



## CHAPTER 10

# IBM Proventia Management/ISS SiteProtector 2.0

---

This chapter contains the following topics:

- [IBM Proventia Management/ISS SiteProtector to Define Global Event Policies, page 10-1](#)
- [IBM Proventia Management/ISS SiteProtector 2.0 as A Reporting Device, page 10-5](#)

## IBM Proventia Management/ISS SiteProtector to Define Global Event Policies

To define SiteProtector as a reporting device, see [IBM Proventia Management/ISS SiteProtector 2.0 as A Reporting Device, page 10-5](#).



### Note

This topic describes how to use Site Protector to configure the ISS NIDS and HIDS; Site Protector is not a device type that can be monitored or used as an aggregation point for ISS event data from the perspective of MARS. Prior to 4.3.1 and 5.3.1, MARS could not parse event data from Site Protector, unless you developed a custom event parser for each event type.

MARS supports ISS NIDS and HIDS event retrieval via SNMP. However, when configuring ISS RealSecure sensors (NIDS) and hosts (HIDS), you must configure each active signature to send an alert to the MARS Appliance. This task can be very tedious as it must be done for each sensor and after each signature upgrade, as it resets the redirect configuration. One approach to simplifying this task is to use the SiteProtector management console to define these changes globally and apply them to each sensor.

SiteProtector 2.0 allows you to centrally manage SNMP alert destinations, such as the MARS Appliance, for group policies. You can then push these group policies to all desired host and network sensors. For each ISS signature update, you must specify the MARS Appliance as an SNMP alert destination before you apply the downloaded signatures to sensors using Site Protector.



### Note

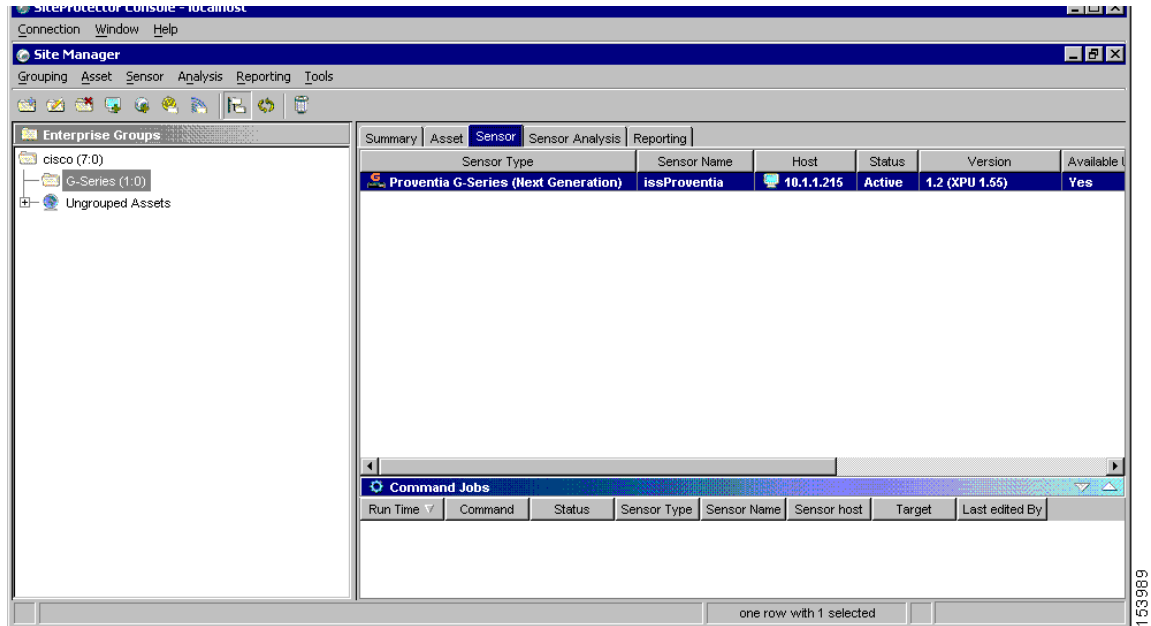
By default, the group policy response configuration is supported only on Proventia G400 and G2000 models. For all other models, including the G100 mentioned, a firmware upgrade is required. See the documentation that came with SiteProtector for more information.

