Tivoli Endpoint Manager for Core Protection

User's Guide

Note: Before using this information and the product it supports, read the information in Notices.

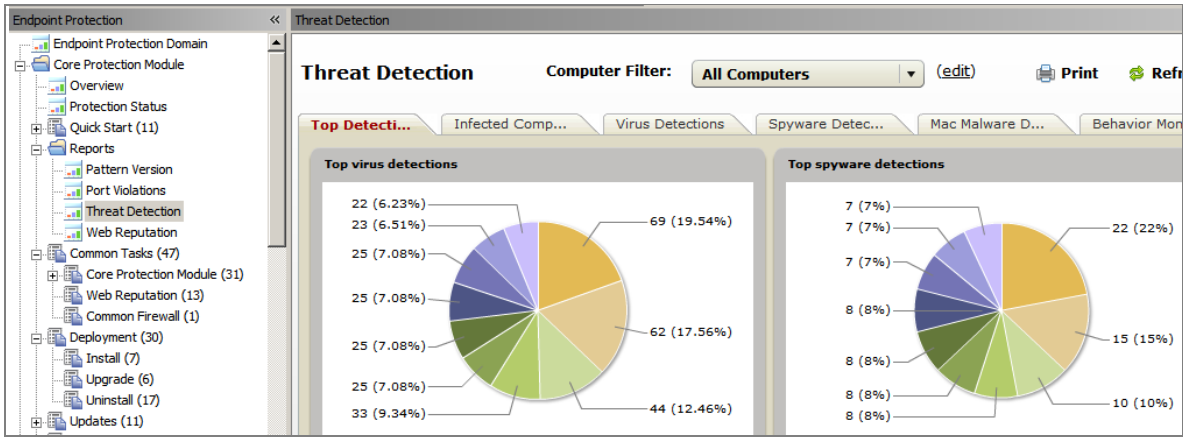
Contents

Part One

Prerequisites

Tivoli® Endpoint Manager for Core Protection (CPM) uses the highly scalable Tivoli Endpoint Manager platform to deliver immediate protection against all types of malware attacks, such as-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 shows you how to use the CPM navigation tree in the Tivoli Endpoint Manager console to install, configure, and customize this product for your environment.



With this product, you can:

- Install server components and endpoints
- Configure updates
- Enable and disable tasks
- View reports

How CPM works

CPM uses BigFix's patented Fixlet® technology to identify agents with outdated antivirus and malware protection. You can trigger 50,000 computers to update their 10MB pattern file and have confirmation of the completed action in as short a time as 15 minutes.

When CPM is installed, you will find it easy to protect your networked computers and keep them secure, all from the console. Deploying Core Protection to your endpoints can be accomplished in minutes. After completing this process, you can track the progress of each computer as you apply CPM component updates. Tracking makes it easy to measure the level of protection across your entire enterprise.

Additionally, you can chart the status of your overall protection with web-based reports through the Web Reporting Module.

New features in this version

Feature	Description
Smart Protection Server	Highly-scalable locally installed versions of Trend Micro Smart Protection Network. Smart Protection Servers host Web Reputation and File Reputation Services to protect your network.
Smart Protection Relay	High-scalable and integrated with Tivoli Endpoint Manager Relays to achieve 100,000 endpoint scalability, while reducing operating costs.
Virtual Desktop Infrastructure (VDI)	Performance optimization to help you maintain a high level of VDI utilization to reduce your operating costs.
Zero Day Threat Protection	Detection and blocking of applications for "Zero Day" threats and suspicious behavior with real time reputation updates.
Enhanced Reporting	Reporting with in-depth reports providing actionable reports for IT operations and management.

Extended platform support

Core Protection Module works with the following versions of Microsoft Windows®:

- Microsoft Windows XP ®32/64-bit
- Microsoft Windows Vista® 32/64 bit
- Microsoft Windows Server 2003® 32/64-bit (including R2)
- Microsoft Windows Server 2008® 32/64-bit (including R2)
- Microsoft Windows 7®
- Microsoft Windows Embedded POSReady 2009® 32/64-bit
- Mac OS™ X version 10.4.11 or higher
- Mac OS™ X version 10.5.5 or higher
- Mac OS™ X version 10.6

Incompatible software

Spyware, Virus, and Malware Programs

- Symantec Software Virtualization Solution
- Symantec AntiVirus
- McAfee VirusScan
- Sophos Antivirus
- eTrust Antivirus
- Bit9 Parity Agent
- Computer Associates ARCserve Backup
- HSM (Hierarchical Storage Management) Backup Software
- BigFix Antivirus
- Norton AntiVirus for Mac
- Norton Internet Security for Mac
- McAfee VirusScan
- Intego VirusBarrier
- Intego NetBarrier
- Avast! Mac Edition
- Sophos Anti-Virus for Mac OS X
- PC Tools iAntiVirus
- Kaspersky
- MacScan
- ClamXav

Trend Micro Software

These software programs must be removed from the endpoints before deploying Core Protection clients to those computers. Use the program's native uninstaller to remove them.

- OfficeScan versions 8 and 10
- Internet Security 2008
- Pc-cillin 2007
- Pc-cillin 2006
- Pc-cillin 2005
- Pc-cillin 2004 (AV)
- Pc-cillin 2004 (TIS)
- PC-cillin 2003
- PC-cillin 2002
- PC-cillin 2000 (WinNT)
- PC-cillin 2000 7.61 (WinNT)
- PC-cillin 98 Plus (WinNT)
- PC-cillin NT 6
- PC-cillin NT
- HouseCall Pro
- Trend Micro Security for Macintosh 1.0
- Trend Micro Smart Surfing for Mac 1.0
- Trend Micro Security for Macintosh 1.5
- Trend Micro Smart Surfing for Mac 1.5
- Virus Buster 2000 for NT ver.1.20-
- Virus Buster 98 for NT
- Virus Buster NT

Programs Incompatible with CPM

- Trend Micro ServerProtect
- ServerProtect for Windows NT

Part Two

Installation

To use the following procedures, you must have already installed the Tivoli Endpoint Manager console and be familiar with the contents of the *Tivoli Endpoint Manager Console Operators Guide*.

CPM clients can use conventional scan or smart scan when scanning for security risks. The default scan method in this release is Conventional Scan. You can change scan method settings using the Enable Smart Scan or Disable Smart Scan tasks.

Installing for conventional scans

Conventional scan is the scan method used in all earlier CPM versions. A conventional scan client stores all CPM components on the client computer and scans all files locally.

Perform the following steps for a conventional scan installation:

1. Add CPM to the Tivoli Endpoint Manager server
2. Activate necessary analyses
3. Install server components
4. Download latest engine/pattern from ActiveUpdate server
5. Deploy and update CPM clients
6. Set up Automatic Update

Installing for Smart Scan

Smart scan is a next-generation, cloud-based endpoint protection solution. At the core of this solution is an advanced scanning architecture that uses threat signatures, which are stored in-the-cloud. A Smart Protection Relay is required for this installation.

Perform the following steps for a Smart Scan installation:

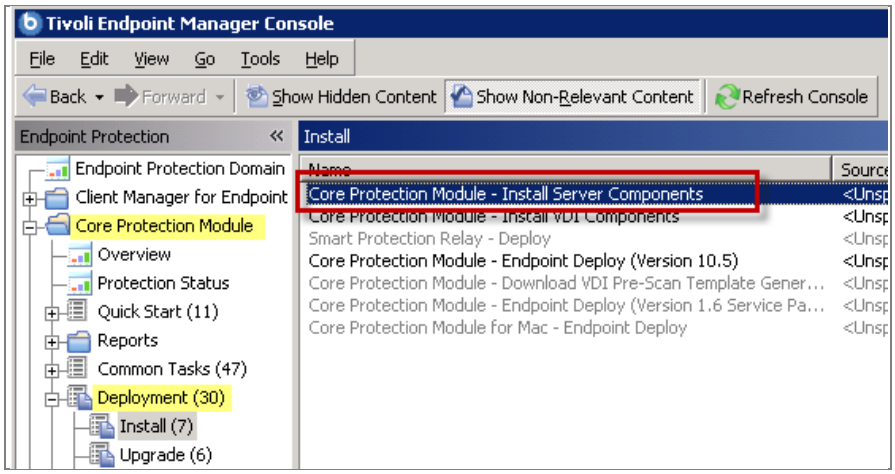
1. Add CPM to the Tivoli Endpoint Manager
2. Install Smart Protection Servers
3. Install the Tivoli Endpoint Manager Agent on Smart Protection Servers
4. Activate necessary analyses
5. Install server components
6. Download the latest engine/pattern from ActiveUpdate server
7. Set up the Smart Protection Server List
8. Create Smart Protection Server List tasks
9. Deploy Smart Protection relays
10. Deploy Smart Protection Server list to endpoints and relays
11. Deploy and update CPM clients
12. Set up Automatic Updates

Installing in a mixed environment

You configure clients differently depending on types of scan. For a mixed environment, switch some clients to Smart Scan mode.

Installing server components

To install server components, click *Deployment* in the CPM navigation tree, click *Install* to view the applicable installation tasks in the List Panel, and click the *Install Server Components* task.



When the Install Server Components task opens in the work panel, review the text under the Description tab and click in the Actions box to initiate the action. For more information about using the Take Action dialog, see the Console Operators Guide.

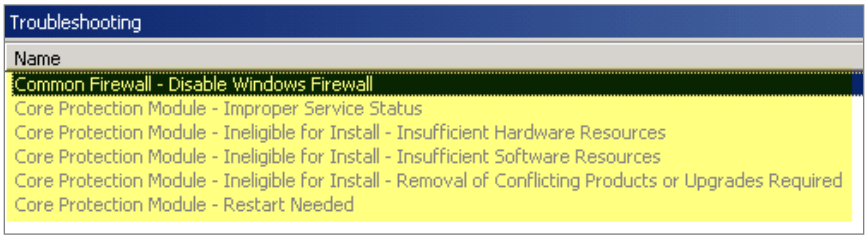
> ***Note:*** *The Install Server Components task automatically restarts the BES root server service.*

Removing conflicting products

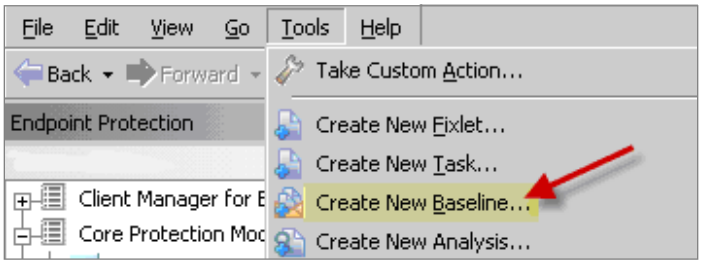
Before deploying the Core Protection client to your endpoints, you must uninstall any programs that conflict with Core Protection functions. For more information about incompatible software, see the Incompatible Software section of this Guide.

