Core Protection Module 1.5

powered by 

User's Guide

June, 2009

Contents

CONTENTS

Part 1

Prerequisites

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

This User's Guide will help you install, configure, and customize this product for your environment. Specifically, you will be installing server components, installing endpoints, activating analyses, customizing your configurations, enabling tasks, and viewing reports.

How CPM Works

BigFix Core Protection Module *powered by Trend Micro* uses Fixlet technology to identify agents with outdated antivirus and malware protection. This technology allows you to trigger thousands of computers to update a pattern file and have confirmation of the completed action in minutes, rather than hours or days.

Protect your endpoints from security risks by deploying the CPM client across your network. The client provides real-time, on-demand, and scheduled malware protection, Web security, and a client-side firewall. You can track the progress of each computer as updates or configuration policies are applied, making it easier to gauge compliance levels.

Once CPM is installed, the CPM dashboard within the BigFix console will help protect your networked computers and keep them secure. Deploying CPM to your endpoints can be accomplished in minutes. Thereafter, you can track the progress of each computer as you apply CPM component updates, thus making it easy to gauge the level of protection across your entire enterprise.

Additionally, the Web Reports feature allows you to chart the status of your overall protection with Web-based reports.

Types of Scanning in CPM

Core Protection Module offers three types of Malware scans: On-Demand, Real-Time, and Scheduled scans. You can apply the same scan to all endpoints, or create different scan configurations and apply them to different sets of endpoints based on criteria that you set. Users can be notified before a scheduled or on-demand scan runs, but do not receive notification if a detection occurs on their machine. Detections are logged and available for review in the Reports node of the navigation tree.

You may associate any of these scans with selected computers, users, or other conditions. As a result, you can define multiple scan settings and then attach a particular scan configuration to a given set of computers. Scan settings are saved in the CPM Dashboard.

- **On-Demand scans**—Use On-Demand scans to run a one-time scan of client hard drives and/or the boot sector. Launch the default scan with the Scan Now Task. On-Demand scans can take

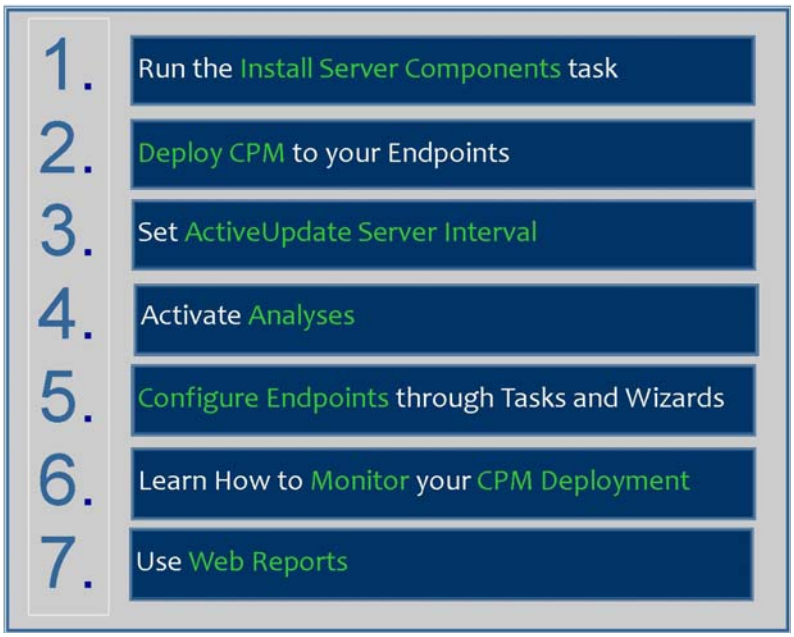
from a few minutes to a few hours to complete, depending on client hardware and how many files are scanned.

- **Real-Time scans**— This type of scan checks files for malicious code and activity as they are opened, saved, copied or otherwise being accessed. These scans are typically imperceptible to the end-user. Real-time scans are especially effective in protecting against Internet-borne threats and harmful files being copied to the client.

- **Scheduled scans**— You can schedule an On-Demand scan to trigger at a given time, day, or date. You can also have the scan automatically reoccur according to the schedule you set to configure and run the default Start Scan Now task.

Process Overview

What you are about to do:

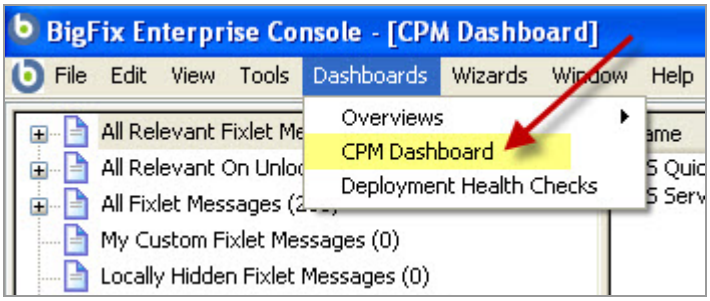


The purpose behind these actions:

1.	**Install Server Components**	Install components that gather pattern updates from Trend Micro
2.	**Deploy CPM**	Deploy the CPM engine onto each machine
3.	**Set ActiveUpdate Server**	Set interval at which the server checks if new pattern files have been published by Trend Micro
4.	**Activate Analyses**	Tell clients to report data on their configuration and status
5.	**Configure Endpoints**	Use Tasks and Wizards to customize settings used by your endpoints and server
6.	**Monitor CPM Deployment**	Monitor the settings, details, and overall health of your deployment
7.	**Web Reports**	View high level reports and information on endpoint status and infections

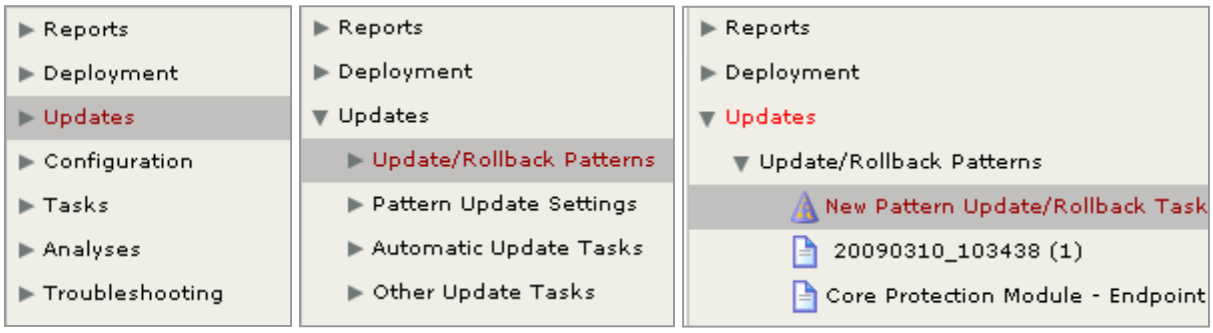
Basic Navigation

First, click the *Dashboards* pull down menu at the top of your screen and select *CPM Dashboard*.

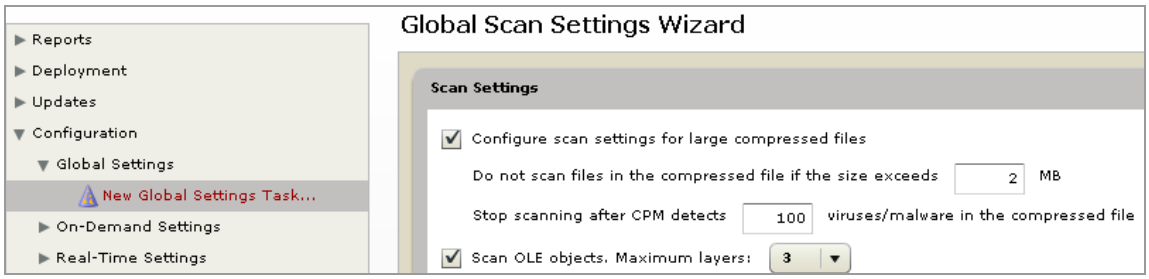


Navigation Tree

The Navigation Tree, located in the left hand side of the CPM dashboard, is where you will access the CPM features available in the console. While working with navigation tree menus, click the *arrows* to open the primary and sub-nodes of the tree.



The navigation tree is structured to show high level categories on the left with corresponding detail displayed on the right, as shown below:



View the primary “nodes” of the navigation tree:

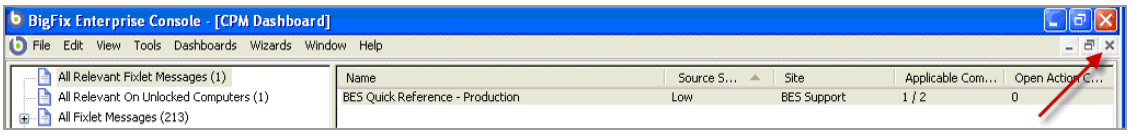
Each “node” in the tree expands to display a list of sub-nodes that can include reports, wizards, tasks and Fixlets. See a description of each node below:

Node	Description
Reports	Displays reports that depict aspects of the state of your CPM deployment and infection information
Deployment	Provides installation and upgrade Fixlets to set up your CPM deployment, and uninstall Fixlets to remove incompatible software prior to installation
Updates	Manage pattern updates for your endpoints
Configuration	Allows you to customize your CPM deployment through wizard-generated custom tasks, Fixlets, and actions
Tasks	Provides access to tasks such as starting/stopping scans and uploading quarantined files and client logs
Analyses	Reports detailed information about machines within your CPM deployment
Troubleshooting	Addresses health-related issues and detects machines ineligible for CPM installation

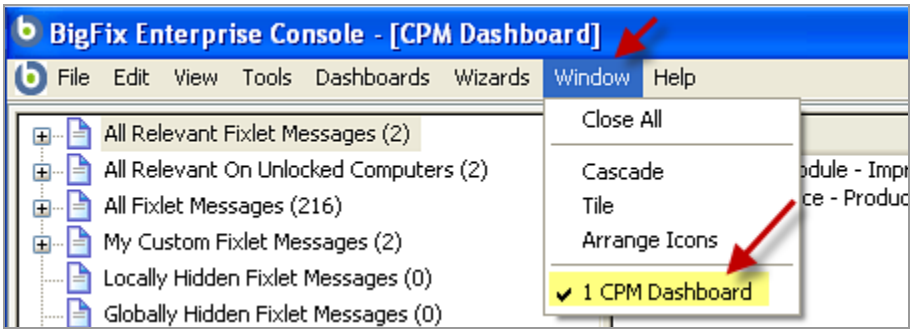
Returning to the Dashboard

When you’re deploying a task, activating an analysis, or configuring settings on your server, there are several ways to get back to the CPM Dashboard:

Click the small “X” at the top right of your screen. This will close the top-most window and bring you back to the CPM Dashboard.



Select *CPM Dashboard* in the Dashboards or Window pull down menus at the top of your screen.



New Features in This Version

- ### Automatic Pattern File Updates

The previous version of CPM required you to manually deploy updates to your endpoints. The new Automatic Pattern File Updates feature now allows you to automatically flow pattern updates to your endpoints.

This sophisticated feature enables you to optionally set up your BigFix deployment to automatically take downloaded pattern files and distribute them to specific clients without BigFix console operator action. When configured, this delivery method will automatically update ESP Clients with the latest pattern and engine files.

Additional configuration steps are required to enable Automatic Updates. Refer to Page 22 of this document for more detail.

- ### Pattern Set Rollback

Pattern Set Rollback allows you to roll back recently deployed (the last 15) pattern sets if an issue or conflict is found with those patterns. Access this feature through the Updates node of the navigation tree, then select *Update/Rollback Patterns*. Select the Pattern Update wizard, deploy the rollback action, and target it to applicable machines.

Once a client is in the rollback state, no pattern update actions will be relevant until the rollback flag is cleared. Use the Clear Rollback Flag task under Update > Other Update Tasks to clear the flag.

Spyware/Grayware Restore

The Spyware/Grayware Restore feature allows you to restore (or essentially un-quarantine) objects that your system has quarantined as potential Spyware/Grayware. Quarantined Spyware/Grayware files are stored as a snapshot. Each "snapshot" can include multiple Spyware/Grayware files. CPM will store up to 15 of these snapshots on any given client.

In the event that CPM tags a legitimate file as spyware, this feature gives you the flexibility to restore the file to its original location. From the navigation tree, select *Tasks > CPM > Restore Spyware/Grayware Wizard*. Then select the items you want to restore, click *Restore*, and target your action in the Take Action dialog.

Update From the Cloud

This new feature allows you to set BigFix clients to get pattern updates directly from the Trend Micro Smart Protection Network "in the cloud". This feature is useful for laptops in your environment that operate remotely outside of your main corporate infrastructure. For details about how to configure this update, see page 24 of this document.