To perform the major configuration steps required to use Site Protector to forward the SNMP alerts generated by sensors to MARS Appliance, follow these steps:

**Step 1** Using the Add Sensor Wizard, register the sensor to Site Protector Console.

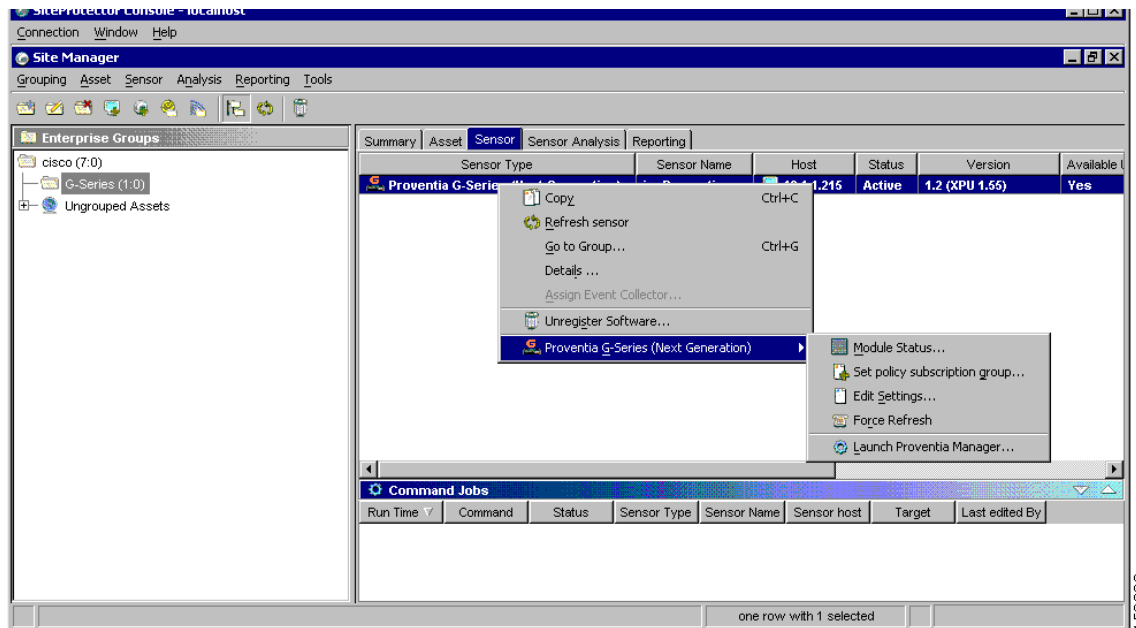
Other methods exist for registering sensors in Site Protector. For more information on using the Wizard as well as these other methods, see *Chapter 9, Registering Software Managed by SiteProtector*, on page 105 at the following URL:

<http://documents.iss.net/literature/SiteProtector/SPUserGuideforSecurityManagers20SP52.pdf>

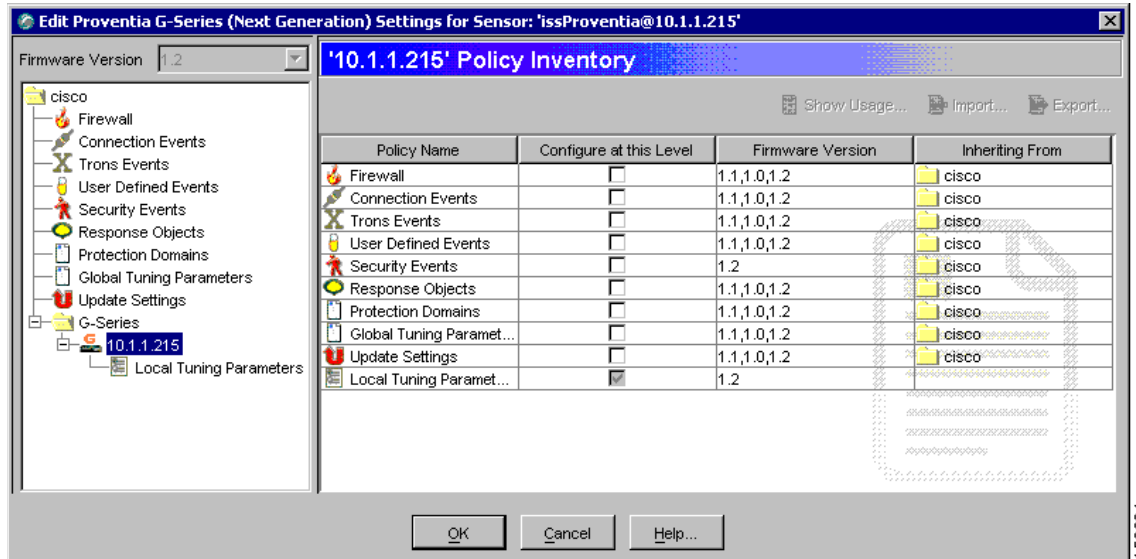


**Step 2** Right-click the sensor to edit, and click **Edit Settings** on the shortcut menu.

The Edit Settings dialog appears.