If a computer is relevant to the *Removal of Conflicting Product* Fixlet, you cannot 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.

CPM includes several audit Fixlets that automatically detect the presence of incompatible software or hardware in your environment. Click the *Troubleshooting* node in the navigation tree to find the applicable Fixlets.



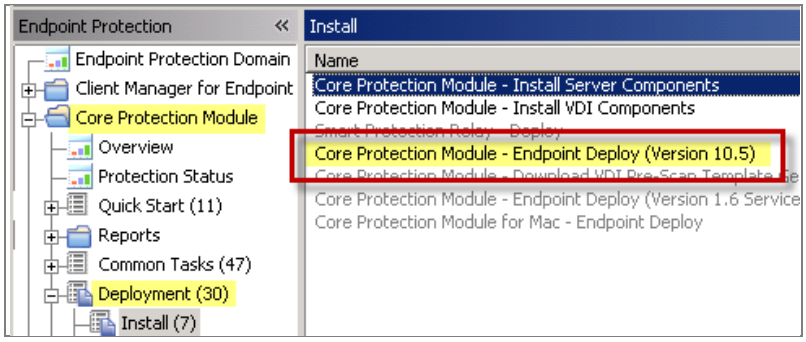
You can create a baseline composed of the uninstall Fixlets to remove the conflicting products. To do this, select *Create New Baseline* from the Tools menu.



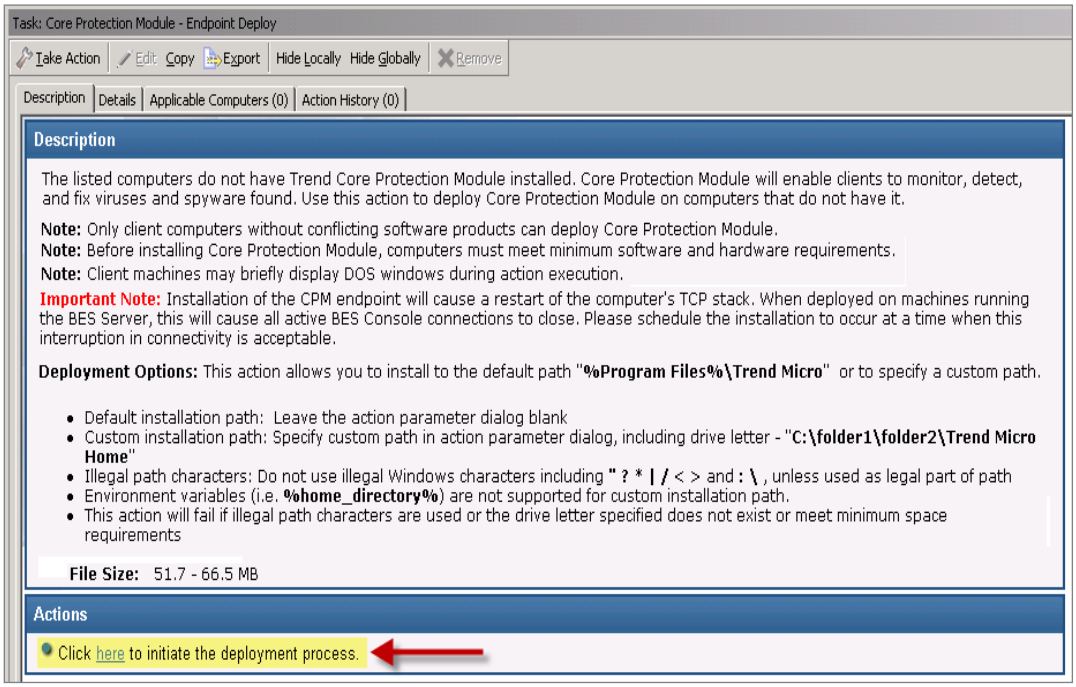
For more information about creating baselines, see the Tivoli Endpoint Manager Console Operators Guide.

Installing endpoints

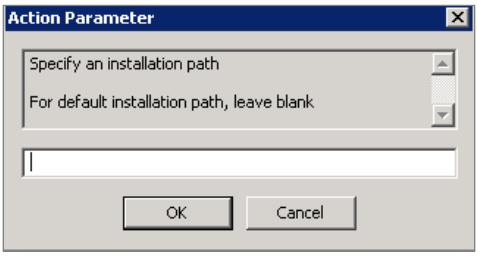
To install endpoints, go to the Deployment node of the navigation tree, select *Install,* and click *Install Core Protection Module - Endpoint Deploy* to target and deploy CPM to relevant computers.



From the Endpoint Deploy Task window, click in the Actions box to initiate the deployment process.



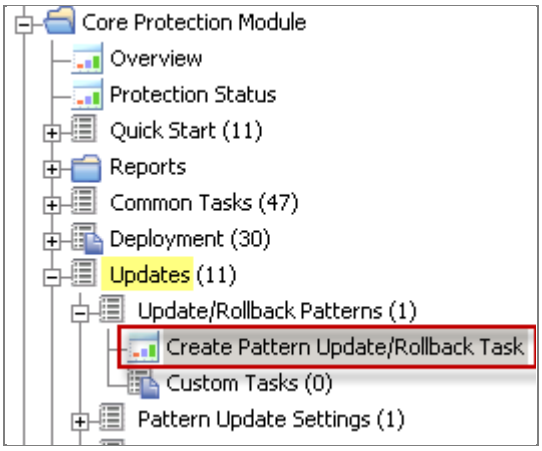
For a custom installation, select an installation path. For a default installation, leave blank, click *OK,* and enter your Private Key Password. The Take Action dialog is displayed, where you can customize the parameters needed for this action.



Set ActiveUpdate Server Pattern Update Interval

When you run the ActiveUpdate Server Pattern Update Interval, the Core Protection server checks for new patterns published by Trend Micro. New patterns are downloaded and made available for deployment using the Pattern Update/Rollback Wizard in the Core Protection navigation tree. If automatic updates have been configured and enabled for server components, endpoints that are configured for automatic updates download and apply the new patterns immediately.

Click the *Updates* node of the navigation tree and click *Create Pattern Update/Rollback Task*.

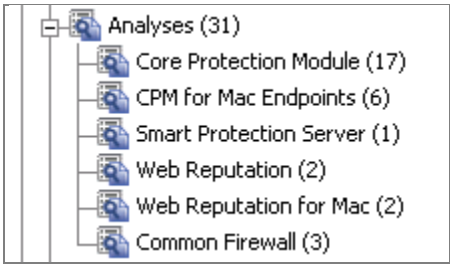


Set this action to run as a policy with periodic reapplicability behavior. It is recommended that you apply this task through the Take Action dialog and select the following action parameters under the Execute tab:

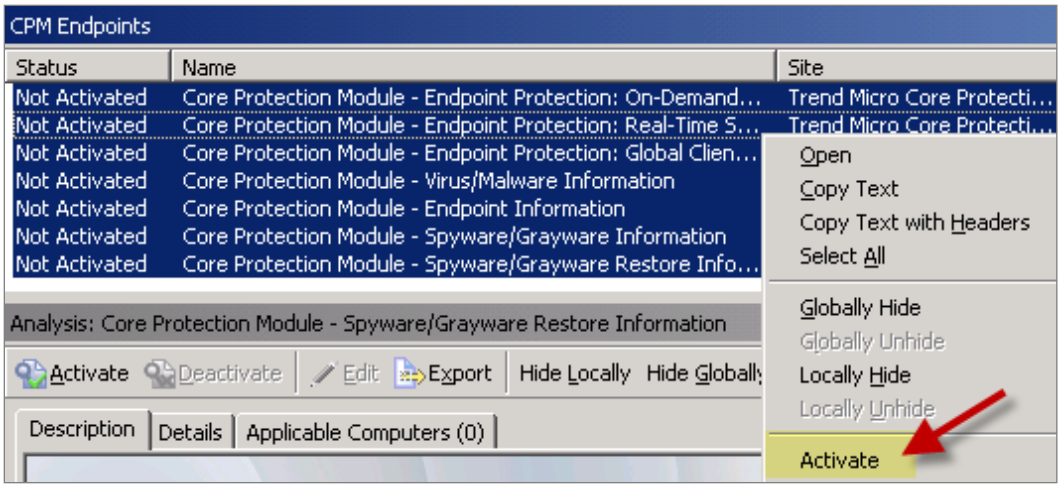
- Never expire
- Run once an hour
- Retry up to 99 times on failure
- Reapply an unlimited number of times

Activating analyses

Click the *Analyses* node in the navigation tree. CPM analyses are organized into the following subgroups: *Core Protection, CPM for Mac, Smart Protection Server, Web Reputation*, Web Reputation for Mac, and *Common Firewall*. You can activate analyses by subgroup or all at the same time.



The designated analyses display in the list panel on the right. Analyses display as Not Activated in the status column. Select all the analyses that you want to activate, then right-click and select *Activate* from the dropdown menu. Enter your Private Key Password. This action changes the status of each analysis to *Activated Globally.*



You can also activate analyses individually. If you have not previously activated a required analysis for viewing a dashboard, you will see a yellow notification bar. Click *Activate* to enable the appropriate analysis.

To activate the Common Firewall analyses, select *Analyses* from the navigation tree and click *Common Firewall* to display the applicable analyses. 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.

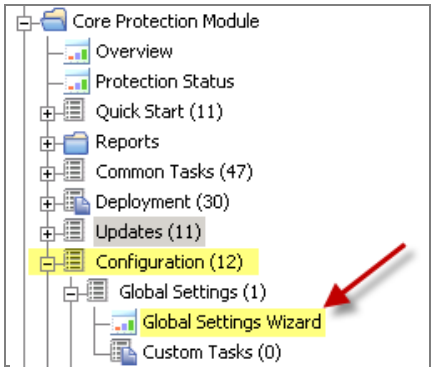
Part Three

Configuration

The Configuration node in the navigation tree includes content for customizing your CPM deployment:

- Global Settings
- ActiveUpdate Server Settings
- Common Firewall Settings
- On-Demand Scan Settings
- Real-Time Scan Settings
- Spyware Approved List
- Web Reputation Blocked-Approved List
- Behavior Monitoring Settings wizard
- Client Self Protection
- Smart Protection Server Settings
- Virtual Desktop Settings

Each subnode under Configuration contains a related wizard for customizing the CPM settings on your endpoints.



