CHAPTER 9

Configuring Antivirus Devices

Revised: November 11, 2007

Antivirus (AV) devices provide detection and prevention against known viruses and anomalies.

This chapter describes how to configure and add the following devices and systems:

- Symantec AntiVirus Configuration, page 9-1
- McAfee ePolicy Orchestrator Devices, page 9-10
- Cisco Incident Control Server, page 9-15

Symantec AntiVirus Configuration

To enable a Symantec AntiVirus agent as a reporting device in MARS, you must identify the Symantec System Center console as the reporting device. The Symantec System Center console receives alerts from the AV agents that it monitors, and it forwards those alerts to MARS as SNMP notifications.

When MARS receives the SNMP notification, the source IP address in the notification is that of the AV agent that originally triggered the event, rather than the Symantec System Center console that forwarded it. Therefore, MARS requires host definitions for each of the AV agents that can potentially trigger an event. These definitions are added as sub-components under the device definition of the Symantec System Center console.

As of MARS, release 4.2.1, the MARS Appliance discovers AV agents as they generate alerts, eliminating the need to manually define them. MARS parses the alert to identify the AV agent hostname and to discover the host operating system (OS). MARS uses this information to add any undefined agents as children of the Symantec System Center console as a host with either the Generic Windows (all Windows) or Generic (Unix or Linux) operating system value. You are still required to define the Symantec System Center console; however, you are not required to define each agent. The default topology presentation for discovered AV agents is within a cloud.

Note The first SNMP notification from an unknown AV agent appears to originate from the Symantec System Center console. MARS parses this notification and defines a child agent of the Symantec System Center console using the discovered settings. Once the agent is defined, all subsequent messages appear to originate from the AV agent.

Prior to 4.2.1, you were required to manually add each agent or by using an exported agent list, as defined in Export the AntiVirus Agent List, page 9-8.

Configuring the Symantec AntiVirus integration requires performing two tasks:

- Configure the AV Server to Publish Events to MARS Appliance, page 9-2
- Add the Device to MARS, page 9-8

In addition, you can perform the following task to expedite populating the Agent list in MARS:

- Export the AntiVirus Agent List, page 9-8

Configure the AV Server to Publish Events to MARS Appliance

To configure the AV server to publish events to MARS, follow these steps:

Step 1 Log in to the Windows server running Symantec AV.

Step 2 To identify the Local Controller as a valid SNMP trap destination, click **Administrative Tools > Services > SNMP Service > Traps > Trap destinations**.

Step 3 Enter the IP address of the Local Controller in the Trap Destination page, and click **OK** to close all open windows.

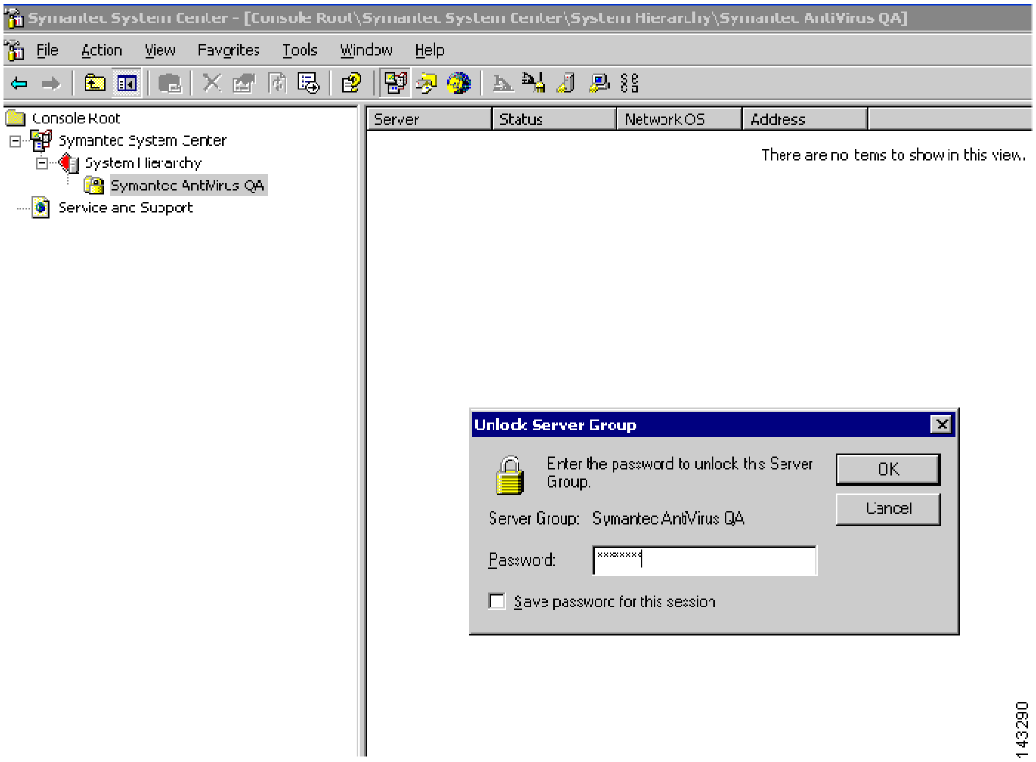
Step 4 Select **Start > All Programs > Symantec System Center Console**.

Step 5 In the Symantec System Center window, click **System Hierarchy**.

Step 6 Under System Hierarchy, right-click the appropriate server group name and unlock the server group by supplying the configured password.

Unlocking the server enables you to configure it.

Figure 9-1 Symantec Unlock Server



Server	Status	Network OS	Address

There are no items to show in this view.

Enter the password to unlock this Server Group.