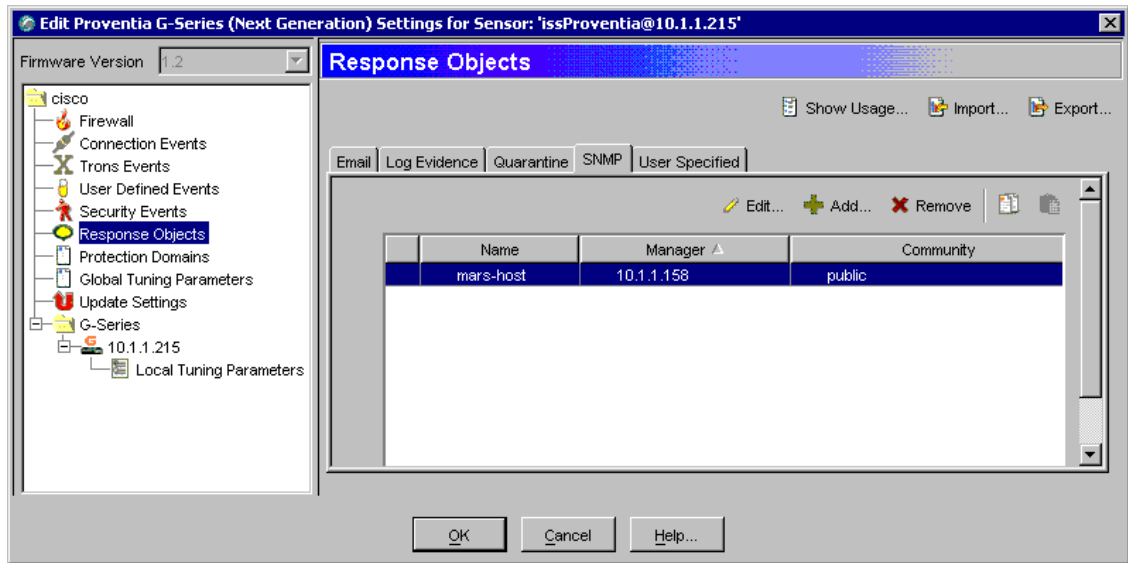


153990



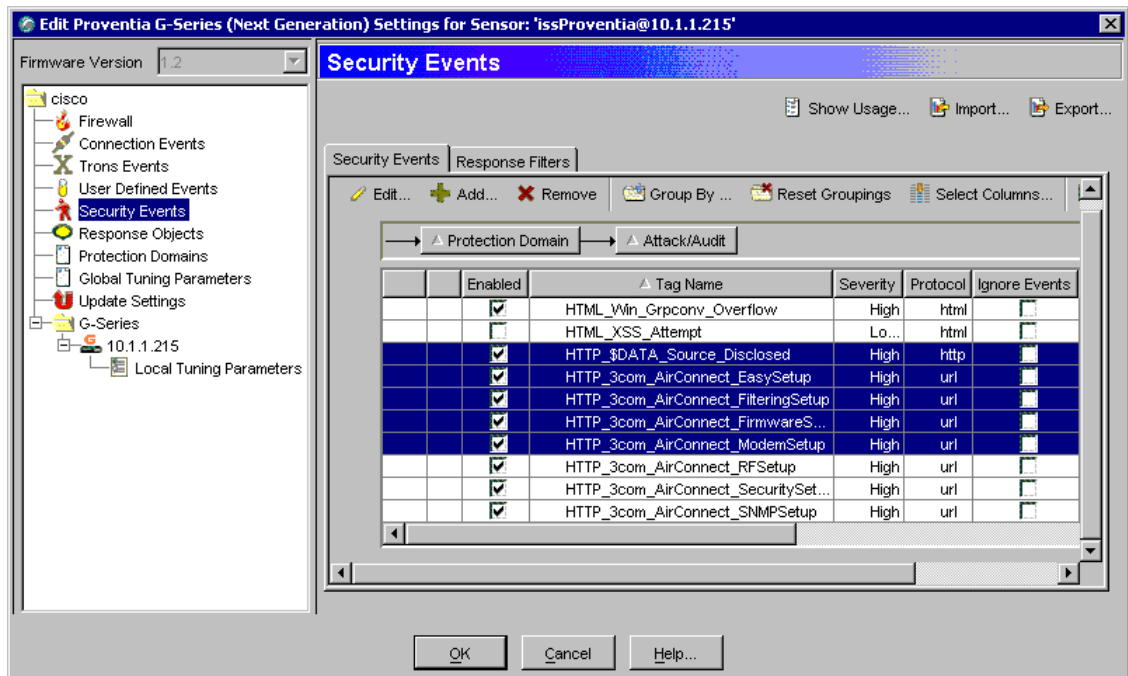
153994

- Step 3** Create a new SNMP response that sends messages to the IP address of the MARS Appliance:
- a. Select **Response Objects** from the settings tree.
  - b. Select the **SNMP** tab.
  - c. Click **Add** to create a new SNMP response object using the IP address of the MARS Appliance.



