Configuring a Cisco Secure IDS Sensor in CSPM

Document ID: 6117

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configuration
Define the Network on Which the CSPM Host Resides
Add the CSPM Host
Add the Sensor Device
Configure the Sensor
Related Information

Introduction

This document explains the procedure used to configure a Cisco Secure Intrusion Detection System (IDS) Sensor on Cisco Secure Policy Manager (CSPM). This document assumes that you have installed CSPM version 2.3.I on your computer. Version "I" allows management of IDS devices (appliance Sensors, Cisco IOS® routers, or IDS Blades) in a Cisco Catalyst® 6000 switch. This document also assumes that the IDS postoffice parameters are correctly defined. These include HOSTID, ORGID, HOSTNAME, and ORGNAME. Please note that for the CSPM host to communicate with a Sensor, the ORGID and ORGNAME must match what is defined on the Sensor.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on CSPM 2.3.I and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

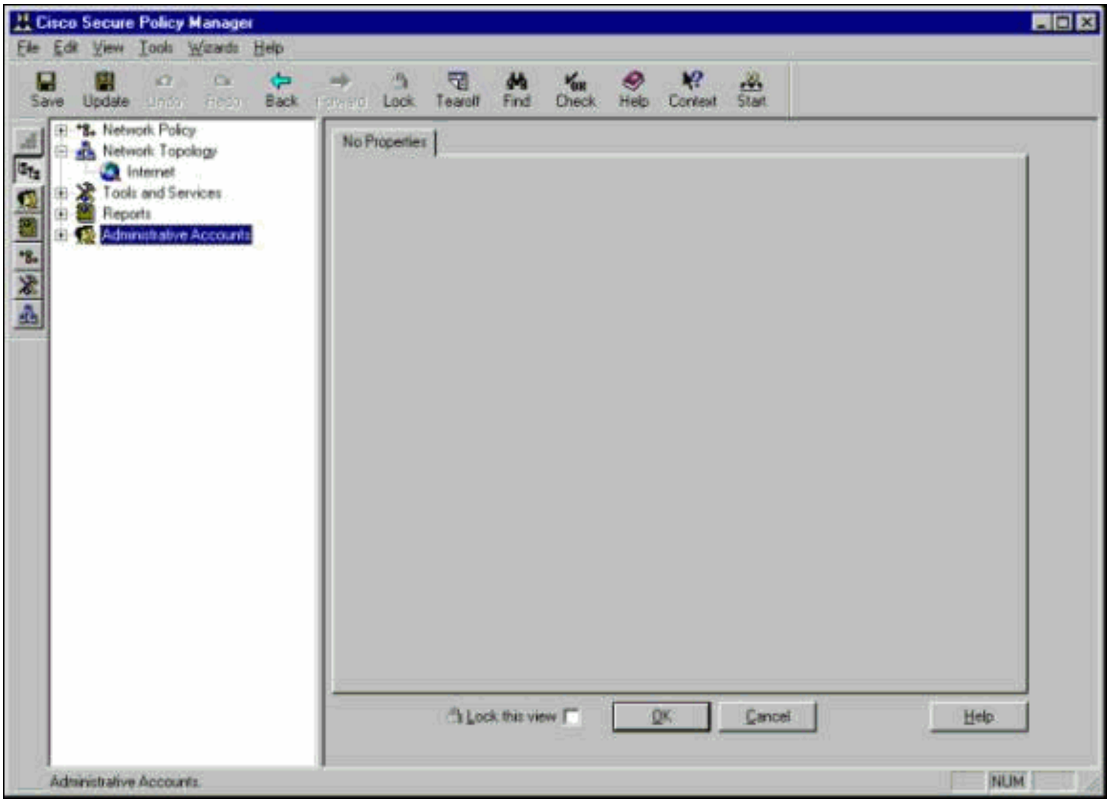
Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configuration

These sections explain the process used to configure an IDS sensor in CSPM.

Launch CSPM and log in. A blank template appears (initial launch) that allows you to define your network.



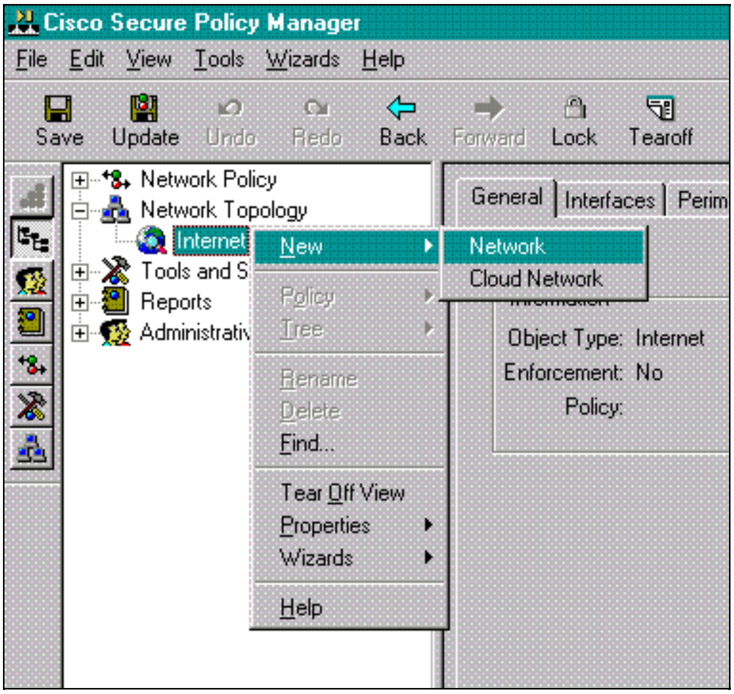
These three definitions are required in the CSPM topology for IDS.

1. Define the network in which the control interface of the Sensor resides and the network in which the CSPM host resides. If they are on the same subnet, then only one network needs to be defined. Define this network first.
2. Define the CSPM host in its network. Without the CSPM host definition, the Sensor cannot be managed.
3. Define the Sensor in its network.

