



CHAPTER 30

McAfee ePolicy Orchestrator Devices

The McAfee ePolicy Orchestrator (ePO) is a central management application for many McAfee product. Antivirus (AV) devices provide detection and prevention against known viruses and anomalies, as do host-based IPS solutions. MARS is able to receive event data about the following devices that can be managed by ePO:

- McAfee VirusScan 8.0(I)/8.5(I)
- McAfee HIPS 6.0 (via ePO 3.6.x)
- McAfee HIPS 7.0 (via ePO 4.0)

Configuring MARS to receive and process the data generated by a McAfee ePolicy Orchestrator server requires you to perform two procedures.

- Configure the ePO server to forward SNMP traps to MARS
- Define the ePO server in the MARS web interface
- (Optional) Export a list of ePO agents from the ePO server and import that list as agents of the ePO server you defined in MARS. This step is not required as the list of managed agents is dynamically discovered by MARS as the ePO server forwards events generated by the agents.



Caution

Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

This chapter contains the following topics:

- [Configure ePolicy Orchestrator 4.0 to Generate Required Data, page 30-1](#)
- [Configure ePolicy Orchestrator 3.5 and 3.6 to Generate Required Data, page 30-6](#)
- [Add and Configure ePolicy Orchestrator Server in MARS, page 30-10](#)

Configure ePolicy Orchestrator 4.0 to Generate Required Data

To prepare the ePolicy Orchestrator server to forward SNMP events to MARS, follow these steps:

- Step 1** Select **Start > Program Files > Network Associates > ePolicy Orchestrator 4.x Console**.

- Step 2** In the tree, select **McAfee Security > ePolicy Orchestrator**, and click the **Log on to server** link under Global Task List.

- Step 3** In the Log On to Server dialog box, enter the user name and password required to access the ePolicy Orchestrator server, and click **Log on**.
- Step 4** Click **Automation**, and then click the **SNMP Servers** subtab.
- Step 5** Click **New SNMP Server**.

Name	Address	Actions
Ashu 4.3.5	10.1.1.31	Edit Duplicate Delete
ashu-g2	10.1.3.42	Edit Duplicate Delete
Ashutosh MARS	10.1.1.29	Edit Duplicate Delete
Chin-Lappy	64.103.134.148	Edit Duplicate Delete
Dev MARS	10.1.3.33	Edit Duplicate Delete
GC-LC	10.1.1.23	Edit Duplicate Delete
HurdleMARS	10.1.1.12	Edit Duplicate Delete
LABPDC-Server	192.168.10.13	Edit Duplicate Delete
MARS-Chin	10.1.3.19	Edit Duplicate Delete
MARS-Nandini	10.1.1.31	Edit Duplicate Delete
My_Gen2	10.1.3.37	Edit Duplicate Delete
naggs-mars	10.1.3.13	Edit Duplicate Delete
Nandini-MARS	10.1.3.22	Edit Duplicate Delete
PNOC-MARS	10.64.119.187	Edit Duplicate Delete
Prabha's laptop	64.104.136.31	Edit Duplicate Delete
Prabha-Gen1-MARS	10.1.1.31	Edit Duplicate Delete

- Step 6** Specify the following values, and click **OK**:
- **Name**—Enter the hostname of the Local Controller.
 - **Server address**—Enter the IP address of the eth0 interface, the monitoring interface for the MARS Appliance.

The SNMP server is added to represent the MARS Appliance.

- Step 7** Click the **Notification Rules** subtab.

The list of active notification rules appears.

The screenshot shows the McAfee ePolicy Orchestrator 4.0 interface. The top navigation bar includes icons for Dashboards, Reporting, Software, Systems, Network, Automation, and Configuration. Below this, a secondary navigation bar shows 'Server Tasks' and 'Notification Rules' (selected). The main area displays a table of notification rules with columns for Name, Status, Defined at, Products, Category, Recipients, and Actions. A 'New Rule' button is visible at the bottom left.