Client UI Dashboard, Client UI Offers

Client UI Dashboard:
The Client UI dashboard allows you to optionally display a client side dashboard containing basic computer information, CPM information and statistics, as well as recently detected viruses or spyware infections. There is also a hidden Technician Dashboard that will display more technical computer information and relevant Fixlet messages for that computer. To display the Technician Dashboard, enter the keyboard shortcut Control-Alt-Shift "T" from the Client Dashboard. You may enable/disable client side dashboards through the Tasks node of the navigation tree under CPM.

Client UI Offers:
An "offer" is an action that gives end users the freedom to choose if or when to take an action. This feature allows you to issue an "offer" with re-applicability behavior to give end users control over CPM features. Actions taken as offers will be displayed in the client UI. For example, you can set up the client UI to give end users the ability to initiate a Scan Now or an Update from the Cloud task.

> **Note:** This feature requires BigFix client version 7.2.4.60 or higher.

Web Reputation

This version of the CPM has integrated the functionality and features of the previously standalone product, Web Protection Module. Within CPM, the integrated product is now called Web Reputation. The Web Reputation feature prevents Web-based malware from infecting your users' computers by intercepting malware before it reaches your users' computers. Access and enable Web Reputation tasks through the Reports and Configuration nodes of the navigation tree.

If you currently have the Web Protection Module deployed in your environment, it must be uninstalled prior to installation of CPM. You can use the Blacklist/Whitelist wizard available in the CPM Dashboard to migrate any Blacklist/Whitelist policies created using the standalone Web Protection Module.

- Common Firewall

Common Firewall will block attempts by applications to send network traffic over prohibited ports. This feature can be configured to protect against both inbound and outbound port violations on your endpoints. You can set the Firewall to low, medium, or high security levels, which can be configured through the Common Firewall wizards in the Configuration node. You can monitor firewall policies through the Port Violation reports found under the Reports node of the navigation tree.

> **Note:** This feature will only appear in your CPM Dashboard if you have purchased and are subscribed to the Trend Micro Common Firewall site.

System Requirements

Minimum requirements for the Core Protection Module endpoints are outlined below by operating system:

For Windows 2000

Supported operating systems

- Microsoft™ Windows™ 2000 with Service Pack 3 or 4
- Microsoft Cluster Server 2000

Hardware Requirements

- 300MHz Intel Pentium processor or equivalent
- 512MB of RAM
- 700MB of available disk space
- Monitor that supports 800 x 600 resolution at 256 colors

For Windows XP/2003 32-bit Edition

Supported operating systems

- Microsoft Windows XP Professional 32-bit Edition with Service Pack 1 or 2
- Microsoft Windows Server 2003 32-bit Edition with or without Service Pack 1 or 2
- Microsoft Windows 2003 Web Edition, 32-bit Edition with or without Service Pack 1 or 2
- Microsoft Windows Server 2003 R2 32-bit Edition with or without Service Pack 1 or 2
- Microsoft Windows Storage Server 2003 32-bit Edition

Hardware requirements

- 300MHz Intel Pentium processor or equivalent; AMD(TM) x64 or Extended Memory 64 Technology (EM64T) processor architectures also supported
- 512MB of RAM
- 700MB of available disk space
- Monitor that supports 800 x 600 resolution at 256 colors

For Windows XP/2003 64-bit Edition

Supported operating systems

- Microsoft Windows XP Professional 64-bit Edition with Service Pack 1 or 2
- Microsoft Windows Server 2003 64-bit Edition with or without Service Pack 1 or 2
- Microsoft Windows 2003 Web Edition, 64-bit Edition with or without Service Pack 1 or 2
- Microsoft Windows Server 2003 R2 64-bit Edition with or without Service Pack 1 or 2
- Microsoft Windows Storage Server 2003 64-bit Edition
- Microsoft Cluster Server 2003 64-bit Edition

Hardware requirements

- Intel x64 processor, AMD x64 processor
- 512MB of RAM
- 700MB of available disk space
- Monitor that supports 800 x 600 resolution at 256 colors

For Windows Vista

Supported operating systems

- Microsoft Windows Vista Business 32-bit Edition (with latest service pack)
- Microsoft Windows Vista Enterprise 32-bit Edition (with latest service pack)
- Microsoft Windows Vista Ultimate 32-bit Edition
- Microsoft Windows Vista Business 64-bit Edition
- Microsoft Windows Vista Enterprise 64-bit Edition
- Microsoft Windows Vista Ultimate 64-bit Edition

Hardware requirements

- 800MHz Intel Pentium processor or equivalent; AMD x64 or Extended Memory 64 Technology (EM64T) processor architectures also supported
- 1GB of RAM
- 700MB of available disk space
- Monitor that supports 800 x 600 resolution at 256 colors

Incompatible Software

- Other AntiVirus software
- Computer Associates ARCserve Backup
- HSM (Hierarchical Storage Management) Backup Software
- Symantec Software Virtualization Solution
- Bit9 Parity Agent

In addition, the following list of products should be removed using their respective uninstallers prior to CPM deployment:

- Trend Micro ServerProtect
- Trend Micro Internet Security 2008
- Trend Micro Pc-cillin 2007

- Trend Micro Pc-cillin 2006
- Trend Micro Pc-cillin 2005
- Trend Micro Pc-cillin 2004 (AV)
- Trend Micro Pc-cillin 2004 (TIS)
- Trend PC-cillin 2003
- Trend PC-cillin 2002
- Trend PC-cillin 2000(WinNT)
- Trend PC-cillin 2000 7.61(WinNT)
- Trend PC-cillin 98 Plus(WinNT)
- Trend PC-cillin NT 6
- Trend PC-cillin NT
- Trend Micro HouseCall Pro
- Virus Buster 2000 for NT ver.1.20-
- Virus Buster 98 for NT
- Virus Buster NT
- ServerProtect for Windows NT

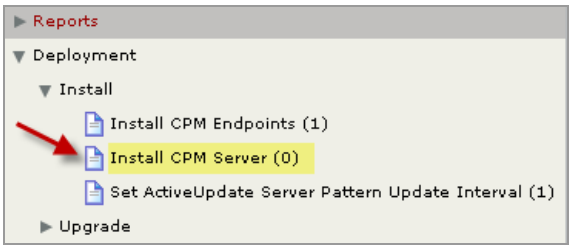
Part 2

Installation

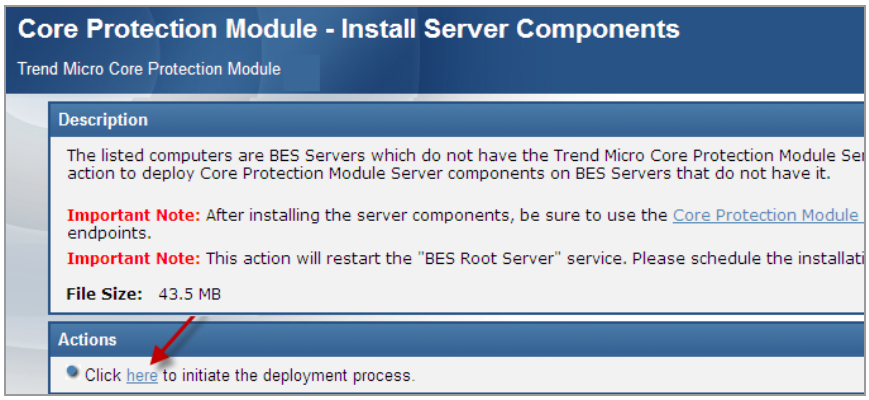
This procedure assumes that you have already installed the BigFix Unified Management Platform and are familiar with the *BigFix Console Operators Guide*.

Installing Server Components

To install the server components, click *Deployment* in the navigation tree. Then click *Install CPM Server*.



At the Install Server Components window, review the Description text and click where indicated in the Actions box to initiate the deployment process.



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

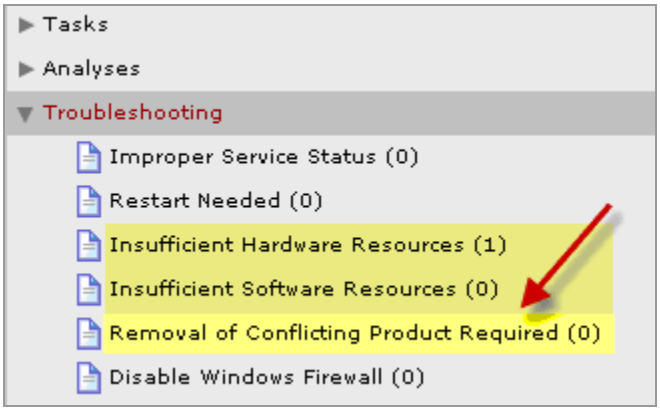
Note: The Install Server Components task automatically restarts the BES root server service.

Next, you will remove conflicting products and deploy CPM to your endpoints.

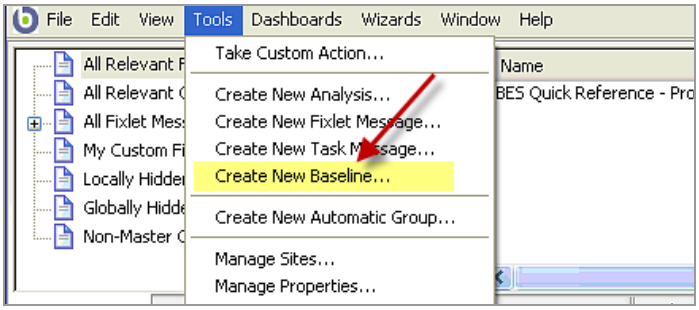
Removing Conflicting Products

If a computer is "relevant" to the *Removal of Conflicting Product* Fixlet, you will not be able to install CPM on that endpoint. To resolve this issue, use the uninstall Fixlets in the Deployment/Uninstall node of the navigation tree to remove conflicting products from your deployment.

The Core Protection Module includes several audit Fixlets that automatically detect the presence of incompatible software or hardware in your environment. Click the *Troubleshooting* node to find the *Insufficient Hardware, Insufficient Software*, and *Removal of Conflicting Product* Fixlets.



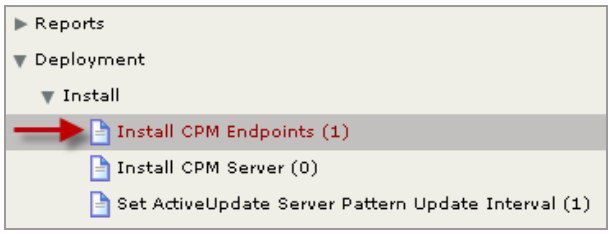
Consider making a baseline composed of the uninstall Fixlets to remove the conflicting products. To do this, select *Create New Baseline* from the Tools menu at the top of your screen.



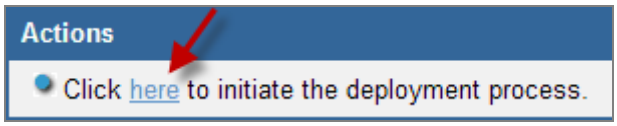
For more information on creating baselines, consult the *BigFix Console Operators Guide*.

Installing Endpoints

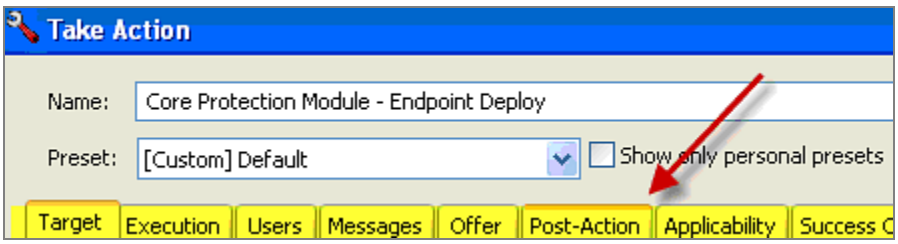
To install endpoints, go to the Deployment node of the navigation tree, select *Install,* then click on the *Install CPM Endpoints* task to target and deploy CPM to relevant computers.



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



Set your desired parameters for this task in the Take Action dialog and click *OK*.



For more detailed information on using the Take Action dialog to deploy your endpoints, check the *BigFix Console Operators Guide*.

Set ActiveUpdate Server Pattern Update Interval

When this action is run, the CPM server will check if any new patterns have been published by Trend Micro. Any new patterns will be downloaded and made available for deployment using the Pattern Update/Rollback Wizard in the CPM Dashboard. If automatic updates have been configured and enabled for server components, endpoints configured for automatic updates will download and apply the new patterns immediately.