153981

**Step 4** Select the Security Events to configure new SNMP destination.



153993

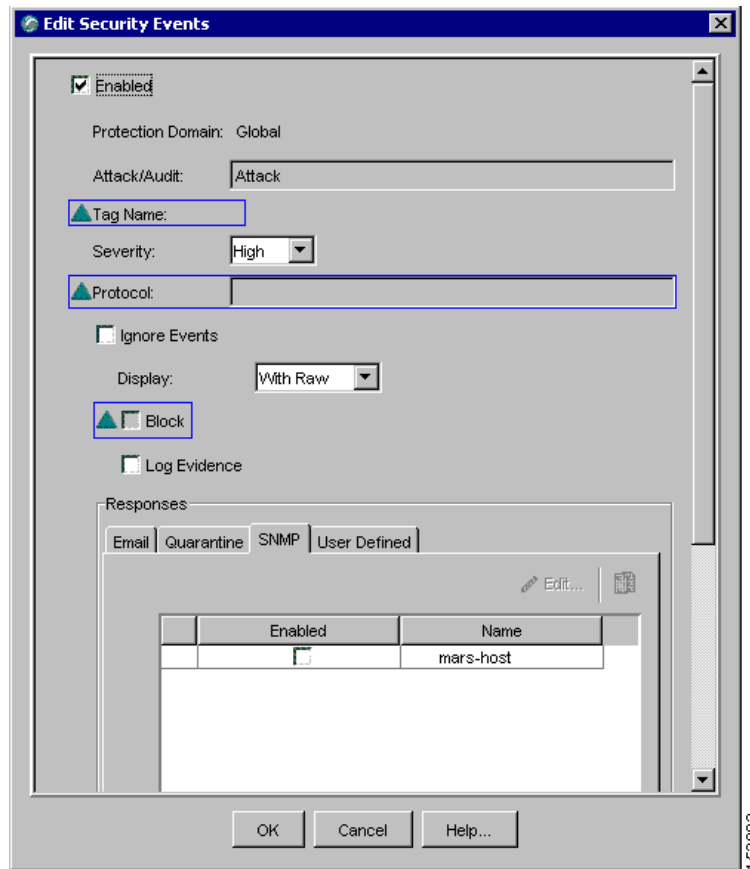
- a. Select **Security Events** under the sensor folder.
- b. Select the required security events from the Security Events tab.  
The Group By button allows you to group policies using any number of parameters.



**Note** You can also select policies and edit them at the group level.

- c. Click **Edit** to configure SNMP response of all the selected policies.

**Step 5** Select the MARS Appliance on SNMP tab.



- a. Enable all the security events by selecting the **Enabled** checkbox located at the top of the Edit Security Events dialog box.
- b. Select the **SNMP** tab under Responses, and then select the **Enabled** checkbox next to the name of MARS Appliance created in [Step 3](#).
- c. Click **OK**.

The security events and updated response target are applied to the selected sensor during the next synchronization.

## IBM Proventia Management/ISS SiteProtector 2.0 as A Reporting Device

MARS supports ISS NIDS and HIDS event retrieval via SNMP. However, when configuring ISS RealSecure sensors (NIDS) and hosts (HIDS), you must configure each active signature to send an alert to the MARS Appliance. This task can be very tedious as it must be done for each sensor and after each signature upgrade, as it resets the redirect configuration. Two approaches that simplify this task exist:

- **Use the SiteProtector management console to define these changes globally and apply them to each sensor.** In this case, MARS parses SNMP event data from the managed ISS NIDS and HIDS devices.

SiteProtector 2.0 allows you to centrally manage SNMP alert destinations, such as the MARS Appliance, for group policies. You can then push these group policies to all desired host and network sensors. For each ISS signature update, you must specify the MARS Appliance as an SNMP alert destination before you apply the downloaded signatures to sensors using Site Protector.

By default, the group policy response configuration is supported only on Proventia G400 and G2000 models. For all other models, including the G100 mentioned, a firmware upgrade is required. See the documentation that came with SiteProtector for more information.

- **Define Site Protector as a reporting device.** It acts as an aggregation point for ISS NIDS and HIDS event data . In this case, MARS parses SNMP event data from Site Protector.

This topic describes how to configure and define Site Protector as a reporting device. To enable SiteProtector as a reporting device in MARS, define the SiteProtector console as the reporting device. The SiteProtector receives alerts from the ISS 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 ISS agent that originally triggered the event, rather than the SiteProtector that forwarded it. Therefore, MARS requires host definitions for each of the ISS agents that can potentially trigger an event. These definitions are added as sub-components under the device definition of the SiteProtector console.

MARS discovers ISS agents as they generate alerts, eliminating the need to manually define them. MARS parses the alert to identify the ISS agent hostname and to discover the host operating system (OS). MARS uses this information to add any undefined agents as children of the SiteProtector 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 SiteProtector; however, you are not required to define each agent. The default topology presentation for discovered ISS agents is within a cloud.

