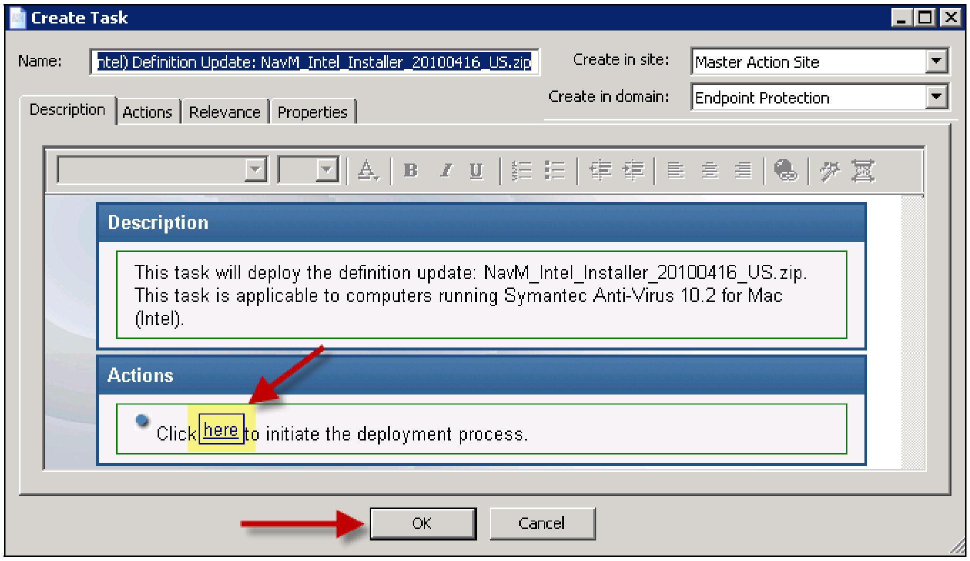
You will see the following screen as the virus definitions are downloaded to your system:



Downloading File

http://definitions.symantec.com/defs/NavM_Intel_Inst

Next, you will see the Create Task window. Review the content in the Description, Actions, Relevance, and Properties tabs, click *Okay,* and enter your Private Key Password.



Create Task

Name: ntel) Definition Update: NavM_Intel_Installer_20100416_US.zip

Create in site: Master Action Site

Create in domain: Endpoint Protection

**Description**

This task will deploy the definition update: NavM_Intel_Installer_20100416_US.zip. This task is applicable to computers running Symantec Anti-Virus 10.2 for Mac (Intel).

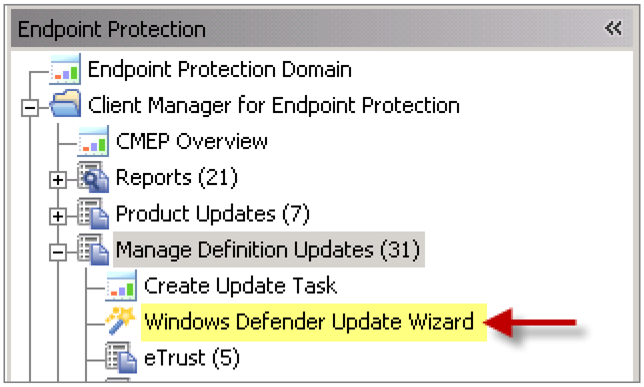
**Actions**

- Click here to initiate the deployment process.

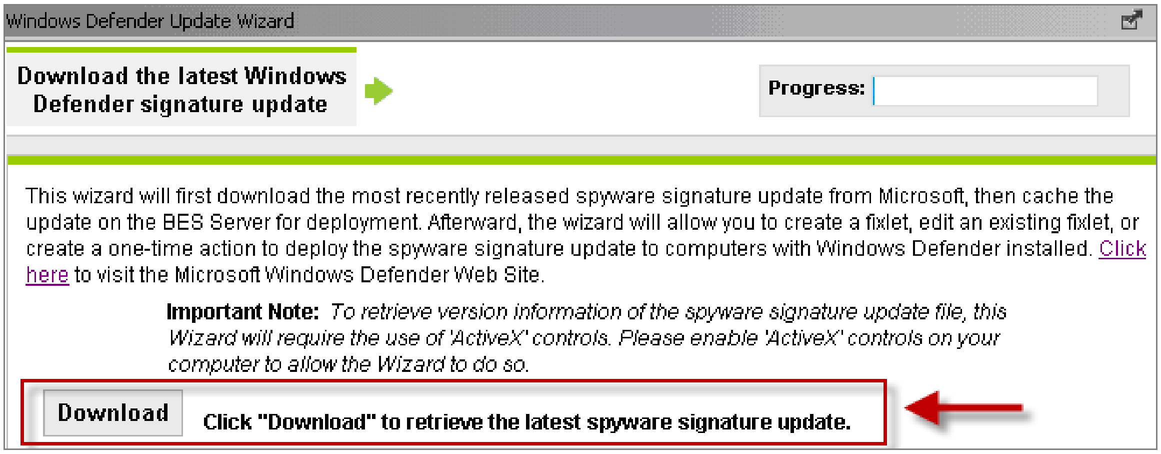
At the next task window, click where indicated in the Actions box to initiate deployment. This will open the Take Action dialog, where you can set specific parameters of the action.