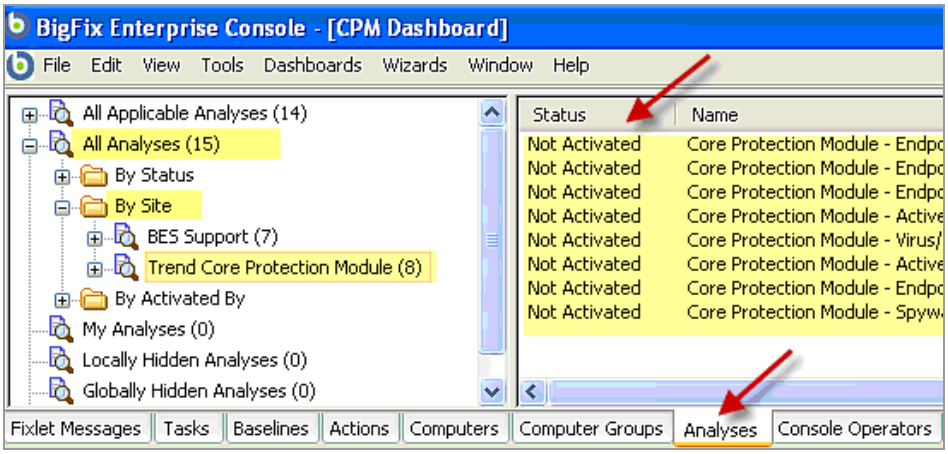
Click the Deploy node of the navigation tree and click Install to locate this task. You should set this action to run as a policy with periodic re-applicability behavior. It is recommended that you apply this Task through the Take Action dialog and select the following action parameters under the Execute tab:

- Never expire
- Run once an hour
- Retry up to 99 times on failure
- Reapply an unlimited number of times

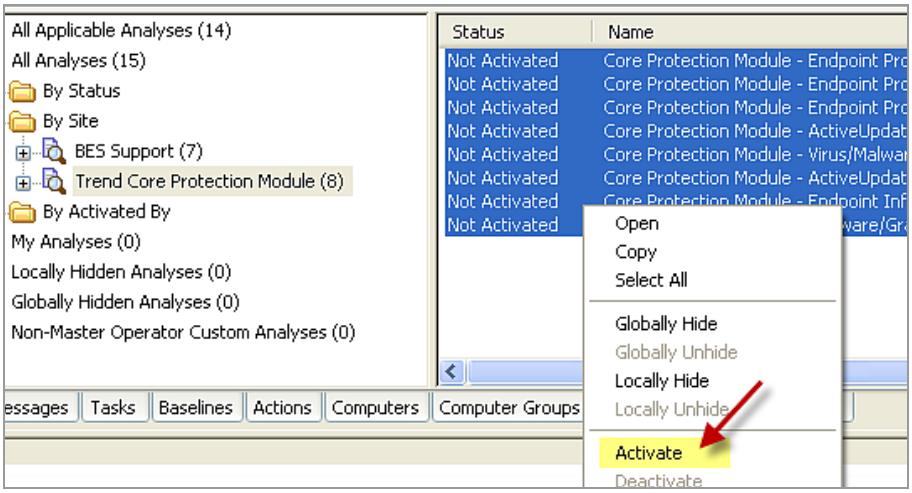
Activating Analyses

Now, you will provide additional information about endpoints and activate the Analyses in the CPM site. As the analyses results feed the CPM reports and provide additional information about endpoints, activating analyses allows you to see those reports displayed in the CPM Dashboard.

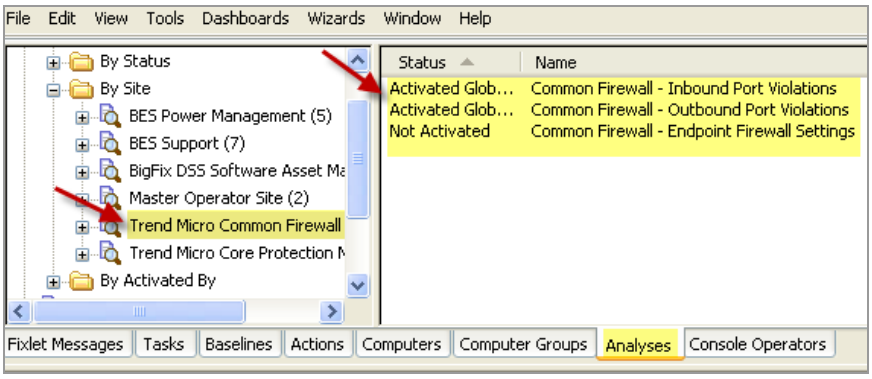
Click the *Analyses* tab located in the middle of the CPM Console. On the upper left part of the console, select the "+" sign next to All Analyses, click *By Site*, then click *Trend Core Protection Module*. You will see a list of corresponding tasks on the right designated as "Not Activated" in the Status column.



To activate these tasks, select them all at once, then right-click to display the menu shown below. Select *Activate*, then enter your Private Key Password.

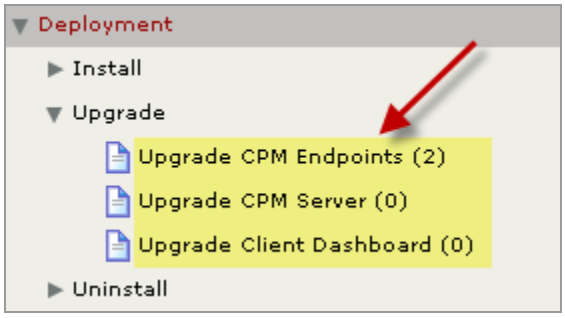


To activate the Firewall analyses, select *All Analyses* > *By Site* > *Trend Micro Common Firewall*. Select all analyses that have not been activated and right-click to display the drop down menu. Select *Activate*, and enter your Private Key Password.

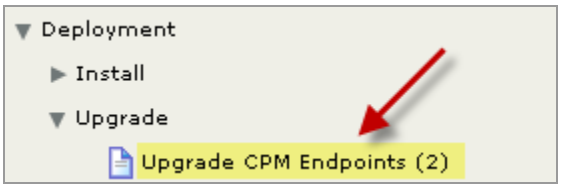


Upgrading from CPM Version 1.0

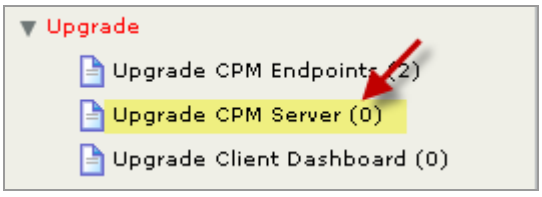
To upgrade to the latest version of CPM from an earlier version, click *Upgrade* under the Deployment node of the navigation tree. From here, you can upgrade your CPM endpoints, your CPM Server, and your Client Dashboard. Only client computers without conflicting software products can deploy Core Protection Module, and computers must meet minimum software and hardware requirements.



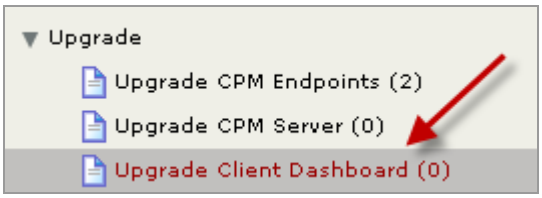
Start by upgrading your CPM Endpoints. Click the appropriate Task under Upgrade, and when the dialog opens, click where indicated in the Actions box to deploy the task.



Once you've upgraded your CPM endpoints, you will use the same method to upgrade your CPM Server.



If you're using the Client Dashboard, you may also upgrade this to the latest version of CPM. Do this by clicking the Upgrade Client Dashboard task, and then click in the *Actions* box of the dialog to initiate.



Note: Any old 'Check server for pattern update' tasks should be stopped and a new policy action should be issued from the 'Set ActiveUpdate Pattern Update Interval' task.

Note the Following Prior to Upgrading:

- Option 1. Update CPM clients to version 1.5 first. Once all CPM clients have been updated, update the CPM server components to version 1.5. You will not be able to update firewall patterns on any of your endpoints until you update the CPM server components.

- Option 2. If you are unable to wait until all CPM clients have been updated to version 1.5, you may proceed with updating your CPM server component to version 1.5. Then use the "Server Settings Wizard" to change the update source to:

  CPM 1.0: http://cpm-p.activeupdate.trendmicro.com/activeupdate <http://cpm-p.activeupdate.trendmicro.com/activeupdate>

  You will not be able to update firewall patterns on your endpoints while the update source is set to the CPM 1.0 AU server.

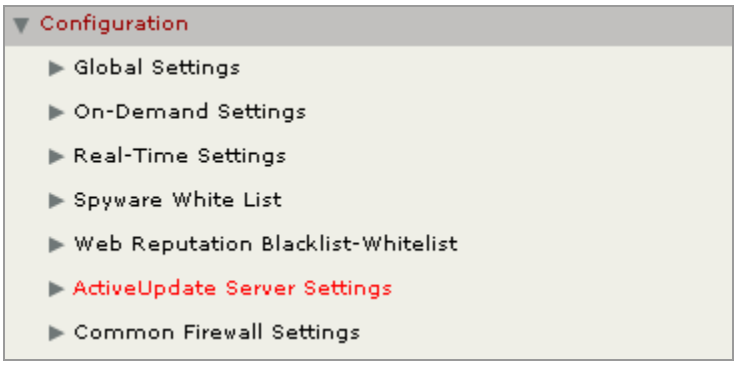
  After you have updated all of your CPM clients to version 1.5, use the "Server Settings Wizard" to change the update source back to the CPM 1.5 AU Server:

  CPM 1.5: http://cpm15-p.activeupdate.trendmicro.com/activeupdate <http://cpm15-p.activeupdate.trendmicro.com/activeupdate>

Part 3

Configuration

The Configuration node in the navigation tree includes tasks, Fixlets, and wizards for customizing your CPM deployment.



Configuring Updates

There are three ways to get updates with Core Protection Module version 1.5:

- **Manual Updates:** ESP Administrator issues update action for each pattern-set
- **Automatic Updates:** ESP Administrator configures automatic updates once and issues update policy action once
- **Update from Cloud:** Clients update from the Trend Micro ActiveUpdate (cloud) server

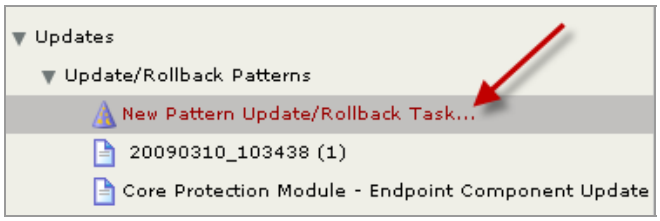
Note: These update types are not mutually exclusive. You may elect to use manual updates in some parts of your environment while other parts are set to use automatic updates. Similarly, Update from Cloud actions can be applied by clients using either automatic or manual updates.

Manual Updates

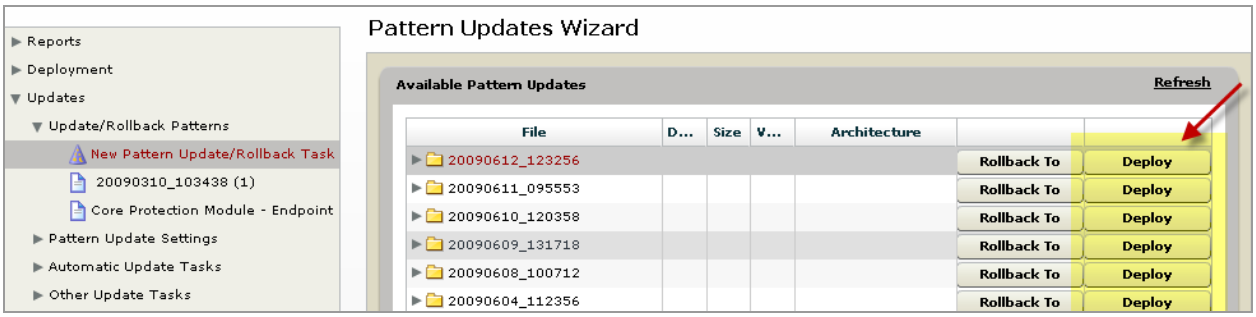
Configure a policy action to run on your server that periodically checks for available updates. If updates are found, they are made available for deployment to your endpoints using the New Pattern Update Rollback wizard.

Note: You should take this action only once when you first install the CPM server components. As long as you configure it to run as a periodic policy action and don't stop the action, server installation is the only time you need to use the *Set ActiveUpdate Server Pattern Update Interval* task. If you do not correctly configure this action or if the action is stopped, you will not see new pattern updates available in the Pattern Update wizard.

From the Updates node of the navigation tree, click *Update/Rollback Patterns* and then select the *New Pattern Update/Rollback* wizard.