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

This section contains the following topics:

- [Configure SiteProtector to Forward SNMP Notifications to MARS, page 10-6](#)
- [Add and Configure a SiteProtector Device in MARS, page 10-10](#)

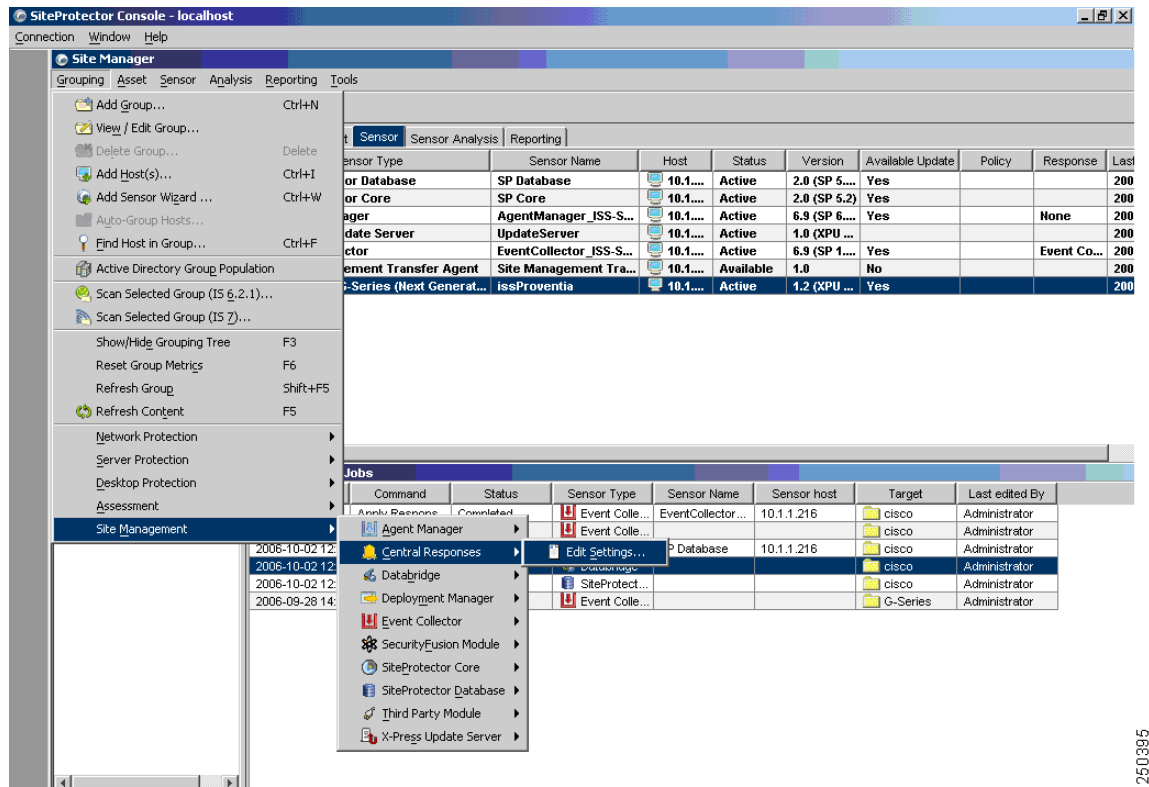
## Configure SiteProtector to Forward SNMP Notifications to MARS

The only required configuration is to ensure that SiteProtector forwards the SNMP notifications that it receives from agents to MARS. From these notifications, MARS is able to discover the agent and its relevant settings. It is also from these events that MARS learns about the host-level activities transpiring on your network.

To forward all notifications to the MARS Appliance, follow these steps:

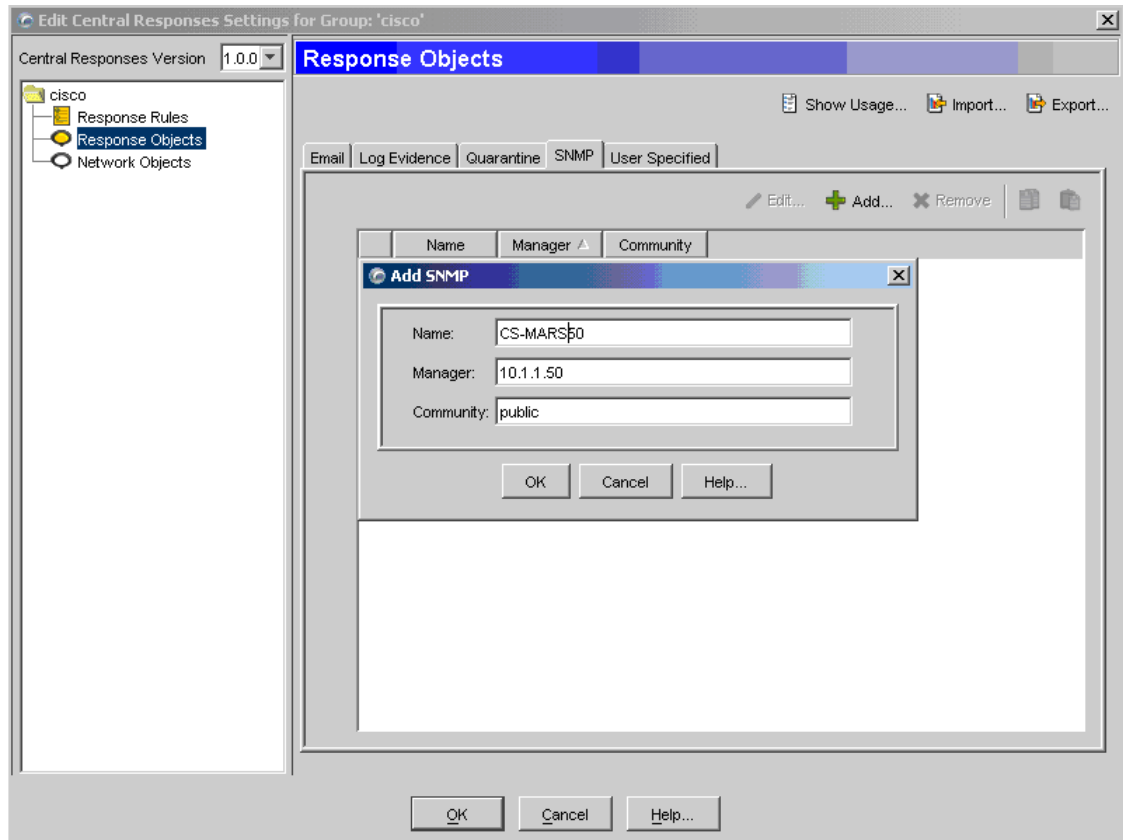
- 
- Step 1** Log in to the Site Protector console.
- Step 2** Click **Grouping > Site Management > Central Responses > Edit settings**.

