ePolicy Orchestrator - McAfee Virtual Technician 1.0

Walkthrough Guide

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Introducing ePolicy Orchestrator - McAfee Virtual Technician

ePolicy Orchestrator - McAfee Virtual Technician (ePO-MVT) collects system specifications such as information regarding McAfee products, operating system, browser, physical memory, and system architecture from your computer to diagnose and resolve any problems related to your McAfee software. It helps resolving any deviations in McAfee product that may have occurred since you have installed the product.

ePO-MVT integrates with McAfee ePolicy Orchestrator version 4.0 (patch 5 minimum) or 4.5 which provides a single point of control for all the systems.

Contents

ePO-MVT features

- **Centralized management** — Provides support for deploying and managing ePO-MVT on managed nodes using ePolicy Orchestrator.
- **Health check and remediation** — Allows you to diagnose and/or resolve issues in McAfee product as required.
- **Selective remediation** — Allows you to select deviations to be resolved in required product or component.
- **Override ageing of content** — Allows you to run health check and resolve any deviations in McAfee product even if MVT content is not updated.
- **Upload health check report** — Allows you to upload the health check report to MVT server from an ePolicy Orchestrator server or a managed node.
- **Pre-defined queries** — Allows you to run pre-defined queries which query the ePolicy Orchestrator database and generate an output in tabular format.
- **Purge MVT results** — Allows you to delete the selected instance of query result from ePolicy Orchestrator server.
- **Pre-defined notifications** — Alerts you when MVT or a supported McAfee product installed on managed node is unhealthy.
- **Policy management** — Allows ePO administrator to enforce policies on managed nodes, which define user permissions and product patch to be used.

- **Reporting on client system** — Provides managed node users with HealthCheck reports and a log which lists the deviations in the McAfee products.

System requirements

Prerequisites for ePO-MVT managed node:

Item	Requirements
Operating system	• Windows 2000 Server with Service Pack 4 or later • Windows 2000 Advanced Server with Service Pack 4 or later • Windows Server 2003 Enterprise (32 bit and 64 bit) with Service Pack 2 or later • Windows Server 2003 Standard (32 bit and 64 bit) with Service Pack 2 or later • Windows Server 2003 Web with Service Pack 2 or later • Windows Server 2008 Enterprise edition (32 bit and 64 bit) • Windows Server 2008 Standard edition (32 bit and 64 bit) • Windows Server 2003 R2 Enterprise with Service Pack 2 or later • Windows Server 2003 R2 Standard with Service Pack 2 or later • Windows XP Home with Service Pack 3 or later • Windows XP Professional with Service Pack 3 or later • Windows 2000 Professional with Service Pack 4 or later • Windows Vista with latest service pack (32 bit and 64 bit) • Windows 7 (32 bit and 64 bit)
Browser supported	• Microsoft Internet Explorer 6 or later • Mozilla firefox 2.0 or later

About this guide

This guide provides detailed instructions for installing and configuring ePO-MVT.

Default instructions in this guide refer to ePolicy Orchestrator 4.0. However, appropriate notes have been provided if you are using ePolicy Orchestrator 4.5.

To use this guide effectively, you must be familiar with ePolicy Orchestrator versions 4.0 and/or 4.5. For more information, see ePolicy Orchestrator product documentation.

Target Audience

This guide is intended for ePolicy Orchestrator administrators.

Downloading ePO-MVT

To download ePO-MVT packages, use the McAfee WebMER site.

1. Go to http://mer.mcafee.com/enduser/downloadepomvt.aspx.
2. Accept the license agreement, select the required package from the **Select your option to be downloaded** drop-down list then click **Download**.

Installing ePO-MVT

This chapter describes how to install ePO-MVT using McAfee ePolicy Orchestrator management software version 4.0 and 4.5. To use this chapter effectively, you need to be familiar with ePolicy Orchestrator.

NOTE: This document does not provide detailed information about installing or using ePolicy Orchestrator software. See the McAfee ePolicy Orchestrator product documentation for more information.

Topic covered in this chapter:

- Installing using ePolicy Orchestrator

Installing using ePolicy Orchestrator

ePolicy Orchestrator provides a scalable platform for centralized policy management and enforcement of your security products on the managed nodes. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

Tasks

- Checking in the ePO-MVT package
- Installing the ePO-MVT extension
- Installing the ePO help extension
- Deploying ePO-MVT on managed nodes
- Uninstalling ePO-MVT from managed nodes
- Removing ePO-MVT deployment package
- Removing the product extension

Checking in the ePO-MVT package

Use this task to check in the ePO-MVT deployment package to the master repository.

Task

For option definitions, click **?** in the interface.

1. Copy the **epomvt_Deployment** archive to a temporary location of your ePolicy Orchestrator computer.
2. Log on to the ePolicy Orchestrator server as an administrator.

3 Click **Software** | **Master Repository** | **Check In Package**. The Check In Package wizard appears.

NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Software** | **Master Repository**, then click **Actions** | **Check In Package**.

4 In the Package page, select the **Package type** as **Product or Update (.ZIP)** and browse in **File path** to locate **epomvt_Deployment** saved in a temporary folder.

5 Click **Next**. The Package Options page appears with the package information.

6 Click **Save**.

Installing the ePO-MVT extension

Use this task to install the ePO-MVT extension. The extension file is in .ZIP format.

NOTE: The ePO-MVT product extension must be installed before checking in the ePO-MVT content update package. Refer *Updating ePO-MVT content* for more details.

Task

For option definitions, click **?** in the interface.

1 Copy the **epomvt_Extension** archive to a temporary location of your ePolicy Orchestrator computer.

2 Log on to the ePolicy Orchestrator server as an administrator.

3 Click **Configuration** | **Extensions** | **Install Extension**. The Install Extension dialog box appears.

NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Software** | **Extensions** | **Install Extension**.

4 Click **Browse** to locate the extension file **epomvt_Extension**, then click **OK**. The Install Extension page appears with the extension name and version details.