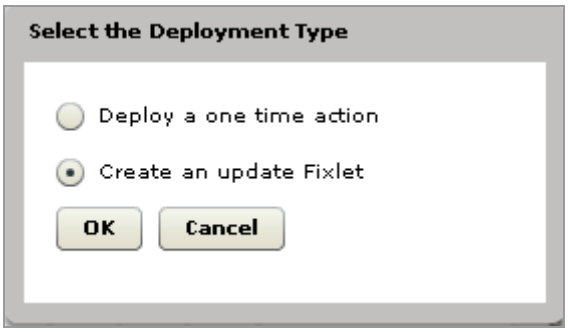


A list of update components is automatically pre-set as a default. Click the *Deploy* buttons from the wizard shown below to update all of these components to your endpoints.

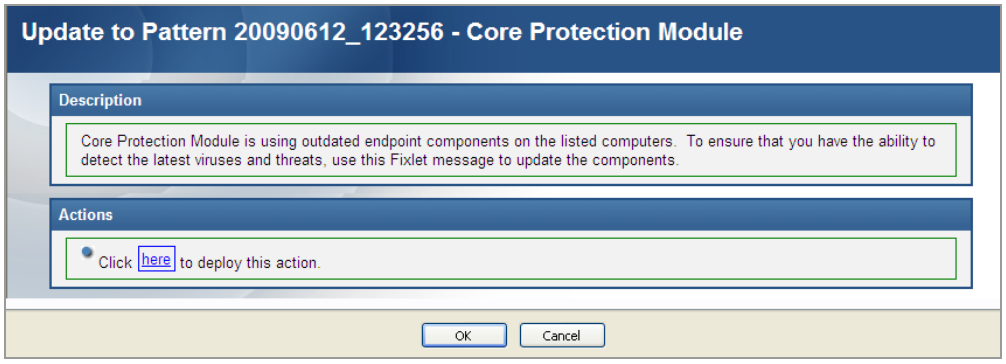


After clicking the Deploy button, a dialog will ask you to select a Deployment Type. To deploy a one time action, click the applicable button, click *OK*, and select your desired parameters in the Take Action Dialog.

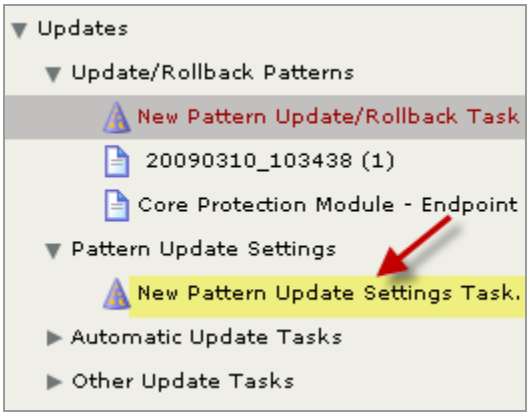
To create an update fixlet, click the applicable button, then click *OK*.



When the window opens, edit the Fixlet parameters and click *OK* to save the Fixlet. In the new Fixlet, click where indicated in the Actions box to deploy the action.



To select only specific pattern file types for updating, use the New Pattern Update Settings wizard to apply a custom update settings configuration to your endpoints.



Automatic Updates

Offered as a new feature in CPM version 1.5, Automatic Updates allows you to automatically deliver and apply pattern file updates to your endpoints whenever new patterns are made available by Trend Micro.

To enable automatic updates, take the following steps:

1. Download the CPMAutoUpdateSetup.vbs script and run it on your server.
2. Ensure that there is a periodic policy action issued from the 'Set ActiveUpdate Server Pattern Update Interval' task.
3. Target a policy action against all endpoints from the Apply Automatic Updates task.
4. Run the Enable Automatic Updates – Server task on your server.
5. Run the Enable Automatic Updates – Endpoint task on your endpoints.

These steps are described in detail below.

1. Run CPMAutoUpdateSetup.vbs Script

Download and run the CPMAutoUpdateSetup.vbs script on your server. You will need your deployment's site administrator credentials and password. These are required in order to create a new console operator account. This account is used to send a manifest of the latest available pattern file versions to your endpoints whenever new patterns are downloaded from Trend Micro.

Note: This operator account should not be given administrative rights on any endpoints.

Note: It is recommended that you do not change the default values supplied by the script.

Note: The manifest of the latest pattern versions will only be made available to endpoints if automatic updates are enabled on the server. See step 4 below.

Note: If you have difficulty running the script on your server, see the following Knowledge Base article on the BigFix support website that contains recommendations for running the script on various operating systems.

2. Issue a policy action from the Set ActiveUpdate Server Pattern Update Interval task

You have most likely already configured a policy action from this task. If you have not, please see the instructions on Page 16 of this document.

3. Issue a policy action from the Apply Automatic Updates task

This policy action monitors the latest pattern file versions and applies them to endpoints with automatic updates enabled (see step 4 below). The action should be targeted at all computers and set with the following parameters:

- Reapply whenever relevant
- Reapply an unlimited number of times
- Retry up to 99 times on failure

4. Run the Enable Automatic Updates – Server task

This action sets a flag on the server. When the flag is set, the 'Set ActiveUpdate Server Pattern Update Interval' policy action configured in step 2 will send a manifest of the latest available pattern updates to CPM endpoints.

Note: There is a corresponding 'Disable Automatic Updates – Server' Task. Use this task if you want to stop all endpoints from automatically updating pattern files.

5. Run the Enable Automatic Updates – Endpoint task

This action sets a flag on the endpoints targeted by the action. When the flag is set, the 'Apply Automatic Updates' policy action configured in step 3 will become relevant whenever new pattern files are made available by the policy action configured in step 2. Only endpoints with the flag set will automatically apply pattern file updates.

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

Updating from the Cloud

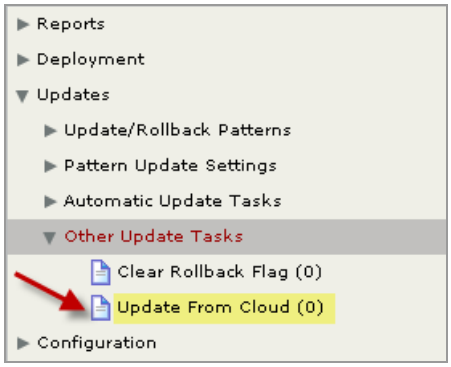
You can now set a specific task to instruct clients to update "from the cloud" as opposed to an internal BigFix/ESP server.

This feature can be set as a policy, so that endpoints automatically get updates from the cloud when roaming, and use the BigFix infrastructure when within the corporate network. This task will instruct clients to update from the public Trend Micro Automatic Update server (the cloud), as opposed to an internal BigFix/ESP server.

Note: This task will ignore "selected components to update" (as set by the Update Settings Wizard) and will simply update all out-of-date components on the endpoint.

Note: As the task's relevance is not restricted to roaming computers, it is up to the administrator to target computers correctly. Because endpoints will bypass the BigFix infrastructure and go directly to the internet to download pattern files, there is a potential to adversely impact your network if this task is applied incorrectly. Please target carefully and test thoroughly.

From the Updates node, click *Other Update Tasks* and then *Update from the Cloud.* When the dialog opens, click where indicated in the Actions box to initiate this task.



Note: Like manual and automatic updates, Update from the Cloud actions will not be relevant when the rollback flag is set.

You may select to create Update from the Cloud actions as client "offers" to allow end users more flexibility in when to update.

Rolling Back Updates

Version 1.5 of CPM provides you with a new Pattern Rollback feature, which gives you the ability to roll back patterns to previous versions. From the Updates node, select *Update/Rollback Patterns*, then open the Pattern Update Wizard.

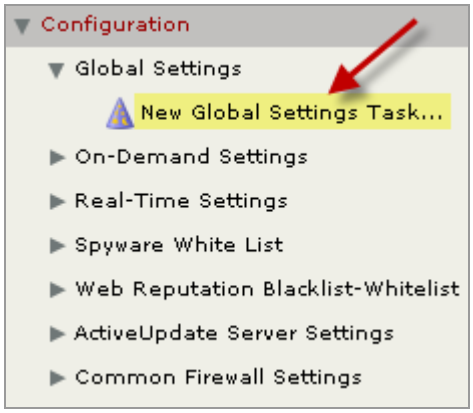
Note: Rollback actions are ordered. That means rollback tasks/actions will not be relevant after

a newer rollback action has been applied.

Note: Once a client is in the rollback state, no pattern update actions will be relevant until the rollback flag is cleared. Use the Clear Rollback Flag task under Update > Other Update Tasks to clear the flag.

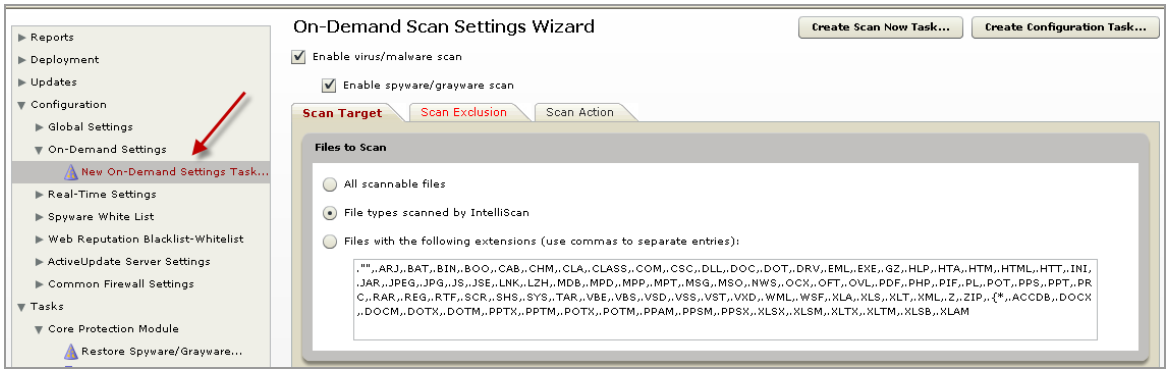
Using the Configuration Wizards

You will use the Configuration "wizards" to customize your deployment and create tasks and actions that define the behavior of your CPM endpoints and servers. In the navigation tree, click the Configuration node arrow to expand the list of configuration options, and click the arrows beside each option to display the corresponding wizards. Click on the wizard to customize your settings, then click *Create* to generate a configuration task or action. Any configuration tasks you create will be displayed below the particular wizard that generated the task.