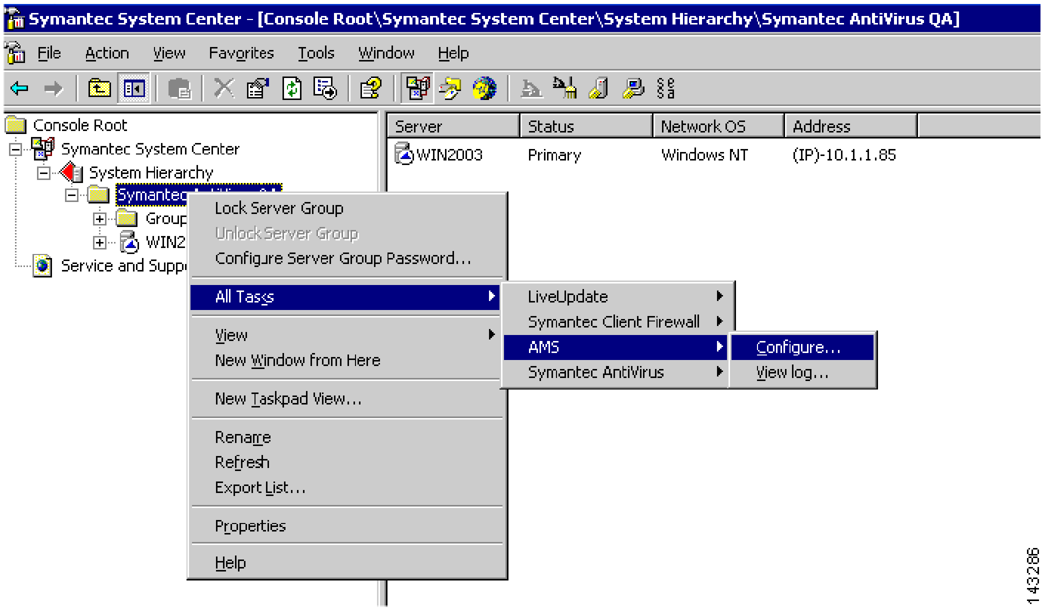
Server Group: Symantec AntiVirus QA

Password: ********

☐ Save password for this session

Step 7 Configure Symantec server (AMS-Alert Management System) to send SNMP traps to MARS. Right click the unlocked server group name, then select **All Tasks > AMS > Configure**.

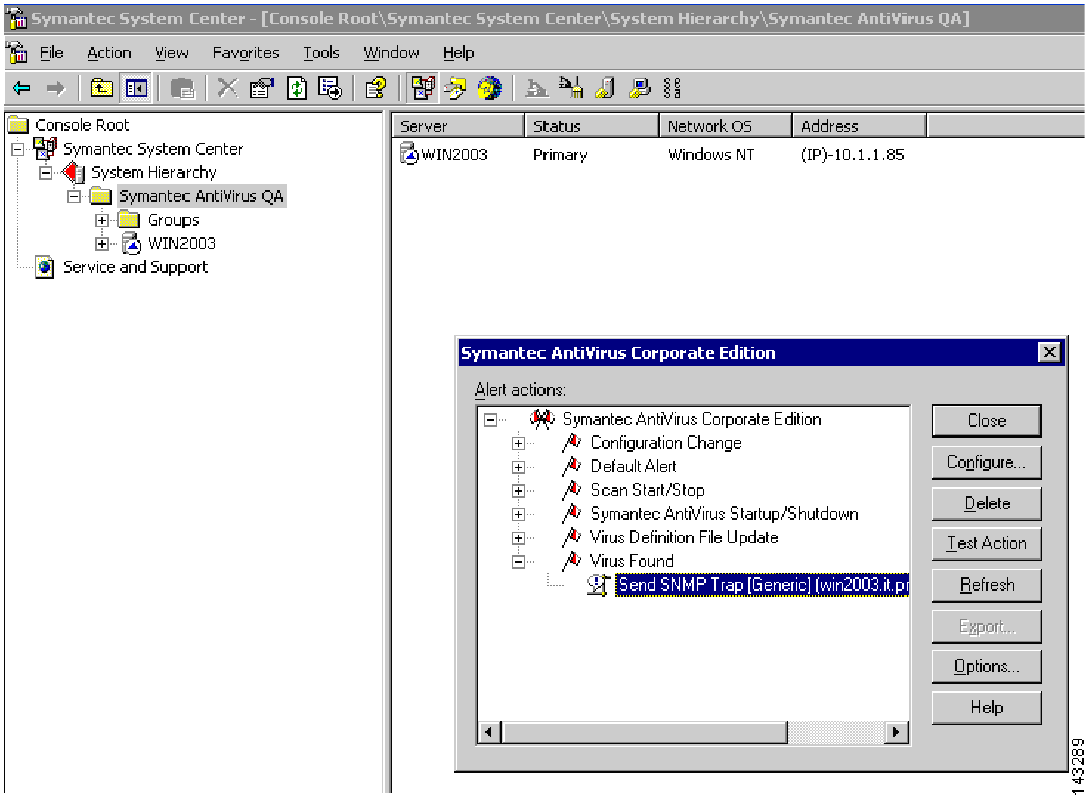
Figure 9-2 Symantec AV AMS



Server	Status	Network OS	Address
WIN2003	Primary	Windows NT	(IP)-10.1.1.85

Step 8 Select **Send SNMP Trap** under each Alert Action, then click **Configure**.

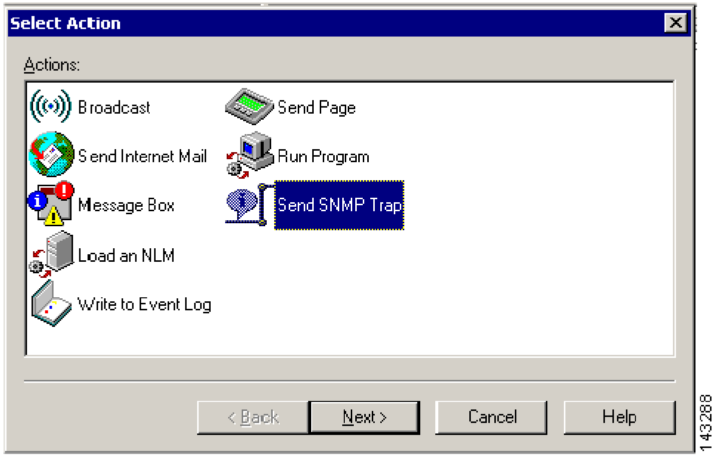
Figure 9-3 Symantec AV Trap



Server	Status	Network OS	Address
WIN2003	Primary	Windows NT	(IP)-10.1.1.85

Step 9 Click **Send SNMP trap**, and then click **Next**.