5 Click **OK**.

Installing the ePO help extension

You can install the ePO help extension separately on the ePolicy Orchestrator 4.5 server using the **Software** tab. The Help extension is a .ZIP file.

NOTE: Help extensions can not be installed on ePolicy Orchestrator 4.0.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator

2 Click **Menu** | **Software** | **Extensions** | **Install Extension**. The Install Extension dialog box appears.

3 Click **Browse**, then select the extension file help_epomvt_100.ZIP, then click **OK**. The Install Extension page appears with the extension name and version details.

4 Click **OK**.

Deploying ePO-MVT on managed nodes

Use this task to deploy ePO-MVT on the managed nodes. ePolicy Orchestrator allows you to create tasks to deploy product on a single node, or on groups of the system tree.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Systems | System Tree | Client Tasks**, select the required group in the System Tree, then click **New Task**. The Client Task Builder wizard appears.

   NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Systems** | **System Tree** | **Client Tasks**, select the required group in the System Tree, then click **Actions** | **New Task**.

3. In the Description page, type a **Name** for the task, **Notes** (optional), select the **Type** as **Product Deployment (McAfee Agent)**, then click **Next**.
4. In the Configuration page, select **Target Platforms** as **Windows**, **Products and components** as **ePO-MVT 1.0.X.0**, **Action** as **Install**. Select an appropriate **Language**, then click **Next**.
5. Schedule the task to run immediately or as required, then click **Next** to view a summary of the task.
6. Review the summary of the task, then click **Save.** The task is added to the list of client tasks for the selected group and any group that inherits the task.
7. Send an agent wake-up call.

Uninstalling ePO-MVT from managed nodes

Use this task to uninstall ePO-MVT from managed nodes.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Systems | System Tree | Client Tasks**, select the desired group in the System Tree, then click **New Task**. The Client Task Builder wizard appears.

   NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Systems** | **System Tree** | **Client Tasks**, select the required group in the System Tree, then click **Actions** | **New Task**.

3. In the Description page, type a **Name** for the task, **Notes** (optional), select the **Type** as **Product Deployment (McAfee Agent)**, then click **Next**.
4. In the Configuration page, select **Target Platforms** as **Windows**, **Products and components** as **ePO-MVT 1.0.X.0**, **Action** as **Remove**. Select an appropriate **Language**, then click **Next**.
5. Schedule the task to run immediately or as required, then click **Next** to view a summary of the task.
6. Review the summary of the task, then click **Save**.
7. Send an agent wake-up call.

Removing ePO-MVT deployment package

Use this task to remove the ePO-MVT deployment package from the ePolicy Orchestrator.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Software** | **Master Repository**.

   NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Software** | **Master Repository**.

3. Click the **Delete** link of the **ePO-MVT** package.
4. Click **OK** on the Delete Package page.

Removing the product extension

Use this task to remove the product extension from the ePolicy Orchestrator server.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Configuration** | **Extensions**.

   NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Software** | **Extensions**.

3. Select the ePO-MVT extension file, then click **Remove**.
4. Select **Force removal, bypassing any checks or errors**, then click **OK**.

Configuring ePO-MVT

This chapter describes how to configure ePO-MVT using McAfee ePolicy Orchestrator.

Topics covered in this chapter are:

Working with client tasks

ePolicy Orchestrator allows you to create and schedule client tasks that run on managed systems.

You can define tasks for the entire System Tree, for a specific group, or for an individual system. Client tasks are inherited from parent groups in the System Tree.

Client tasks are commonly used for:

- Product deployment
- Product functionality (for example, the VirusScan Enterprise On-Demand Scan task)
- Upgrades and updates

ePO-MVT supports two client tasks:

- **MVT Diagnostic task** — This task can be configured either to diagnose or to diagnose and resolve issues in the supported product(s).
- **MVT Remediate task** — This task can be configured to diagnose and resolve issues in the supported product(s) or required component(s).

Tasks

- Creating a MVT Diagnostic task
- Creating a MVT Remediate task

Creating a MVT Diagnostic task

You can schedule multiple diagnostic tasks to run immediately, at specific times, or at regularly-scheduled intervals across managed nodes.

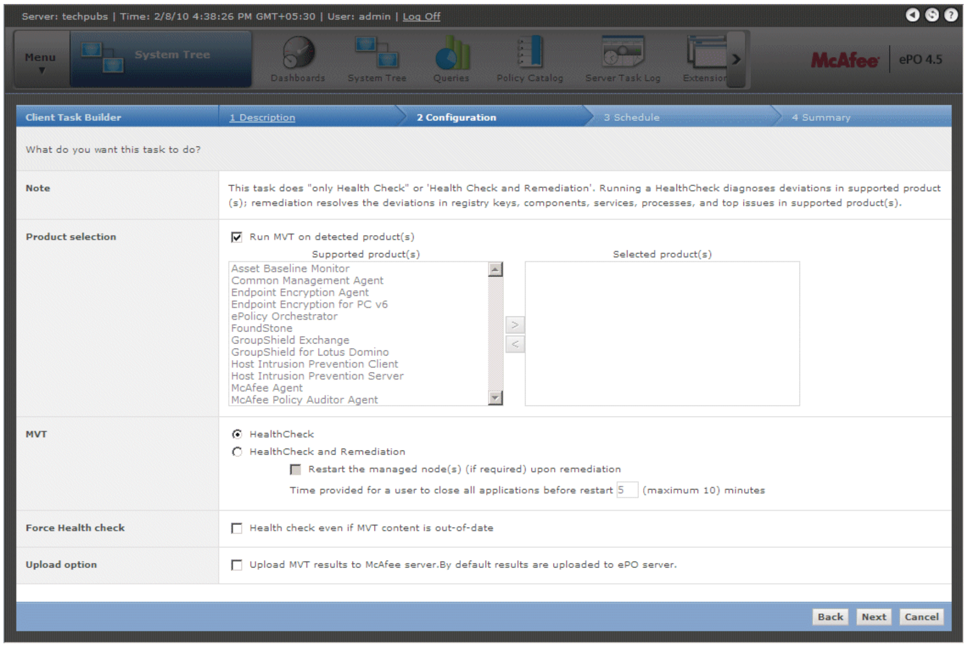
Task

For option definitions, click **?** in the interface.