Configuring updates

There are several ways to get updates with CPM:

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

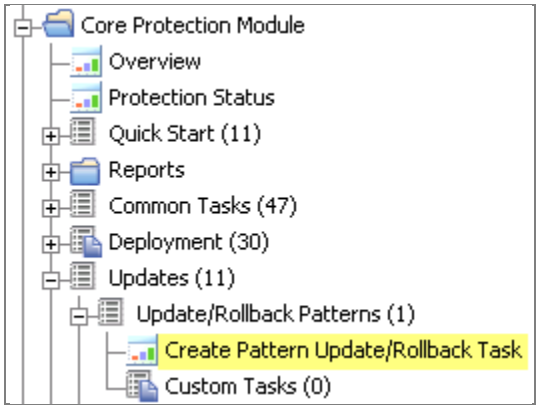
> ***Note:*** *You can use manual updates in some parts of your environment and automatic updates in others. Similarly, Update from Cloud actions can be applied by clients using either automatic or manual updates.*

Manual updates

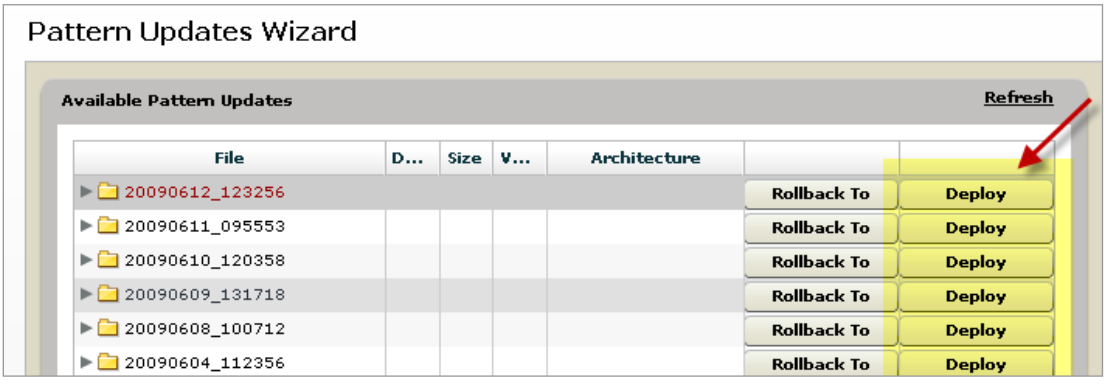
Configure a policy action to run on your server that periodically checks for available updates. If updates are found, they are made available for deployment to your endpoints using the New Pattern Update Rollback wizard.

> **Note:** *Perform this action only once when you first install the Tivoli Endpoint Manager server components. If you configure it to run as a periodic policy action and do not 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 cannot see new pattern updates available in the Pattern Update wizard.*

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



A list of update components is automatically pre-set as a default. Click *Deploy* to update these components to your endpoints.



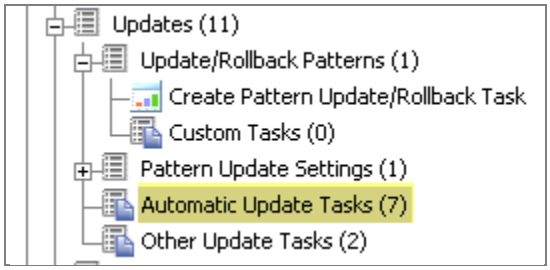
After clicking Deploy, you are prompted to select a Deployment Type. Select either *Deploy a one-time action* or *Create an update Fixlet*. Click *OK* and enter your chosen parameters in the Take Action dialog.

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

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

Automatic Updates

Using Automatic Updates, you can automatically deliver and apply pattern file updates to your endpoints whenever new patterns are made available by Trend Micro.



To enable automatic updates:

1. Download and run the CPM Automatic Update Setup Script and run it on your server.

2. Configure a periodic policy action issued from the Set ActiveUpdate Server Pattern Update Interval task.

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

Note: *An endpoint's automatic update flag is set after CPM is deployed. When the flag is set, the Apply Automatic Updates policy action becomes relevant whenever new pattern files are made available by the policy action configured in Step 2. Only endpoints that have the flag set will automatically apply pattern file updates.*

For a detailed description of each step, see the related Knowledge Base article.

Updating from the cloud

You can now set a specific task to instruct clients to update "from the cloud" instead of from an internal Tivoli Endpoint Manager server.

This task can be set as a policy, to have endpoints automatically get updates from the cloud when roaming, and to use the BigFix infrastructure within the corporate network. This task instructs clients to update from the public Trend Micro Automatic Update server (the cloud), instead of from an internal Tivoli Endpoint Manager server.

Note: *This task ignores selected components to update, as set by the Update Settings Wizard, and updates all out-of-date components on the endpoint.*

Note: *Because the task's relevance is not restricted to roaming computers, the administrator must target computers correctly. Because endpoints 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. Target carefully and test thoroughly.*

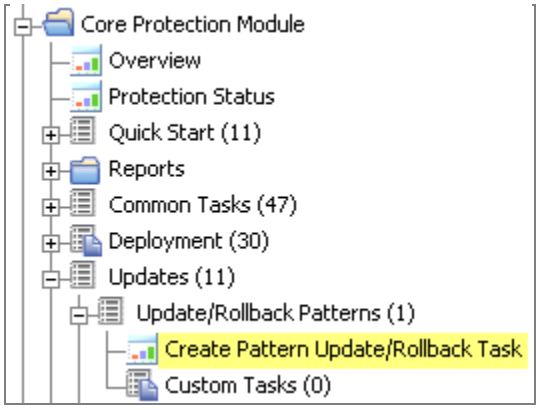
From the Updates node in the navigation tree, click *Other Update Tasks* and *Update from Cloud.* When the dialog opens, click the Actions box to initiate this task.

Note: *Similar to manual and automatic updates, Update from Cloud actions are not relevant when the rollback flag is set.*

To allow more flexibility in update parameters, you can set Update from Cloud actions as client offers.

Rolling back updates

You can roll back patterns to previous versions using the CPM Pattern Rollback feature. From the Updates node, select *Update/Rollback Patterns* and open the *New Pattern Update Rollback* Task.

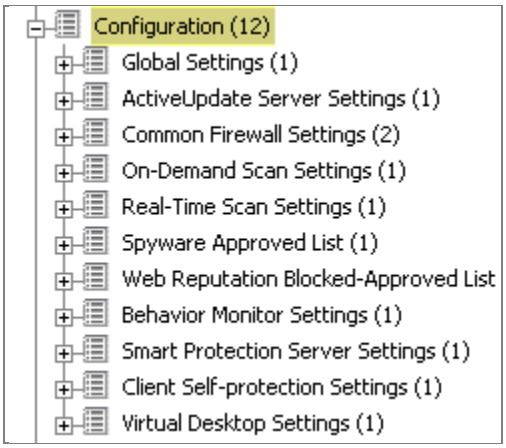


Note: *Because rollback actions are ordered, rollback tasks and actions are not relevant after a newer rollback action has been applied.*

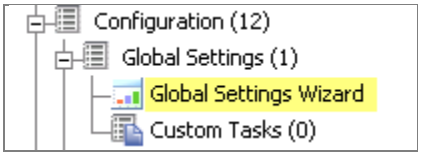
Note: *When a client is in the rollback state, no pattern update actions are relevant until the rollback flag is cleared. To clear the flag, use the Clear Rollback Flag task under Update > Other Update Tasks.*

Using the Configuration wizards

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 to expand the list of configuration options and expand subnodes to display corresponding wizards.

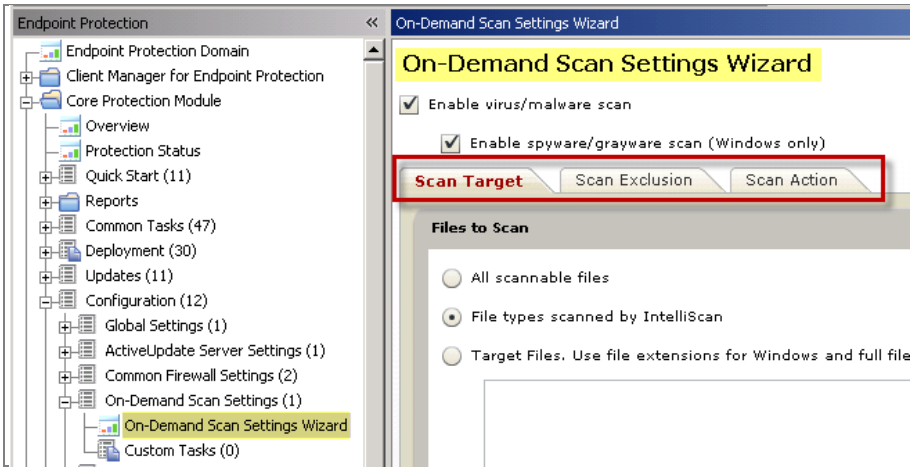


Click the wizard to customize your settings, and click *Create Configuration Task* to generate a configuration task or action. Any configuration tasks that you create are displayed below the wizard that generated the task.