Define the Network on Which the CSPM Host Resides

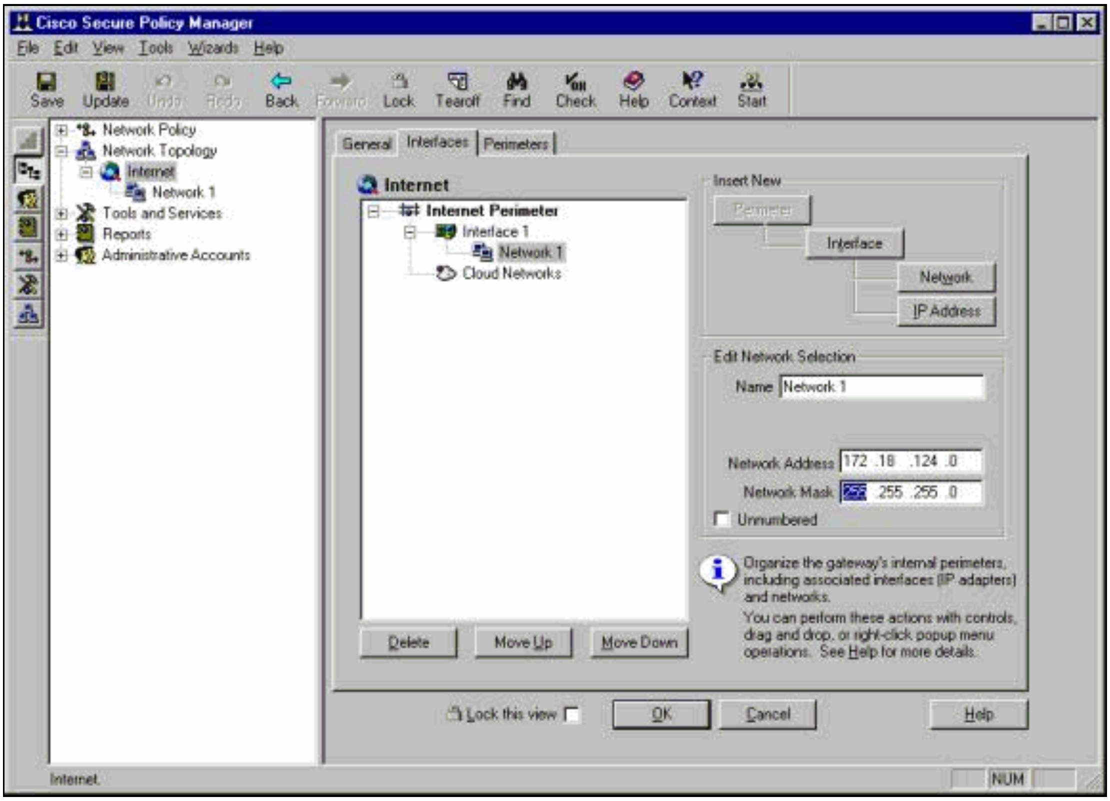
Complete these steps:

1. Right−click on the **Internet** icon in the topology and select **New** > **Network** to create a new network.



Object Type: Internet
Enforcement: No
Policy:

2. On the right hand side of the Network Panel, add the name of the new network, the network address, and the netmask that will be used.



Name: Network 1

Network Address: 172 .18 .124 .0

Network Mask: 255 .255 .255 .0

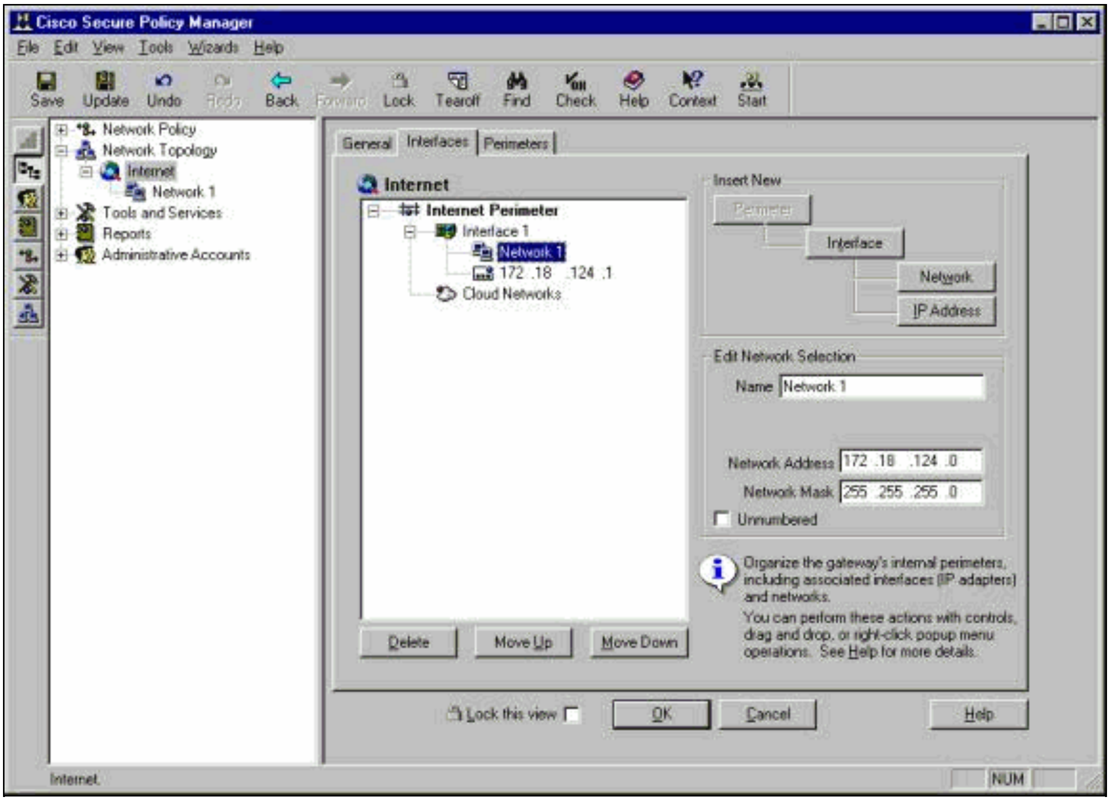
☐ Unnumbered

Organize the gateway's internal perimeters, including associated interfaces (IP adapters) and networks.
You can perform these actions with controls, drag and drop, or right-click popup menu operations. See Help for more details.

3. Click the **IP Address** button, and enter the IP address for your network that it uses to reach the Internet.

   Normally it is the Default Gateway for the network.

   Note: When you manage Sensors, the gateway address does not necessarily have to be correct since the Sensor is not sent this default gateway information. It should already be defined in the Sensor.
4. Click **OK**. The network is added to the topology map without any errors.



Edit Network Selection

Name: Network 1

Network Address: 172 .18 .124 .0

Network Mask: 255 .255 .255 .0

□ Unnumbered

Organize the gateway's internal perimeters, including associated interfaces (IP adapters) and networks.

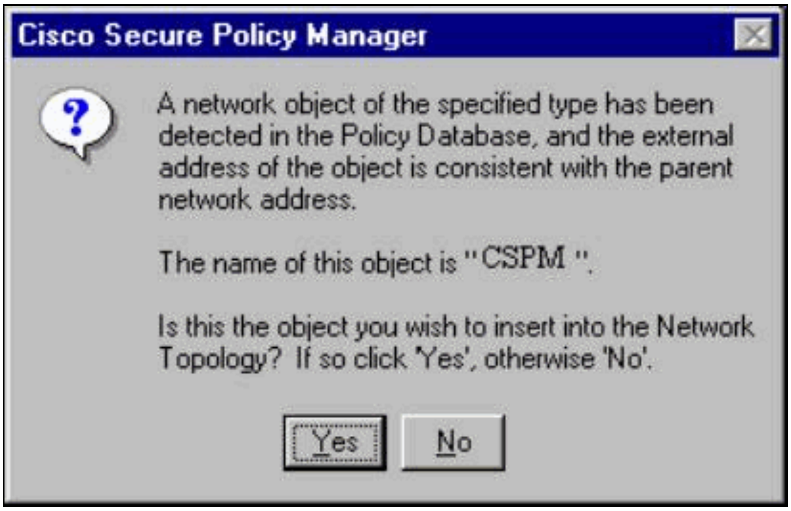
You can perform these actions with controls, drag and drop, or right-click popup menu operations. See Help for more details.