## Windows Defender Update Wizard

To access the Windows Defender Update Wizard, click on the Wizard from the *Manage Definition Updates* sub-node in the navigation tree.


Endpoint Protection
Endpoint Protection Domain
Client Manager for Endpoint Protection
CMEP Overview
Reports (21)
Product Updates (7)
Manage Definition Updates (31)
Create Update Task
Windows Defender Update Wizard
eTrust (5)

The Wizard will open in the Work Panel on the right.

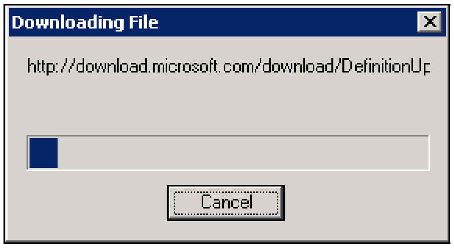

Windows Defender Update Wizard
Download the latest Windows Defender signature update
Progress:
Download

This wizard will first download the most recently released spyware signature update from Microsoft, then cache the update on the BES Server for deployment. Afterward, the wizard will allow you to create a fixlet, edit an existing fixlet, or create a one-time action to deploy the spyware signature update to computers with Windows Defender installed. Click here to visit the Microsoft Windows Defender Web Site.

**Important Note:** *To retrieve version information of the spyware signature update file, this Wizard will require the use of 'ActiveX' controls. Please enable 'ActiveX' controls on your computer to allow the Wizard to do so.*

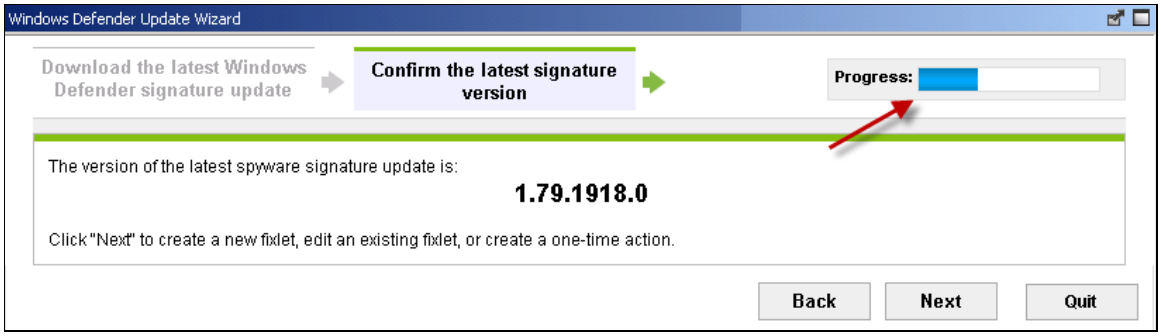
**Click "Download" to retrieve the latest spyware signature update.**

Click *Download* and you will see a progress window appear as the Wizards retrieves spyware updates.



http://download.microsoft.com/download/DefinitionUp

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



Windows Defender Update Wizard

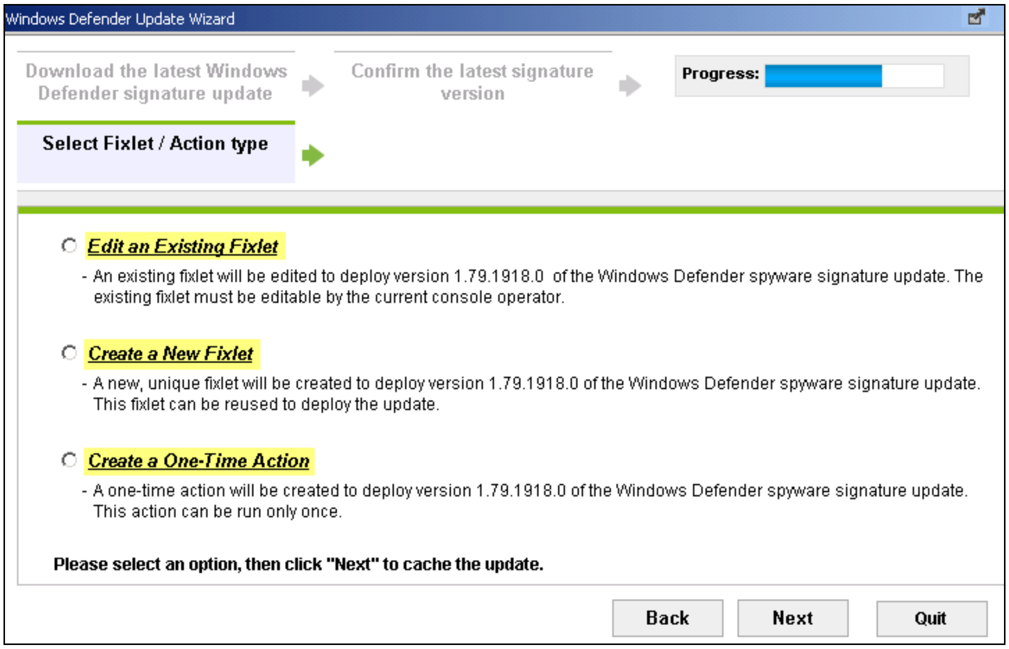
Download the latest Windows Defender signature update
Confirm the latest signature version
Progress:

The version of the latest spyware signature update is:

**1.79.1918.0**

Click "Next" to create a new fixlet, edit an existing fixlet, or create a one-time action.