1. Click **Systems** | **System Tree** | **Client Tasks**, select the desired group in the System Tree, then click **New Task**. The Client Task Builder wizard appears.

   NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Systems** | **System Tree** | **Client Tasks**, select the desired group in the System Tree, then click **Actions** | **New Task**.

2. In the Description tab, type a name and add any notes for the diagnose task.
3. Select the task type as **MVT Diagnostic Task (ePO-MVT 1.0)**, then click **Next**. The Configuration tab appears.



What do you want this task to do?

Note: This task does "only Health Check" or 'Health Check and Remediation'. Running a HealthCheck diagnoses deviations in supported product (s); remediation resolves the deviations in registry keys, components, services, processes, and top issues in supported product(s).

Product selection: ☑ Run MVT on detected product(s)

Supported product(s):
Asset Baseline Monitor
Common Management Agent
Endpoint Encryption Agent
Endpoint Encryption for PC v6
ePolicy Orchestrator
FoundStone
GroupShield Exchange
GroupShield for Lotus Domino
Host Intrusion Prevention Client
Host Intrusion Prevention Server
McAfee Agent
McAfee Policy Auditor Agent

Selected product(s):

MVT: ● HealthCheck
○ HealthCheck and Remediation
□ Restart the managed node(s) (if required) upon remediation
Time provided for a user to close all applications before restart 5 (maximum 10) minutes

Force Health check: □ Health check even if MVT content is out-of-date

Upload option: □ Upload MVT results to McAfee server.By default results are uploaded to ePO server.

4. Configure these options as required.

Option	Definition
Product selection	• **Run MVT on detected products** — Select this option to run MVT on managed nodes to diagnose and resolve issues in all the detected products. • Select and add the supported products to diagnose and resolve issues in the selected products.
MVT	• **HealthCheck** — Select this option to diagnose issues in the detected or selected product(s) and report them to ePolicy Orchestrator sever. • **HealthCheck and Remediation** — Select this option to diagnose and resolve issues in the detected or selected product(s) and report them to ePolicy Orchestrator sever. • **Restart the managed node (if required) upon remediation** — Select this option to restart the managed node (if required, to complete remediation) after resolving the issues in the detected or selected product(s). • **Time provided for a user to close all applications before restart** — Specify the time in minutes within which the user should

Option	Definition
	close all applications before restarting the node. The maximum time that can be set is 10 minutes.
Force Health check	**Health check even if MVT content is out-of date** — Select this option to diagnose issues in the detected or supported product(s) even if the MVT content is not updated. NOTE: If MVT content is not updated regularly, it may not be able to diagnose and resolve any new issues in the product.
Upload option	**Upload MVT results to McAfee server. By default results are uploaded to ePO server.** — Select this option to upload the diagnostic results to the McAfee server. This result can be further used by the Technical Support representative to help you resolve the issue (if required).

5 Click **Next** and schedule the task as required.

6 Click **Next** to review the summary of the diagnose task.

7 Click **Save**, then send an agent wake-up call.

Creating a MVT Remediate task

You can schedule multiple remediate tasks to run immediately, at specific times, or at regularly-scheduled intervals across managed nodes.

Task

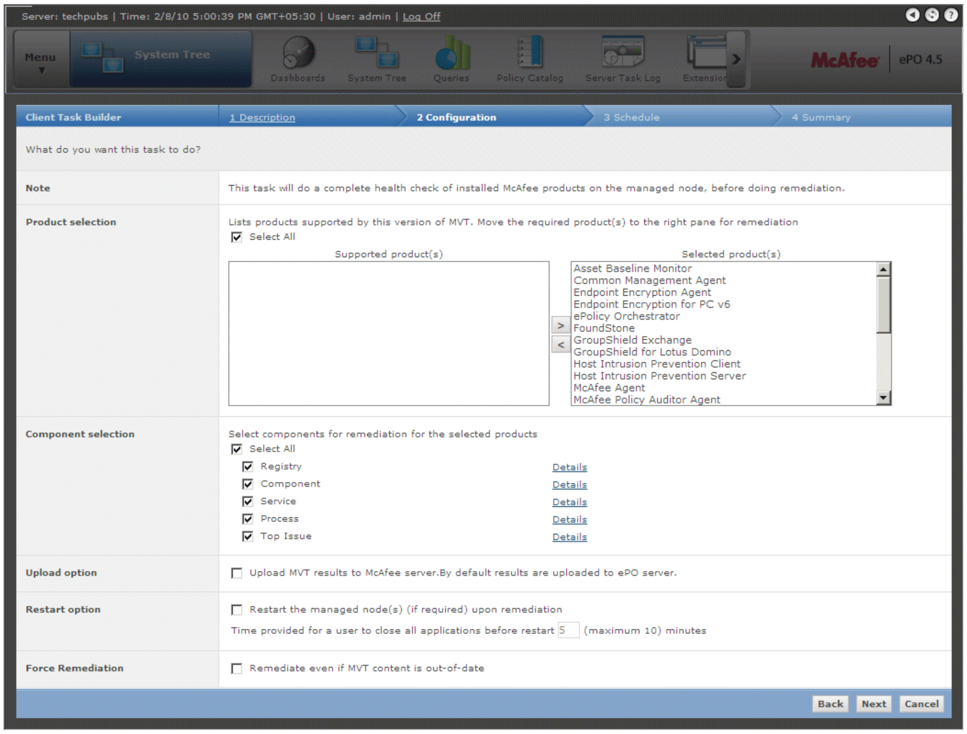
For option definitions, click **?** in the interface.

1 Click **Systems** | **System Tree** | **Client Tasks**, select the desired group in the System Tree, then click **New Task**. The Client Task Builder wizard appears.

NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Systems** | **System Tree** | **Client Tasks**, select the desired group in the System Tree, then click **Actions** | **New Task**.