Add the CSPM Host

Use this procedure to add the CSPM host.

1. In the Network Topology, right−click on the network you just added and select **New** > **Host**.

   CSPM brings up a screen similar to this. If not, then the network you just defined is not the network in which your CSPM host is located. Check the IP address on your CSPM host again.



Cisco Secure Policy Manager

A network object of the specified type has been detected in the Policy Database, and the external address of the object is consistent with the parent network address.

The name of this object is "CSPM ".

Is this the object you wish to insert into the Network Topology? If so click 'Yes', otherwise 'No'.

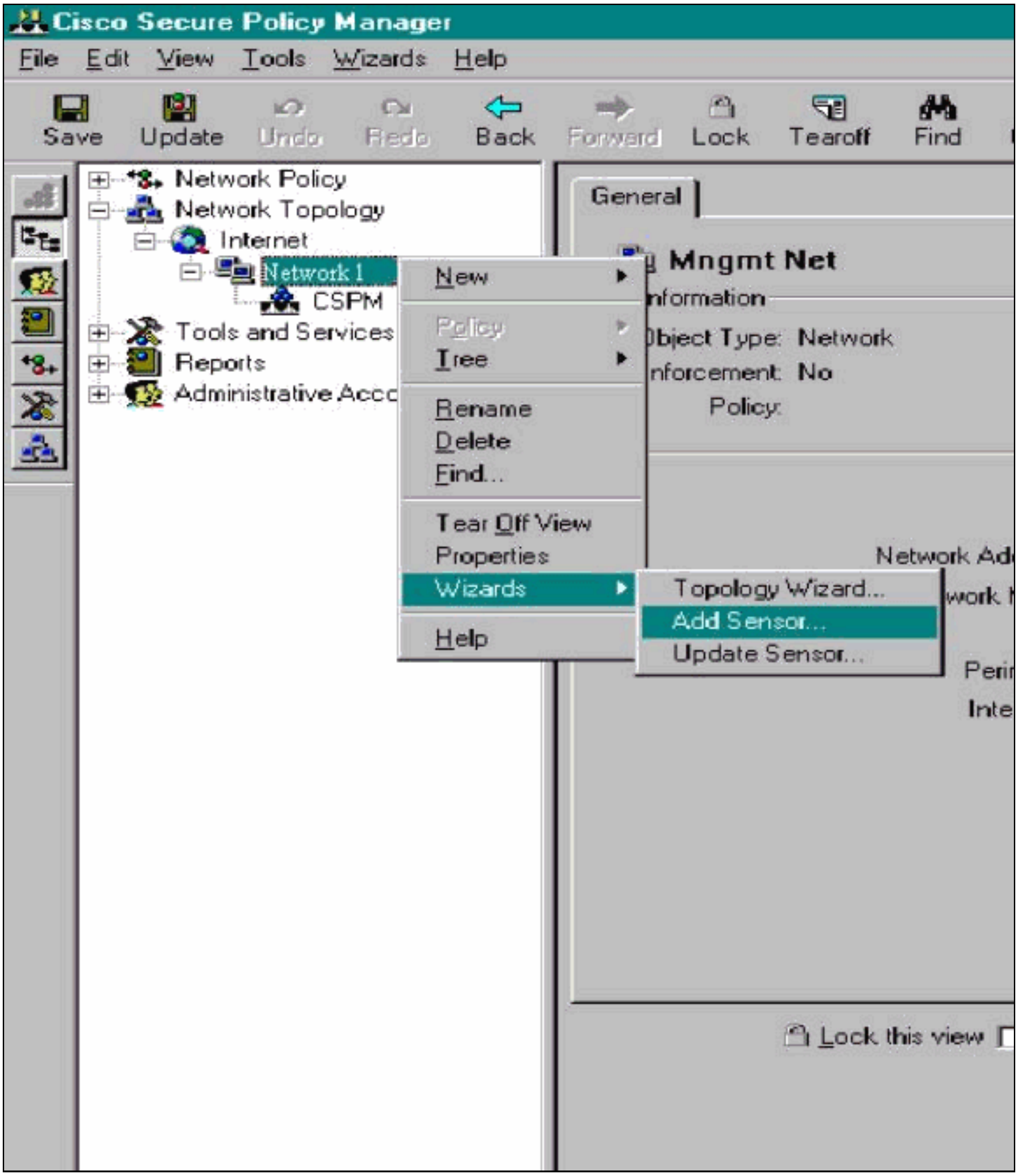
2. Click **Yes** to install the CSPM host into the topology.
3. Verify that the information on the General screen for the CSPM host is ok.
4. Click **OK** on the General screen of the CSPM host.

Add the Sensor Device

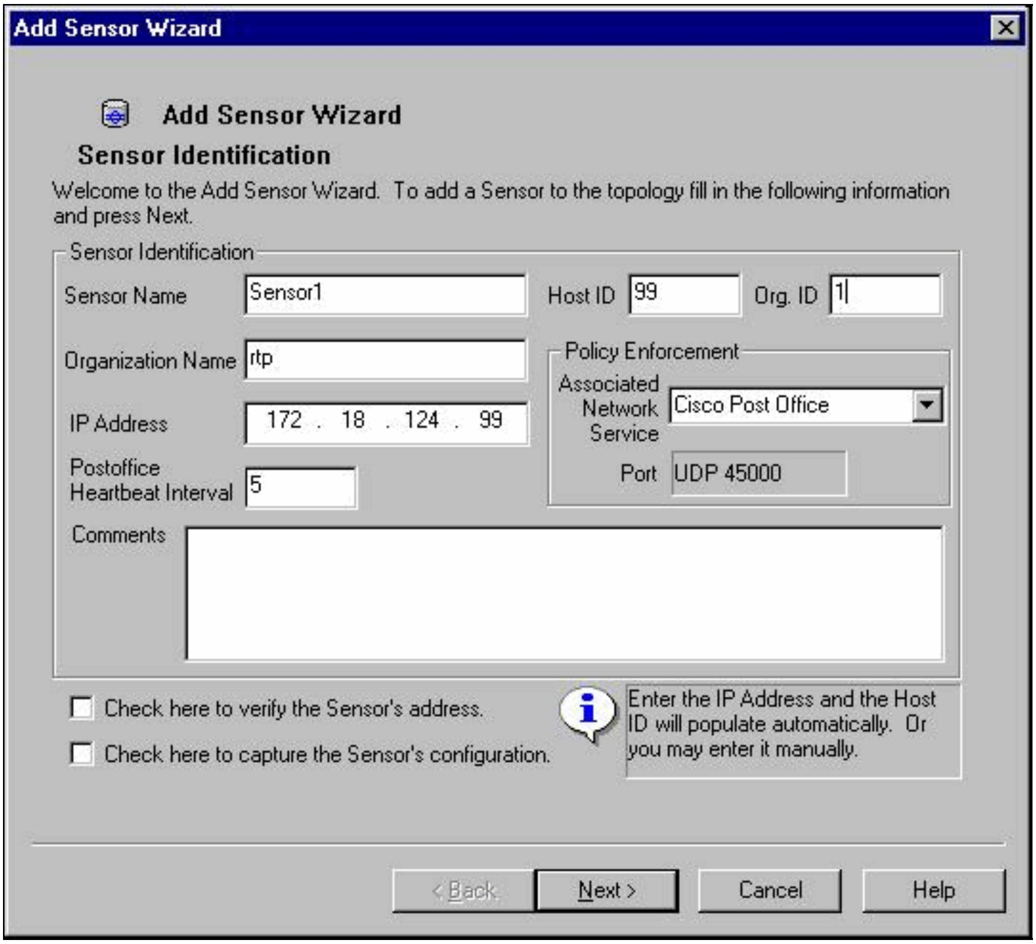
Use this procedure to add the Sensor device.