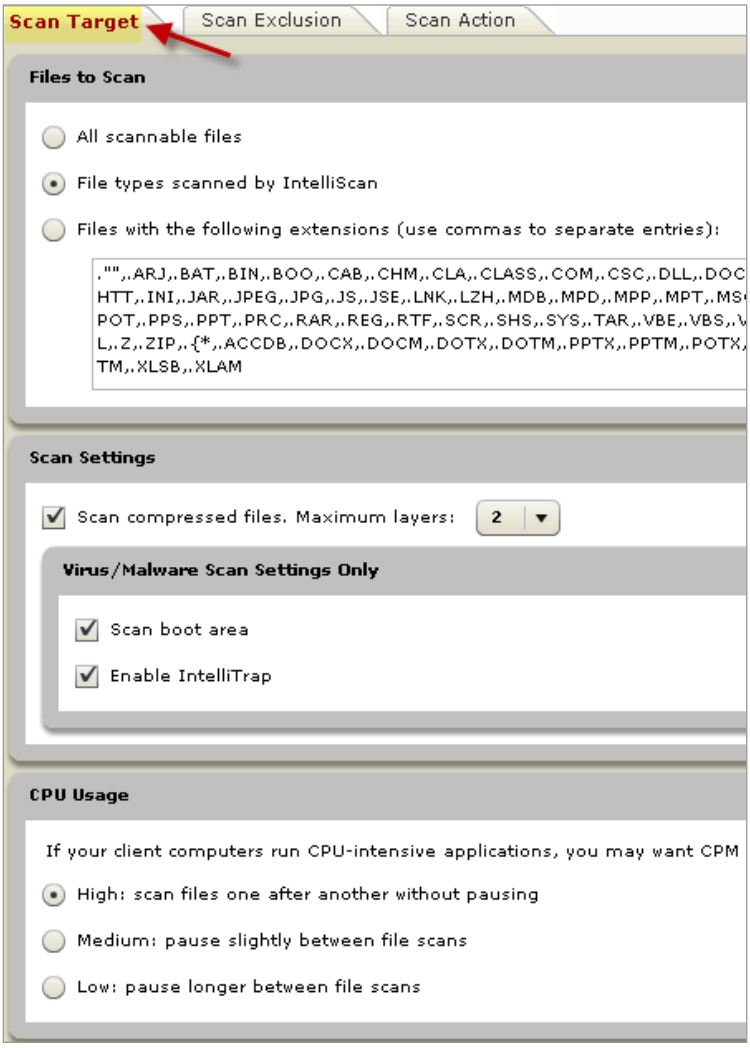
Navigating through a configuration wizard

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

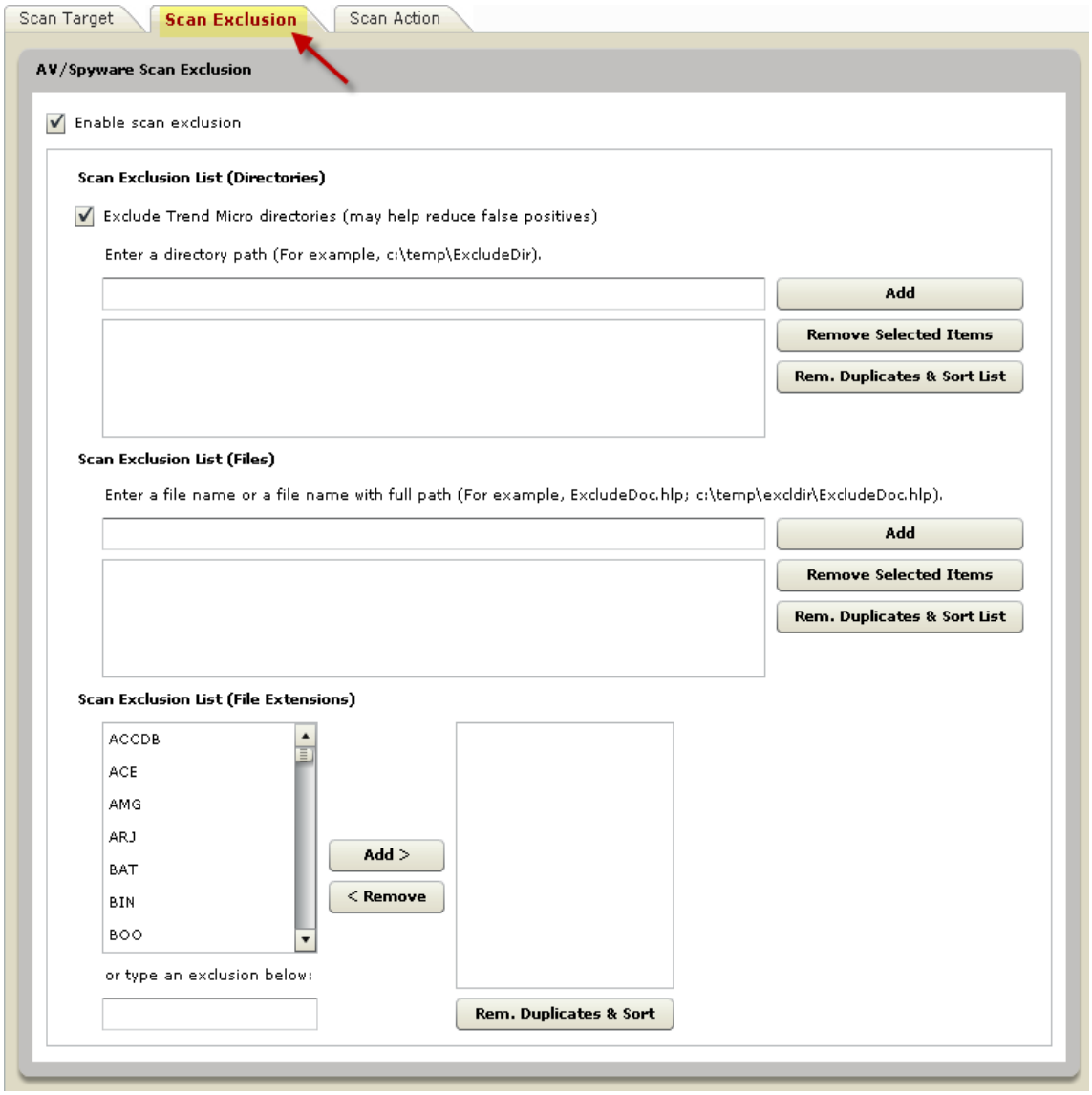


The wizard is organized by tabs, each of which contains a different set of customization options: Scan Target, Scan Exclusion, and Scan Action.

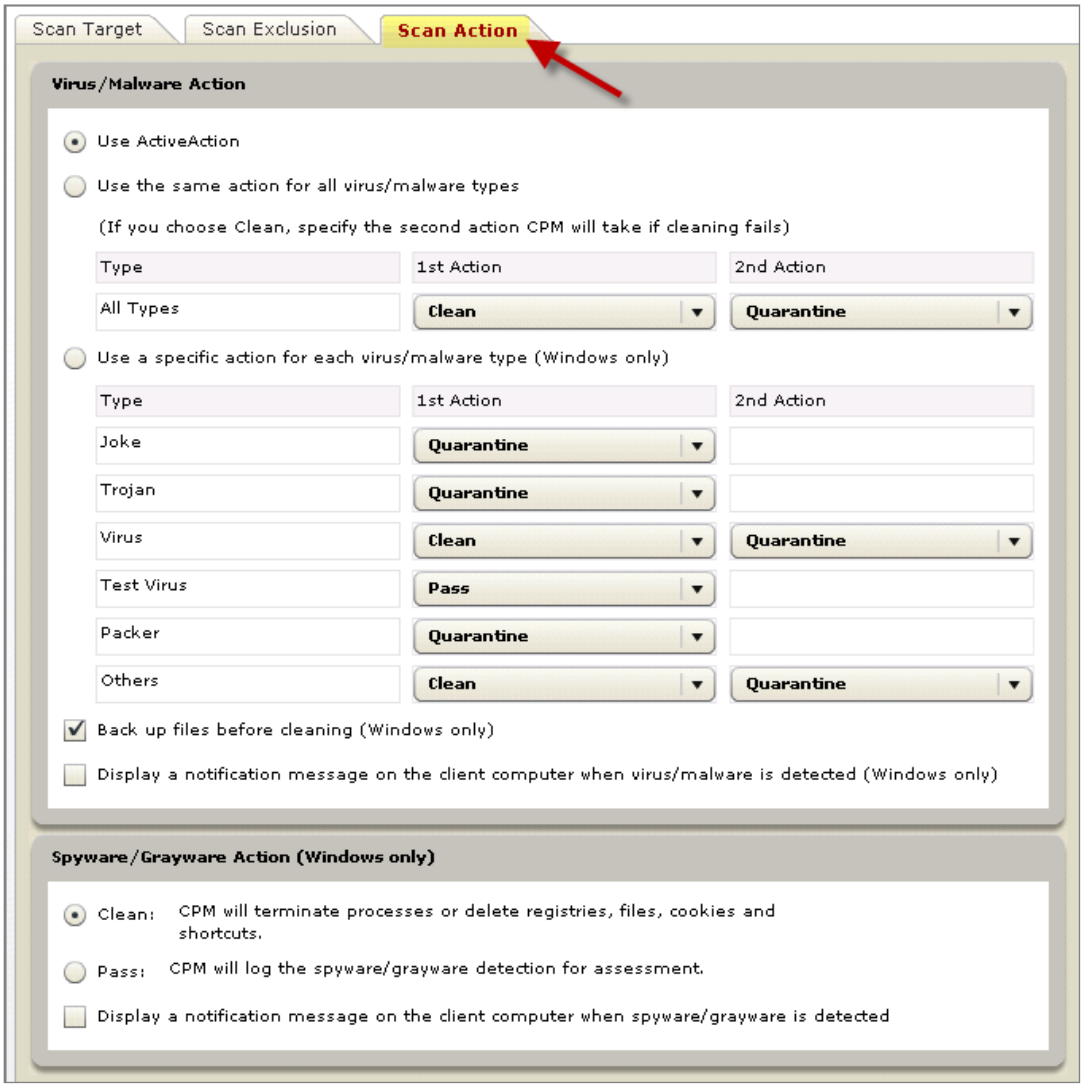
The Scan Target tab includes Files to Scan, Scan Setting, and CPU Usage boxes that contain customization parameters for your target.



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

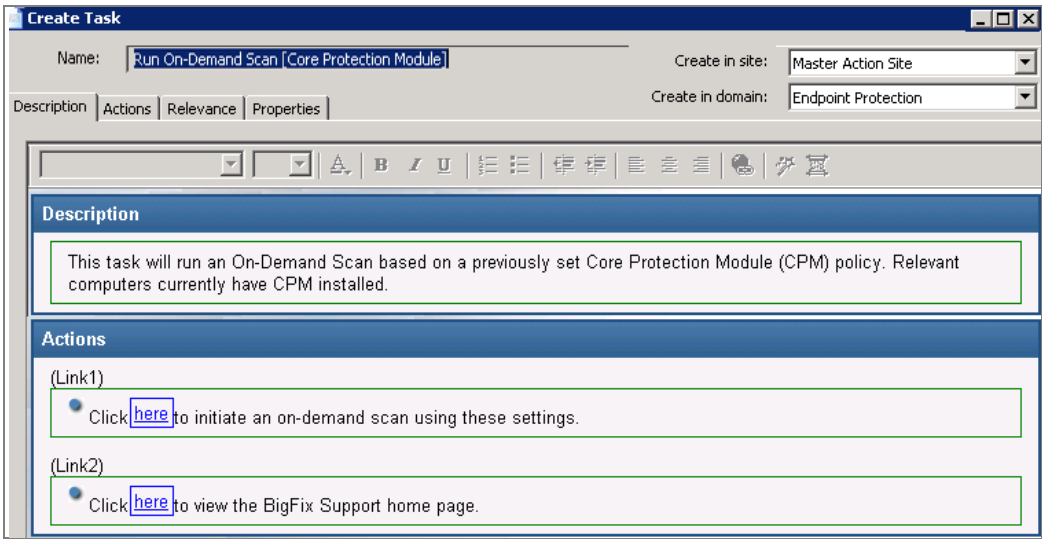


Set custom parameters for Virus / Malware Action and Spyware / Grayware Action in the Scan Action tab.