Name	Status	Defined at	Products	Category	Recipients	Actions
AV Test Rule	Disabled	My Organization	VirusScan	Any	SNMP: Nandini-M...	View Edit Duplicate Delete
Daily unknown category notification	Disabled	My Organization	Any	Unknown category	Email: administra...	View Edit Duplicate Delete
Daily unknown product notification	Disabled	My Organization	Unknown Product	Any	Email: administra...	View Edit Duplicate Delete
HIPS Rule	Enabled	My Organization	Host Intrusion Pr...	Any	SNMP: naggs-mars	View Edit Duplicate Delete
Non-compliant computer detected	Disabled	My Organization	ePO Server	Non-compliant co...	SNMP: naggs-mars	View Edit Duplicate Delete
PNOC AV Test Rule	Enabled	My Organization	Any	Any	SNMP: naggs-mars	View Edit Duplicate Delete
PNOC HIPS Rule	Disabled	My Organization	Host Intrusion Pr...	Any	SNMP: ashu-g2	View Edit Duplicate Delete
Repository update or replication failed	Disabled	My Organization	ePO Server	Repository updat...	Email: administra...	View Edit Duplicate Delete
Virus detected and not removed	Disabled	My Organization	Any	Virus detected an...	Email: administra...	View Edit Duplicate Delete
Virus detected heuristics and not re...	Disabled	My Organization	Any	Virus detected (h...	Email: administra...	View Edit Duplicate Delete

Step 8 Edit each enabled rule in the list so that all notifications are sent to the SNMP server that represents the MARS Appliance. To edit a rule, follow these steps:

- a. Click the rule.

The Describe Rule wizard page appears.

The screenshot shows the 'Notification Rule Builder' wizard, Step 1: Description. The wizard has five steps: 1 Description, 2 Filters, 3 Thresholds, 4 Notifications, and 5 Summary. The current step asks for the rule's name, scope, priority, and status. The form includes fields for Name (set to 'New Rule'), Notes, Defined at (set to '/My Organization'), Priority (radio buttons for High, Medium, Low), and Status (radio buttons for Enabled, Disabled). 'Back', 'Next', and 'Cancel' buttons are at the bottom right.

- b. Click **Next** to proceed to Set Filters page.

Notification Rule Builder

1 Description 2 Filters 3 Thresholds 4 Notifications 5 Summary

What types of events trigger this rule?

Operating systems:

- Workstation
- Server
- Unknown

Products:

- Any product
- Selected products: (1 selected)
 - ePO Server
 - GroupShield Domino
 - GroupShield Exchange
 - Host Intrusion Prevention

Categories:

- Any category
- Selected categories: (0 selected)
 - Active Directory discovery failed
 - Active Directory discovery succeeded
 - Audit Log purge failed
 - Audit Log purge succeeded

Back Next Cancel

251180

- c. Under Add or Edit Notification Rule, click the **3. Set Thresholds** link.

Figure 30-1 Set Threshold Values

Notification Rule Builder

1 Description 2 Filters 3 Thresholds 4 Notifications 5 Summary

How often should a notification be sent?

Aggregation:

- Send a notification for every event
- Send a notification if multiple events occur within: 5 Minutes
- When the number of affected systems is at least: 100
- or
- When the number of events is at least: 100

Throttling:

- At most, send a notification every: 5 Minutes

Back Next Cancel

251181

- d. Verify the Aggregation and Throttling values are set as shown in [Figure 30-1](#) [Figure 30-3](#)
- e. Click **Next** to proceed to the Create Notifications page.

Figure 30-2 Notification Rule Builder: Notifications Step

Notification Rule Builder

1 Description 2 Filters 3 Thresholds 4 Notifications 5 Summary

What notifications should be sent? You can have one or more notifications.

SNMP Trap

SNMP server: My Gen2

Replace variables with their values in: English

Variables to include:

- Actual categories
- Actual number of events
- Actual number of systems
- Actual products
- Actual threat or rule names
- Additional information
- Affected objects
- Affected system IP addresses
- Affected systems names
- Event descriptions
- Event IDs
- First event time
- Notification rule name
- Rule defined at
- Rule group
- Selected categories
- Selected products
- Selected threat or rule name
- Source systems
- Time notification sent

Back Next Cancel

- f. In the SNMP server list, select the SNMP server that represents the MARS Appliance.
- g. Verify that all the variables are selected as shown in [Figure 30-2](#), and click **Next**.

Notification Rule Builder

1 Description 2 Filters 3 Thresholds 4 Notifications 5 Summary

Name:	New Rule
Notes:	
Defined at:	My Organization
Priority:	High
Status:	Enabled
Operating systems:	Workstation Server Unknown
Products:	Any product
Categories:	Any category
Threat name:	(Any)
Aggregation:	Send a notification for every event
Throttling:	

Back Save Cancel

- h. Click **Save** to add the SNMP trap to the list of notifications for the selected rule.
- i. Click **Finish** to save the changes to the selected rule.
- j. Repeat [a.](#) through [i.](#) for each rule.