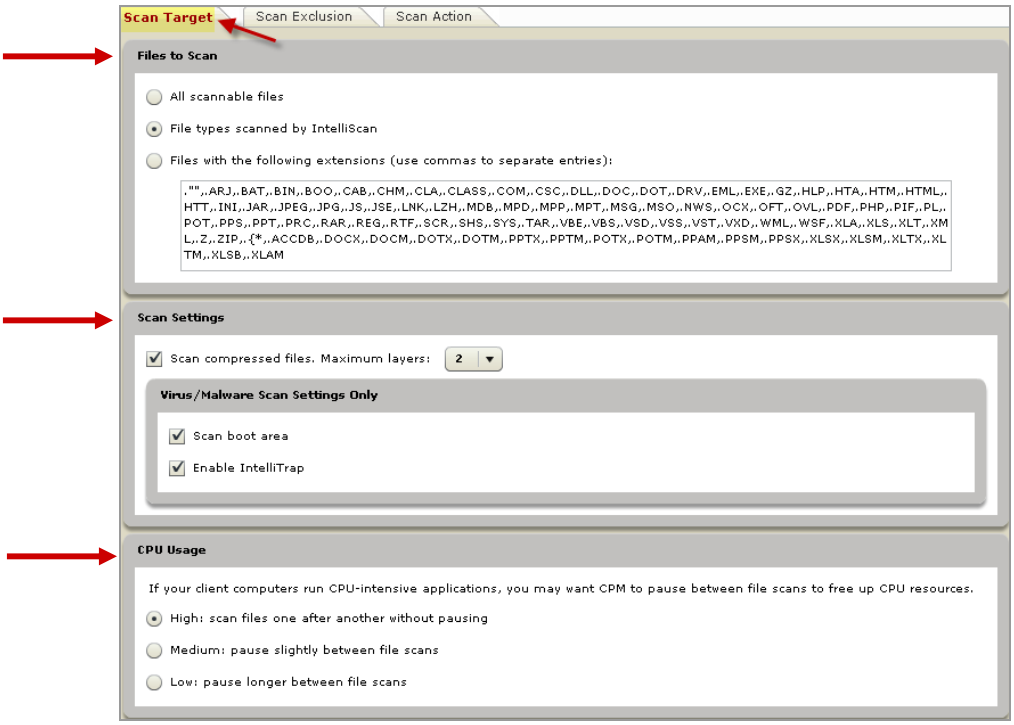


Navigating Through a Configuration Wizard

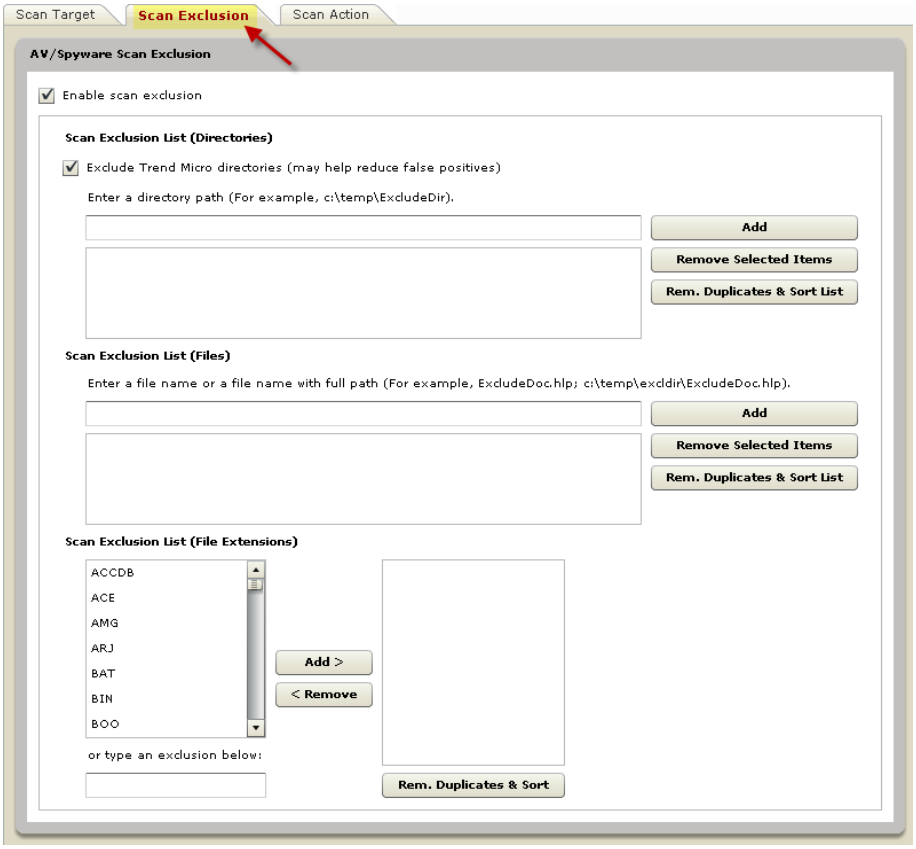
To demonstrate the process of using a configuration wizard, select the *New On-Demand Settings Task* wizard under On-Demand Settings in the Configuration node.



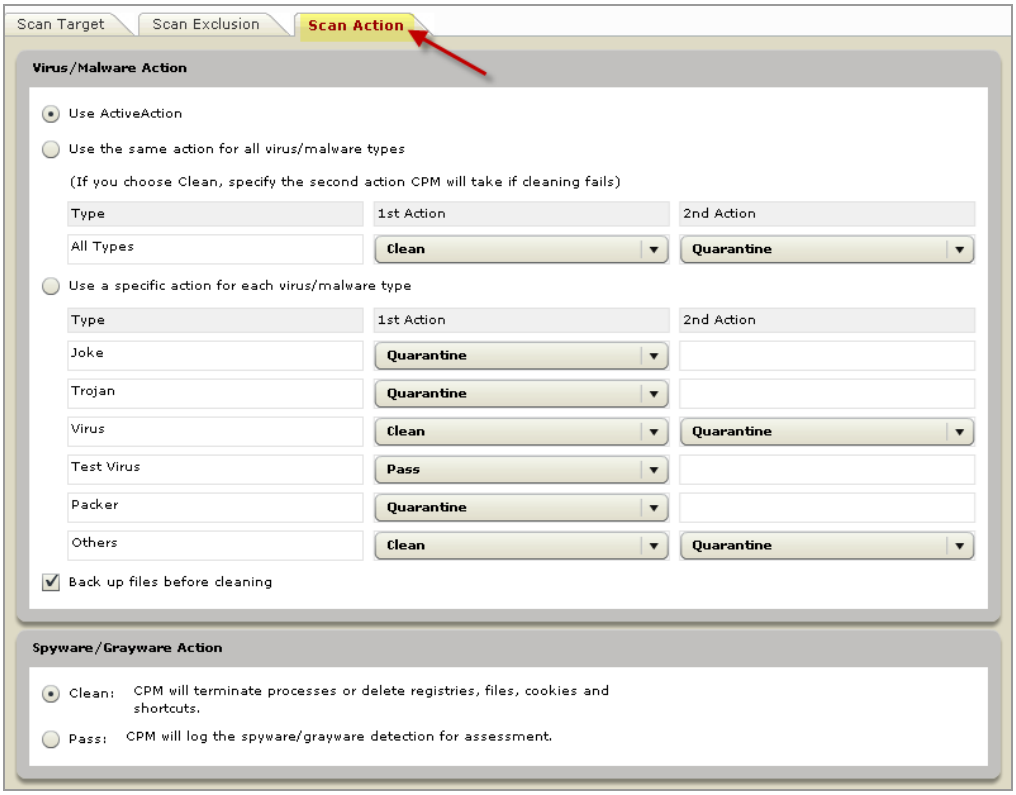
The Wizard is organized by 3 tabs, which each contain a different set of customization options: Scan Target, Scan Exclusion and Scan Action. The Scan Target tab includes Files to Scan, Scan Setting, and CPU Usage boxes that contain customization parameters for your target.



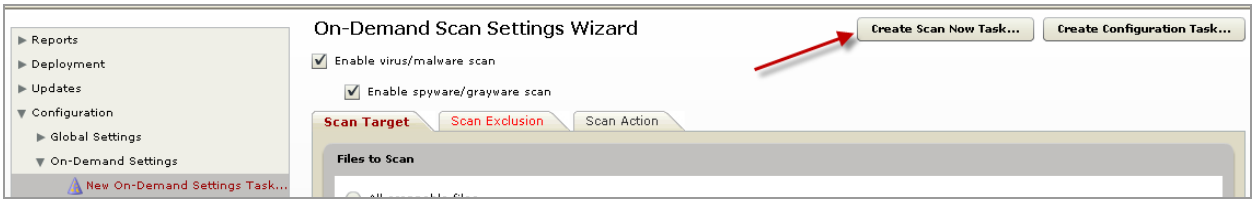
The Scan Exclusion tab includes an AV/Spyware Scan Exclusion box that allows you to set Scan Exclusion parameters for directories, files, and file extensions.



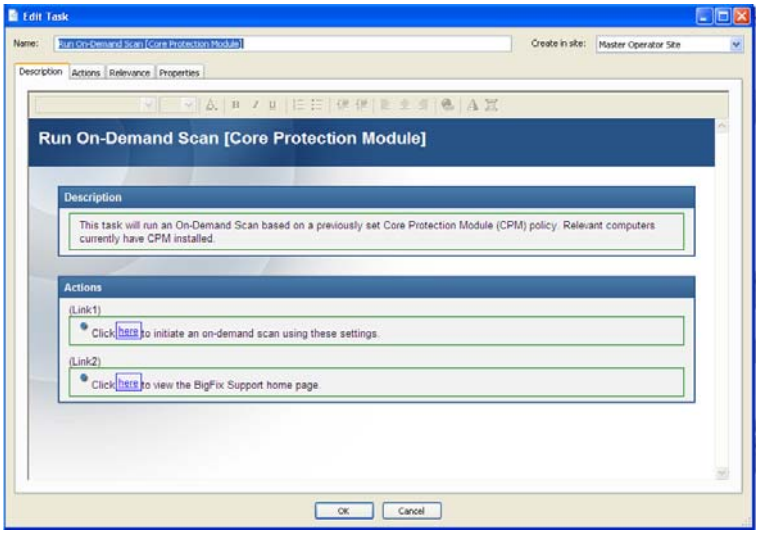
The Scan Action tab allows you to set custom parameters for Virus / Malware Action and Spyware / Grayware Action.



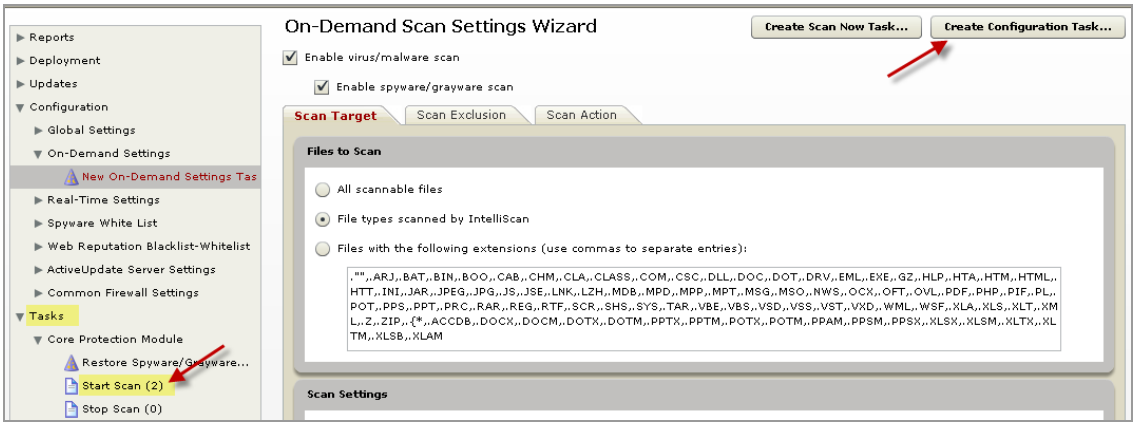
Once you've set all of the parameters that you need, select either the *Create Scan Now Task* or the *Create Configuration Task* button located in the top right of your screen.



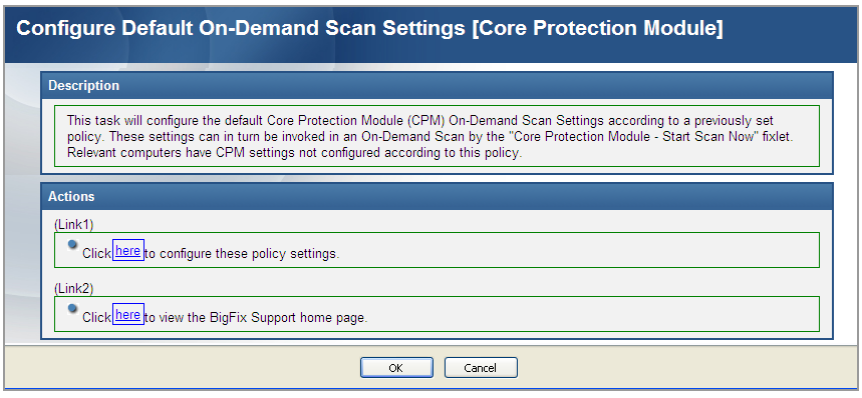
The Create Scan Now Task button will bring up a task window, where you can turn the scan into a custom Scan Now task. From that window, click where indicated in the Actions box and click *OK* to initiate the Task.



The Create Configuration Task button sets a scan configuration as a default task to be used when you deploy the Start Scan task located under *Tasks* > *Core Protection Module* in the navigation tree.

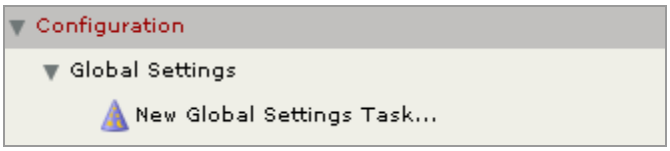


Click the *Create Configuration Task* button. When the window opens, click where indicated in the Actions box to configure policy settings and click *OK*.

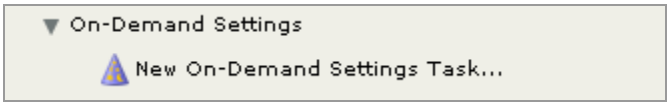


Use this basic Wizard navigation process for each of the wizards in the Configuration node of the navigation tree.

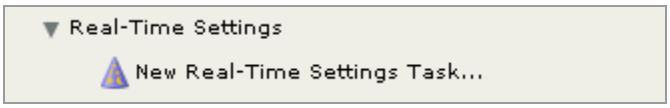
- Use the **Global Settings Wizard** to configure global scan, virus and spyware settings on CPM endpoints.



- Use the **On-Demand Scan Settings Wizard** to configure on-demand scan settings and/or run an on-demand scan on CPM endpoints.

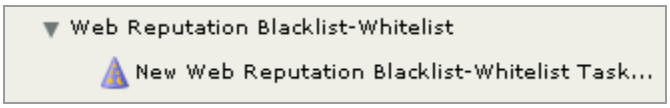


- Use the **Real-Time Scan Settings Wizard** to configure real-time scan settings on CPM endpoints.