1. Right−click on the network in which your Sensor resides and select **Wizards** > **Add Sensor**.

   Note: If the CSPM host and the control interface of your Sensor are not in the same network, define the network in which your Sensor resides.

2. Enter the correct postoffice parameters for the Sensor.



Add Sensor Wizard

Add Sensor Wizard

Sensor Identification

Welcome to the Add Sensor Wizard. To add a Sensor to the topology fill in the following information and press Next.

Sensor Identification

Sensor Name: Sensor1

Host ID: 99

Org. ID: 1

Organization Name: rtp

IP Address: 172 . 18 . 124 . 99

Postoffice Heartbeat Interval: 5

Comments:

Policy Enforcement

Associated Network Service: Cisco Post Office

Port: UDP 45000

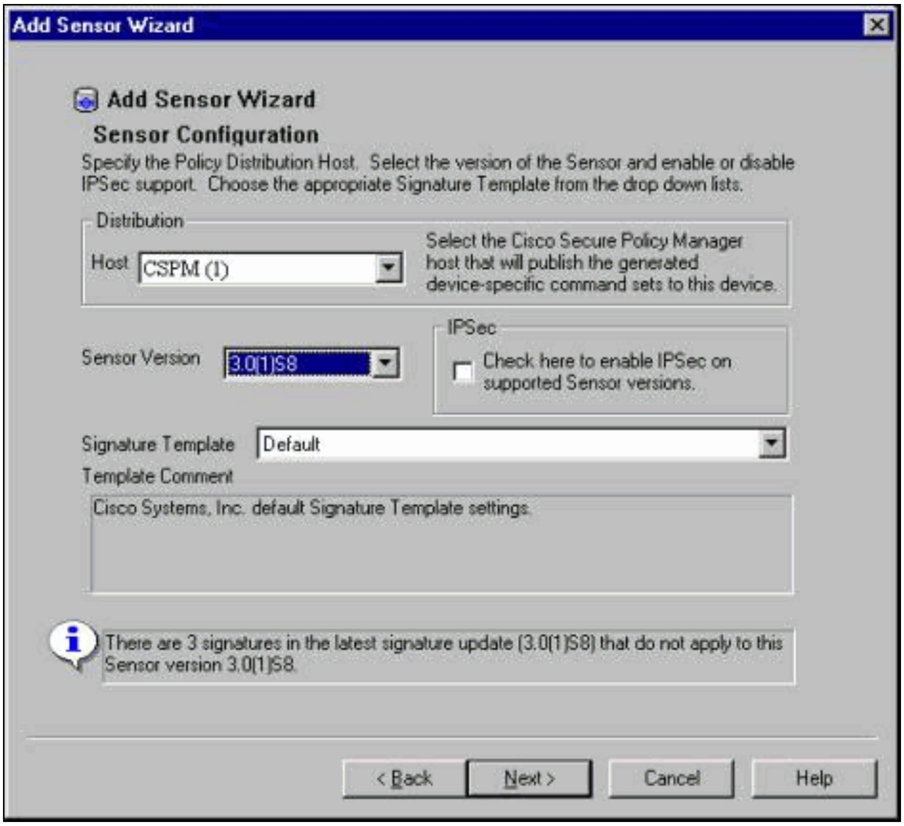
☐ Check here to verify the Sensor's address.

☐ Check here to capture the Sensor's configuration.

Enter the IP Address and the Host ID will populate automatically. Or you may enter it manually.

3. Click the **Check here to verify the Sensor's address** box.

   Note: If this is the first time you are setting up this Sensor, you do not want to capture the Sensor's configuration. If you have previously configured this Sensor elsewhere either via a UNIX director or another CSPM host and have made configuration changes to the Sensors signatures, then you want to capture the Sensor's configuration.
4. Click **Next** to define the signature versions on the Sensor. You can also issue the **nrvers** command to check this on the Sensor.



Add Sensor Wizard

Add Sensor Wizard

Sensor Configuration

Specify the Policy Distribution Host. Select the version of the Sensor and enable or disable IPSec support. Choose the appropriate Signature Template from the drop down lists.

Distribution

Host: CSPM (1)

Select the Cisco Secure Policy Manager host that will publish the generated device-specific command sets to this device.

Sensor Version: 3.0(1)S8

IPSec

□ Check here to enable IPSec on supported Sensor versions.

Signature Template: Default

Template Comment

Cisco Systems, Inc. default Signature Template settings.

There are 3 signatures in the latest signature update (3.0(1)S8) that do not apply to this Sensor version 3.0(1)S8.

Note: If CSPM does not have the correct Sensor version that you are running on your Sensor, update the signatures on your CSPM host. Please see Software Download (registered customers only) for updates.

5. Click the **Next** button to continue.
6. Click **Finish** to complete the installation of the Sensor into the topology.
7. From the main CSPM menu, select **File** > **Save** and **Update** to compile the information entered in the topology into CSPM. Please note that this step is necessary to start the postoffice protocol on the CSPM host.
8. Verify that everything works by logging into your Sensor as the netrangr user.
9. Execute the **nrconns** command.

```
>nrconns

Connection Status for gacy.rtp

               cspm.rtp Connection 1: 172.18.124.106   45000 1
               [Established]  sto:0004 with Version 1

netrangr@gacy:/usr/nr

>
```

Note: If the Sensor and CSPM host are not communicating, output similar to this appears instead:

```
netrangr@gacy:/usr/nr

>nrconns

Connection Status for gacy.rtp

          insane.rtp Connection 1: 172.18.124.194   45000 1 [SynSent]
          sto:5000  syn NOT rcvd!
```

```
netrangr@gacy:/usr/nr
```

If this is the case, get a sniffer trace to see if both sides are sending UDP 45000 packets. UDP 45000 is what IDS devices use to communicate with each other. To test this on the Sensor, **su** to root and (depending on what Sensor you have) execute **snoop −d iprb1 port 45000** (for an IDS 4210 Sensor) and **snoop −d iprb0 port 45000** (for any other model of Sensor).