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



Windows Defender Update Wizard

Download the latest Windows Defender signature update
Confirm the latest signature version
Progress:
Select Fixlet / Action type

○ *Edit an Existing Fixlet*

- An existing fixlet will be edited to deploy version 1.79.1918.0 of the Windows Defender spyware signature update. The existing fixlet must be editable by the current console operator.

○ *Create a New Fixlet*

- A new, unique fixlet will be created to deploy version 1.79.1918.0 of the Windows Defender spyware signature update. This fixlet can be reused to deploy the update.

○ *Create a One-Time Action*

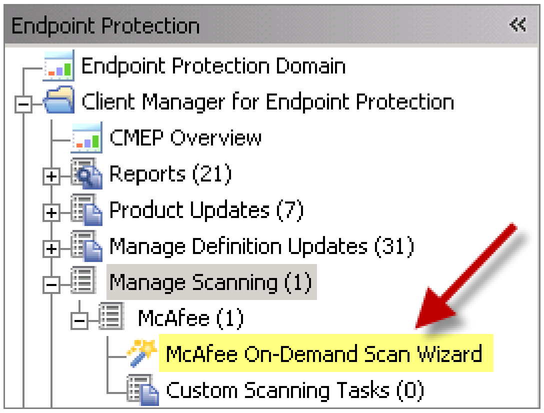
- A one-time action will be created to deploy version 1.79.1918.0 of the Windows Defender spyware signature update. This action can be run only once.

**Please select an option, then click "Next" to cache the update.**

Click *Next* to proceed through the Wizard.

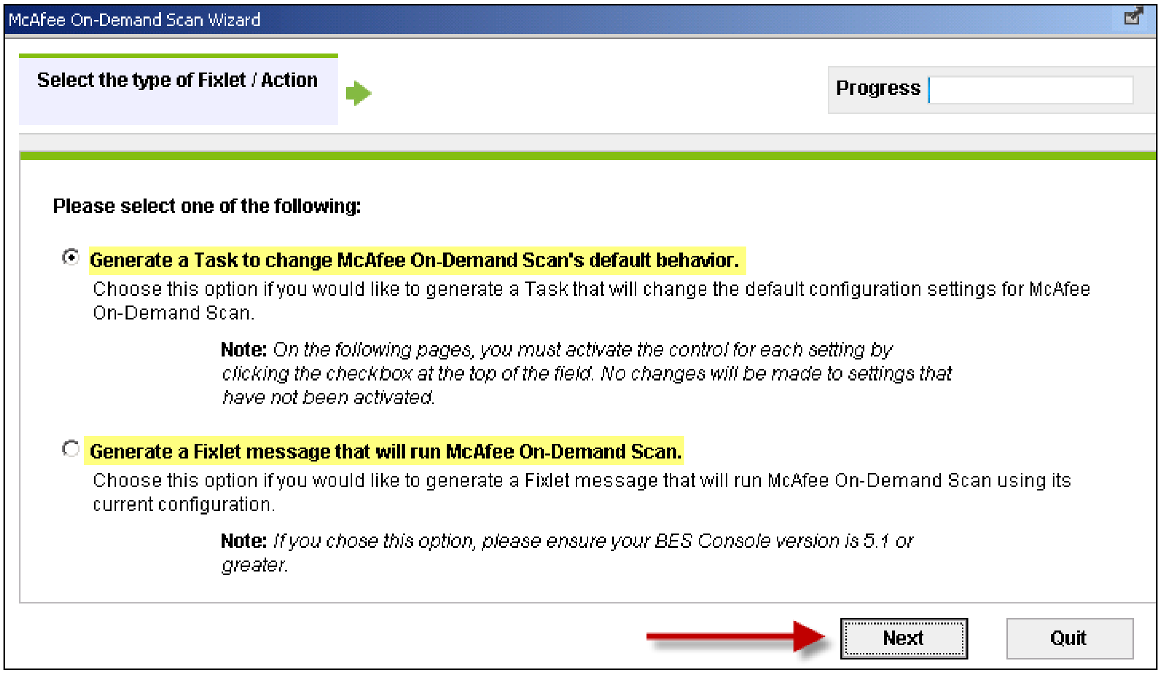
## McAfee On-Demand Scan Wizard

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


Endpoint Protection
Endpoint Protection Domain
Client Manager for Endpoint Protection
CMEP Overview
Reports (21)
Product Updates (7)
Manage Definition Updates (31)
Manage Scanning (1)
McAfee (1)
McAfee On-Demand Scan Wizard
Custom Scanning Tasks (0)

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

Once you click to open the Wizard, you will select to either generate a Task to change the default behavior, or generate a Fixlet message that will run the scan. Make a selection and click *Next.*


McAfee On-Demand Scan Wizard
Select the type of Fixlet / Action
Progress

Please select one of the following:

● 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.