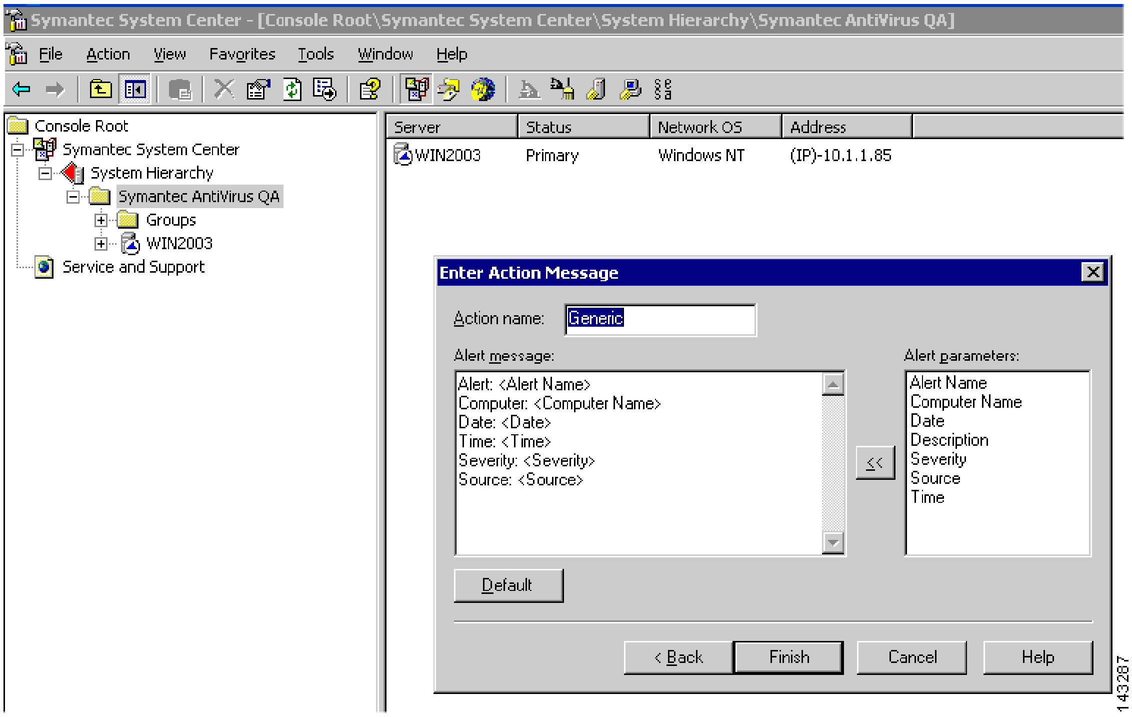
Figure 9-4 Symantec AV Send SNMP Trap



Step 10 Select the Local Controller to send the SNMP trap to as defined in Step 3, and then click **Next** to view the Action Message window.

Step 11 Add alert parameters to the Alert message list according to the following information:

Figure 9-5 Symantec AV Action Msg



Server	Status	Network OS	Address
WIN2003	Primary	Windows NT	(IP)-10.1.1.85

Action name: Generic

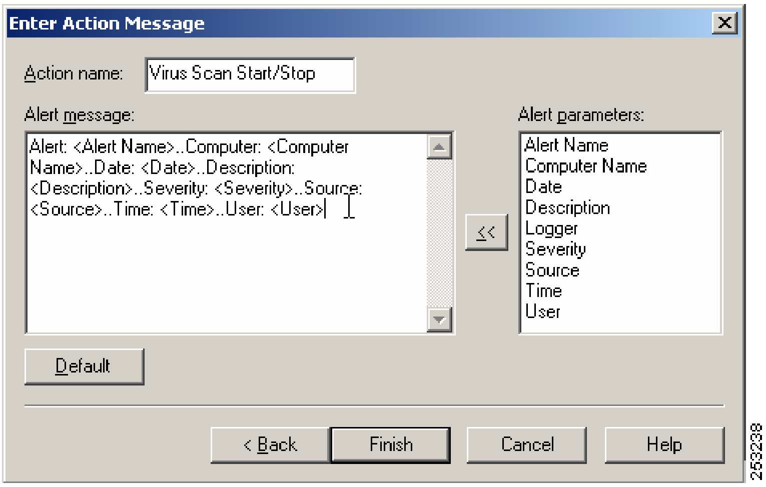
Alert message:

```
Alert: <Alert Name>
Computer: <Computer Name>
Date: <Date>
Time: <Time>
Severity: <Severity>
Source: <Source>
```

Alert parameters: Alert Name, Computer Name, Date, Description, Severity, Source, Time

The following mandatary fields are required for MARS to parse AV traps. If these fields are among those possible, you must define these fields in order before defining any of the optional fields.

Note For MARS Appliance models 25, 55, 110, 210, and GC2, do not include a CR/LF (Enter key) in the action message.



Action name: Virus Scan Start/Stop

Alert message:

```
Alert: <Alert Name>..Computer: <Computer
Name>..Date: <Date>..Description:
<Description>..Severity: <Severity>..Source:
<Source>..Time: <Time>..User: <User>
```

Alert parameters: Alert Name, Computer Name, Date, Description, Logger, Severity, Source, Time, User

- Alert: <*Alert Name*>
- Computer: <*Computer Name*>

- Date: <*Date*>
- Time: <*Time*>
- Action: <*Actual Action*>
- Description: <*Description*>

Note This ordering is required is because some optional fields can be so long as to prevent Mars from correctly parsing the mandatory fields if they do not appear first in the list of attributes.