The Edit Central response Settings Window appears.



250395

**Step 3** Click **Response Objects > SNMP > Add** to add a new response object that represents the MARS Appliance to which events should be forwarded.  
The Add SNMP dialog box appears.



**Step 4** Enter values for the following fields that correspond to the MARS Appliance:

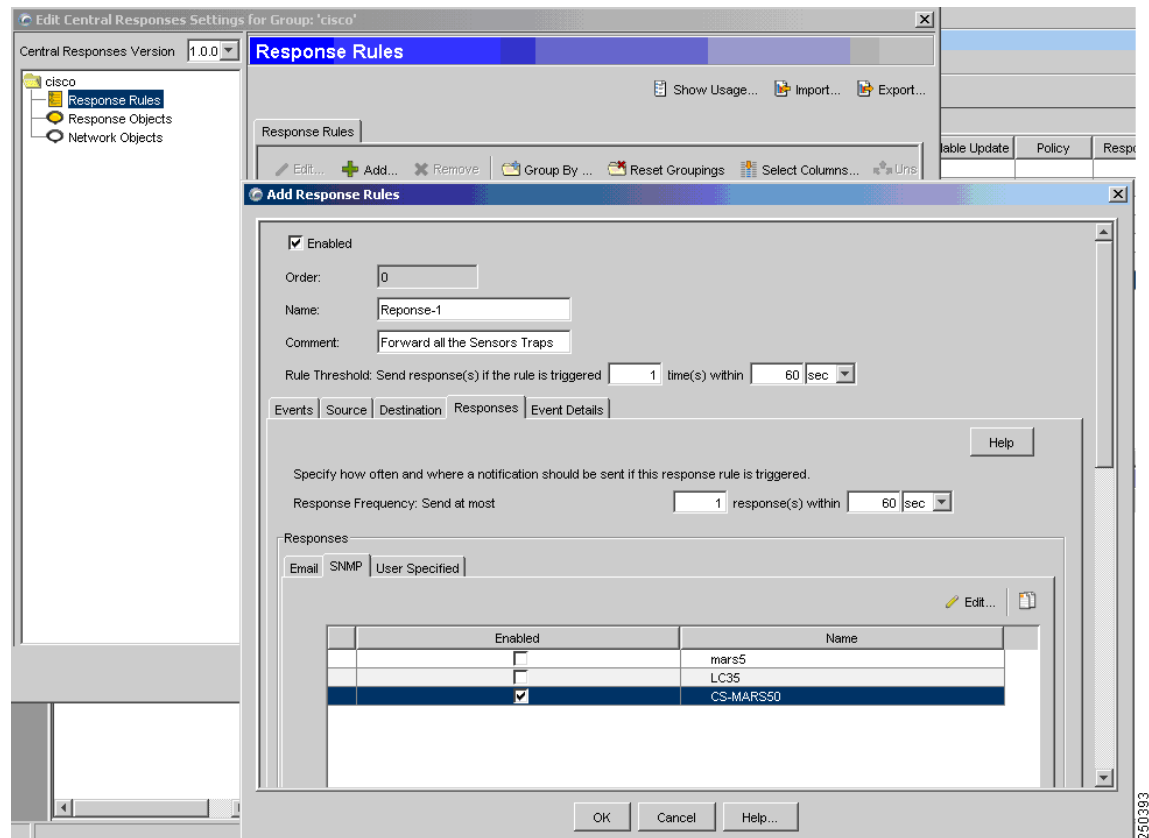
- **Name**—(hostname)
- **Manager**—(IP address)
- **Community**—(public)

**Step 5** Click **OK**.

The MARS Appliance appears as a response object. You can now define response rules forward SNMP traps to this object. The default SNMP port is 612. One or more response object is associated with each response rule. Therefore, the response object is not used until it is associated with an enabled response rule.