When you have set all the parameters you want, select either the *Create Scan Now Task* or the *Create Configuration Task* in the top right of the wizard.

The Create Scan Now Task button opens 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 Now* task located under *Common Tasks* > *Core Protection Module* in the navigation tree. Click *Create Configuration Task*.

When the window opens, click in the Actions box to configure policy settings and click *OK.*

Use this navigation process for each wizard in the Configuration node of the navigation tree.

Wizard	Description
Global Settings Wizard	Configures CPM global settings according to a previously set policy
ActiveUpdate Server Settings	Updates settings from Trend's "in the cloud" server
Common Firewall Settings	Enables Common Firewall and configures firewall rules. Use the Global Exception Rules Wizard to create and edit template rules
On-Demand Scan Settings	Configures on-demand scan settings and runs on-demand scans on CPM endpoints
Real-Time Scan Settings	Configures real-time scan settings on CPM endpoints.
Spyware Approved List	Configures spyware approved list settings on CPM endpoints
Web Reputation Blocked / Approved list	Manages blocked and approved list policies and templates

Behavior Monitor Settings	Configures settings to monitor and prevent malicious modifications to the operating system or applications on CPM endpoints.
Smart Protection Server Settings	Configures Smart Protection Server connection priority list for CPM endpoints.
Client Self-protection Settings	Configures settings to prevent modification or disabling of CPM clients.
Virtual Desktop Settings	Configures connection settings to virtual desktop infrastructure (VDI) servers on your network.

Using the Web Protection Module Blocked and Approved List wizard, you can create and maintain global lists of websites in the form of policies to control web access. When you have defined these policies, use them to create Custom Tasks to apply to your endpoints.

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

Blocked	Blocked websites. If the endpoint tries to access a blocked site, it receives a message indicating that access to the site is blocked.
Approved	Websites that allow your endpoints unrestricted access.

Configuring Smart Protection Server Settings

Smart Protection Server Settings need to be configured and deployed if there are Smart Protection Servers deployed on your network. CPM automatically detects Smart Protection Servers if an agent is installed on the server hosting a Smart Protection Server. Use the following process to protect your network using Smart Scan:

1. Configure the Smart Protection Server List
2. Deploy the Smart Protection Server List
3. Enable Smart Scan

Behavior Monitoring

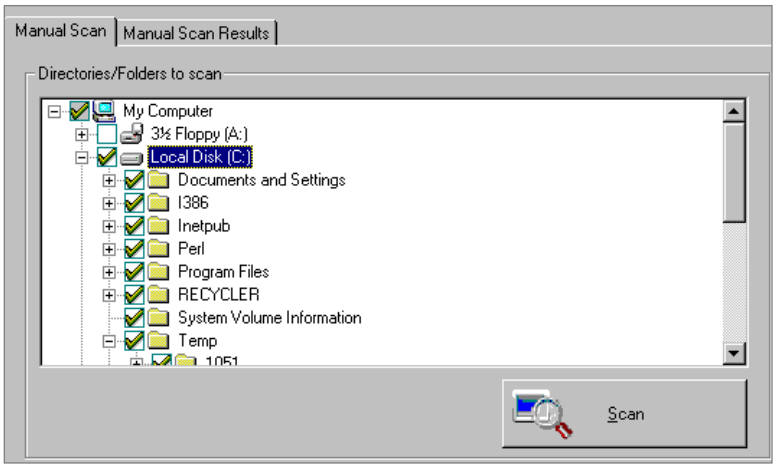
Behavior monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. See the steps below to use Behavior Monitoring:

1. Configure Behavior Monitoring Settings
2. Configure Client Self-Protection Settings
3. Configure Unauthorized Change Prevention Service
4. Configure Certified Safe Software Service

Using the Client Console

Using the Client Console involves accessing the console, connecting the client with the Tivoli Endpoint Manager server, performing manual scans, testing the client console, and updating.

The CPM client provides security risk protection by reporting events and gathering updates from the Tivoli Endpoint Manager server. A system tray icon for the client console informs you of the current scan service status of CPM and provides you access to the client console. When enabled, the client console installation starts a manual scan from Windows Explorer.



Enabling the Client Console

To enable the Client Console, perform the following steps:

1. Go to Configuration > Global Settings > Global Scan Settings Wizard.
2. Scroll down to the Client Console Settings.
3. Check the appropriate boxes:

    - Click the *Enable System Tray* icon to display the icon used to access the client console on the relevant endpoints

    - Click *Enable the Manual Scan* in the Windows Explorer menu to allow the starting of a manual scan

4. Click *Create Global Scan Settings Configure Task*. The Edit Task window opens.
5. Type a descriptive name for the task, such as Enable Client Console.
6. Click *OK* to close the Windows, enter your Private Key Password, and click *OK* to create the new global policy.

The new settings are now shown in the Configuration > Global Settings Dashboard.

Enabling notifications on the client

Use the On-Demand or Real-Time Scan Settings wizards to display notifications on the client computer about virus/malware or spyware/grayware detections.

Client Dashboard and Client Console

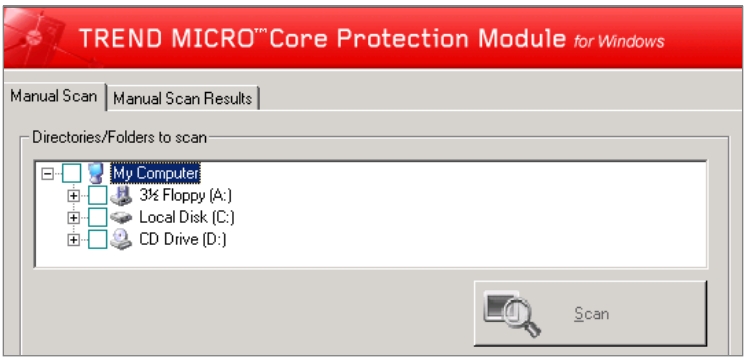
The CPM Client Dashboard displays information about client computers. Before using it, you must enable and deploy it from the CPM dashboard.

The CPM Client Console displays on-demand scan information about client computers. Before using it, you must enable and deploy it from the CPM dashboard.

1 = Client Dashboard
2 = Client Console

Client Dashboard

Client Console



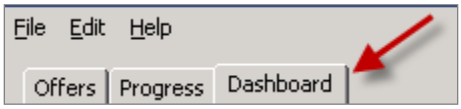
Accessing the Client Console and Client Dashboard

To access the Client Console:

1. Right-click the Client Console in the system tray.
2. Move the mouse pointer over the icon to display client connection information.
3. Select *Core Protection Module Console.* The CPM client console opens.

To access the Client Dashboard:

1. Double-click the Client Dashboard icon in the system tray.
2. Select *Dashboard* from the tabs at the top of the window.



Client connection with Tivoli Endpoint Manager server

Icons in the system tray of the client computer indicate the client's scan service status with the Tivoli Endpoint Manager server. See the table below for a description of each icon:

Conventional Scan

Icon	Purpose	Description
	**Normal**	All components are up-to-date and services work correctly.
	**Scanning**	Manual or On-Demand scan is in progress.
	**No real-time protection**	The Real-time scan service is disabled.
	**Improper service**	Improper scan service. User cannot perform scans.

Smart Scan

	**Normal**	The client can connect to a Smart protection Server or the Smart Protection Network. All services work correctly.
	**No real-time protection**	The client can connect to a Smart protection Server or the Smart Protection Network. Real-time Scan is disabled.
	**Improper service**	The client can connect to a Smart protection Server or the Smart Protection Network. Improper scan service status.
	**Improper service**	The client cannot connect to a Smart protection Server or the Smart Protection Network.
	**Improper service**	The client cannot connect to a Smart Protection Server or the Smart Protection Network. Real-time Scan is disabled.
	**Improper service**	The client cannot connect to a Smart Protection Server or the Smart Protection Network. Improper scan service status.

Manually scanning the Client Console

A Manual Scan is an on-demand scan that starts immediately when you click Scan Client Console. Scan duration time depends on the number of files scanned and the hardware resources of the client computer.

> **Note:** *When you initiate a Manual Scan from the CPM client console, the scan settings used are the latest settings configured by the administrator for an on-demand scan.*

Initiating a manual scan from the system tray icon

To manually scan for security risks:

1. Right-click the client console icon () in the system tray.
2. Select *Core Protection Module Console*.
3. Click the *Manual Scan* tab.
4. Select the drives, folders, and files you want to scan manually.
5. Click *Scan*.
6. Click the *Manual Scan Results* tab after completing the scan.

> **Note:** *Scan results are only available during the scan session. If the console is closed, scan results are no longer available.*

Initiating a manual scan from Windows Explorer

You must enable a manual scan from the CPM dashboard before that scan is available.

To initiate a scan from Windows Explorer:

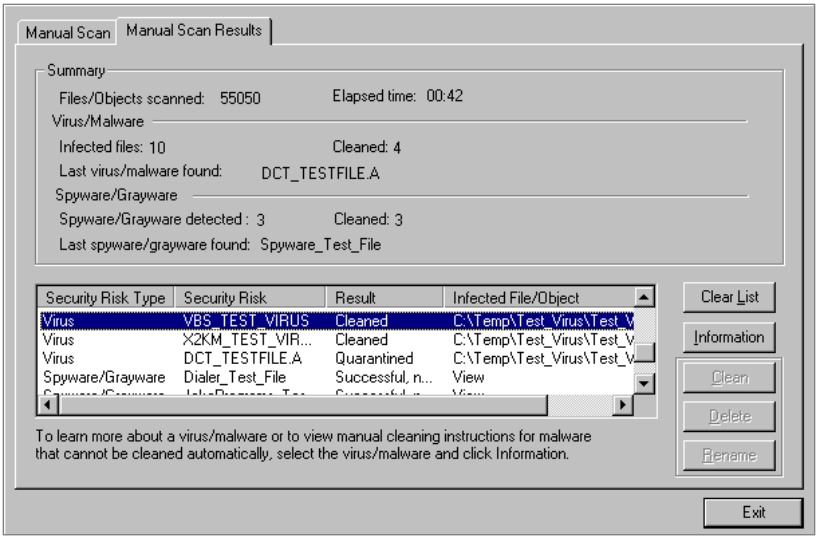
1. Open Windows Explorer on the endpoint computer.
2. Right-click the folder or file to be scanned.
3. Select *Scan with Core Protection Module* to initiate the scan. Results indicate if the scan was successful, as follows:
   - If nothing was found, click *OK* in the confirmation dialog box.
   - If the scan found an issue, the action for handling malware (configured by the system administrator) occurs.
4. Click the *Manual Scan Results* tab, immediately after completing the scan, for details.