- Run the **Spyware White List Wizard** to configure spyware white list settings on CPM endpoints.

- Use the **Web Reputation Blacklist/Whitelist Wizard** to manage your blacklist and whitelist policies and templates.



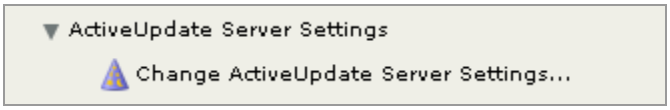
The Web Protection Module Blacklist-Whitelist Wizard enables you to create and maintain global lists of Web sites in the form of policies that you can use to control your users' Web access. Once you have defined these policies, you use them to create Custom Tasks, which you can then apply to your endpoints.

There are two types of URL lists you can create and group into policies using the Wizard:

Blacklists These are lists of blocked Web sites. If the endpoint tries to access a Blacklisted site, they receive a message in their Web browser indicating that access to the site is blocked.

Whitelists These are lists of Web sites you allow your endpoints to access without restriction.

- Run the **ActiveUpdate Server Settings Wizard** to update settings from Trend's "in the cloud" server.



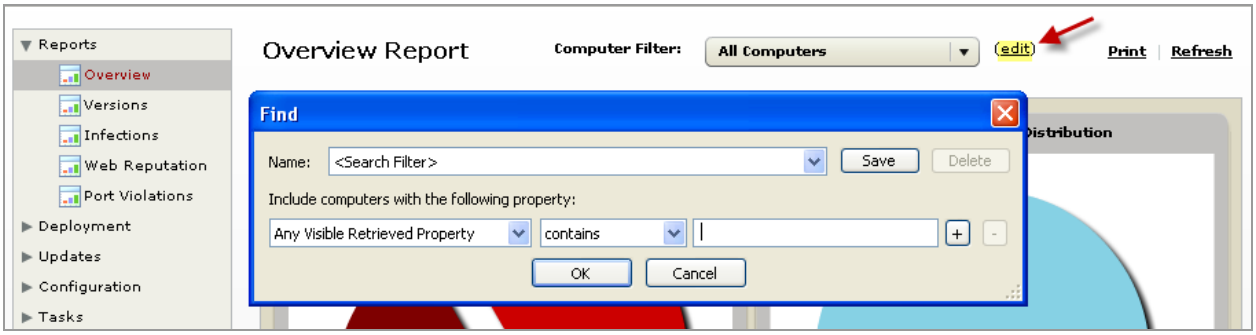
- Use the **Common Firewall Policy Wizards** to enable Common Firewall and configure the firewall rules. Use the Global Exception Rules Wizard to create and edit template rules.

Part 4

Viewing Reports

The Reports node of the navigation tree encompasses five types of reports to provide a real-time view of the state of your CPM deployment – *Overview, Versions, Infections, Web Reputation, and Port Violations* reports.

Reports can be filtered according to the computers in your deployment that you wish to analyze. Click the *edit* link next to the Computer Filter pull down menu to select properties by which to include computers in your report.

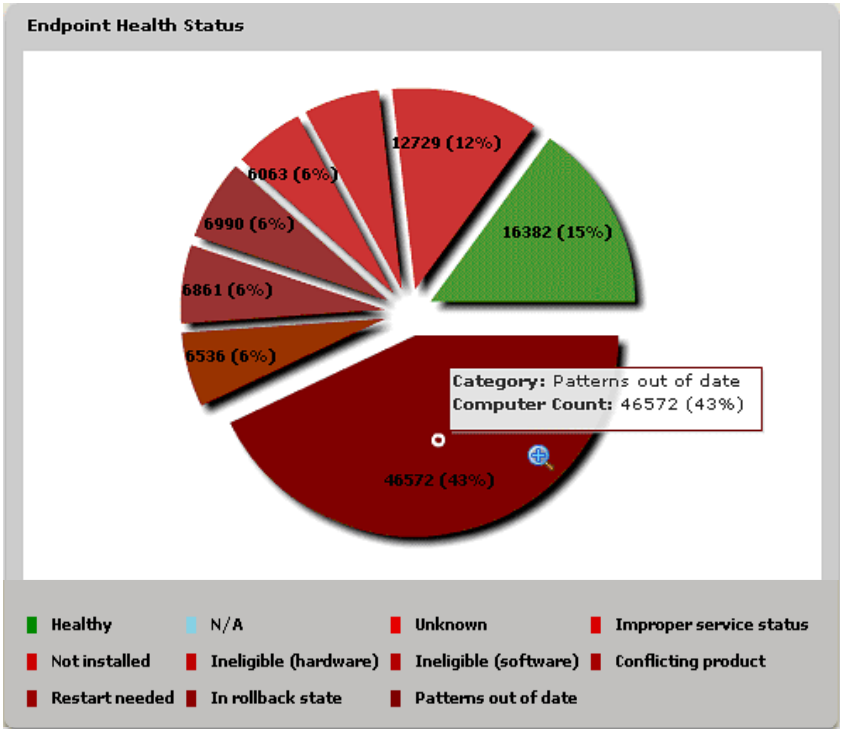


Overview

The Overview Report provides three graphs illustrating different aspects of your CPM deployment:

- Endpoint Health Status - depicting the health of your CPM deployment
- AntiVirus/AntiSpyware Vendor Distribution - showing the anti-malware vendors in your system
- Time to Protection - showing how long it takes for an update to be applied to your endpoints

Endpoint Health Status



Status Category	Description
Healthy	Systems do not fall into any of the unhealthy categories and are, therefore, currently healthy.
N/A	Systems are not relevant to any of the content in the CPM site.
Unknown	Systems have not yet reported property results.
Improper service status	Services required by CPM are not configured properly on systems.
Not installed	Eligible systems have not installed CPM endpoint components.
Ineligible (Hardware)	Systems have insufficient hardware or memory to install CPM.
Ineligible (Software)	The system's O/S is too old or out of date or is incompatible to install CPM.
Conflicting Product	Systems have software installed that is incompatible with components of CPM.
Restart Needed	Systems require a reboot to complete an update, installation or malware removal.
In Rollback State	ESP Clients have taken a pattern-set rollback action - clients in the rollback state cannot be updated until the rollback flag is cleared.
Patterns Out of Date	Systems do not have the latest available patterns.

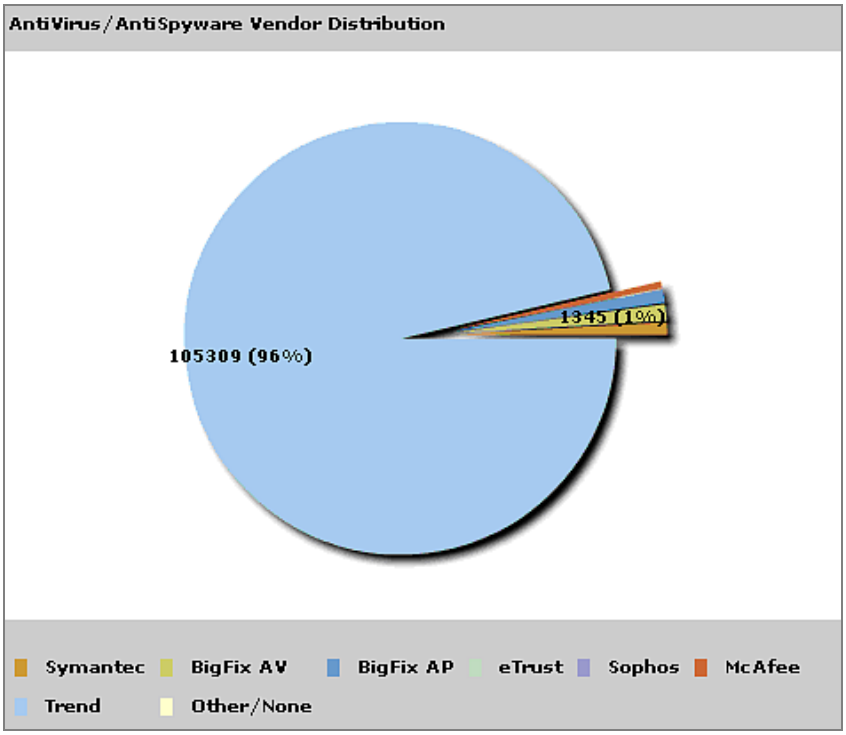
Note: Each computer can be in only one health status category at a time.

The criteria for a “Healthy” designation within the Endpoint Health Status pie chart are as follows:

- Relevant to at least one Fixlet/Task/Analysis in the CPM site
- Not relevant to any of the following Fixlets:
  - *Deploy CPM Endpoint*
  - *Improper Service Status*
  - *Ineligible (software)*
  - *Ineligible (hardware)*
  - *Ineligible (conflicting product)*
  - *Restart Needed*
  - *Clear Rollback Flag*
- Patterns up-to-date - this is checked by comparing the values of the pattern version properties from the client (in the Endpoint Information analysis) against the values of the pattern version properties reported for the server (in the Server Information analysis).

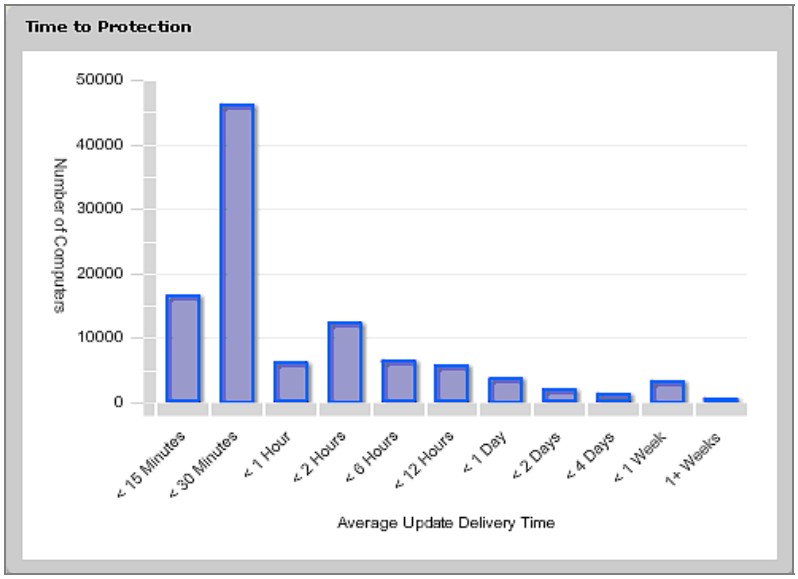
AntiVirus/AntiSpyware Vendor Distribution

The graph below displays how anti-malware vendors are distributed within your deployment.



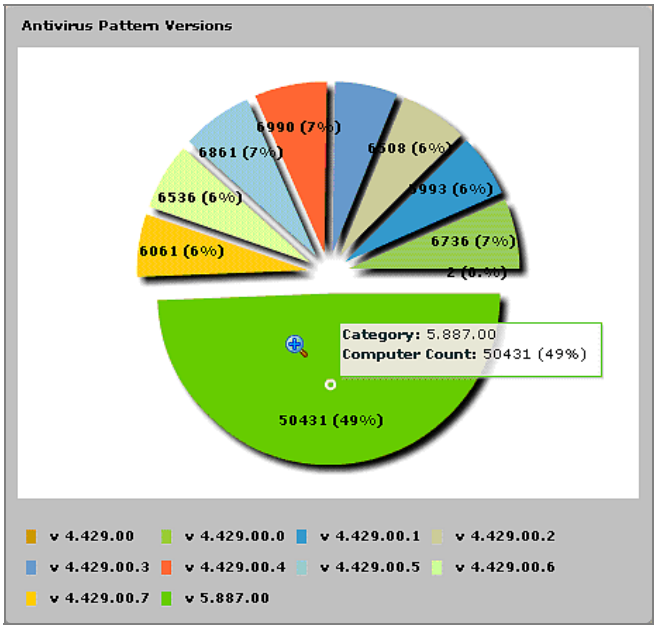
Time to Protection

This statistic represents the end-to-end time of the pattern update process. In other words, the Time to Protection graph illustrates the time from which an update reaches your CPM server to the time it's applied to your endpoints. The graph is measured by the Average Update Delivery Time and the Number of Computers in a deployment. Average Update Time is when a pattern set is downloaded and available on the ESP server to the time at which it is successfully applied at the endpoint.