The following optional fields can be defined after all mandatory fields are defined:

- User: <*User*>
- Virus Name: < *Virus Name*>
- File Path: <*File Path*>
- Severity: <*Severity*>
- Source: <*Source*>

The following list identifies the trap type and the full list of possible fields:

Alert: Virus Found

- Alert: <*Alert Name*>
- Computer: <*Computer Name*>
- Date: <*Date*>
- Time: <*Time*>
- Action: <*Actual Action*>
- Severity: <*Severity*>
- Source: <*Source*>
- File Path: <*File Path*>
- Logger: <*Logger*>
- Requested Action: < *Requested Action*>
- User: <*User*>
- Virus Name: <*Virus Name*>

Alert: Virus Definition File Update

- Alert: <*Alert Name*>
- Computer: <*Computer Name*>
- Date: <*Date*>
- Time: <*Time*>
- Description: <*Description*>
- Severity: <*Severity*>
- Source: <*Source*>

Alert: Symantec AntiVirus Startup/Shutdown

- Alert: <*Alert Name*>

- Computer: <*Computer Name*>
- Date: <*Date*>
- Time: <*Time*>
- Description: <*Description*>
- Severity: <*Severity*>
- Source: <*Source*>

Alert: Scan Start/Stop

- Alert: <*Alert Name*>
- Computer: <*Computer Name*>
- Date: <*Date*>
- Time: <*Time*>
- Severity: <*Severity*>
- Source: <*Source*>
- Source: <*Source*>
- Logger: <*Logger*>
- User: <*User*>

Alert: Scan Start/Stop

- Alert: <*Alert Name*>
- Computer: <*Computer Name*>
- Date: <*Date*>
- Time: <*Time*>
- Description: <*Description*>
- Severity: <*Severity*>
- Source: <*Source*>
- Logger: <*Logger*>

Alert: Default Alert

- Alert: <*Alert Name*>
- Computer: <*Computer Name*>
- Date: <*Date*>
- Time: <*Time*>
- Severity: <*Severity*>
- Source: <*Source*>
- Failed Alert: <*Failed Alert*>

Alert: Configuration Change

- Alert: <*Alert Name*>
- Computer: <*Computer Name*>
- Date: <*Date*>
- Time: <*Time*>

- Severity: <*Severity*>
- Source: <*Source*>
- Failed Alert: <*Failed Alert*>

Alert: Configuration Change

- Alert: <*Alert Name*>
- Computer: <*Computer Name*>
- Date: <*Date*>
- Time: <*Time*>
- Description: <*Description*>
- Severity: <*Severity*>
- Source: <*Source*>

Step 12 Repeat Step 8 through Step 11 for each alert event.

Export the AntiVirus Agent List

While MARS discover the list of anitvirus agents that report to the Symantec System Center console automatically, you can export the list of Symantec AntiVirus Clients and Agents as a CSV file (*.csv), which enables you to use the CSV file to manually load the agents into MARS. For more information on adding agents from the file, Add Agents from a CSV File, page 9-10. This approach is much faster than if you had to identify the agents manually.

To generate the CSV file, follow these steps:

Step 1 Select = View > Default Console View to ensure the generated CVS file will be based on the Console Default View.

Step 2 Right-click the name of the server that you want to export, choose **Export List**, and save it as Text (Comma Delimited) (*.csv) file.

Step 3 Copy the file to an FTP server that the MARS Appliance can access.

You will use this file when you add the AntiVirus agents within the web interface.

Add the Device to MARS

Before you can identify the agents, you must add the Symantec System Center console to MARS. All AntiVirus agents forward notifications to the Symantec System Center console, and the Symantec System Center console forwards SNMP notifications to MARS. Once you define the Symantec System Center console and activate the device. MARS can discover the agents that are managed by that Symantec System Center console. However, you can also chose to manually add the agents.

Tip For Symantec AntiVirus, the Symantec agent hostname (AV client computer name) appears in the "Reported User" column of the event data. Therefore, you can define a query, report or rule related to this agent based on the "Reported User" value.

To add the host and application configuration information, follow these steps:

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

Step 2 Select **Add SW Security apps on a new host** or **Add SW security apps on existing host** from the Device Type list.

Step 3 To add a new host, enter the device name and IP addresses.

Step 4 Click **Apply**.

Step 5 Click the **Reporting Applications** tab.

Step 6 From the Select Application list, select one of the following values:

- **Symantec AntiVirus 9.x**
- **Symantec AntiVirus 10.x**

Step 7 Click **Add**, then add the agents.

Step 8 Done one of the following:

- To save your changes and allow the AntiVirus agents to be discovered automatically, click **Submit**, and then click **Done**.
- To add agents using an exported seed file, continue with Add Agents from a CSV File, page 9-10.
- To add a single agent manually, continue with Add Agent Manually, page 9-9.

Add Agent Manually

MARS can automatically discover agents or you can manually add them one at a time or in bulk using a CSV file (see Add Agents from a CSV File, page 9-10.) This topic explains how to manually add a single agent. The value of defining an agent is that is accelerates the discover process; however, it is not required.

To add an agent manually, follow these steps:

Step 1 Click **Add Agent**.

Step 2 Select the existing device or click **Add New.**

Step 3 Enter the following information for new device.

- **Device Name—**The DNS entry for this device.
- **Reporting IP—**The IP address that the agent uses to send logs to the console.

Step 4 Under the Interfaces list, specify the IP address and netmask values asscoaited with each interface installed in the host on which the agent is running.

MARS uses interface information to calculate attack paths.

Step 5 Click **Submit**.

Add Agents from a CSV File

You can generate a CSV file that contains the list of agents managed by the Symantec AV server as defined in Export the AntiVirus Agent List, page 9-8. Once the file is generated, you can use the file to import the list of agents into the MARS web interface as child modules of the Symantec AV server.

Note Other population options exist: MARS can automatically discover agents (default) or you can manually add them one at a time (see Add Agent Manually, page 9-9.)

To import the list of AV agents into MARS. follow these steps:

Step 1 Click **Load From CSV**.

Step 2 Enter the FTP server information and location of the CSV (comma-separated values) file.

Step 3 Click **Submit**.