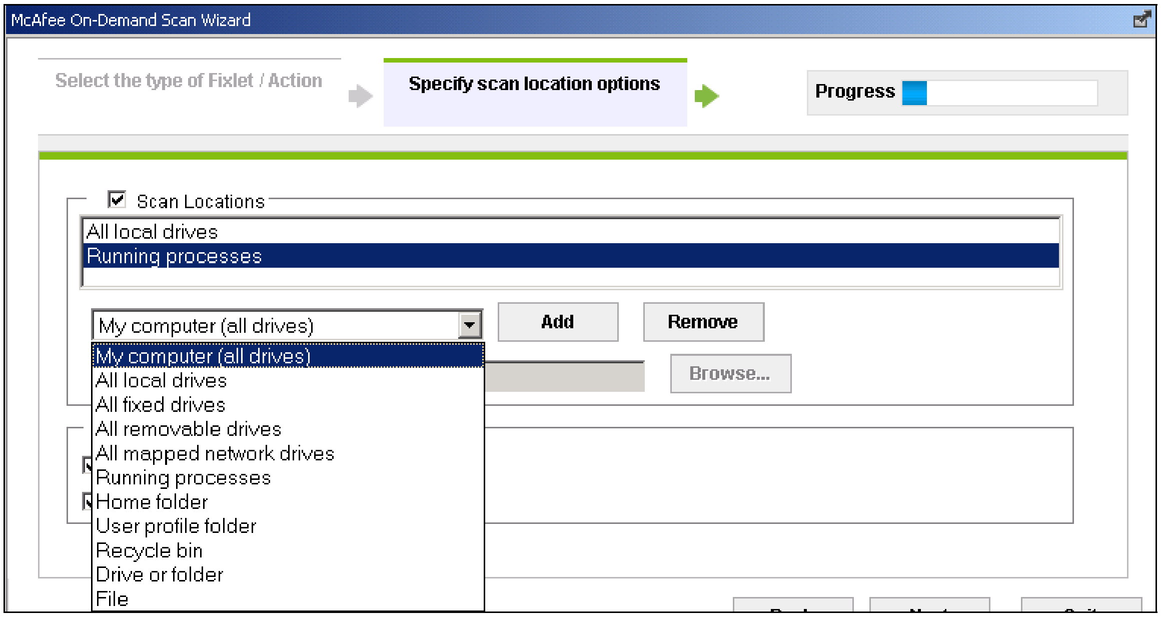
**Note:** *On the following pages, you must activate the control for each setting by clicking the checkbox at the top of the field. No changes will be made to settings that have not been activated.*

○ 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.*

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

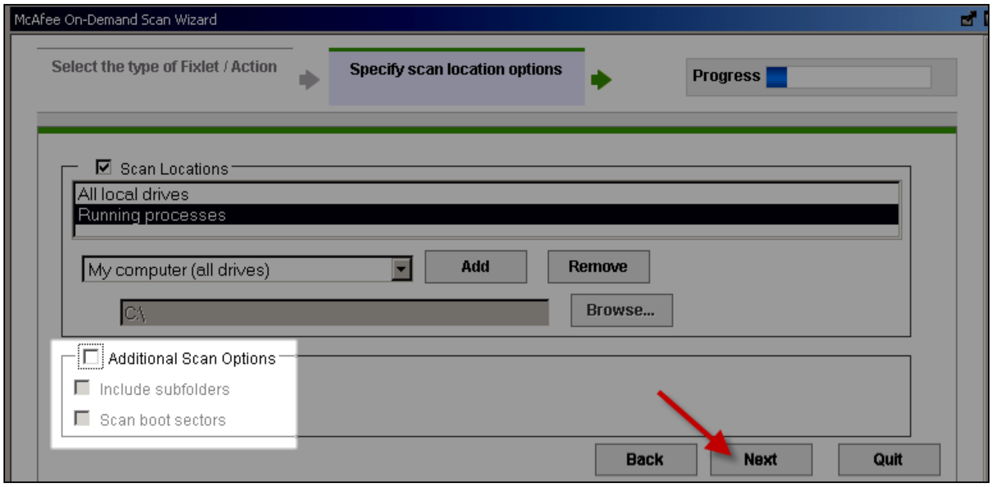


☑ Scan Locations

All local drives
Running processes

My computer (all drives)

If desired, select additional scan options, then click *Next.*


McAfee On-Demand Scan Wizard
Select the type of Fixlet / Action
Specify scan location options
Progress
Add
Remove
Browse...
Back
Next
Quit

☑ Scan Locations

All local drives
Running processes

My computer (all drives)