Use **<control−c>** to break out of a snoop session.

This output appears if there is no communications between the Sensor and CSPM:

```
netrangr@gacy:/usr/nr

>su −

Password:

Sun Microsystems Inc.   SunOS 5.8       Generic February 2000

# snoop −d spwr0 port 45000

Using device /dev/spwr (promiscuous mode)

  172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52

  172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52

  172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52

  172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52

^C#
```

In the above output, the Sensor sends UDP 45000 packets, but does not receive any. A correct configuration produces output similar to this:

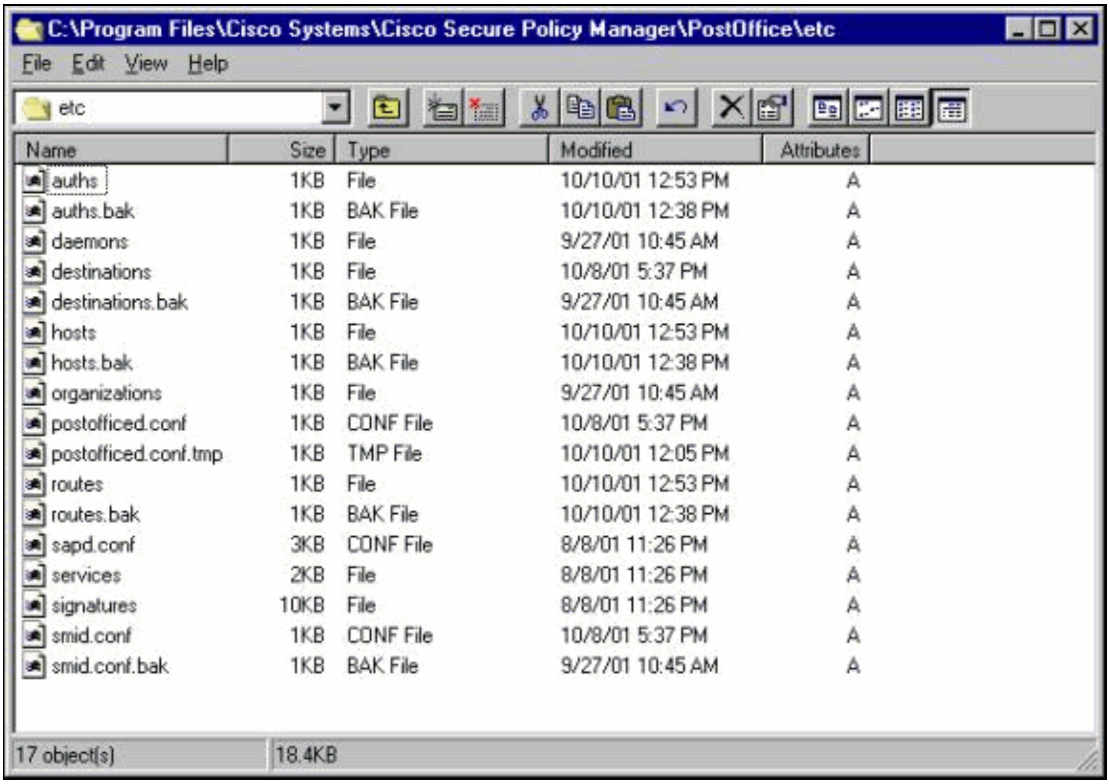
```
# snoop −d spwr0 port 45000

Using device /dev/iprb (promiscuous mode)

172.18.124.106 -> gacy         UDP D=45000 S=45000 LEN=56

        gacy -> 172.18.124.106 UDP D=45000 S=45000 LEN=56

172.18.124.142 -> gacy         UDP D=45000 S=45000 LEN=56

        gacy -> 172.18.124.194 UDP D=45000 S=45000 LEN=56
```

In the above output, UDP 45000 traffic goes in both directions.

If UDP 45000 packets flow in both directions and the output of **nrconns** on the Sensor still says that there is no connection established, the postoffice parameters on the Sensor and the CSPM host do not match.

To check the postoffice parameters on the CSPM host manually:

a. Use Windows Explorer to navigate to where you have CSPM installed on the NT machine.



C:\Program Files\Cisco Systems\Cisco Secure Policy Manager\PostOffice\etc

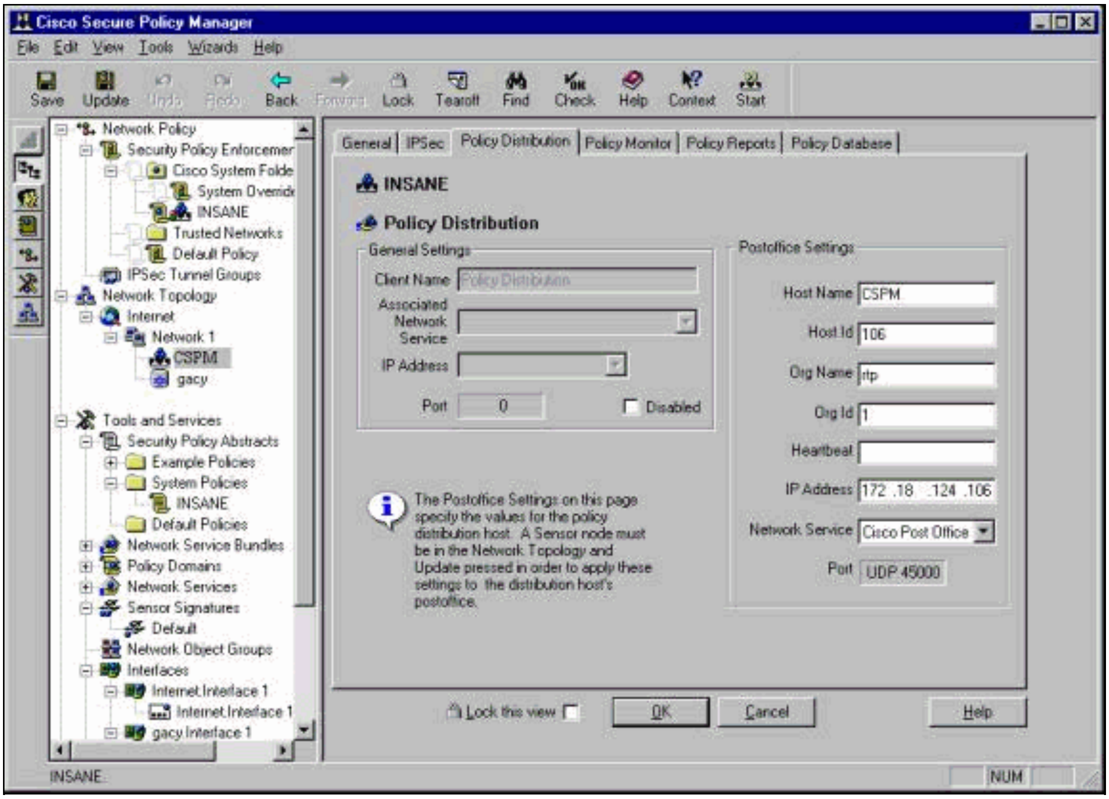
Name	Size	Type	Modified	Attributes
auths	1KB	File	10/10/01 12:53 PM	A
auths.bak	1KB	BAK File	10/10/01 12:38 PM	A
daemons	1KB	File	9/27/01 10:45 AM	A
destinations	1KB	File	10/8/01 5:37 PM	A
destinations.bak	1KB	BAK File	9/27/01 10:45 AM	A
hosts	1KB	File	10/10/01 12:53 PM	A
hosts.bak	1KB	BAK File	10/10/01 12:38 PM	A
organizations	1KB	File	9/27/01 10:45 AM	A
postofficed.conf	1KB	CONF File	10/8/01 5:37 PM	A
postofficed.conf.tmp	1KB	TMP File	10/10/01 12:05 PM	A
routes	1KB	File	10/10/01 12:53 PM	A
routes.bak	1KB	BAK File	10/10/01 12:38 PM	A
sapd.conf	3KB	CONF File	8/8/01 11:26 PM	A
services	2KB	File	8/8/01 11:26 PM	A
signatures	10KB	File	8/8/01 11:26 PM	A
smid.conf	1KB	CONF File	10/8/01 5:37 PM	A
smid.conf.bak	1KB	BAK File	9/27/01 10:45 AM	A