McAfee ePolicy Orchestrator Devices

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

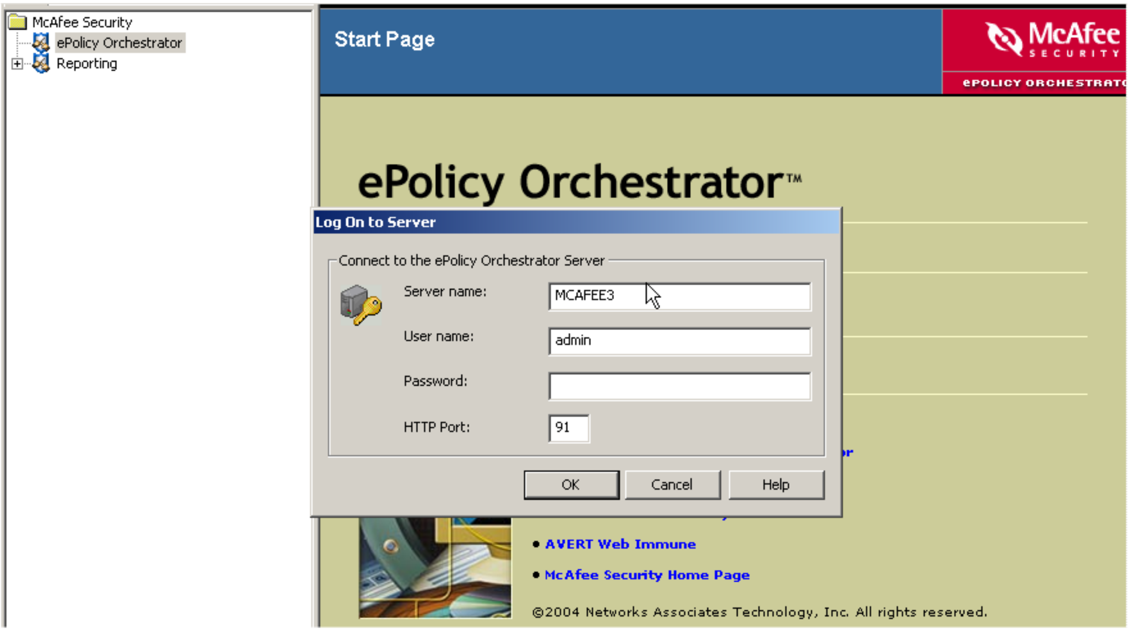
- Configure ePolicy Orchestrator to Generate Required Data, page 9-10
- Add and Configure ePolicy Orchestrator Server in MARS, page 9-14

Configure ePolicy Orchestrator 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.



Log On to Server

Connect to the ePolicy Orchestrator Server

Server name: MCAFEE3

User name: admin

Password:

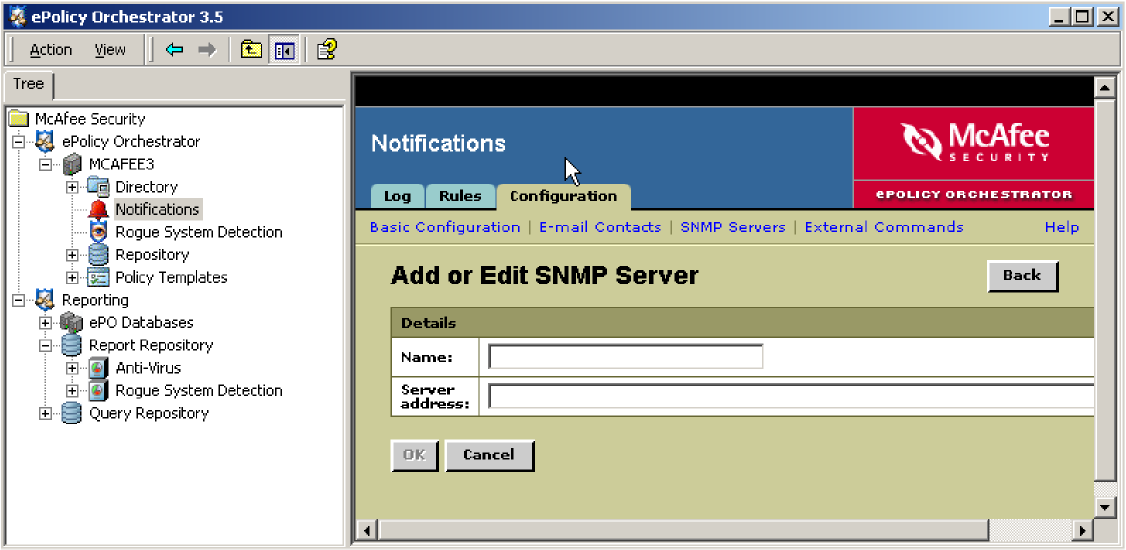
HTTP Port: 91

143277

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**.



Add or Edit SNMP Server

Details

Name:

Server address:

143276

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.