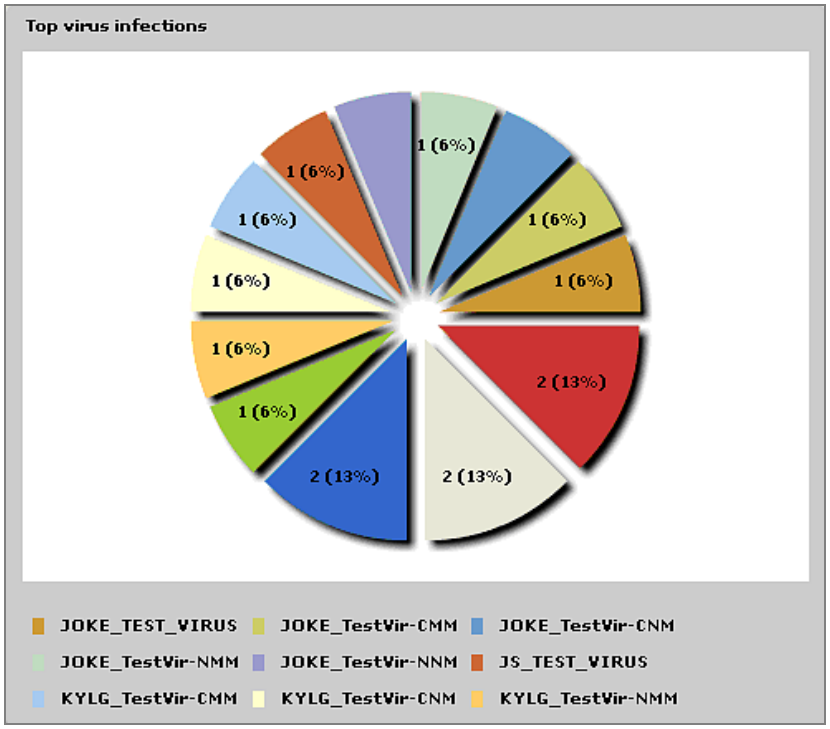
Versions

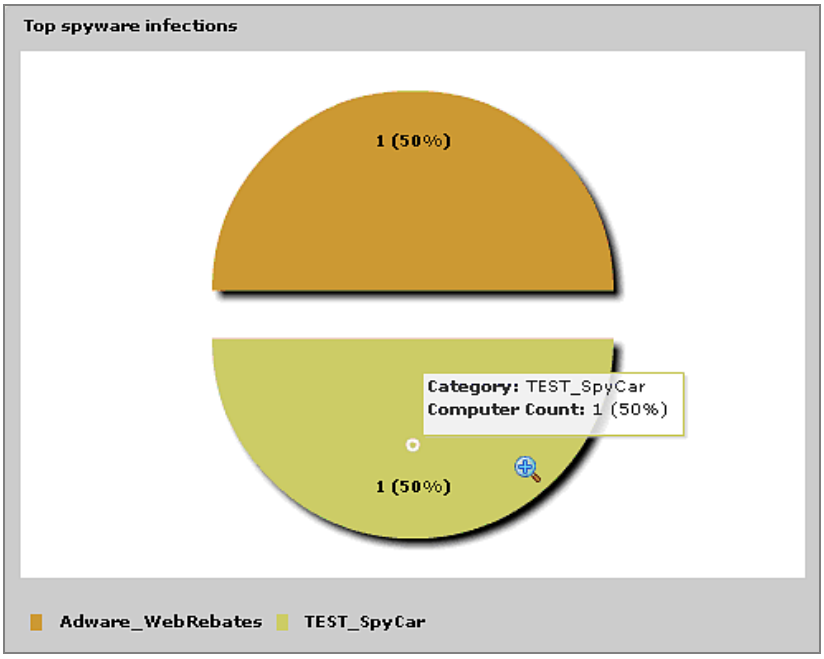
In this graph, view the distribution of versions of each component that can be updated by CPM (located in the Configuration/Pattern Update Settings node of the navigation tree).



Infections

View the infection reports to see your top virus and spyware infections, as well as individual infections by computer, virus or spyware.

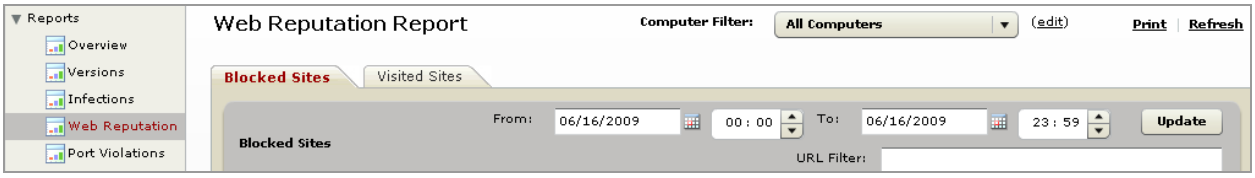




Web Reputation

Web Reputation, which was formerly the standalone product Web Protection Module, is now an integrated feature of CPM version 1.5. Its function is to intercept malware “in-the-cloud” before it reaches users’ systems, reducing the need for resource-intensive threat scanning and clean-up. Specifically, Web Reputation monitors outbound web requests, stops web-based malware before it’s delivered, and blocks users’ access to potentially malicious websites in real time.

Web Reputation displays blocked and visited site reports under the Reports node of the navigation tree.



Port Violations

Port violations are attempts by applications to send network traffic over TCP and/or UDP ports that are blocked on an endpoint by the Common Firewall.

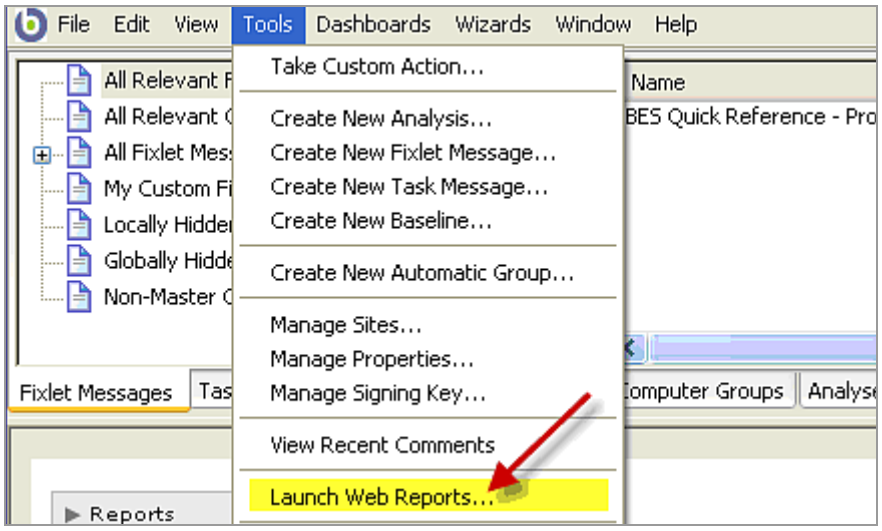
Inbound Inbound port violations occur when external systems try to send packets to the endpoint over blocked ports. Violations of this type may be indicative of network attacks being directed at the endpoint.

Outbound Outbound port violations occur when applications running on the endpoint try to send packets to external systems over blocked ports. Tracking these violations can point to worms, spyware or bots running on the endpoint that are trying to contact external systems for malicious purposes. If the firewall is configured to block outgoing network traffic, any attempts to connect out over a blocked port will be tracked as an outbound port violation event.

You can set the Common Firewall to low, medium, or high security levels, which can be accessed through the Firewall Policy wizards in the Configuration node.

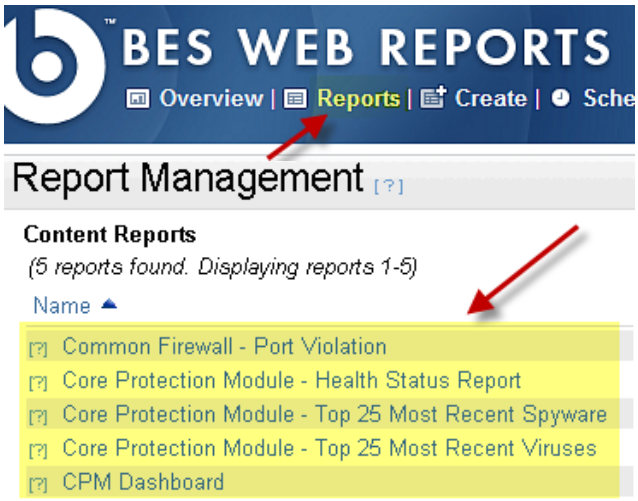
Web Reports

Open Web Reports to configure notifications on new infection detections and view additional reports. To get started, click the *Tools* pull down menu at the top of your screen and select *Launch Web Reports*.



After you're logged into Web Reports, click the *Reports* link to find a list of CPM-specific reports:

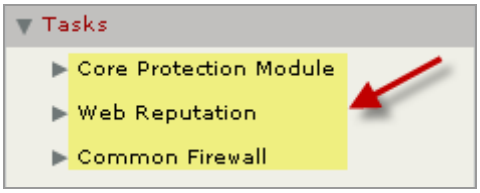
- Port Violation
- Health Status Report
- Top 25 Most Recent Spyware
- Top 25 Most Recent Viruses
- CPM Dashboard



To receive notification emails on new infections, configure a scheduled activity to notify you any time one of the Top 25 reports change. You can also set the Health Status Report to email current "healthiness" numbers on a periodic basis (e.g., once a day). For more information on scheduled activities, see the BigFix Web Reports User's Guide.

Core Protection Module Tasks

The Tasks node of the navigation tree enables you to start and stop scans, upload specific files from your endpoints to your BigFix server, and enable or disable a Client Dashboard. Tasks are organized into three main categories – Core Protection Module, Web Reputation, and Common Firewall.



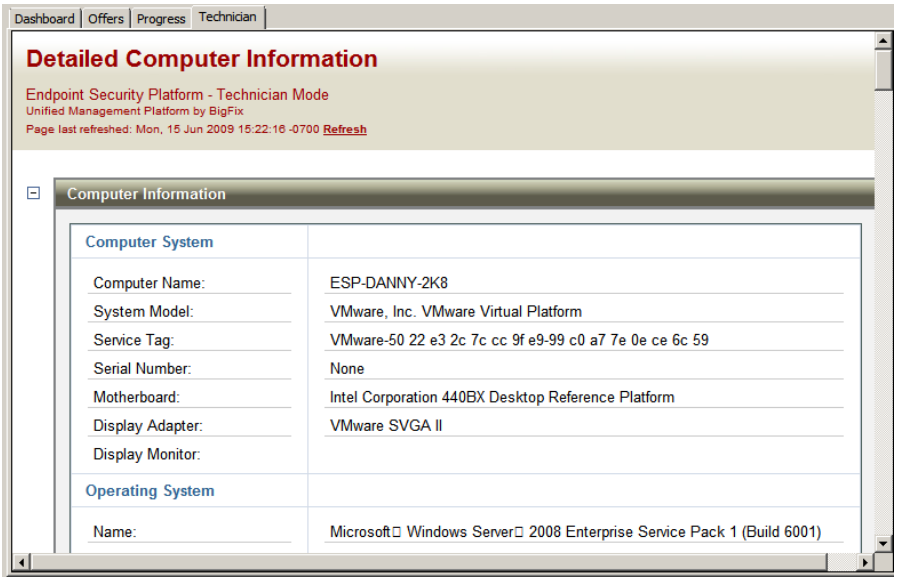
Scanning

To start or stop an On-Demand scan, use the Tasks node of the navigation tree, or create a custom *Scan Now* task using the On-Demand Settings wizard under the Configuration node. By creating custom *Scan Now* tasks, you can configure an On-Demand scan to run on a regular basis – for example, a light (partial) scan performed every morning and a complete scan performed only on weekends.

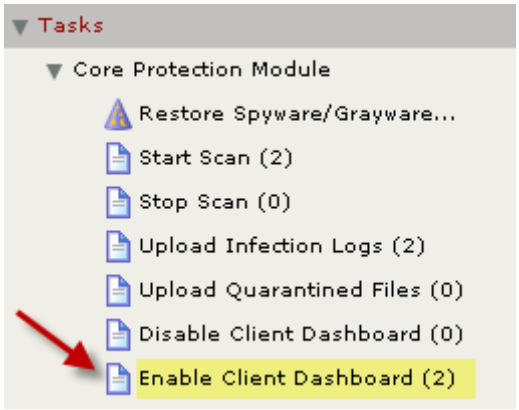
Enable Client Dashboards

This feature allows you to enable or disable a dashboard that's visible to end users. If enabled, you get an icon in the system tray in bottom right corner of your computer. Clicking the icon will display the client UI which will now have a new dashboard tab. The Client Dashboard displays computer information, version information about your CPM deployment, status information (e.g. the last time a scan was run or pattern was updated), and recently-detected spyware/virus.

A related dashboard, called the Technician Dashboard, is also available after enabling the client dashboard by hitting “Control-Alt-Shift-T”. The Technician Dashboard provides additional technical information about the endpoint.