17 object(s) 18.4KB

b. Edit the host, route, and organization files with Write or Wordpad (do not use Notepad because the formatting will be corrupted).

c. Ensure that these files look correct for your installation. If any of the values are not correct, edit them and reboot your NT computer using these steps:

a. Click on the **CSPM** icon in the network topology.
b. Click on the Policy Distribution tab to enter your postoffice parameters.
c. **Save** and **Update** your changes.
d. Reboot the NT computer.



Cisco Secure Policy Manager

INSANE

Policy Distribution

General Settings

Client Name: Policy Distribution
Associated Network Service:
IP Address:
Port: 0
□ Disabled

Postoffice Settings

Host Name: CSPM
Host Id: 106
Org Name: rtp
Org Id: 1
Heartbeat:
IP Address: 172 .18 .124 .106
Network Service: Cisco Post Office
Port: UDP 45000

The Postoffice Settings on this page specify the values for the policy distribution host. A Sensor node must be in the Network Topology and Update pressed in order to apply these settings to the distribution host's postoffice.

Configure the Sensor

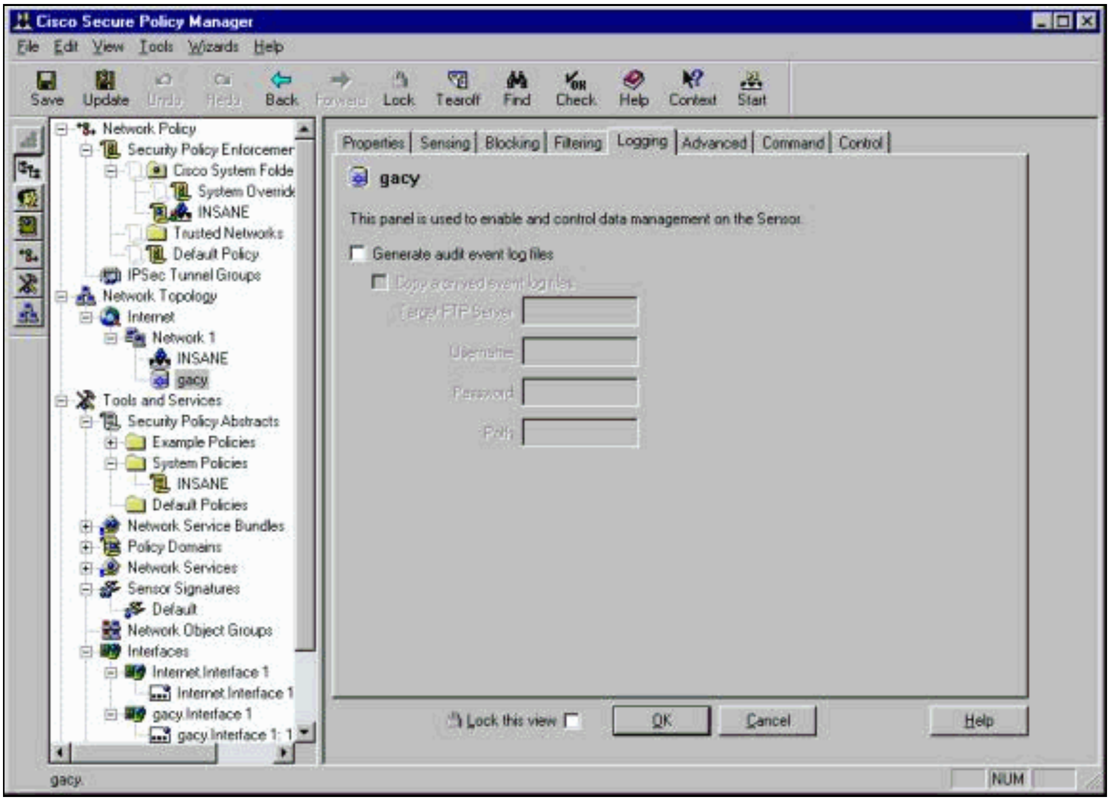
After the configuration is saved in CSPM, configure the Sensor. In order to do this, first set the Sensor to write the alarms that it sees to its own log. Then set the Sensor to "sniff" on the correct interface.

Write Alarms to the Log

Use this procedure to write alarms to the log.

1. Click the **Generate audit event log files** box to tell the Sensor to send the alarms to its local logs.

   It also sends alarms to the CSPM box by default after you push a configuration down to it.

   gacy

   This panel is used to enable and control data management on the Sensor.