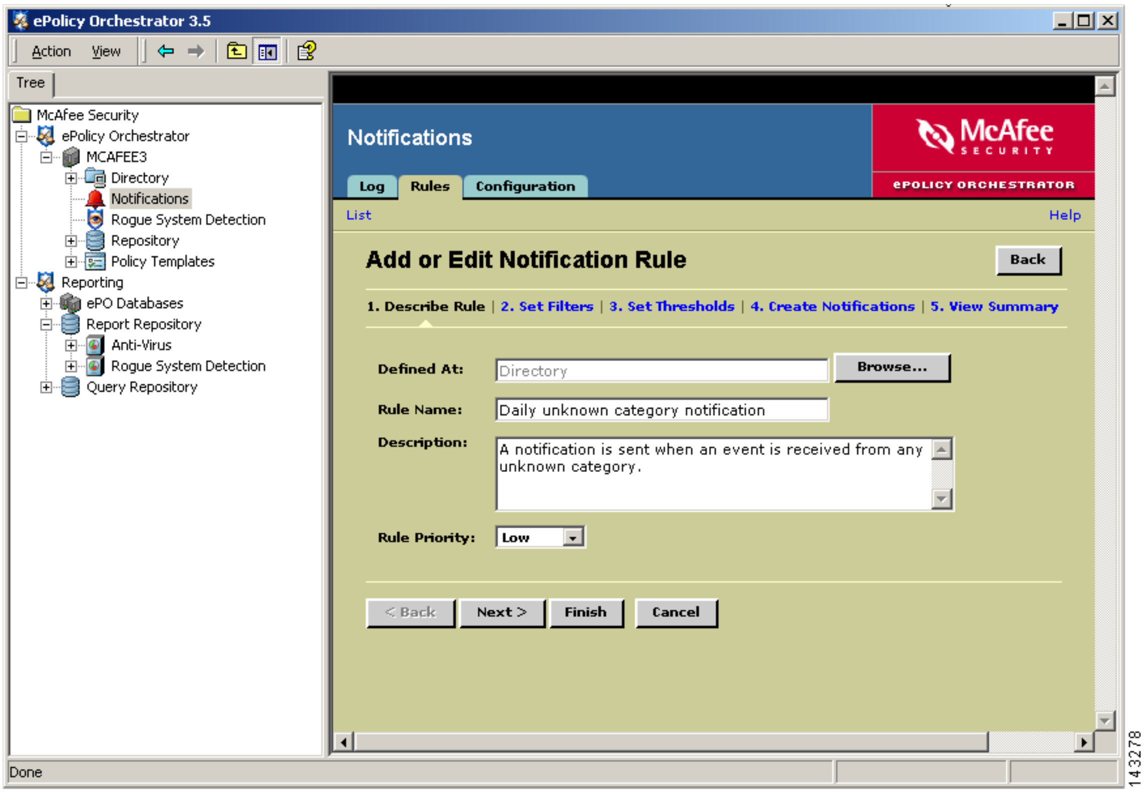
Step 8 Click the **Rules** tab.

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.



Add or Edit Notification Rule

Defined At: Directory

Rule Name: Daily unknown category notification

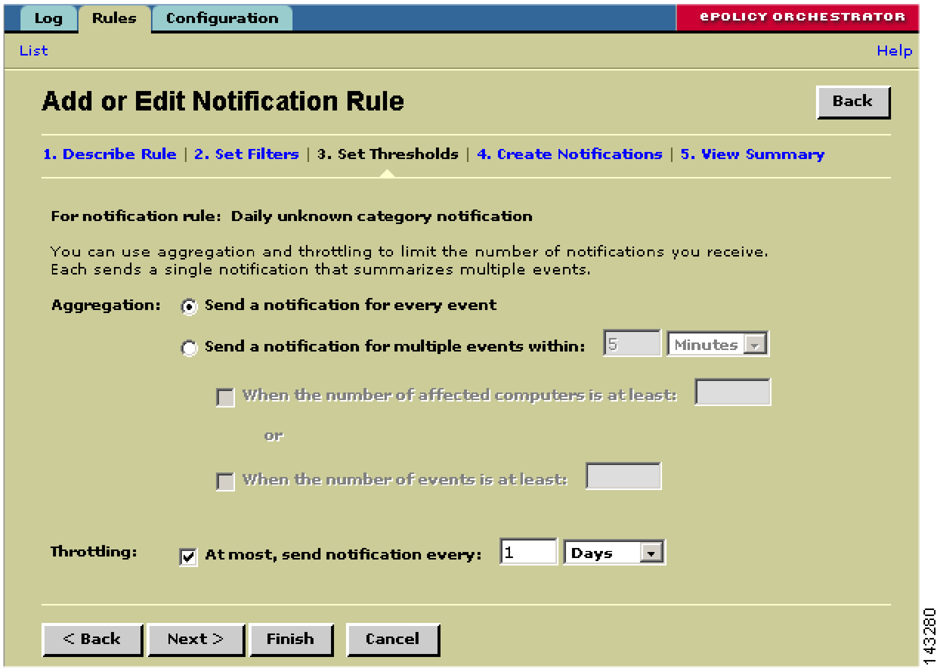
Description: A notification is sent when an event is received from any unknown category.

Rule Priority: Low

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

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

Figure 9-6 Set Threshold Values



Add or Edit Notification Rule

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: 5 Minutes

□ When the number of affected computers is at least:

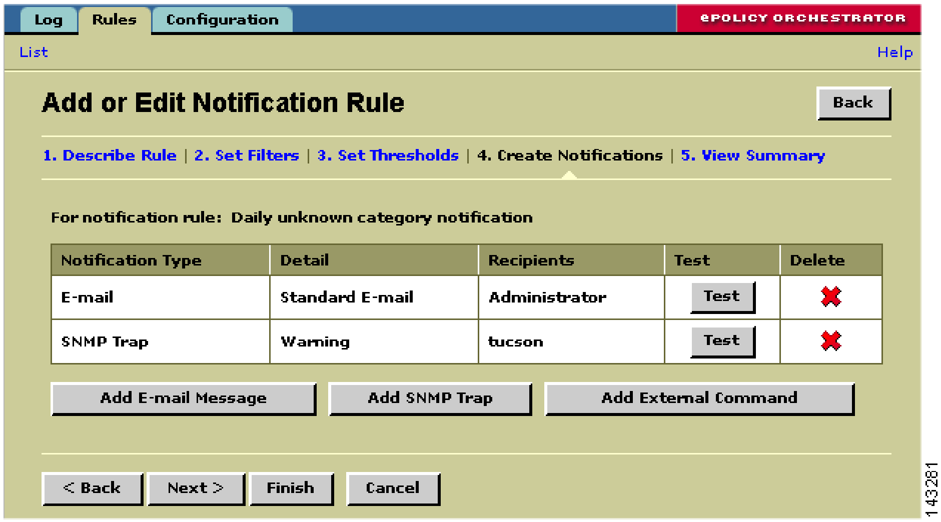
or

□ When the number of events is at least:

Throttling: ☑ At most, send notification every: 1 Days

d. Verify the Aggregation and Throttling values are set as shown in Figure 9-6 on page 9-13.

e. Click **Next** to proceed to the Create Notifications page.