C:\

☐ Additional Scan Options

☐ Include subfolders

☐ Scan boot sectors

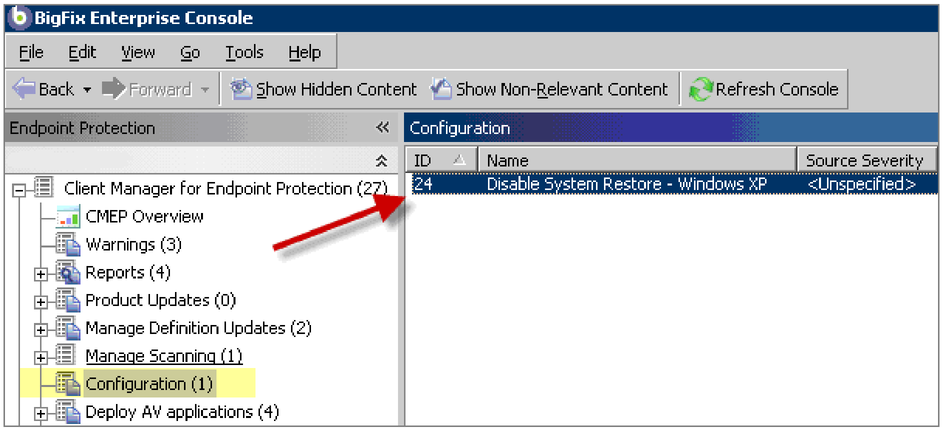
Use the *Next, Back* and *Quit* navigation buttons at the bottom of each window to proceed through the Wizard. The remaining windows will enable you to select scan inclusions and exclusions, specify advanced scan options, specify virus detection options, specify destination options for unwanted programs,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

# Configuration Tasks

Anti-Malware configuration tasks enable you to manage aspects of McAfee AVERT Stinger, Symantec UPX Parsing Engine and Windows Defender. Click on any title in the list of Anti-Malware tasks to display the related Fixlet window.

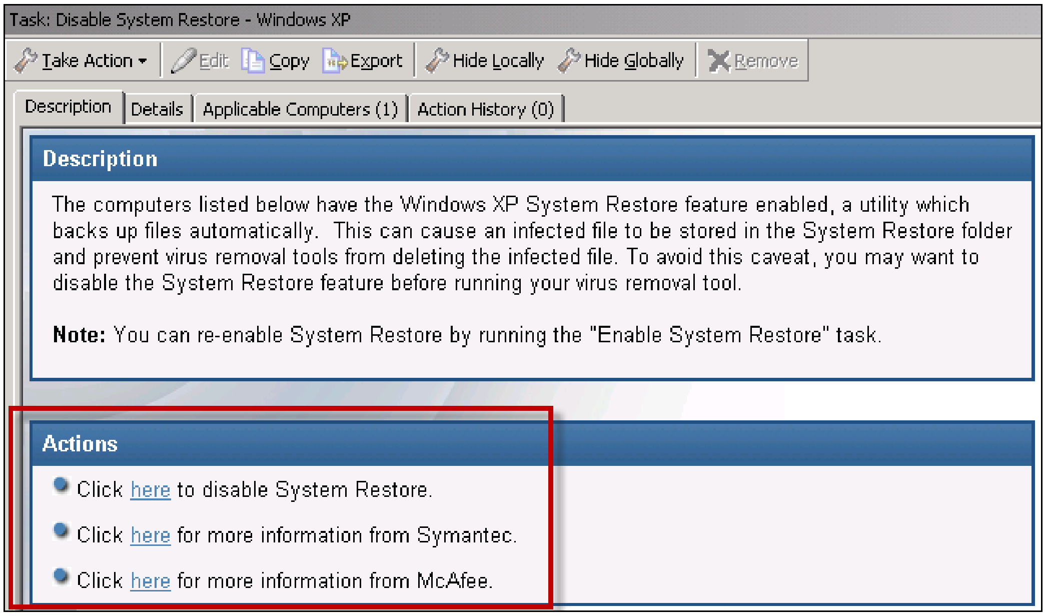
## Disable and Enable System Restore

The Disable/Enable System Restore task can be accessed through the Configuration node of the navigation tree.


BigFix Enterprise Console
File Edit View Go Tools Help
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
Endpoint Protection
Client Manager for Endpoint Protection (27)
CMEP Overview
Warnings (3)
Reports (4)
Product Updates (0)
Manage Definition Updates (2)
Manage Scanning (1)
Configuration (1)
Deploy AV applications (4)
Configuration

| ID | Name | Source Severity |
|---|---|---|
| 24 | Disable System Restore - Windows XP | <Unspecified> |

Click on the task to display the task screen in the lower panel. If System Restore is currently enabled, using this task will allow 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 may also select an Action from the *Take Action* pull-down at the top of the panel.


Task: Disable System Restore - Windows XP
Take Action Edit Copy Export Hide Locally Hide Globally Remove
Description Details Applicable Computers (1) Action History (0)

**Description**

The computers listed below have the Windows XP System Restore feature enabled, a utility which backs up files automatically. This can cause an infected file to be stored in the System Restore folder and prevent virus removal tools from deleting the infected file. To avoid this caveat, you may want to disable the System Restore feature before running your virus removal tool.