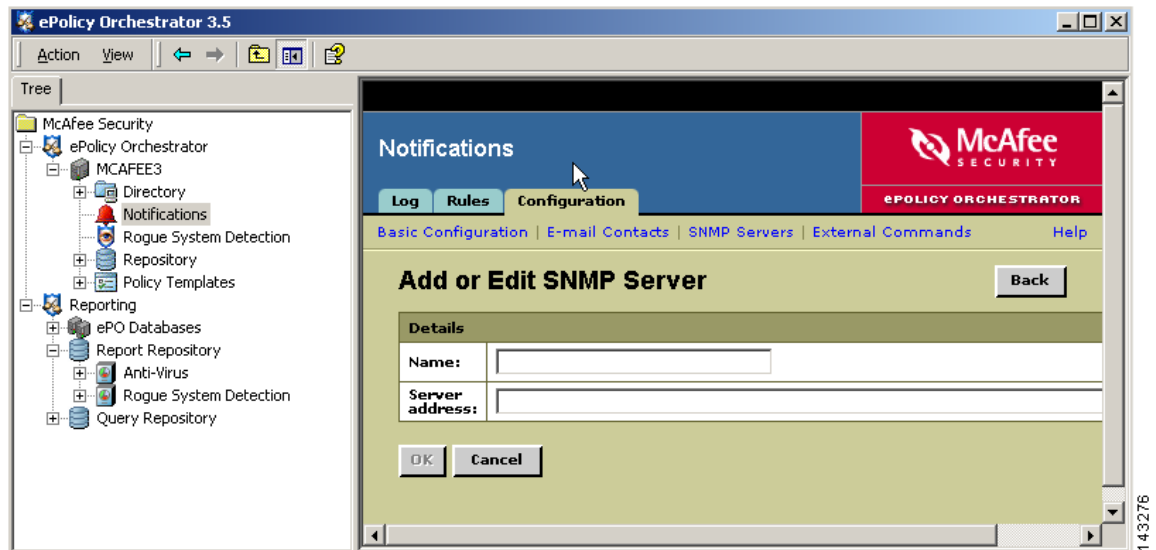
Configure ePolicy Orchestrator 3.5 and 3.6 to Generate Required Data

To prepare the ePolicy Orchestrator server to forward SNMP events to MARS, follow these steps:

- Step 1** Select **Start > Program Files > Network Associates > ePolicy Orchestrator 3.x Console**.
- Step 2** In the tree, select **McAfee Security > ePolicy Orchestrator**, and click the **Log on to server** link under Global Task List.



- Step 3** In the Log On to Server dialog box, enter the username and password required to access the ePolicy Orchestrator server, and click **OK**.
- Step 4** In the tree, select **McAfee Security > ePolicy Orchestrator > <Server_Name> > Notifications** and click the **Configuration** tab and click the **SNMP Servers** link.
- Step 5** Click **Add**.



Step 6 In the Name field, enter the hostname of the MARS Appliance.

Step 7 In the Server address field, enter the IP address of the eth0 interface, the monitoring interface for the MARS Appliance, and click **OK**.

The SNMP server is added to represent the MARS Appliance.