Add or Edit Notification Rule

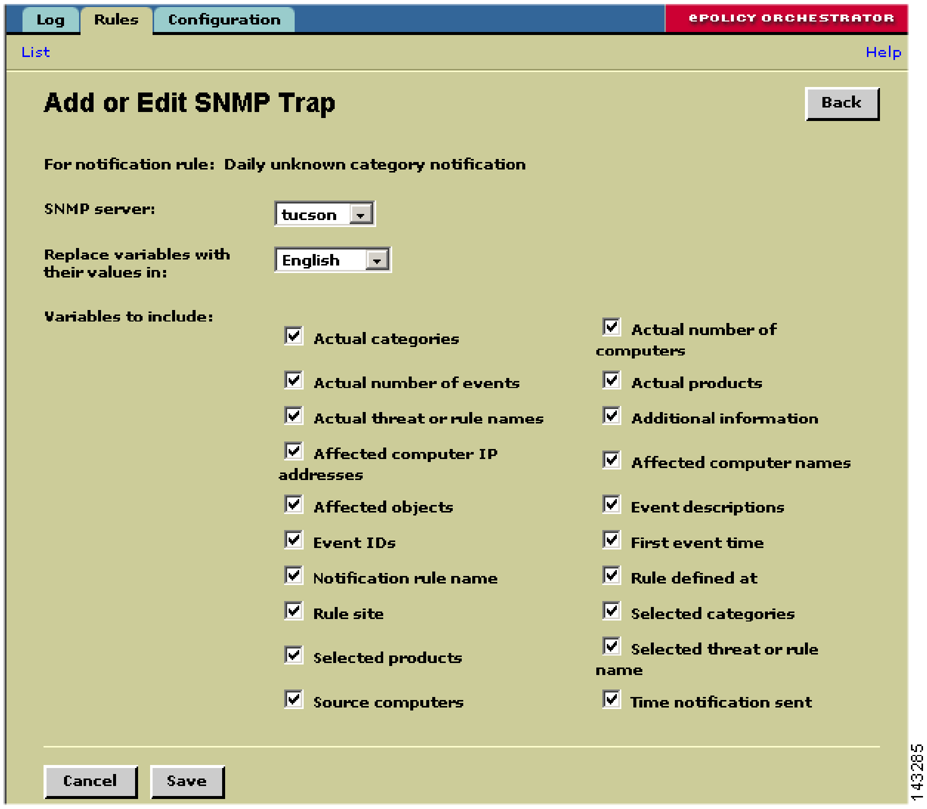
1. Describe Rule | 2. Set Filters | 3. Set Thresholds | 4. Create Notifications | 5. View Summary

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	✖

f. Click **Add SNMP Trap**.

Figure 9-7 SNMP Trap Settings



Add or Edit SNMP Trap

For notification rule: Daily unknown category notification

SNMP server: tucson

Replace variables with their values in: English

Variables to include:

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

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 9-7 on page 9-14.

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 Steps 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 Ochestrator 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 > 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.

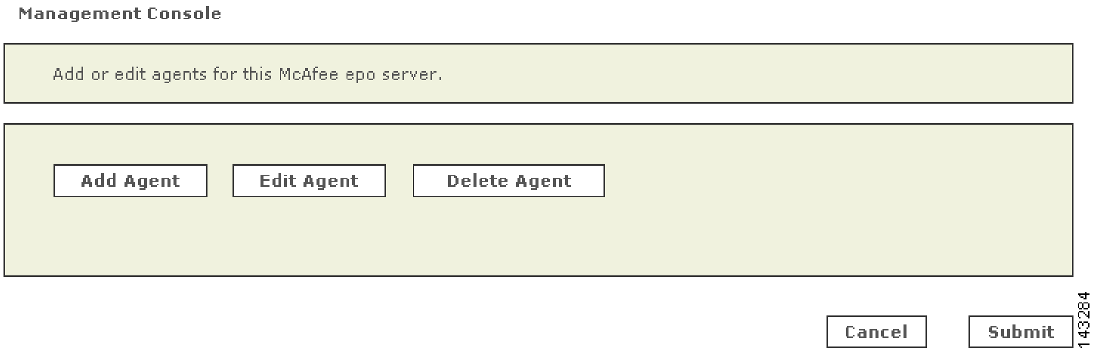
Step 5 Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in the ePolicy Orchestrator server from which syslog messages will originate.

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**, and then click **Add**.


Management Console

Add or edit agents for this McAfee epo server.

Step 9 Click **Done** to save the changes.

Step 10 Click **Submit**.

Step 11 To activate the device, click **Activate**.

Cisco Incident Control Server

The Cisco Incident Control Server (Cisco ICS) enables extended protection across Cisco IOS routers, switches, and IPS devices. In coordination with Trend Micro's incident control solutions, Cisco ICS prevents the spread of day-zero outbreaks in three ways:

- First, Cisco ICS issues temporary ACLs to those Cisco mitigation devices that can block such traffic, typically using a protocol and port pair block. This temporary block is referred to as an Outbreak Prevention ACL (OPACL).
- Second, as soon as a signature is available, Cisco ICS updates all Cisco IPS and IDS devices running on your network with the signature required to detect and prevent the specific threat. This signature is referred to as an Outbreak Prevention Signature (OPSig).
- Third, Cisco ICS can manage supporting products (sold seperately), such as Tend Micros's Damage Cleanup Services (DCS), which cleans infected hosts by removing trojans and other malware.

To complete the Cisco ICS communication settings, you must perform two tasks: configure Cisco ICS to send syslog messages to the MARS Appliance, and add the Cisco ICS management server to the MARS web interface as a reporting device.