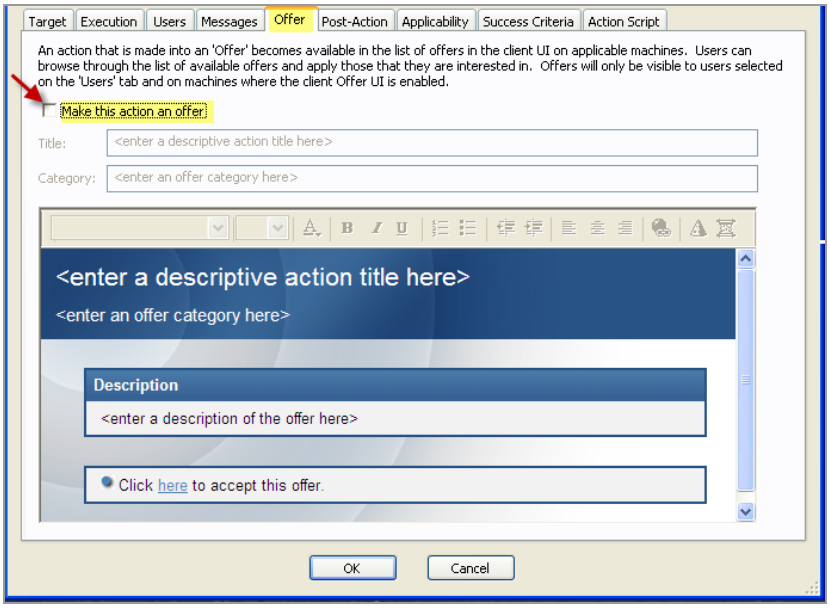


You can enable/disable client side dashboards through the following path in the navigation tree: *Tasks > Core Protection Module > Enable Client Dashboard*. Click *Enable Client Dashboard,* and when the window opens, scroll down to the Actions box and click where indicated to initiate the deployment process.



Client Offers

You can offer end users actions that they can select at their own discretion (also referred to as self-provisioning).



For example, you can issue offers from the 'Update from Cloud' and 'Scan Now' tasks to allow end users to initiate these tasks themselves. For more information on "making offers", see p. 28 of the BigFix Console Operator's Guide.

Note: This feature requires BigFix client version 7.2.4.60 or higher.

Uploading Quarantined Files

Quarantined malware is stored on the endpoint for further analysis. In order to further investigate the nature of specific malware, you can use this task to upload any quarantined malware files stored on your targeted endpoints to your server.

From the navigation tree, select *Tasks* > *Core Protection Module* > *Upload Quarantined Files*. When the dialog opens, scroll down to the Actions box and click where indicated to upload the designated files to the server.

Uploading Infection Logs

This task will enable you to upload virus and spyware log files on targeted endpoints to the BigFix Server. This can be useful if an Administrator needs further investigation of log files aside from what is already offered from the Infection Report in the CPM Dashboard.

From the navigation tree, select *Tasks* > *Core Protection Module* > *Upload Infection Logs*. When the dialog opens, scroll down to the Actions box and click where indicated to upload logs to the BigFix server.

Web Reputation Tasks

The Web Reputation feature prevents Web-based malware from infecting your users' computers. Web Reputation reduces the need for threat scanning and clean-up by intercepting malware before it reaches your users' computers. Specifically, Web Reputation monitors outbound web requests, stops web-based malware before it's delivered, and blocks users' access to potentially malicious websites.

Enabling Web Reputation

To enable CPM Web Reputation, select *Tasks* from the navigation tree, click *Web Reputation*, then select *Enable Web Reputation*. In the Actions box, click where indicated to enable the task. To disable Web Reputation, select that task from the Navigation bar under Web Reputation.

> **Note:** Review the Knowledge Base article on the BigFix support website for details about how to migrate policies from Web Protection Module to the Web Reputation component of CPM version 1.5.

Setting the Security Level

To set desired security levels for Web Reputation, select *Tasks* from the navigation tree, click Web Reputation, then select *Configure Web Reputation Security Level*.

The following security levels determine how/if Web Reputation will allow or block access to a URL:

- High: Blocks URLs that are unrated, a Web threat, very likely to be a Web threat, or likely to be a Web threat
- Medium: Blocks URLs that are unrated, a Web threat, or very likely to be a Web threat
- Low: Blocks only URLs that are a Web threat

In the Actions box, click where indicated next to your desired security level to deploy this task.

Log Maintenance

When Web Reputation is enabled, the URL history and web threat logs increase in size as web requests are issued. The Log Maintenance task archives current URL history and web threat logs and deletes archived logs that are older than the deletion threshold. The deletion threshold will default to 14 days if not specifically set.

> **Note:** The default execution behavior of this task is to apply this action once a day whenever a computer is relevant / applicable. To change this behavior, modify the Execution section in the Take Action dialog.

In the Actions box, click where indicated to maintain current and archived Web Protection URL logs.

> **Note:** If you enable Web Reputation, it is very important that you also use this task to archive logs. If you do not, the log files will never be removed and can eventually consume significant disk space.

Configuring Proxies

Web Reputation requires internet access. In certain network environments, the use of a proxy server may be required.

> **Note:** The proxy server password MUST be encrypted for this action. The task window will provide a utility for encrypting the password.

To configure proxy settings, select *Tasks* > *Web Reputation* > *Enable/Configure Proxy Settings* from the navigation tree.

To disable a proxy server, select *Tasks* > *Web Reputation* > *Disable Proxy Server* task from the navigation tree.

Uploading Web Reputation Logs

Web Reputation maintains logs for web-based threats. These logs are stored on your endpoints, and can be uploaded to the server. To do this, select *Tasks* > *Web Reputation* > *Upload Web Threat Logs* from the navigation tree. From the Actions box, click where indicated to upload the selected logs to the server.

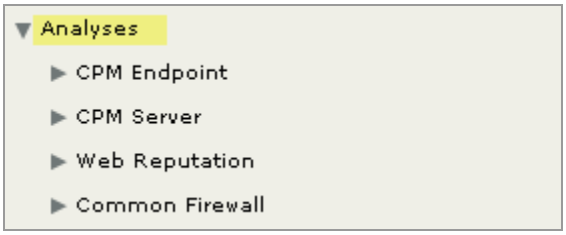
Common Firewall

Uploading Firewall Logs

Use this task to upload firewall log files on targeted endpoints to the server. From the navigation tree, select *Tasks* > *Common Firewall* > *Upload Firewall Logs*.

Viewing Analyses

To locate information about CPM endpoints, use the Analyses node of the navigation tree.



Note: The data in some of the analyses is intended for viewing through the CPM Dashboard reports and may not be useful in its raw form.

CPM Endpoint
Click the *CPM Endpoint* menu under Analyses to view information about your endpoints, including general Endpoint Information, On-Demand Scan Settings, Real-Time Scan Settings, Global Client Settings, Virus/Malware, Spyware/Grayware, and Spyware/Grayware Restore.

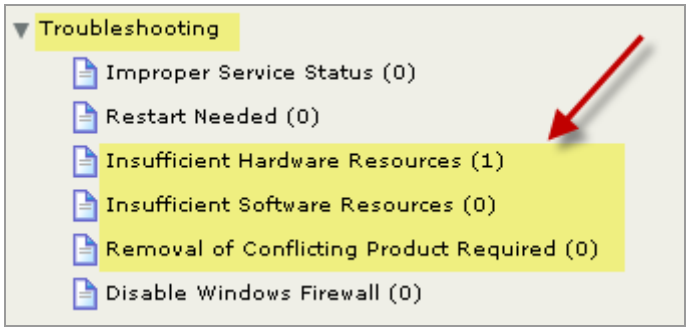
CPM Server
Click the *CPM Server* menu under Analyses to view information about the ActiveUpdate settings on your CPM server.

Web Reputation
Click the *Web Reputation* menu under Analyses to view details of your Web Reputation Site Statistics and Client Information.

Common Firewall
Common Firewall analyses display firewall settings on your endpoints, as well as any inbound and outbound port violations.

Troubleshooting

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

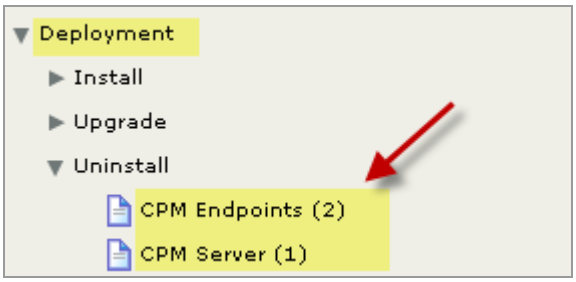


The remaining two Fixlets identify machines where services are not running or configured correctly, and machines that are in need of a reboot.

This node also contains a task to disable the Windows Firewall, which may be required for proper functioning of the Common Firewall component.

Uninstalling CPM

To uninstall CPM from your environment, click the *Uninstall CPM Server* and the *Uninstall CPM Endpoint* tasks under Deployment/Uninstall in the navigation tree.



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

FAQs

The following are a list of Frequently Asked Questions. If you have a question about this product and don't see your question below, check the Technical Support section of this document below for a list of available resources.

What is the definition of "healthy" in the endpoint Health Status Chart?

- Relevant to at least one Fixlet/Task/Analysis in the CPM site
- Not relevant to any of the following Fixlets:
  - *Deploy CPM Endpoint*
  - *Improper service status*
  - *Ineligible (software)*
  - *Ineligible (hardware)*
  - *Ineligible (conflicting product)*
  - *Restart needed*
  - *Clear Rollback Flag*
- Patterns up-to-date

Why does my Health Status Chart only show 3 categories in the legend?

The Endpoint Health Status chart includes 11 categories shown below. If all of these categories are not displayed on your screen, try expanding the size of the dashboard window.

- Healthy
- N/A
- Unknown
- Improper service status
- Not installed
- Ineligible (Hardware)
- Ineligible (Software)
- Conflicting Product
- Restart Needed
- In Rollback State
- Patterns Out of Date

How do I create exclusions?
Go to the Scan Exclusion tab in the On Demand and Real Time wizards (Configuration node).

How do I configure an action when a virus is detected?
Go to the Scan Action tab in the On Demand and Real Time wizards (Configuration node).

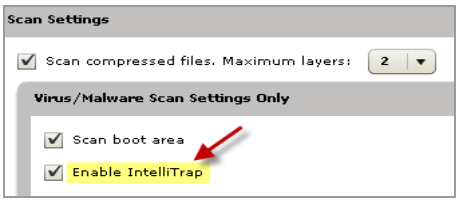
How do I tune spyware detection?
You can set spyware detection to assessment mode in the "Spyware Grayware Scan Settings Only" section of the Global Settings wizard (Configuration node). Instead of quarantining spyware that's been found, this feature allows you to simply report spyware so you can view the infection reports and set appropriate exclusions.

Can I automatically flow updates through clients without operator approval?
Yes. However, you need to manually enable Automatic Updates. See Page 22 of this document, or check the list of Knowledge Base articles located on the BigFix support site.

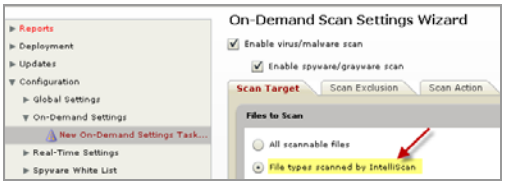
How do I get notified when my system detects a new spyware or virus infection?
Using Web Reports, configure a Scheduled Report based on the Top 25 Spyware and Virus reports, and set it to email you anytime it changes.

How can end users monitor infection information?
By enabling the Client Dashboard.

What is *IntelliTrap*, referenced in the On Demand Scan Wizard?
IntelliTrap helps reduce the risk of virus/malware entering your network by blocking files with real-time compressed executable files.



What is *IntelliScan*, referenced in the On Demand Scan Wizard?
IntelliScan is a Trend feature that will only scan files known to potentially harbor malicious code, even those disguised by an innocuous-looking extension name.



Do the On Demand, Global, and Real Time settings features come with default settings, or do I need to set parameters on them before I use this product?
CPM is packaged with default settings for each of these functions, but the wizards enable you to configure them with customized parameters (for example, use the wizard to customize exclusions to a scan).

What is *ActiveAction*, referenced in the Real Time Wizard Scan Action tab?
ActiveAction is a set of pre-configured scan actions for specific types of viruses/malware. It is recommended to use ActiveAction if you are not sure which scan action is suitable for each type of virus/malware.

What is the *ActiveUpdate Server* and what is it used for?
TMAU, or the Trend ActiveUpdate Server, is Trend's "In the Cloud" server from which our CPM server downloads pattern set files.

Technical Support

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

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

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

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