**Note:** You can re-enable System Restore by running the "Enable System Restore" task.

**Actions**

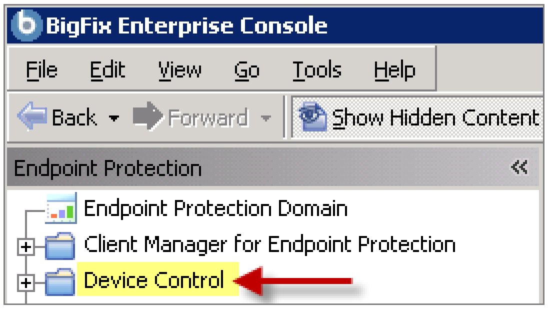
- Click here to disable System Restore.
- Click here for more information from Symantec.
- Click here for more information from McAfee.

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

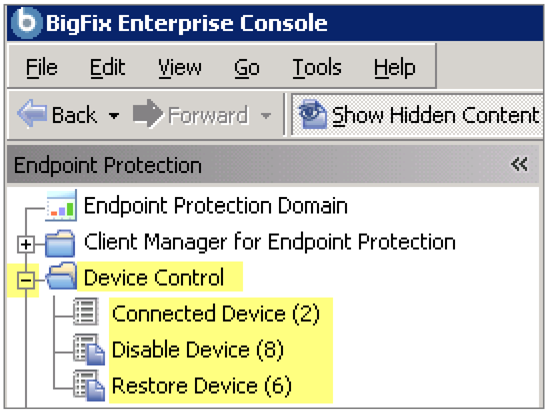
# Part Five
# Device Control

The Device Control functionality within CMEP allows you to control and manage various devices in your deployment, including USB storage devices, CD-ROMS drives, etc.

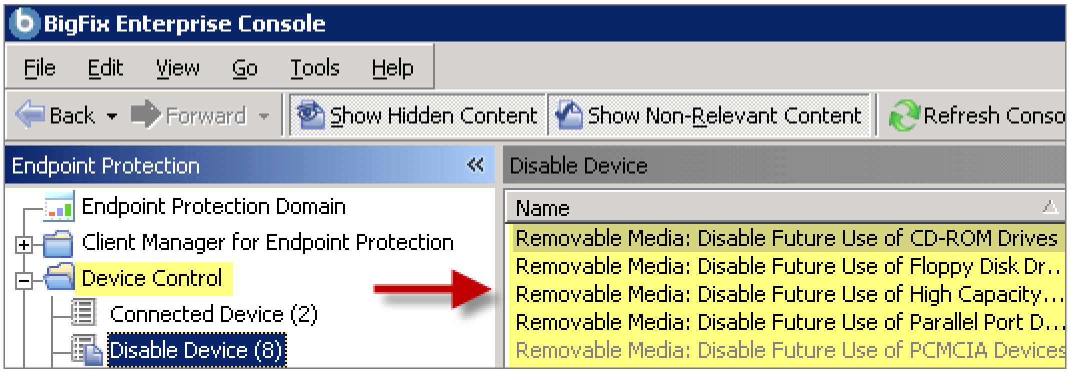
To view applicable tasks related to Device Control, click the *Device Control* site located below the *Client Manager for Endpoint Protection* site within the Endpoint Protection domain.


BigFix Enterprise Console
File
Edit
View
Go
Tools
Help
Back
Forward
Show Hidden Content
Endpoint Protection
Endpoint Protection Domain
Client Manager for Endpoint Protection
Device Control

Click the "+" next to Device Control to display a list of tasks, analyses, or Fixlets related to Device Control



You may click on 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 Device Control component of CMEP.