2 In the Description tab, type a name and add any notes for the remediate task.

3 Select the task type as **MVT Remediation Task (ePO-MVT 1.0)**, then click **Next**. The Configuration tab appears.



Client Task Builder | 1 Description | 2 Configuration | 3 Schedule | 4 Summary

What do you want this task to do?

Note — This task will do a complete health check of installed McAfee products on the managed node, before doing remediation.

Product selection — Lists products supported by this version of MVT. Move the required product(s) to the right pane for remediation

☑ Select All

Supported product(s)

Selected product(s): Asset Baseline Monitor, Common Management Agent, Endpoint Encryption Agent, Endpoint Encryption for PC v6, ePolicy Orchestrator, FoundStone, GroupShield Exchange, GroupShield for Lotus Domino, Host Intrusion Prevention Client, Host Intrusion Prevention Server, McAfee Agent, McAfee Policy Auditor Agent

Component selection — Select components for remediation for the selected products

☑ Select All

- ☑ Registry — Details
- ☑ Component — Details
- ☑ Service — Details
- ☑ Process — Details
- ☑ Top Issue — Details

Upload option — □ Upload MVT results to McAfee server.By default results are uploaded to ePO server.

Restart option — □ Restart the managed node(s) (if required) upon remediation

Time provided for a user to close all applications before restart 5 (maximum 10) minutes

Force Remediation — □ Remediate even if MVT content is out-of-date

Back | Next | Cancel

4 Configure these options as required.

Option	Definition
Product selection	• **Select all** — Select this option to diagnose and resolve issues in all the listed products. • Select and add the supported products to diagnose and resolve issues.
Component selection	• **Select all** — Select this option to remediate all the listed components. ◦ **Registry** — Select this option to remediate issues in registry keys related to selected product(s). Click **Details** to select the required registry keys. ◦ **Component** — Select this option to remediate issues in Component Object Model (COM) components related to selected product(s). Click **Details** to select the required COM components. ◦ **Process** — Select this option to remediate issues in processes related to selected product(s). Click **Details** to select the required process. ◦ **Service** — Select this option to remediate issues in services related to selected product(s). Click **Details** to select the required services. ◦ **Top Issue** — Select this option to remediate top issues related to selected product(s). Click **Details** to select the required top issues. NOTE: ePO-MVT does not support file remediation.
Upload option	**Upload MVT results to McAfee server. By default results are uploaded to ePO server.** — Select this option to upload the diagnostic results to the McAfee server. This result can be

Option	Definition
	further used by the Technical Support representative to help you resolve the issue (if required).
Restart option	• **Restart the managed node (if required) upon remediation** — Select this option to restart the managed node (if required, to complete remediation) after resolving the issues in products. • **Time provided for a user to close all applications before restart** — Specify the time in minutes within which the user should close all applications before restarting the node. The maximum time that can be set is 10 minutes.
Force Remediation	**Remediate even if MVT content is out-of date** — Select this option to diagnose and resolve issues in the supported product(s) even if the MVT content is not updated. NOTE: If MVT content is not updated regularly, it may not be able to diagnose and resolve new issues in the product.

5 Click **Next** and schedule the task as required.

6 Click **Next** to review the summary of the remediate task.

7 Click **Save**, then send an agent wake-up call.

Setting policies with ePolicy Orchestrator

A policy is a collection of settings that you create, configure, then enforce. Policies ensure that the managed security software products are configured and perform accordingly.

The ePolicy Orchestrator allows you to configure ePO-MVT policies from a central location.

ePO-MVT supports two policies:

- Patch Selection — This policy can be configured to select product patch for which ePO-MVT should diagnose and remediate deviations. If you do not select any patch, default patch settings are applied.
- User Permission — This policy can be configured to assign managed node users permission to allow remediation, upload results to McAfee Server, upload results to ePO Server and set the content aging of ePO-MVT.

Creating Patch Selection policy

Use this task to create a Patch Selection policy.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Systems** | **Policy Catalog**. The Policy Catalog page appears.

NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Policy** | **Policy Catalog**.

3 Select **Product** as **ePO-MVT 1.0.X** and **Category** as **ePO-MVT Policies**.

4 Click **New Policy**. The Create a new policy dialog box appears.

NOTE: If you are using ePolicy Orchestrator 4.5, click **Action** | **New Policy**.

5 Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list, type a name, then click **OK**.

6 On the Patch Selection tab, select the product and its patch for which ePO-MVT must diagnose and remediate deviations, then click **Save**. If you have not selected any patch for the product, default patch settings will be applied to managed nodes.

NOTE: By default ePO-MVT diagnoses the managed node for deviations in the latest patch released for McAfee products.

Creating User Permission policy

Use this task to create a User Permission policy. This policy defines managed node user permissions.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Systems** | **Policy Catalog**. The Policy Catalog page appears.

NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Policy** | **Policy Catalog**.

3 Select **Product** as **ePO-MVT 1.0.X** and **Category** as **ePO-MVT Policies**.

4 Click **New Policy**. The Create a new policy dialog box appears.

NOTE: If you are using ePolicy Orchestrator 4.5, click **Action** | **New Policy**.

5 Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list, type a name then click **OK**.

6 On the User Permission tab, set appropriate permissions for users.

7 Select the age of ePO-MVT content after which the user will not be able to run ePO-MVT from the managed node.

8 Click **Save**.

Reporting

ePolicy Orchestrator ships with its own querying and reporting capabilities. These are highly customizable, flexible and easy to use. Included is the Query Builder wizard, which creates and runs queries that result in user-configured data in user-configured charts and tables.

Reports are pre-defined queries which query the ePolicy Orchestrator database and generate a graphical output. You can create, edit and manage queries through ePolicy Orchestrator.

ePolicy Orchestrator provides the following reports for ePO-MVT:

- **MVT Health Information** — Reports product status after healthcheck and/or remediation, MVT health status, MVT client tasks status, and MVT diagnose result upload status.

- **MVT Deviations** — Reports deviations in the product (with product name and version) and number of managed nodes having the same deviation.

NOTE: For instructions on creating, editing or deleting queries, see ePolicy Orchestrator product documentation.

ePO-MVT also enables users to view HealthCheck results and list of deviations in products from managed nodes.