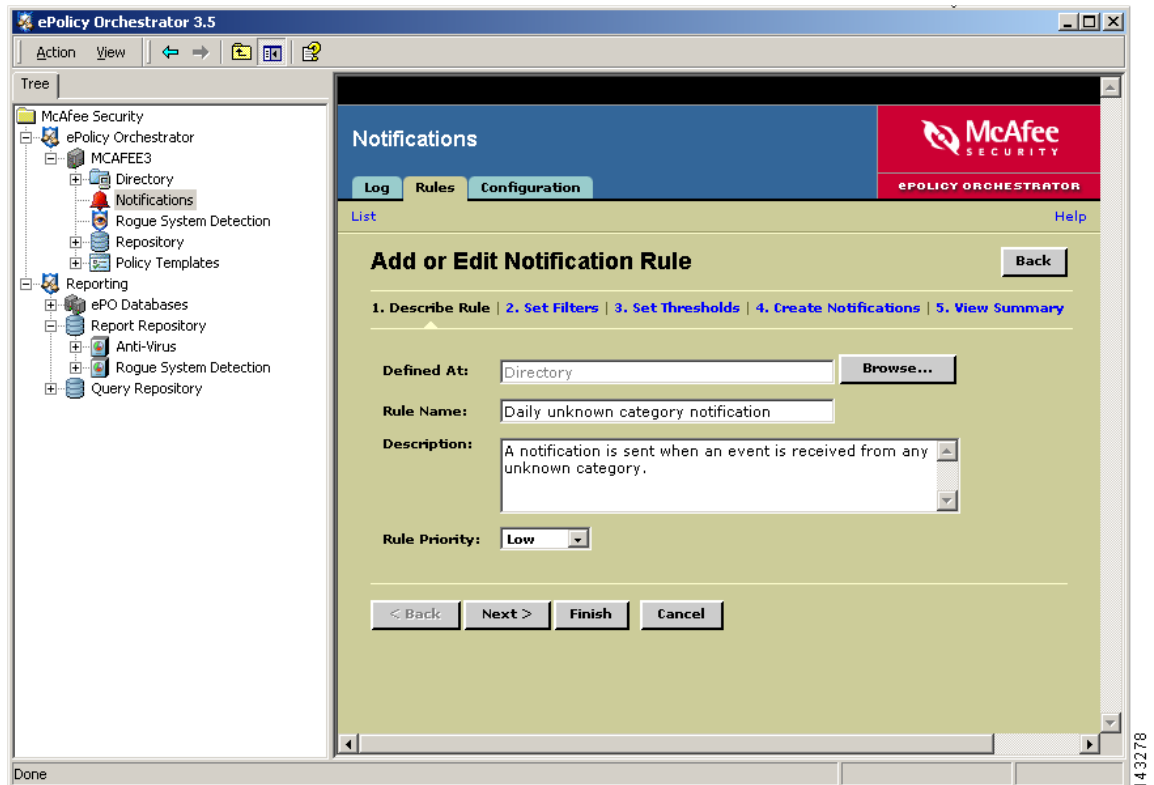
Step 8 Click the **Rules** tab.

You can access the Rules tab by selecting **McAfee Security > ePolicy Orchestrator > <Server_Name> > Notifications >** and then clicking the **Rules** tab.

Step 9 Edit each rule in the list so that all notifications are sent to the SNMP server that represents the MARS Appliance. To edit a rule, follow these steps:

- a. Click the rule.

The Describe Rule wizard page appears.



- b. Click **Next** to proceed to Set Filters page.
- c. Under Add or Edit Notification Rule, click the **3. Set Thresholds** link.

Figure 30-3 Set Threshold Values

Add or Edit Notification Rule Back

1. Describe Rule | 2. Set Filters | 3. Set Thresholds | 4. Create Notifications | 5. View Summary

For notification rule: **Daily unknown category notification**

You can use aggregation and throttling to limit the number of notifications you receive. Each sends a single notification that summarizes multiple events.

Aggregation: Send a notification for every event

Send a notification for multiple events within: Minutes

When the number of affected computers is at least:

or

When the number of events is at least:

Throttling: At most, send notification every: Days

< Back Next > Finish Cancel

143280

- d. Verify the Aggregation and Throttling values are set as shown in Figure 30-1Figure 30-3
- e. Click **Next** to proceed to the Create Notifications page.

Add or Edit Notification Rule Back

1. Describe Rule | 2. Set Filters | 3. Set Thresholds | 4. Create Notifications | 5. View Summary

For notification rule: **Daily unknown category notification**

Notification Type	Detail	Recipients	Test	Delete
E-mail	Standard E-mail	Administrator	Test	✘
SNMP Trap	Warning	tucson	Test	✘

Add E-mail Message Add SNMP Trap Add External Command

< Back Next > Finish Cancel

143281

- f. Click **Add SNMP Trap**.

Figure 30-4 SNMP Trap Settings

Add or Edit SNMP Trap Back

For notification rule: Daily unknown category notification

SNMP server:

Replace variables with their values in:

Variables to include:

<input checked="" type="checkbox"/> Actual categories	<input checked="" type="checkbox"/> Actual number of computers
<input checked="" type="checkbox"/> Actual number of events	<input checked="" type="checkbox"/> Actual products
<input checked="" type="checkbox"/> Actual threat or rule names	<input checked="" type="checkbox"/> Additional information
<input checked="" type="checkbox"/> Affected computer IP addresses	<input checked="" type="checkbox"/> Affected computer names
<input checked="" type="checkbox"/> Affected objects	<input checked="" type="checkbox"/> Event descriptions
<input checked="" type="checkbox"/> Event IDs	<input checked="" type="checkbox"/> First event time
<input checked="" type="checkbox"/> Notification rule name	<input checked="" type="checkbox"/> Rule defined at
<input checked="" type="checkbox"/> Rule site	<input checked="" type="checkbox"/> Selected categories
<input checked="" type="checkbox"/> Selected products	<input checked="" type="checkbox"/> Selected threat or rule name
<input checked="" type="checkbox"/> Source computers	<input checked="" type="checkbox"/> Time notification sent

Cancel Save

143285

- g. In the SNMP server list, select the SNMP server that represents the MARS Appliance.
- h. Verify that all the variables are selected as shown in [Figure 30-4](#).
- i. Click **Save** to add the SNMP trap to the list of notifications for the selected rule.
- j. Click **Finish** to save the changes to the selected rule.
- k. Repeat [a.](#) through [j.](#) for each rule.