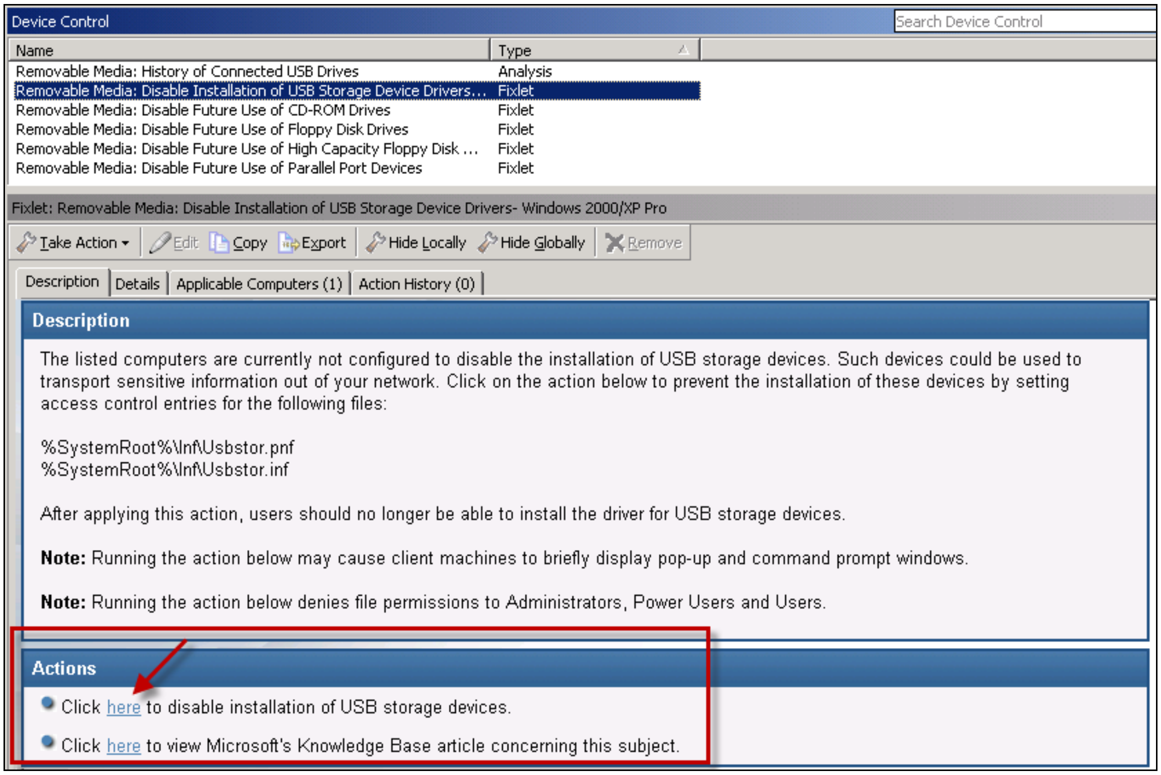


| Name |
|---|
| Removable Media: Disable Future Use of CD-ROM Drives |
| Removable Media: Disable Future Use of Floppy Disk Dr… |
| Removable Media: Disable Future Use of High Capacity… |
| Removable Media: Disable Future Use of Parallel Port D… |
| Removable Media: Disable Future Use of PCMCIA Devices |

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 on each name in the list to display the related Fixlet in the window below.



| Name | Type |
|---|---|
| Removable Media: History of Connected USB Drives | Analysis |
| Removable Media: Disable Installation of USB Storage Device Drivers… | Fixlet |
| Removable Media: Disable Future Use of CD-ROM Drives | Fixlet |
| Removable Media: Disable Future Use of Floppy Disk Drives | Fixlet |
| Removable Media: Disable Future Use of High Capacity Floppy Disk … | Fixlet |
| Removable Media: Disable Future Use of Parallel Port Devices | Fixlet |

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

**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 on 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.

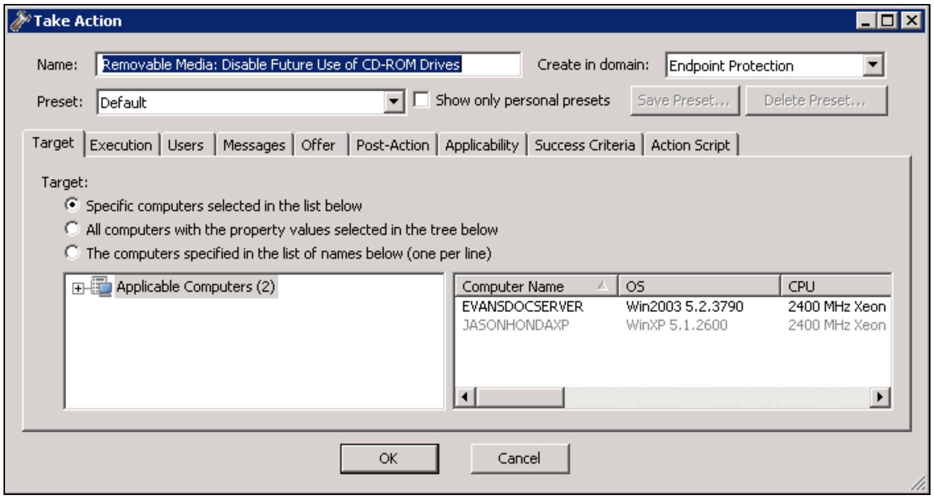
**Note:** Running the action below denies file permissions to Administrators, Power Users and Users.

**Actions**

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

After reviewing the information displayed in the Description box, click the link in the Actions box to deploy the task, then 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 on the BigFix support website.



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

Create in domain: Endpoint Protection

Preset: Default

☐ Show only personal presets

Target:

- ● Specific computers selected in the list below
- ○ All computers with the property values selected in the tree below
- ○ The computers specified in the list of names below (one per line)

Applicable Computers (2)

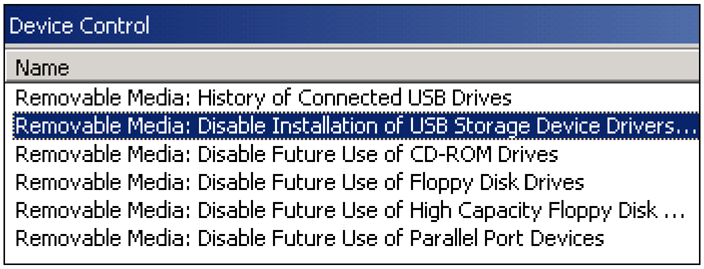
| Computer Name | OS | CPU |
|---|---|---|
| EVANSDOCSERVER | Win2003 5.2.3790 | 2400 MHz Xeon |
| JASONHONDAXP | WinXP 5.1.2600 | 2400 MHz Xeon |

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, as 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.