   □ Generate audit event log files

   □ Copy archived event log files

   Target FTP Server

   Username

   Password

   Path

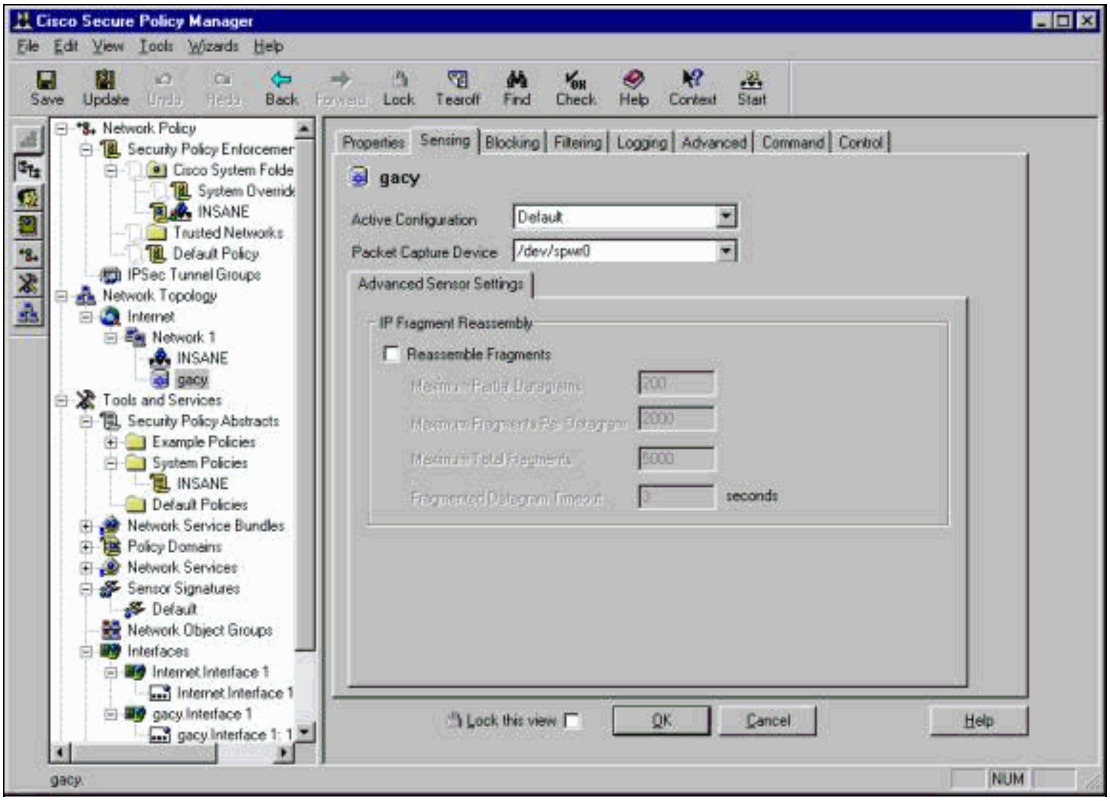
2. Click **OK** to continue.

Set the Sensor to "Sniff"

Use this procedure to set the Sensor to "Sniff".

1. Select the Sensor in your CSPM topology and click the Sensing tab.
2. Define the Packet Capture Device:

   - iprb0 − for an IDS 4210 Sensor
   - spwr0 − for any other Sensor model



gacy

Active Configuration: Default

Packet Capture Device: /dev/spwr0

Advanced Sensor Settings

IP Fragment Reassembly

□ Reassemble Fragments

Maximum Partial Datagrams: 200

Maximum Fragments Per Datagram: 2000

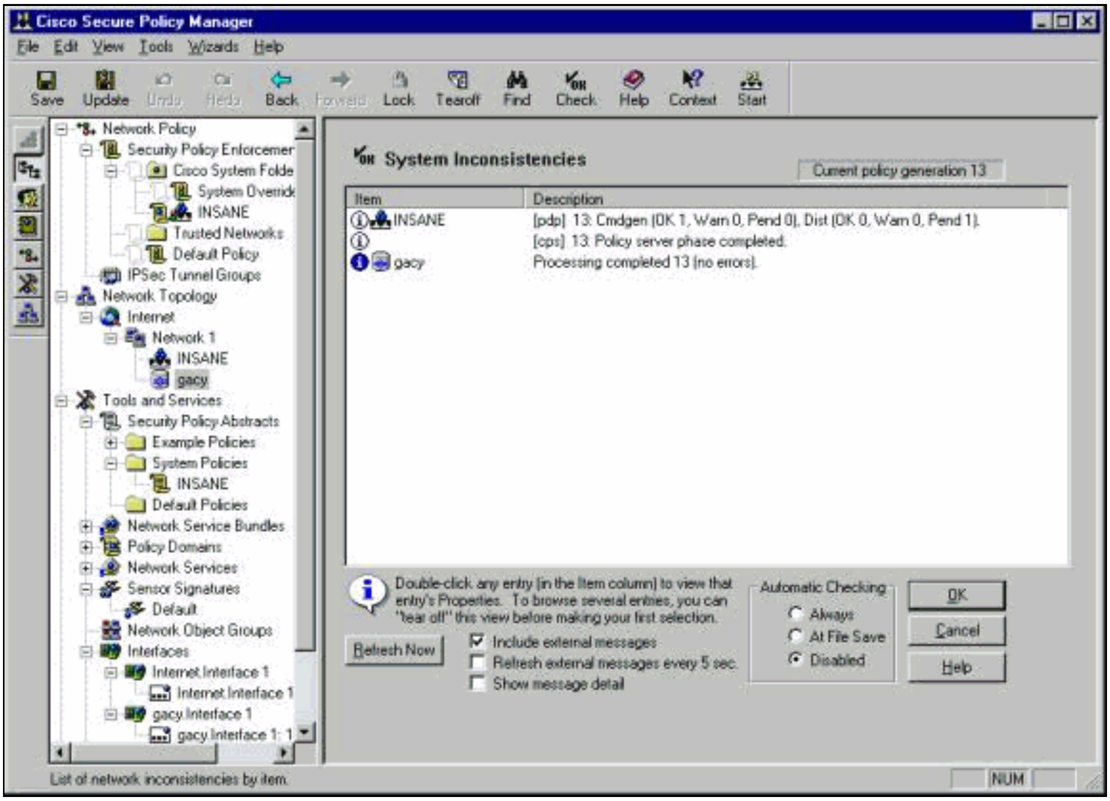
Maximum Total Fragments: 5000

Fragmented Datagram Timeout: 3 seconds

Lock this view □

3. Click **OK** to continue.
4. Click the **Update** icon on the CSPM menu bar to update CSPM with the information.

   Note: If everything goes well, a screen similar to this appears. Notice there are no red errors. Yellow warnings are typically ok.



System Inconsistencies

Current policy generation 13

Item	Description
INSANE	[pdp] 13: Cmdgen (OK 1, Warn 0, Pend 0), Dist (OK 0, Warn 0, Pend 1).
	[cps] 13: Policy server phase completed.
gacy	Processing completed 13 (no errors).

Double-click any entry (in the Item column) to view that entry's Properties. To browse several entries, you can "tear off" this view before making your first selection.

☑ Include external messages

□ Refresh external messages every 5 sec.