This section contains the following topics:

- Configure Cisco ICS to Send Syslogs to MARS, page 9-16

- Add the Cisco ICS Device to MARS, page 9-17
- Define Rules and Reports for Cisco ICS Events, page 9-17

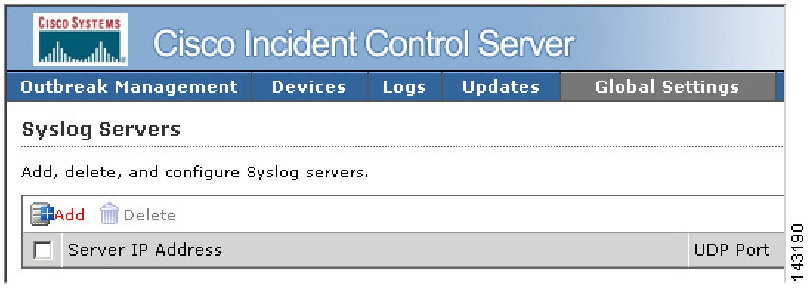
Configure Cisco ICS to Send Syslogs to MARS

Cisco ICS publishes syslog messages to MARS. To configure Cisco ICS, you simply define a syslog server with the IP address of the MARS Appliance. You do not need to enable any special logs, and you cannot tune the messages that are sent to MARS. The Cisco ICS events for which syslog messages are geneerated have been selected to provide the most benefit to your Security Threat Mitigation (STM) system.

To prepare Cisco ICS to publish events to MARS, follow these steps:

Step 1 Log in to the Cisco ICS Management Console.

Step 2 Click **Global Settings > Syslog Servers**.



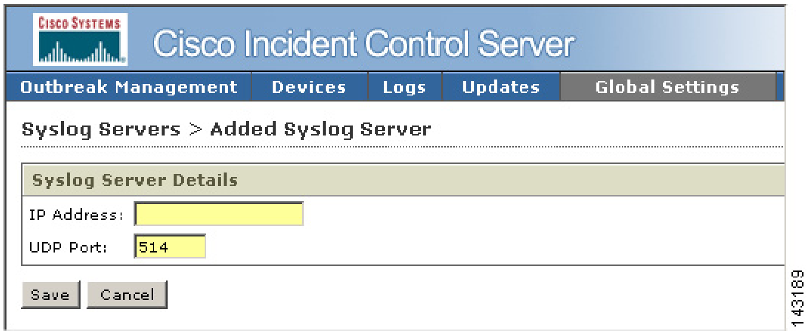
Syslog Servers

Add, delete, and configure Syslog servers.

□	Server IP Address	UDP Port

Step 3 Click **Add**.

A



Syslog Servers > Added Syslog Server

Syslog Server Details

IP Address:

UDP Port: 514

Step 4 In the IP Address field, enter the address of the MARS Appliance to which the Cisco ICS will publish syslog messages.

Step 5 Click **Save**.

Cisco ICS now publishes syslog message to MARS. For MARS to be aware of this device, you must add the Cisco ICS device as a software application running on a host and you must click Activate in the web interface.

Add the Cisco ICS Device to MARS

Before MARS can being processing the syslog messages as Cisco ICS messages, you must define the Cisco ICS management server as an software application running on a host. After Cisco ICS is defined as a reporting device, MARS can process any inspection rules that you have defined using Cisco ICS event types.

To add a Cisco ICS server to MARS, follow these steps:

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Add SW Security apps on a new host**.

You can also select Add SW Security apps on an existing host if you have already defined the host within MARS, perhaps as part of the Management >IP Management settings or if you are running another application on the host, such as Microsoft Internet Information Services.

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 Cisco ICS server from which the syslog messages will originate.

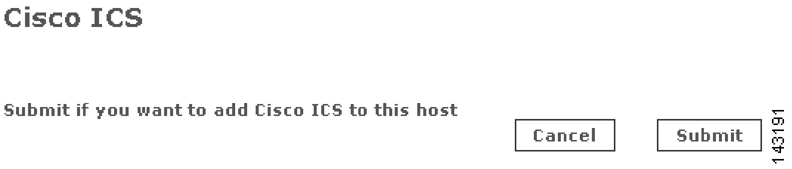
Step 5 Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in Cisco ICS server from which the syslog messages will originate.

This address is the same value as the Reporting IP address.

Step 6 Click **Apply**.

Step 7 Click **Next** to move the Reporting Applications tab.

Step 8 In the Select Application field, select **Cisco ICS 1.x**, then click **Add**.



Submit if you want to add Cisco ICS to this host

Step 9 Click **Select** to add the Cisco ICS application to this host.

Step 10 Click **Done** to save the changes.

Step 11 To activate the device, click **Activate**.

Define Rules and Reports for Cisco ICS Events

From Cisco ICS, MARS receives syslog messages that allow it to identify outbreaks, successful OPACL and OPSig deployments, and failed attempts to deploy. MARS stays abreast of when the OPACLs and OPSigs fire on Cisco IPS devices. MARS also monitors the Cisco ICS server for system issues, such as database failures.

These events assist MARS in providing an accurate, holistic assessment of your network. OPACL and OPSig matching events provide five-tuple correlation, which MARS uses to perform attack path analysis and verify the containment of threats. You can uses the events to define inspection rules that help you perform manual mitigation on devices that cannot use OPACLs and OPSigs.

For example, an inspection rule could be written to match the OPACL event. Your mitigation team can respond by investigating the OPACL that was pushed to the reporting device, from which they can determine the five tuple (source address and port, destination address and port and network service). Using that information, they could push equivalent ACLs to devices not managed by Cisco ICS.

When defining inspection rules or reports, you can access the list of Cisco ICS-specific events by entering *Cisco ICS* in the Description / CVE: field and clicking Search on the Management > Event Management page of the web interface.

There are four predefined system inspection rules for Cisco ICS:

- New Malware Discovered
- New Malware Prevention Deployed
- New Malware Prevention Deployment Failed
- New Malware Traffic Match

In addition, there are five predefined reports:

- Activity: New Malware Discovered - All Events
- Activity: New Malware Prevention Deployment Failure - All Events
- Activity: New Malware Prevention Deployment Success - All Events
- Activity: New Malware Traffic Match - All Events
- Activity: New Malware Traffic Match - Top Sources