Manual scan results

The Manual Scan Results tab displays the result of the most recent Manual Scan. You can view virus/malware or spyware/grayware scanning results.

> ***Note:*** *Closing the client console removes the information displayed on this screen.*

The upper half of the screen contains the scan summary and the lower half contains a table with detailed information about any security risk detected during scanning



Button	Usage
Clear List	Click this button to remove the information in the table.
Information	To learn more about the security risk, click the security risk name and then click this button.
Note:	*The following buttons apply only to virus/malware scan results if the scan action (configured by the CPM administrator) is Pass, which means that CPM detected the file but did not take any action. You can clean, delete, or rename the file.*
Clear	CPM might be unable to automatically clean some files because the file might be encrypted, in a location that does not allow it to be cleaned, or is a Trojan or worm. See scan results for details.
Delete	Delete the virus or malware file.
Rename	Click to change the extension of the file to .VIR, (or to .VI0, .VI1, if there is more than one) to prevent users from opening it accidentally.

Viewing scan results

To view the scan results:

1. Perform a Manual Scan as described in the previous section.
2. Click the *Manual Scan Results* tab. Summary details display at the top of the screen.
3. If CPM configured the scan action to pass, select a detected virus or malware.
4. Click *Clean, Delete,* or *Rename*.

Testing the CPM client console

After enabling the CPM console, your administrator can test it to verify that antivirus protection works. The European Institute for Computer Antivirus Research (EICAR), developed a test script as a safe way to confirm proper installation and configuration of antivirus software. For more information, see the EICAR website at: http://www.eicar.org/

The EICAR test script is an inert text file with a .com extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software applications react to it as if it were a virus.

Notice: *Never use real viruses to test your antivirus installation.*

Contact your CPM administrator for information about how to use the EICAR test script.

Updating the client

You can manually update any time with the Update Now feature. The client connects to an update source to check for updates to security components that detect the latest viruses, spyware, and malware. If updates are available, the client automatically downloads the components.

> **Note:** *Update Now always updates from the cloud and not from the Tivoli Endpoint Manager Server, whether the endpoint runs remotely or connects to the LAN.*

To update the client manually:

1. Right-click the CPM client console icon in the system tray.
2. Click *Update Now* from the console menu.
3. In the Update Status tab, click *Update Now*.

When complete, you see the message, “Component update is complete.

Part Four

Reports

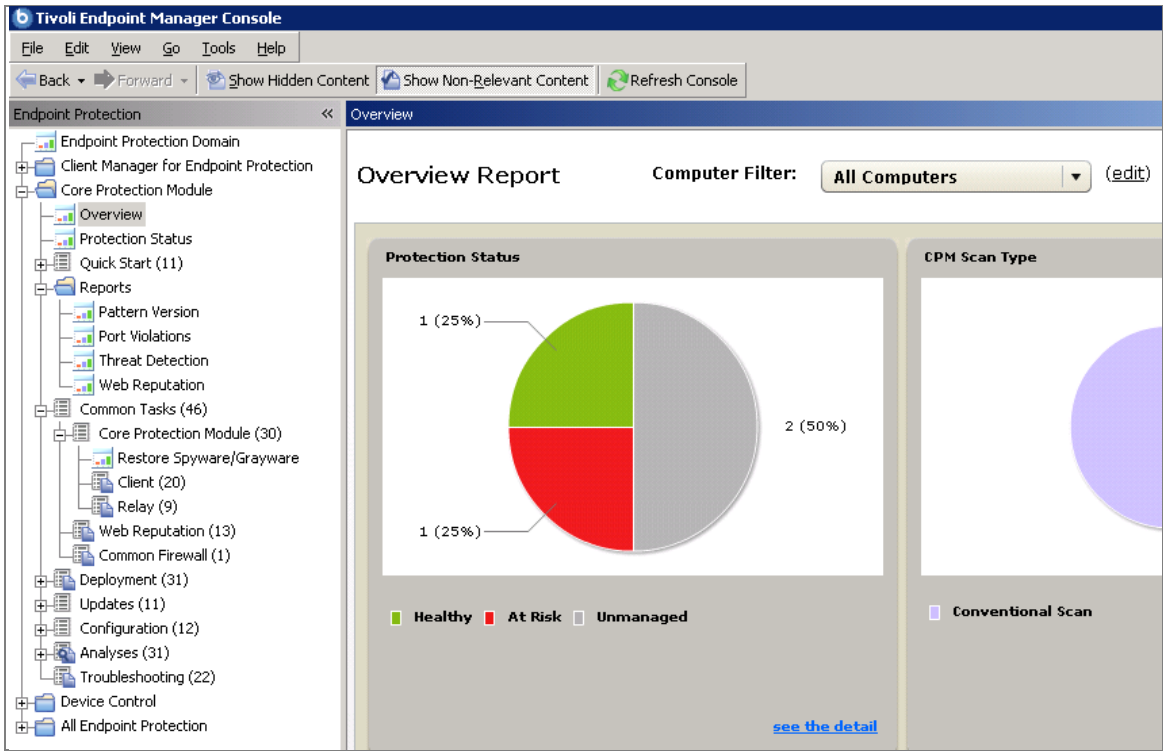
The CPM navigation tree provides a number of graphical reports for monitoring the status of your deployment. The primary reports are Overview and Protection Status. The Reports node of the navigation tree also offers additional reports: *Threat Detection, Port Violations, Pattern Version, and Web Reputation.*

The available status criteria in CPM are:

- Healthy: Endpoints pass all Protection Status criteria
- At risk: Endpoints fail one or more Protection Status criteria.
- Unmanaged endpoints: Endpoints do not have CPM or MPM clients.

Overview

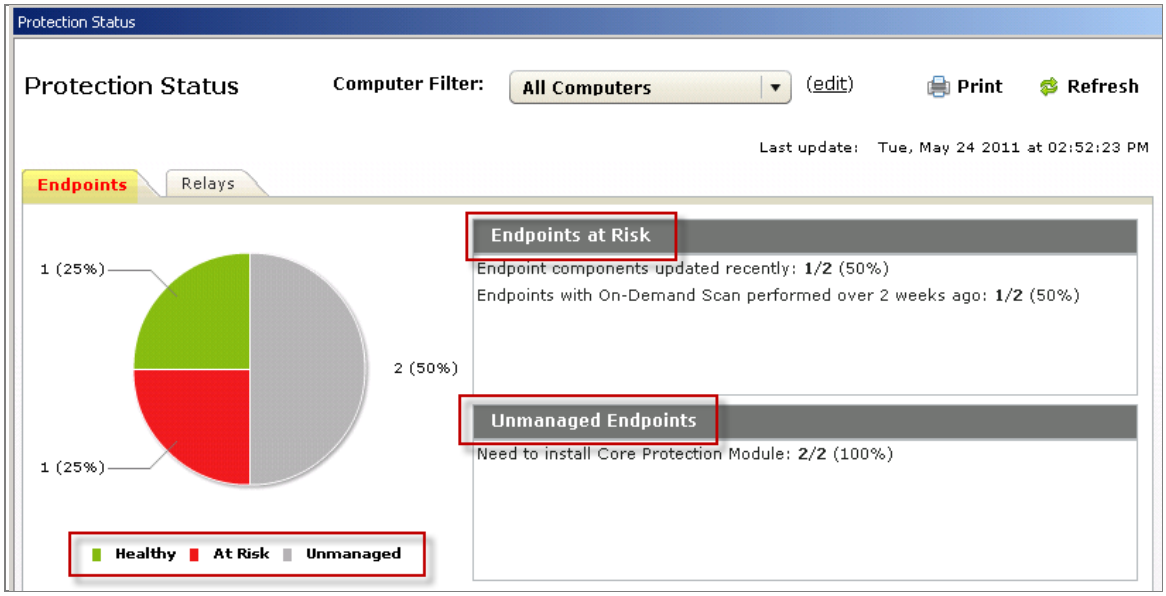
The CPM Overview Report provides a summary of the overall condition of CPM clients in your deployment. The Overview summary graphs include Protection Status, Top Virus and Spyware Detections.



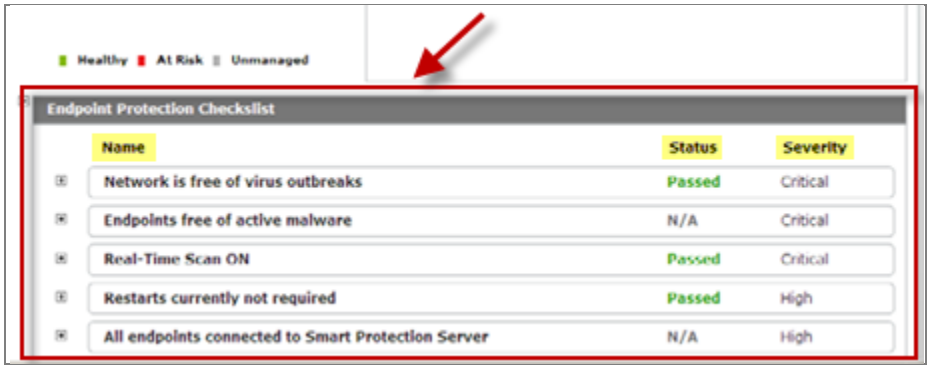
Protection Status

Click the Protection Status report from the navigation tree to monitor specific details of your endpoints and relays.