**Step 6** To add a response rule, click **Response Rules > Add**.

The Add Response Rules dialog box appears.



**Step 7** Specify the following value:

- **Enable**—When selected, it enables the response rule.
- **Name**—Identifies the name of the response rule.
- **Comments**—Provides a description of the response rule.

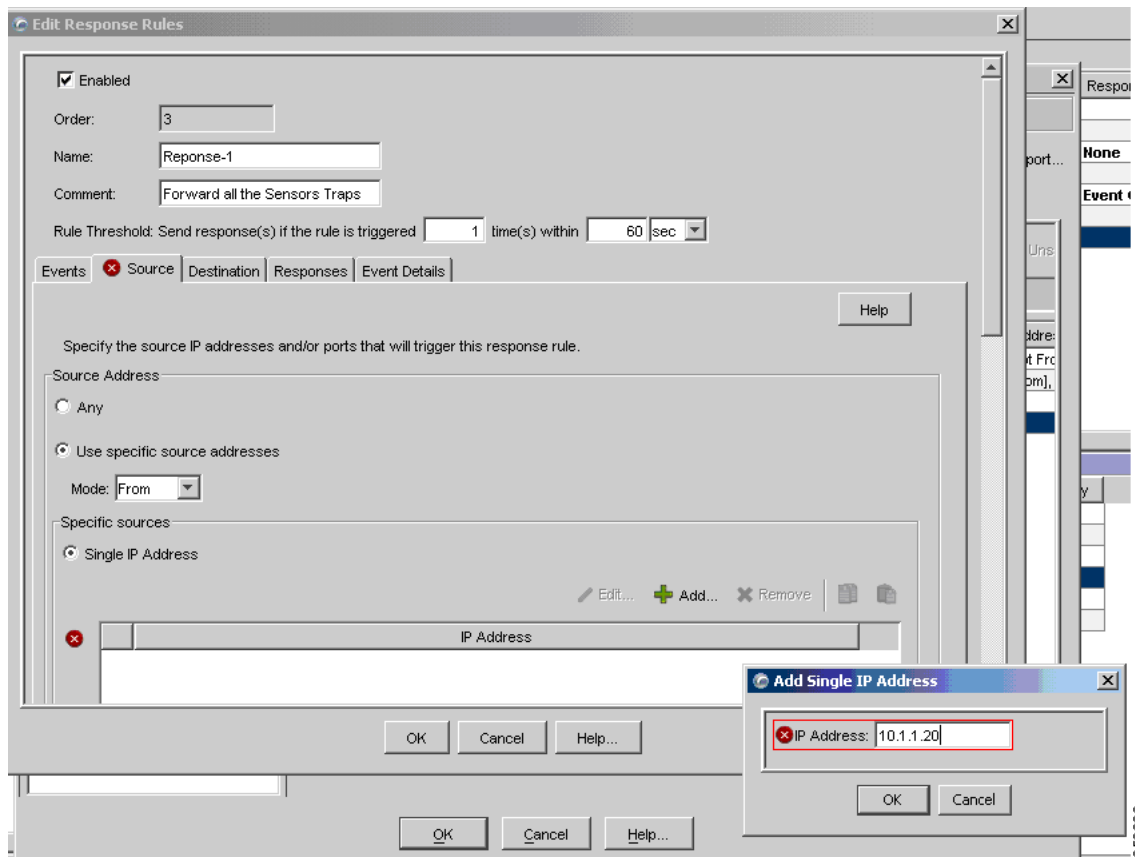
**Step 8** Click the SNMP tab, and under the Enabled column, select the checkbox next to the response object defined in [Step 4](#).



**Note** Multiple response objects can be enabled for each response rule.

**Step 9** Click on **OK** to save the rule, enable it, and enable the response object that represents the MARS Appliance.

**Step 10** (Optional) (Optional) By default, a rule matches on any source or destination IP addresses. To refine the rule to match on a specific source IP address, modify the rule, and then select the Source tab.



Specify the following values:

- **Use specific source addresses**—Select this option to restrict the rule based on IP address of the source.
- **Mode**—Specify that the rule should either be From or Not From the IP address.
- **Click Add**—Define one or more IP addresses to clarify the rule's scope.

Similarly, you can modify the rule depending on the destination IP addresses.

**Step 11** Close the program.

## Add and Configure a SiteProtector Device in MARS

Before you can identify the agents, you must add the SiteProtector to MARS. All ISS agents forward notifications to the SiteProtector, and the SiteProtector forwards SNMP notifications to MARS. Once you define the SiteProtector and activate the device, MARS can discover the agents that are managed by that SiteProtector. However, you can also choose to manually add the agents.