▸ Running a query

▸ Viewing query result

▸ Viewing reports on managed nodes

Running a query

Use this task to run a pre-defined query on ePolicy Orchestrator server.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Reporting**. A list of queries appear on the left pane.

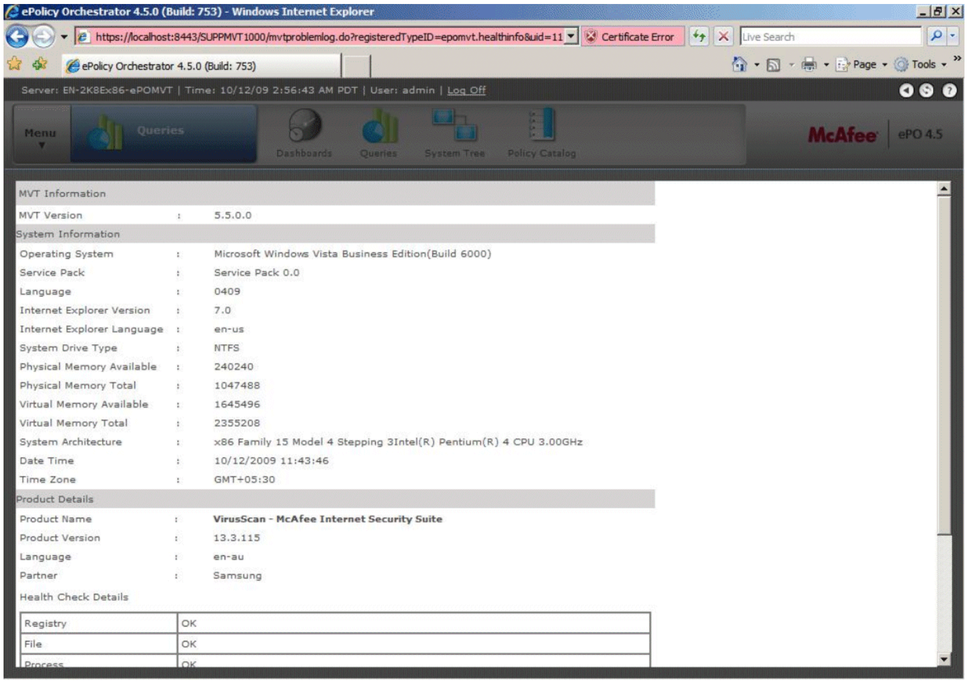
   NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Reporting** | **Queries**.
3. Select a ePO-MVT related query from the list.
4. Click **Run**. The graphical output is displayed.
   You can delete the MVT Health Information query result or upload it to the McAfee server as required.
   To delete the MVT Health Information query result, on the query result page select the required row, then click **Actions** | **Purge**.

   To upload the MVT Health Information query result to McAfee server, on the result page click **Actions** | **Upload MVT results**.

Viewing query result

On the query result page, click on the required row to view more details on the query.

- MVT Health Information query result — On the MVT Health Information query result page, click on the required row to view health information details including product name with their issues and whether it was fixed or not. Click **More** to view MVT details, managed node details, and product details.


ePolicy Orchestrator 4.5.0 (Build: 753) - Windows Internet Explorer
https://localhost:8443/SUPPMVT1000/mvtproblemlog.do?registeredTypeID=epomvt.healthinfo&uid=11
Certificate Error
Live Search
ePolicy Orchestrator 4.5.0 (Build: 753)
Page
Tools
Menu
Queries
Dashboards
Queries
System Tree
Policy Catalog
McAfee
ePO 4.5

Server: EN-2K8Ex86-ePOMVT | Time: 10/12/09 2:56:43 AM PDT | User: admin | Log Off

MVT Information

MVT Version	:	5.5.0.0

System Information

Operating System	:	Microsoft Windows Vista Business Edition(Build 6000)
Service Pack	:	Service Pack 0.0
Language	:	0409
Internet Explorer Version	:	7.0
Internet Explorer Language	:	en-us
System Drive Type	:	NTFS
Physical Memory Available	:	240240
Physical Memory Total	:	1047488
Virtual Memory Available	:	1645496
Virtual Memory Total	:	2355208
System Architecture	:	x86 Family 15 Model 4 Stepping 3Intel(R) Pentium(R) 4 CPU 3.00GHz
Date Time	:	10/12/2009 11:43:46
Time Zone	:	GMT+05:30

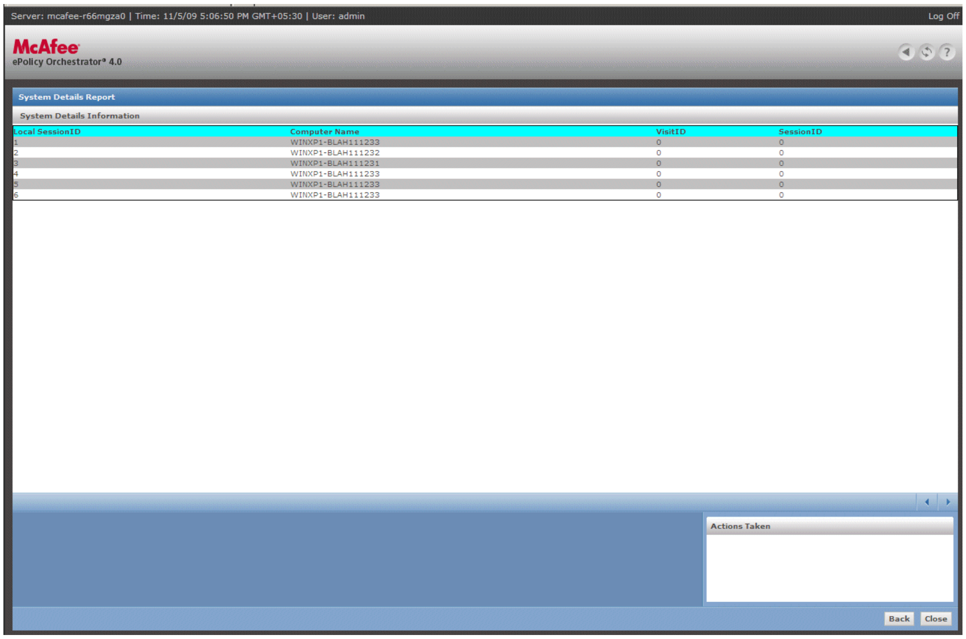
Product Details

Product Name	:	**VirusScan - McAfee Internet Security Suite**
Product Version	:	13.3.115
Language	:	en-au
Partner	:	Samsung

Health Check Details

Registry	OK
File	OK
Process	OK

- MVT Deviations — On the MVT Deviations query result page, click on the required row to view deviation details including the managed node name, session ID, and execution ID.