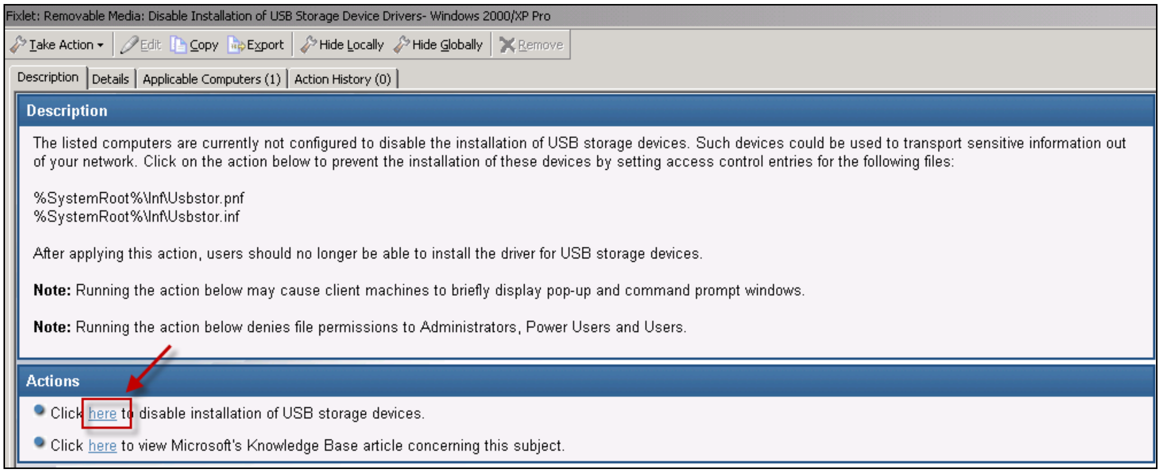
To disable the future use of a USB Storage device, click the applicable task displayed under the Device Control node in the navigation tree.



Device Control

| Name |
|---|
| Removable Media: History of Connected USB Drives |
| Removable Media: Disable Installation of USB Storage Device Drivers... |
| Removable Media: Disable Future Use of CD-ROM Drives |
| Removable Media: Disable Future Use of Floppy Disk Drives |
| Removable Media: Disable Future Use of High Capacity Floppy Disk ... |
| Removable Media: Disable Future Use of Parallel Port Devices |

A Fixlet will open in the window below. Click where indicated in the Actions box to either initiate this task or to view the related article on the Microsoft website.



**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 on 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.

**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 may report back as "Pending Restart" once the action has run successfully. The setting may not take effect until the computer is rebooted.

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

Part Six

# Support

## 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?

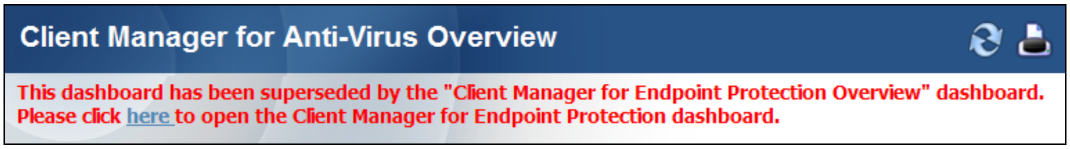
If you have BES 7.2.4 (or an earlier version) installed, Windows 7 and Windows 2008 are not supported. If you upgrade to BES 7.2.5 or later, those operating systems will display as expected in the pie chart.

### 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 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.

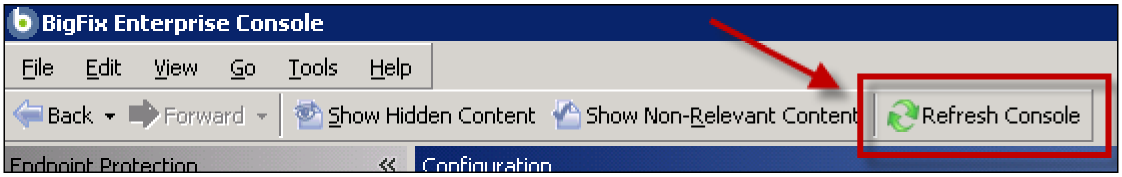
**Note:** If your Console is open and displaying the old dashboard, you will need to close and then re-open the old dashboard in order for the "This dashboard has been superseded" message to display.

### 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 screen. When Fixlets or tasks display, they will open in a window on the lower right part of your screen. See the *Navigation* chapter of this document for more information.

# Tips

- Click the *Refresh Console* button located at the top of the Console to ensure that the data displayed in your reports is always current.



- Data gathering occurs during start-ups and when you refresh the dashboard. Several factors can affect how long this process takes, including deployment size, the performance of the BES server, and the machine the Console is running. If the gathering process seems unreasonably long, restart the dashboard.

# Global 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 |