To add a SiteProtector to MARS, follow these steps:

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

- Step 2** From the Device Type list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.
- Step 3** Enter the Device Name and IP addresses if adding a new host.
- Step 4** Click **Apply**.
- Step 5** Click **Reporting Applications** tab.
- Step 6** From the Select Application list, select **ISS SiteProtector 2.x**.
- Step 7** Click **Add**.

The Management Console page appears.

- Step 8** Do one of the following:
- To save your changes and allow the ISS agents to be discovered automatically, click **Submit**, and then click **Done**.




---

**Note** Discovered agents are named Generic Real Secure agent, as no version information is contained in the SNMP events.

---

- To add a single ISS RealSecure NIDS or ISS RealSecure HIDS agent manually, continue with [Add an ISS Agent Manually, page 10-11](#).
- 

## Add an ISS Agent Manually

MARS automatically discovers ISS agents when it receives an event from the agent. Discovered agents are named Generic Real Secure agent, as no version information is contained in the SNMP events. However, you can manually add a ISS Agent (ISS RealSecure NIDS or ISS RealSecure HIDS devices) as a child of the SiteProtector device. This feature allows you to represent all of your agents, even if they have not generated any notifications. In turn, this definition allows you to identify devices that are not reporting results.



### 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 ISS Agents manually, follow these steps:

---

- Step 1** Click **Admin > Security and Monitoring Devices**.
- Step 2** From the list of devices, select the host running SiteProtector, and click **Edit**.
- Step 3** Click the **Reporting Applications** tab, select **ISS SiteProtector** in the Device Type list, and click **Edit**.
- Step 4** Click the **Add Agent**.
- Step 5** Do one of the following:
- Select the existing device, click **Edit Existing**, and continue with [Step 8](#).  
A page displays with the values pre-populated for hostname, reporting IP address, and at least one interface.

- Click **Add New**, and continue with [Step 6](#).
- Step 6** In the Device Name field, enter the hostname on which this ISS Agent resides.  
This value should reflect the DNS entry for this device.
- Step 7** In the Reporting IP field, enter the IP address that the agent uses to send logs to the SiteProtector.
- Step 8** Define each interface that is configured for this host by specifying the interface name, IP address, and network mask. To add a new interface, click **Add Interface**.  
The interface settings are used for attack path calculation. It is very important that you identify any dual-homed hosts by defining each interface.
- Step 9** In the Device Application field, select one of the following values:
- **ISS RealSecure 6.5**
  - **ISS RealSecure 7.0**
- Step 10** Select either the **NIDS** or **HIDS** option.  
If you select HIDS, the Monitored Networks field disappears.
- Step 11** If you selected NIDS, continue with [Step 12](#). Otherwise, continue with [Step 14](#).

The screenshot displays the configuration interface for adding a new ISS RealSecure agent. The top section, titled "A ISS RealSecure agent will be added to WIN2003 device.", contains the following fields:

- \*Device Name:** WIN2003
- Reporting IP:** Four empty input boxes for IP address.
- Select application:** A dropdown menu with "ISS RealSecure 6.5" selected.
- Device Type:** Radio buttons for  NIDS and  HIDS.

The bottom section, titled "[Optional: for attack path calculation and mitigation enter monitoring networks information]", contains the **Monitored Networks:** field. It features a large empty list box on the left. To the right, there are two options:

- Select a Network:** A radio button that is selected, with a dropdown menu showing "10.1.1.0/255.255.255.0( n-10.1.1.0/24 )".
- Define a Network:** A radio button that is unselected, with input fields for **Network IP:** (four boxes) and **Mask:** (four boxes).

Buttons for **Add** and **Remove** are located between the list box and the network selection options. A vertical ID number "250391" is visible on the right side of the interface.

- Step 12** For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:
- To manually define the networks, select the **Define a Network** radio button.
    - Enter the network address in the Network IP field.
    - Enter the corresponding network mask value in the Mask field.
    - Click **Add** to move the specified network into the Monitored Networks field.
    - Repeat as needed.

- To select the networks that are attached to the device, click the **Select a Network** radio button.
  - a. Select a network from in the Select a Network list
  - b. Click **Add** to move the specified network into the Monitored Networks field.
  - c. Repeat as needed.

**Step 13** Continue with [Step 16](#).

**Step 14** For multiple interfaces, click on **Add Interfaces**, and specify the new interfaces' name, IP address, and network mask.

**Figure 10-1** Adding Multiple Interfaces

→ A ISS RealSecure agent will be added to WIN2003 device.

→ \*Device Name: WIN2003

→ Reporting IP: ...

→ Select application: ISS RealSecure 6.5

→  NIDS  HIDS

Name: IP Address: Network Mask:

250390

**Step 15** Click **Apply**.

**Step 16** Click **Submit**, and then click **Done**.

**Step 17** To activate this device, click **Activate**.