Server: mcafee-r66mgza0 | Time: 11/5/09 5:06:50 PM GMT+05:30 | User: admin

System Details Report

System Details Information

Local SessionID	Computer Name	VisitID	SessionID
1	WINXP1-BLAH111233	0	0
2	WINXP1-BLAH111232	0	0
3	WINXP1-BLAH111231	0	0
4	WINXP1-BLAH111233	0	0
5	WINXP1-BLAH111233	0	0
6	WINXP1-BLAH111233	0	0

Viewing reports on managed nodes

ePO-MVT enables users to view HealthCheck results and issue details of last ePO-MVT task on the managed nodes.

MVT Final Report — Displays a brief summary of last MVT task including the problems found and fixed. Click **Start** | **Programs** | **McAfee** | **MVT Final Report** to access Final Report.

MVT Problem Log — Displays a detailed report of the deviations found in products installed on that managed node. Click **Start** | **Programs** | **McAfee** | **MVT Problem Log** to access Problem Log.

Updating ePO-MVT content

To check in client ePO-MVT content update package in ePO server, download the package from http://mer.mcafee.com/enduser/downloadepomvt.aspx then check in the package into Master Repository.

You can also use the **Pull Now** task to check ePO-MVT content updates from a common updater website in to the master repository immediately. Refer to *ePolicy Orchestrator Product Guide* for details.

Use this task to update ePO-MVT content on managed nodes.

Task

For option definitions, click **?** in the interface.

1. Click **Systems** | **System Tree** | **Client Tasks**, select the desired group in the System Tree, then click **New Task**. The Client Task Builder wizard appears.

   NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu** | **Systems** | **System Tree** | **Client Tasks**, select the desired group in the System Tree, then click **Actions** | **New Task**.

2. In the Description tab, type a name and add any notes for the update task.
3. Select the task type as **Update (McAfee Agent)**, then click Next. The Configuration tab appears.

   NOTE: If you are using ePolicy Orchestrator 4.5, then select **Product Update** as task type.

4. Select the package type as **ePO-MVT Content**, then click **Next**. The Schedule page appears.
5. Configure the schedule details as needed, then click **Next**.
6. Review the task settings, then click **Save**.

Setting up Notifications using ePolicy Orchestrator 4.0

ePolicy Orchestrator Notifications feature alerts you to events that occur on your managed systems or on the ePolicy Orchestrator server. You can configure notification rules in ePolicy Orchestrator to send email messages or SNMP traps, as well as run external commands when specific events are received and processed by the ePolicy Orchestrator server. The ability to specify the event categories that generate a notification message and the frequencies with which such messages are sent are highly configurable.

ePO-MVT supports two notifications:

- **Unhealthy MVT detected** — This can be configured to send notification when MVT installed on any managed node is unhealthy.

- **Unhealthy McAfee Product(s) detected** — This can be configured to send notification when unhealthy McAfee product(s) are detected on managed nodes.

Use these tasks to create and configure notifications.

Before using this feature, you must:

- Notifications permissions — Create or edit permission sets and ensure they are assigned to the appropriate users.
- Email server — Configure the email (SMTP) server at **Configuration | Server Settings**.
- Email contacts list — Specify the list from which you select recipients of notification messages at **Configuration | Contacts**.

NOTE: Refer ePolicy Orchestrator product documentation for more details.

Tasks

▶ Describing the rule
▶ Setting filters for the rule
▶ Setting thresholds of the rule
▶ Configuring the notifications for the rule

Describing the rule

Use this task to configure the Description tab on the Notification Rule Builder wizard.

Task

For option definitions click **?** on the page displaying the options.

1. Click **Automation | Notification Rules**, then click **New Rule**. The Notification Rule Builder wizard appears.
2. In the Description tab, type a unique name and add any notes for the rule.
3. Click **...** next to **Defined at**, then select the required system tree group to which the rule applies.
4. Set the priority of the rule to **High**, **Medium**, or **Low** as required.

   NOTE: The priority of the rule is used to set a flag on an email message in the recipient's Inbox. The priority does not affect the rule or event processing in any way.

5. Enable or disable the rule as required, then click **Next**.

Setting filters for the rule

Use this task to set the filters for the notification rule on the **Filters** page of the **Notification Rule Builder** wizard.

Task

For option definitions click **?** on the page displaying the options.

1. Select the types of **Operating systems** from which events can trigger the rule.
2. Select **ePO-MVT** as the **Product**.
3. Select the required **Categories** of events that initiate this rule.

- **Unhealthy MVT detected** — Select this option to trigger the notification rule when MVT installed on any managed node is unhealthy.
- **Unhealthy McAfee Product(s) detected** — Select this option to trigger the notification rule when unhealthy McAfee product(s) are detected on managed nodes.

4 In **Threat name**, define the pattern matching the threat comparison to use:

  a Select an operator from the drop-down list.

  b Type any text for the operator to act on.

  NOTE: If you select to filter on a threat name, the **Products**, **Categories**, and the **Threat name** selections must all be true for the rule to send a notification message.

5 Click **Next**.

Setting thresholds of the rule

Use this task to define when the event triggers the rule on the **Thresholds** tab of the Notification Rule Builder wizard.

A rule’s thresholds are a combination of aggregation and throttling.

Task

For option definitions click **?** on the page displaying the options.