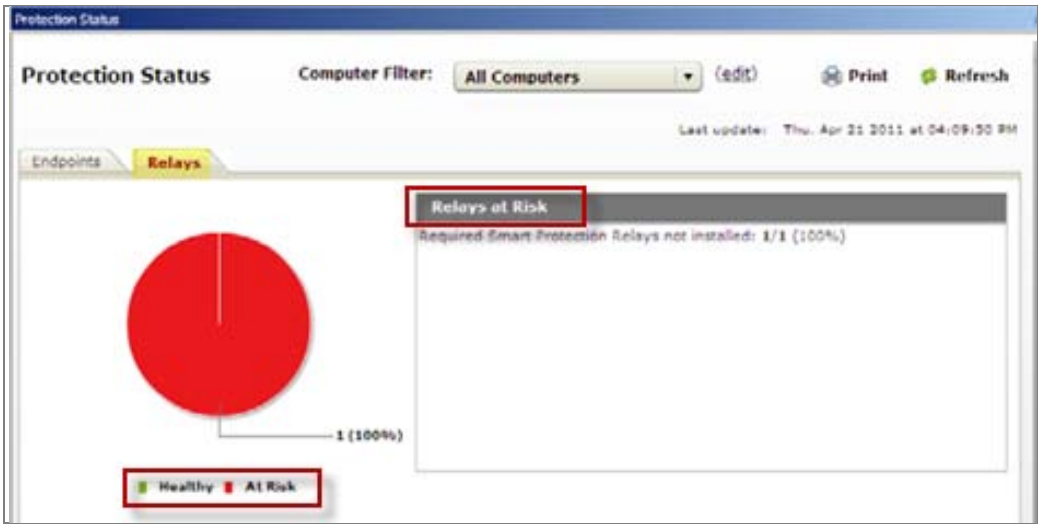
The endpoint tab in the report separates data by Endpoints at Risk and Unmanaged Endpoints.



Below the pie chart is an Endpoint Protection Checklist, which itemizes details of your protection status according to their status and severity.



The relays tab displays a graphical chart of the health status of your relays.



The Relay tab includes two checklists: Smart Protection Status and VDI Components.

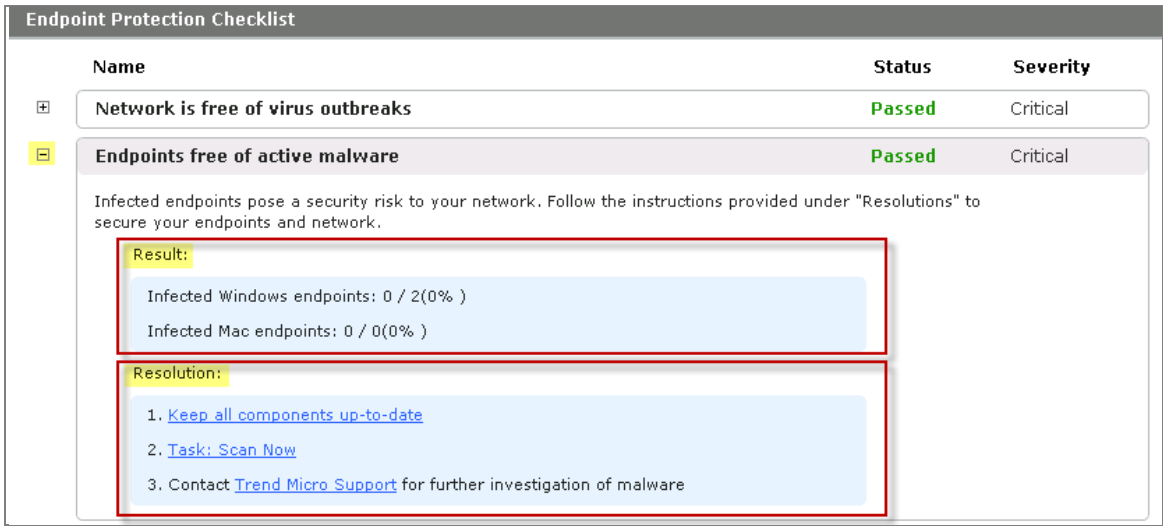
Smart Protection Status

	Name	Status	Severity
⊞	File Reputation available	N/A	Critical
⊞	Web Reputation available	N/A	Critical
⊞	Smart Protection Relays installed in all relays	N/A	Critical
⊞	Smart Protection Relay status is protected	N/A	Critical
⊞	All Smart Protection Relays registered to Smart Protection S...	N/A	Critical

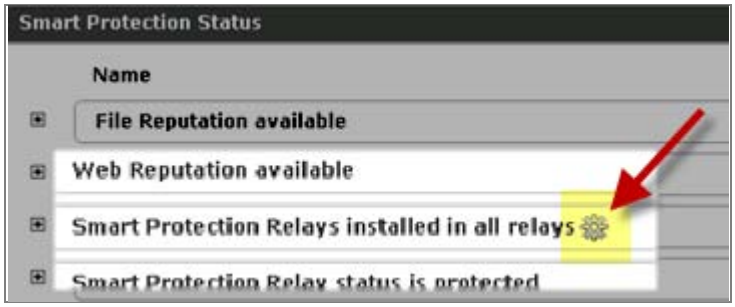
VDI Components

	Name	Status	Severity
⊞	VDI component status is normal	N/A	Critical
⊞	Relay VDI Components	N/A	Critical
⊞	All VDI components connected to VDI servers	N/A	Critical

Click the plus sign beside each item in the list to display the detailed content. The expanded checklist box displays the result of the check and related resolutions to secure your endpoints and network.



You can configure settings in the Relay or Endpoint tab checklists by clicking the gear icon next to each item. The icon displays when you move your cursor over an item in the list.



After clicking the icon, use the dialog box to modify settings for that specific item.

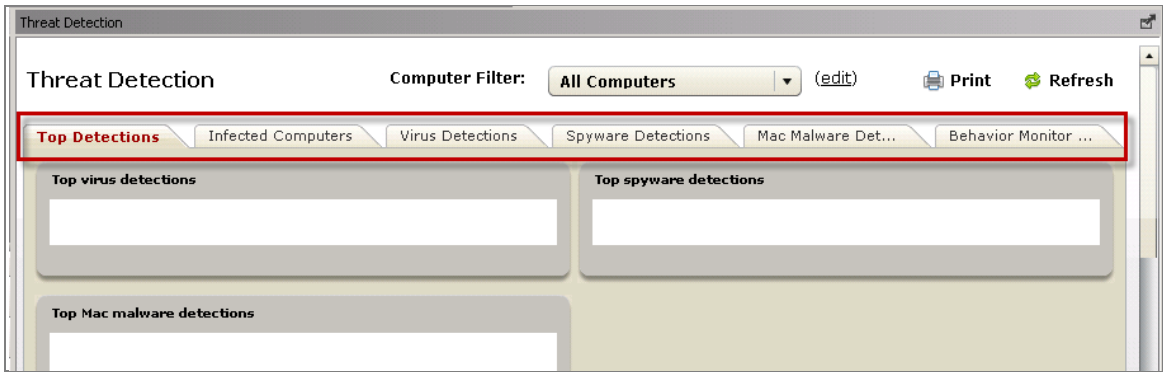
Click *Save,* and then click the next item in the checklist.

Threat Detection

The Threat Detection report displays a summary of threats in your deployment. Threats are categorized as follows:

- Top Detections
- Infected Computers

- Virus Detections
- Spyware Detections
- Mac Malware Detections
- Behavior Monitoring Detections



Port Violations

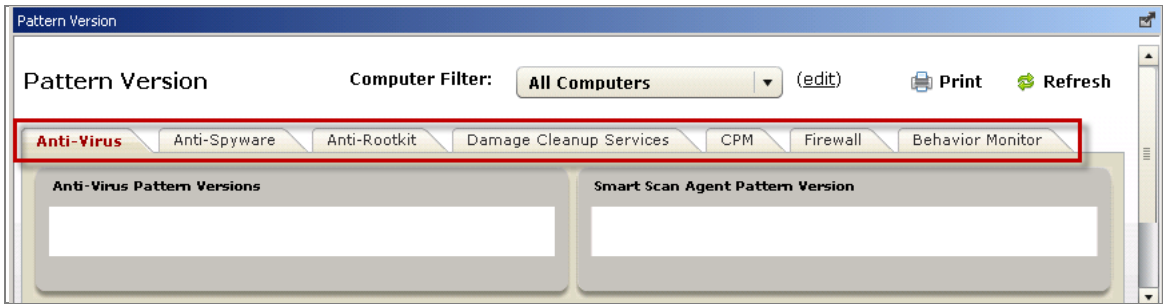
The Port Violations report provides information about inbound and outboard endpoint port violations. Port violations are attempts by applications to send network traffic over TCP or UDP ports that are blocked on an endpoint by the Common Firewall.

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

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 attempt to connect out over a blocked port is tracked as an outbound port violation event.

Pattern Version

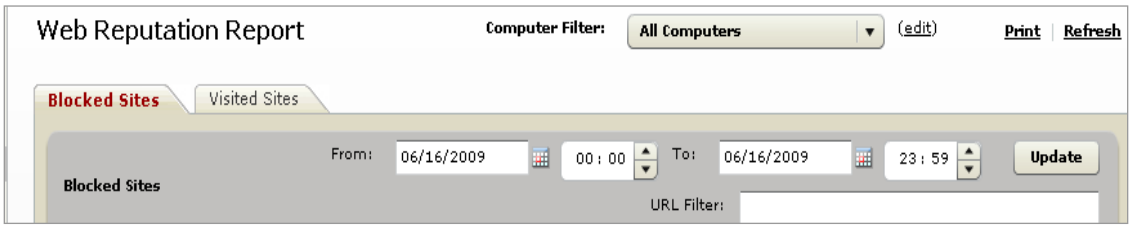
In this graph, you can view the distribution of component versions that can be updated by CPM. Click each tab across the top of the screen to view the related graph.



Web Reputation

The Web Reputation feature intercepts malware in the cloud before it reaches systems. Web Reputation monitors outbound web requests, stops web-based malware before it is delivered, and blocks access to potentially malicious websites in real time.

The Web Reputation report displays blocked and visited site reports. Click each tab to view each related list.



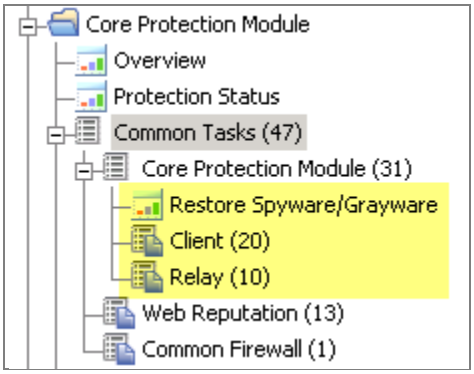
Part Five

Common Tasks

You can start and stop scans, upload specific files from your endpoints to your Tivoli Endpoint Manager server, and enable or disable a Client Dashboard by using CPM tasks. Common Tasks content is organized into three categories: Core Protection Module, Web Reputation, and Common Firewall.

Core Protection Module tasks

The Core Protection Module subnode of Common Tasks includes a Restore Spyware/Grayware dashboard, and two additional subnodes for client- and relay-related tasks.