Add and Configure ePolicy Orchestrator Server in MARS

Before MARS can begin processing SNMP traps from ePolicy Orchestrator, you must define the ePolicy Orchestrator server as software running on a host. When ePolicy Orchestrator is defined as a reporting device, MARS can process any inspection rules that you have defined using ePolicy Orchestrator event types.

After you add the ePolicy Orchestrator server to MARS, the appliance can discover the agents that are managed by the ePolicy Orchestrator server as events are generated by those agents. You do not need to manually define the agents associated with this server.

To add an ePolicy Orchestrator server to MARS, follow these steps:

- Step 1** Select **Admin > System Setup > Security and Monitor Devices > Add**.

- Step 2** From the Device Type list, select **Add SW Security apps on a new host**.
- Step 3** In the Device Name field, enter the hostname of the server.
- Step 4** In the Reporting IP field, enter the IP address of the interface in the ePolicy Orchestrator server from which SNMP traps will originate.
- Step 5** Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in the ePolicy Orchestrator server from which syslog messages will originate.
This address is the same value as the Reporting IP address.
- Step 6** Click **Apply**.
- Step 7** Click **Next** to move to the Reporting Applications tab.
- Step 8** In the Select Application field, select **McAfee ePO 3.5**, **McAfee ePO 3.6.x**, or **McAfee ePO 4.0**, and then click **Add**

Management Console

Add or edit agents for this McAfee epo server.

Add Agent
Edit Agent
Delete Agent

Cancel
Submit

- Step 9** Click **Done** to save the changes.
- Step 10** Click **Submit**.
- Step 11** To activate the device, click **Activate**.

Dynamic discovery of agents is supported. MARS discovers the agents by identifying the originating device in the SNMP traps. Therefore, the agents are discovered as SNMP traps originating from those devices are forwarded by the ePO server.

You are not limited to dynamic discovery for populating agents. For details on manually importing agents into MARS, see [Add ePO Agents From File, page 30-11](#).

Add ePO Agents From File

You can add the complete list of hosts on which ePO Agents are installed by exporting the all hosts report from ePolicy Orchestrator server and importing that file into MARS. The only advantage to adding agents using an export file is that the first notification received that originates from the agent is not attributed to the ePO server.



Note

For 3.6.x and 4.0 releases, you can import reporting agents using a CSV file exported from ePO. In 4.0, you can export from the ePO user interface. In 3.6.x, you can export from the database. Refer to the documentation that came with your product for instructions on exporting a CSV file from ePO.

**Caution**

Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

To add ePO agents from a file, follow these steps:

- Step 1** Click **Admin > Security and Monitoring Devices**.
- Step 2** From the list of devices, select the host running ePolicy Orchestrator server, and click **Edit**.
- Step 3** Click the **Reporting Applications** tab, select **McAfee ePO 3.6.x** or **McAfee ePO 4.0** in the Device Type list, and click **Edit**.
- Step 4** Click **Load From File**.

Remote File Location:

→ *IP Address:

→ *User Name:

→ *Password:

→ *Path:

→ *File Name:

143193

**Caution**

The file should be formatted as a tab delimited file. You cannot use a CSV file. To generate a tab delimited file of the ePO agents managed by the ePolicy Orchestrator server, see the documentation that came with your ePolicy Orchestrator product.

- Step 5** In the IP Address field, enter the address of the FTP server where you stored the exported hosts file.
- Step 6** In the User Name field, enter the name of the account used to authenticate to the FTP server.
- Step 7** In the Password field, enter the password that corresponds to the account specified in [Step 6](#).
- Step 8** In the Path field, enter the path to the folder where the file is stored. If this file is stored in the root folder, you must specify a backslash (\) in this field. The format of this value is `<path_here>\`.
- Step 9** In the File Name field, enter the name of the tab delimited file.
- Step 10** Click **Submit**.

The following message displays and the hosts are added as agents of the ePolicy Orchestrator server:

```
Success:
Status: OK
```

- Step 11** Click **Done**.