1 Select whether to **Send a notification for every event**, or to **Send a notification if multiple events occur within** a defined amount of time in minutes, hours, or days.

2 If you selected **Send a notification if multiple events occur within**, you can choose to send a notification when any of these conditions are met.

- **When the number of affected systems is at least** — To send notification when the specified number of affected systems is reached.
- **When the number of events is at least** — To send notification when the specified number of events is reached.

3 Select **At most, send a notification every**, then define the time that must be passed before this rule can send notification message again. You can specify the duration in minutes, hours, or days.

4 Click **Next**.

Configuring the notifications for the rule

Use this task to configure the notifications that are triggered by the rule on the **Notifications** page of the **Notification Rule Builder** wizard. The size of the message depends on the target, the type of message, and the number of recipients of the message.

You can configure the rule to trigger multiple messages by using the **+** and **-** buttons.

Task

For option definition click **?** on the page displaying the options.

1 If you want the notification message to be sent as an email, select **Email Message** from the drop-down list.

2. Next to **Recipients**, click **...** and select the recipients for the message. This list of available recipients is taken from Contacts (**Configuration | Contacts**). Alternatively, you can manually type email addresses separated by a comma.
3. Type the **Subject** line of the message.

   NOTE: You can also insert any of the available variables directly into the subject.
4. Type any text for the **Body** of the message.

   NOTE: You can also insert any of the available variables directly into the body.
5. Select the language in which you want the variables to appear.
6. Click **Next**, or click **+** to add another notification.
7. Review the summary then click **Save**.

The new notification rule appears in the **Notification Rules** list.

Setting Up Automatic Responses using ePolicy Orchestrator 4.5

Automatic Responses use system events to trigger response rules when a specified condition is met. If the conditions of any such rule are met, designated actions are taken, per the configuration defined in the rule. These actions include:

- Send email messages
- Send SNMP traps
- Run external commands
- Schedule server task
- Create issues

This feature is designed to create user-configured notifications and actions when the conditions of a rule are met.

ePO-MVT supports two notifications:

- **Unhealthy MVT detected** — This can be configured to send notification when MVT installed on any managed node is unhealthy.
- **Unhealthy McAfee Product(s) detected** — This can be configured to send notification when unhealthy McAfee product(s) are detected on managed nodes.

Use these tasks to create and configure Automatic Response rules.

Before using this feature, you must:

- Automatic Responses permissions — Create or edit permission sets and ensure that they are assigned to the appropriate ePO users.
- Email server — Configure the email (SMTP) server at **Menu** | **Configuration** | **Server Settings** | **Email Server.**
- Email contacts list — Specify the list from which you select recipients of notification messages at **Menu** | **User Management** | **Contacts**.

Tasks

▸ Describing the rule

- Setting filters for the rule
- Setting thresholds of the rule
- Configuring the action for Automatic Response rules

Describing the rule

Use this task to configure Description tab on the Response Builder wizard.

Task

For option definitions click **?** in the interface.

1. Click **Menu | Automation | Automatic Responses**, then click **Actions | New Response**. The Response Builder wizard opens.
2. On the Description page, type a unique name and any notes for the rule.
3. From the Language drop-down list, select the language the rule uses.
4. Select the **Event group** as **ePO Notification events** and the required **Event type** that trigger this response.
5. Enable or disable the rule as required.
6. Click **Next**.

Setting filters for the rule

Use this task to set the filters for the response rule on the Filters page on the Response Builder wizard.

Task

For option definitions click **?** in the interface.

1. From the Available Properties list,
   a. Click **...** next to **Defined at**, then select the required system tree group to which the rule applies.
   b. Select **Detecting Product** equal to **ePO-MVT**.
   c. Select one of these **Event Description**:
      - **Unhealthy MVT detected** — Select this option to trigger the rule when MVT installed on any managed node is unhealthy.
      - **Unhealthy McAfee Product(s) detected** — Select this option to trigger the rule when unhealthy McAfee product(s) are detected on managed nodes.
2. Click **Next**.

Setting thresholds of the rule

Use this task to define when the event triggers the rule on the Aggregation page of the Response Builder wizard.

A rule’s thresholds are a combination of aggregation, throttling, and grouping.

Task

For option definitions click **?** in the interface.

1. Select whether to **Trigger this response for every event**, or to **Trigger this response if multiple events occur within** a defined amount of time in minutes, hours, or days.
2. If you selected **Trigger this response if multiple events occur within**, you can choose to trigger a response when any of these conditions are met.
   - **When the number of distinct values for an event property is at least a certain value**. This condition is used when a distinct value of occurrence of event property is selected.
   - **When the number of events is at least** — To send notification when the specified number of events is reached.
3. Select whether to group the aggregated events. If you select to group the aggregated events, specify the property of event on which they must be grouped.
4. Select **At most, trigger this response once every** then define the time that must be passed before this rule can send notification message again. You can specify the duration in seconds, minutes, hours, or days.
5. Click **Next**.

Configuring the action for Automatic Response rules

Use this task to configure the responses that are triggered by the rule on the Responses page of the Response Builder wizard.

You can configure the rule to trigger multiple actions by using the **+** and **-** buttons.

Task

For option definition click **?** in the interface.

1. If you want the notification message to be sent as an email, select **Send Email** from the drop-down list.
2. Click **...** then select the recipients for the message. This list of available recipients is taken from Contacts (**Menu | User Management | Contacts**). Alternatively, you can manually type email addresses, separated by a comma.
3. Select the importance of the notification email.
4. Type the **Subject** of the message.

   NOTE: You can also insert any of the available variables directly into the subject.

5. Type any text for the **Body** of the message.

   NOTE: You can also insert any of the available variables directly into the body.

6. Click **Next** or click **+** to add another notification.
7. On the Summary page, verify the information, then click **Save**.

The new response rule appears in the Responses list.

Permission Sets in ePolicy Orchestrator

A permission set is a group of permissions that can be granted to users or Active Directory (AD) groups by assigning it to those users' accounts. One or more permission sets can be assigned to users who are not global administrators (global administrators have all permissions to all products and features).