Client Tasks Overview

Using the Client Task subnode, you can perform the following actions:

- Start and stop scans
- Upload logs and quarantined files
- Enable and disable the Client Dashboard
- Enable and disable Smart Scan
- Set the Maximum Behavior Monitor Report
- Upgrade the Client Dashboard
- Perform quarantine file maintenance
- Enable and disable Certified Safe Software Service
- Enable and disable Unauthorized Change Prevention
- Enable and disable Smart Protection Server connection
- Set Virus Outbreak time interval
- Set Maximum virus report count
- Set Maximum spyware report count

Relay Tasks Overview

Using the Relay Tasks subnode, you can perform the following actions:

- Set Maximum Concurrent updating of virtual desktops
- Set Maximum Concurrent scanning of Virtual Desktops
- Enable and disable switching to Smart Protection Servers when uplink fails
- Enable and disable switching to Smart Protection networks when uplink fails
- Configure IIS as Web Server
- Improper VDI Component Service Status
- Purge Smart Protection Relay Error Logs
- Network Bandwidth Throttling

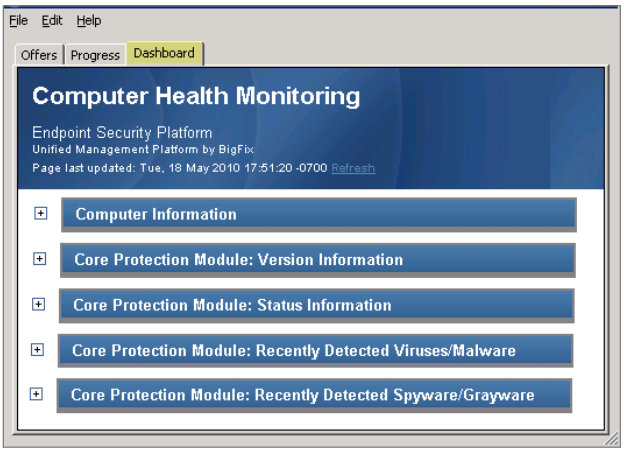
The most common of these tasks are described below:

Scanning

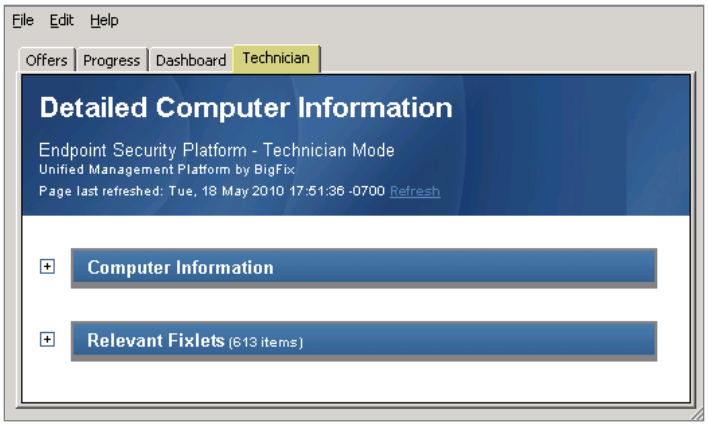
To start or stop an On-Demand scan, use the *Common Tasks* node of the navigation tree, or create a custom *Scan* Now task using the *On-Demand Scan Settings* wizard under the Configuration node. By creating custom *Scan Now* tasks, you can configure an On-Demand scan to run on a regular basis, for example, 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 is visible to users. If enabled, you see an icon in the system tray in the bottom right corner of your screen. Click the icon to display the client UI, which now has a new dashboard tab. The Client Dashboard displays computer information, version information about your CPM deployment, status information (for example, the last time a scan was run or pattern was updated), and recently-detected spyware and viruses.



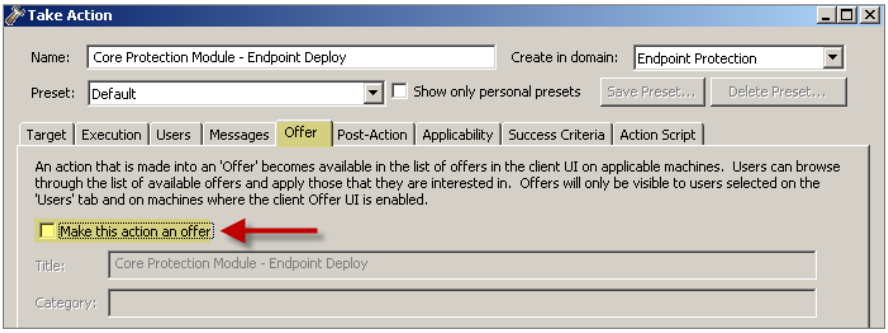
A related dashboard, called the Technician Dashboard, is also available after enabling the client dashboard by hitting “Control-Alt-Shift-T”. The Technician Dashboard provides additional technical information about the endpoint, including sections for Computer and Relevant Fixlets.



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

Client Offers

You can offer users actions that they can select at their own discretion (also referred to as user self-provisioning). For example, you can issue offers to allow users to initiate tasks themselves. Access the *Offers* capability from the Take Action dialog from any Fixlet.



For more information about making offers, see the Dialogs section of the Tivoli Endpoint Manager Console Operator's Guide.

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

Uploading quarantined files

Quarantined malware is stored on the endpoint for further analysis. To further investigate 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

You can 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 different 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.

For information about tasks not listed here, see the Common Tasks subnode in the CPM CPM navigation tree.

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 cleanup by intercepting malware before it reaches your users' computers. Specifically, Web Reputation monitors outbound web requests, stops web-based malware before it is delivered, and blocks user 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 related Knowledge Base article for details about how to migrate policies from Web Protection Module to the Web Reputation component of CPM.*

Setting security levels

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

The following security levels determine if and how Web Reputation allows or blocks access to a URL:

High	Blocks URLs that are unrated and very likely to be a web threat
Medium	Blocks URLs that are unrated and likely to be a web threat
Low	Blocks only URLs that are a web threat

In the Actions box, click next to your chosen security level (high, medium, or low) 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 defaults 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 or 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, you must use this task to archive logs, otherwise the log files are never 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 might be required.

> ***Note:*** *The proxy server password must be encrypted for this action. The task window provides 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.

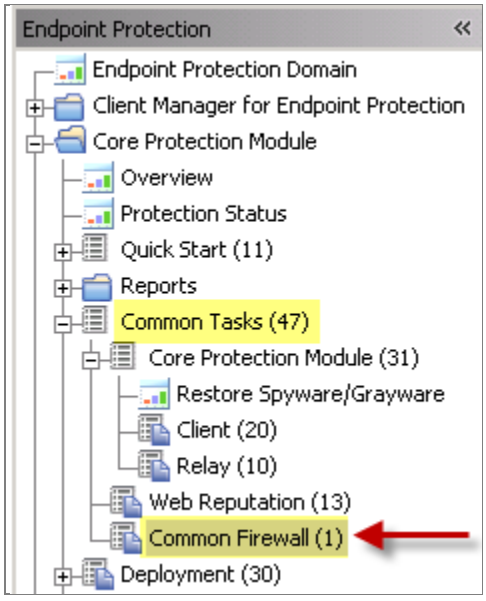
Enable/Disable collection of visited sites

Take this action to stop the collection of visited sites information. Visited sites information exists on the endpoint, but is not transferred to the Tivoli Endpoint Manager Server via the Web Reputation – Site Statistics analysis.

Common Firewall tasks

Uploading firewall logs

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



Part Six

Support

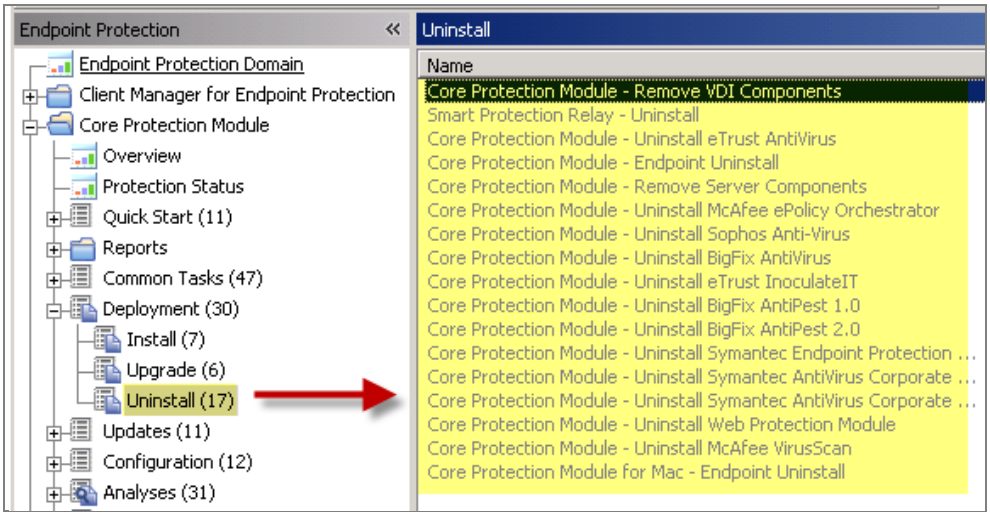
Troubleshooting

Some options in the Troubleshooting node resolve issues identified in the Protection Status Chart in the Overview report. Other audit Fixlets detect computers that are ineligible for a CPM installation:

The remaining Fixlets identify computers where services are not running or not configured correctly, and computers that require a reboot. This node also contains a task to disable the Windows Firewall, which might be required for the Common Firewall component to work correctly.

Uninstalling CPM

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



After removing all binary components, you must also stop any open CPM policy actions and client offers that you have issued.

Frequently asked questions

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

- Relevant to at least one Fixlet, task, or 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 three categories in the legend?

The Endpoint Health Status chart includes 11 categories shown below. If not all are displayed, expand 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 section of the Global Settings wizard, located in the Configuration node. This feature allows you to report spyware to view infection reports and set appropriate exclusions.

Can I automatically flow updates through clients without operator approval?

Yes. However, you must manually enable Automatic Updates. For more information, see 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 users monitor infection information?

Enable 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 only scans 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 you can configure the wizards with customized parameters, for example, you can 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?

Trend ActiveUpdate Server (TMAU) is Trend's "In the Cloud" server from which the Tivoli Endpoint Manager server downloads pattern set files.

Technical support

BigFix technical support site offers a number of specialized support options to help you learn, understand, and optimize your use of this product:

- BigFix Support Site
- Documentation
- Knowledge Base
- Forums and Communities

Part Seven

Notices

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

TRADEMARKS:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

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

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