User accounts and their associated permission sets in ePolicy Orchestrator define the tasks that the users can perform. This allows you to restrict specific users or groups from misusing the ePO-MVT features.

Editing permission sets for user accounts

Use this task to create a permission set. Only global administrators can create permission sets.

Task

For option definitions, click **?** in the interface.

1. Click **Configuration | Permission Sets**. The Permission Set page appears.

   NOTE: If you are using ePolicy Orchestrator 4.5, click **Menu | User Management | Permission Sets**.

2. Click **Edit** next to **ePO-MVT** from the list of Permission Sets on the right pane. The Edit Permission Set page appears.
3. Select the appropriate permission, then click **Save**.

MVT Diagnostic Task - Configuration page

These options allow you to diagnose and resolve issues in detected or selected products. Use this page to configure MVT Diagnostic task for ePO-MVT 1.0.

Option definitions

Option	Definition
Product selection	• **Run MVT on detected products** — Runs MVT on managed nodes to diagnose and resolve issues in all the detected products. • Deselect **Run MVT on detected products** to select the required supported products to diagnose and resolve issues.
MVT	• **HealthCheck** — Diagnoses issues in the detected or selected product(s) and reports them to ePolicy Orchestrator sever. • **HealthCheck and Remediation** — Diagnoses and resolves issues in the detected or selected product(s) and report them to ePolicy Orchestrator sever. • **Restart the managed node (if required) upon remediation** — Restarts the managed node (if required, to complete remediation) after resolving the issues in the detected or selected product(s). • **Time provided for a user to close all applications before restart** — Specifies the time in minutes within which the user should close all applications before restarting the node. The maximum time that can be set is 10 minutes.
Force Health check	**Health check even if MVT content is out-of date** — Diagnoses issues in the detected or supported product(s) even if the MVT content is not updated. NOTE: If MVT content is not updated regularly, it may not be able to diagnose and resolve any new issue in the product.
Upload option	**Upload MVT results to McAfee server. By default results are uploaded to ePO server** — Uploads the diagnostic results to the McAfee server. This result can be further used by the Technical Support representative to help you resolve the issue (if required).

MVT Remediation Task - Configuration page

These options allow you to diagnose and resolve issues in selected products. Remediation task supports **Selective Remediation** that allows you to resolve selected issues in the product. Use this page to configure MVT Remediation task for ePO-MVT 1.0.

Option definitions

Option	Definition
Product selection	• **Select All** — Runs MVT on managed nodes to diagnose and resolve issues in all the products. • Deselect **Select All** to select the required supported products to diagnose and resolve issues.
Component selection	• **Select All** — Remediates all the listed components. • **Registry** — Remediates issues in registry keys related to selected product(s). Click **Details** to select the required registry keys. • **Component** — Remediates issues in Component Object Model (COM) components related to selected product(s). Click **Details** to select the required COM components. • **Service** — Remediates issues in services related to selected product(s). Click **Details** to select the required services. • **Process** — Remediates issues in processes related to selected product(s). Click **Details** to select the required process. • **Top Issue** — Remediates top issues related to selected product(s). Click **Details** to select the required top issues.
Upload option	**Upload MVT results to McAfee server. By default results are uploaded to ePO server.** — Uploads the diagnostic results to the McAfee server. This result can be further used by the Technical Support representative to help you resolve the issue (if required).
Restart option	• **Restart the managed node (if required) upon remediation** — Restarts the managed node (if required, to complete remediation) after resolving the issues in products. • **Time provided for a user to close all applications before restart** — Specifies the time in minutes within which the user should close all applications before restarting the node. The maximum time that can be set is 10 minutes.
Force Remediation	**Remediate even if MVT content is out-of date** — Diagnoses and resolves issues in the supported product(s) even if the MVT content is not updated. NOTE: If MVT content is not updated regularly, it may not be able to diagnose and resolve new issues in the product.

Edit Permission Set: ePO-MVT page

Use this page to define user permissions for configuring ePO-MVT settings.

Option definitions

Option	Definition
Client tasks	• **HealthCheck** — Permits users to schedule and run health check on managed nodes. • **HealthCheck and Remediation** — Permits the user to remediate issues diagnosed in McAfee products installed on managed nodes.
Upload MVT results	• **From managed nodes** — Permits users to upload diagnostic and remediation results from managed nodes to MVT server. • **From ePO server** — Permits users to upload diagnostic and remediation results from ePolicy Orchestrator server to MVT server.
Purge	**Purge result** — Permits users to delete the selected instance of diagnostic and remediation query result from ePolicy Orchestrator server.

Patch Selection page

These options allow you to select the supported product patch. Use this page to configure Patch Selection policy for ePO-MVT 1.0.

Option definitions

Option	Definition
Products	Lists the products for which ePO-MVT diagnoses and resolves issues in the selected product patch.
Patch Level	Lists the patches supported by ePO-MVT for the selected product. By default the latest patch supported by ePO-MVT will be used to diagnose and resolve issues.

User Permission page

These options allow you to set permissions for managed node users. Use this page to configure User Permission policy page for ePO-MVT 1.0.

Option definitions

Option	Definition
User Permission	• **Allow user to perform remediation** — Allows users to resolve issues from the managed node after performing HealthCheck. • **Allow user to upload results to the ePO Server** — Allows managed node users to upload the diagnostic and remediation results to the ePO server. Results are sent to the ePO server as events by McAfee Agent during every Agent-to-Server communication. These results are saved as reports and can be viewed under **Queries** in ePO. • **Allow user to upload result to McAfee** — Allows managed node users to upload the diagnostic and remediation results to the McAfee server. When results are uploaded to the McAfee server, the server generates a Session ID. This Session ID is available in **Final Report** on the managed node and in **Queries** in ePO. The Session ID can be further used by a managed node user or an ePO administrator to contact Technical Support.
Content ageing	**Do not run ePO-MVT if content is older than** — Does not allow the user to run ePO-MVT from a managed node if the content is not updated for more than specified number of days. Default value is 2 days.