□ Show message detail

Automatic Checking

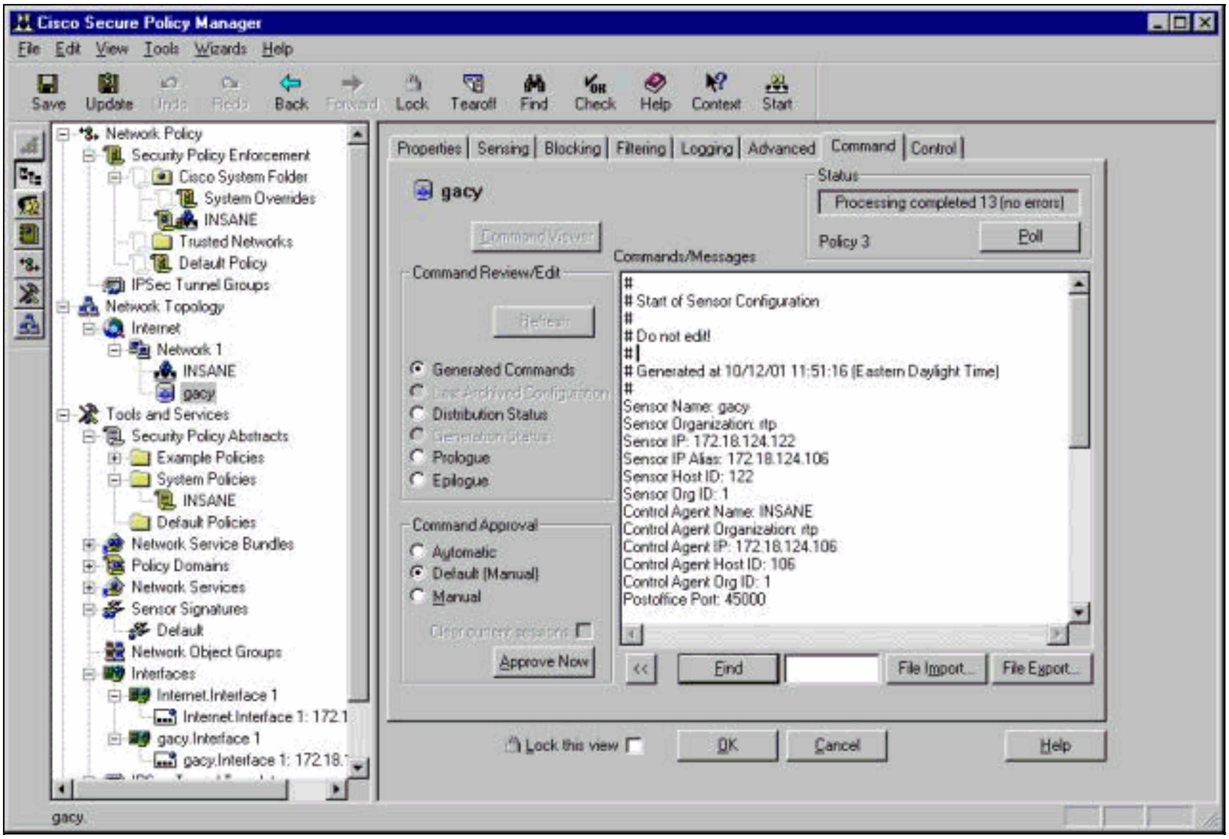
○ Always

○ At File Save

● Disabled

List of network inconsistencies by item.

5. Select the Sensor in the network topology and click the Command tab to send the updated configuration to the Sensor.



Status: Processing completed 13 (no errors)

Policy 3

Command Review/Edit

● Generated Commands
○ Last Archived Configuration
○ Distribution Status
○ Generation Status
○ Prologue
○ Epilogue

Command Approval

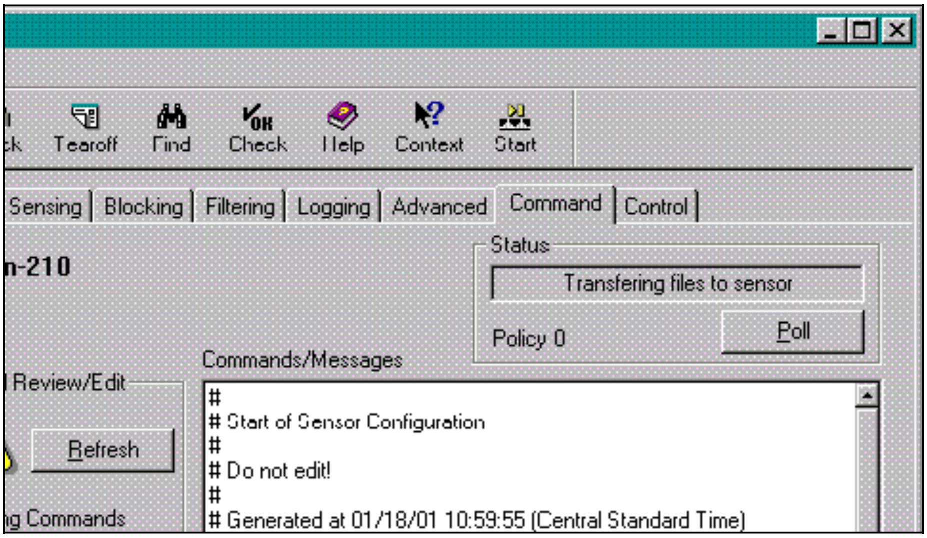
○ Automatic
● Default (Manual)
○ Manual

Clear current sessions □

Commands/Messages

```
#
# Start of Sensor Configuration
#
# Do not edit!
#
# Generated at 10/12/01 11:51:16 (Eastern Daylight Time)
#
Sensor Name: gacy
Sensor Organization: rtp
Sensor IP: 172.18.124.122
Sensor IP Alias: 172.18.124.106
Sensor Host ID: 122
Sensor Org ID: 1
Control Agent Name: INSANE
Control Agent Organization: rtp
Control Agent IP: 172.18.124.106
Control Agent Host ID: 106
Control Agent Org ID: 1
Postoffice Port: 45000
```

6. Click the **Approve Now** button to send the configuration to the Sensor.


k Tearoff Find Check Help Context Start
Sensing Blocking Filtering Logging Advanced Command Control
n-210
Refresh
Poll

Status: Transfering files to sensor

Policy 0

Review/Edit

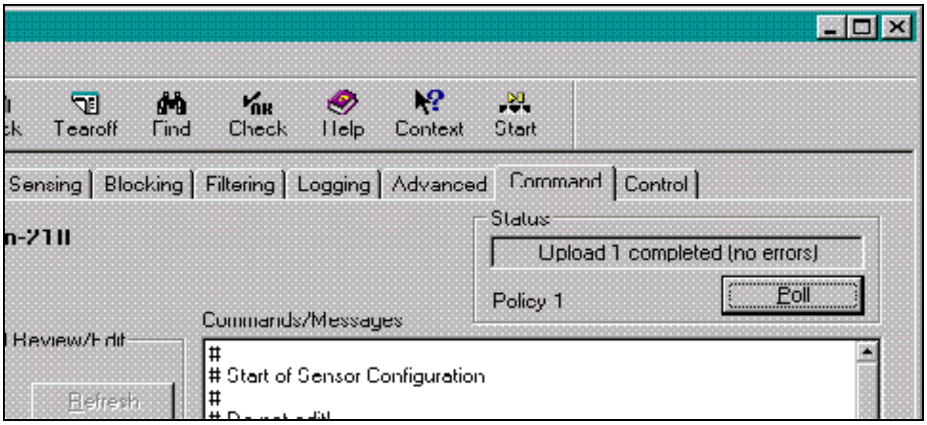
g Commands

Commands/Messages

```
#
# Start of Sensor Configuration
#
# Do not edit!
#
# Generated at 01/18/01 10:59:55 (Central Standard Time)
```

The Status pane displays the "Upload <#> completed" message. This indicates a valid and complete transfer process. The Sensor is now updated and should now run normally.

If the Sensor is not running normally, go back to the Sensor and check the output of the **nrconns** command to make sure that the connection between the CSPM host and the Sensor is established.



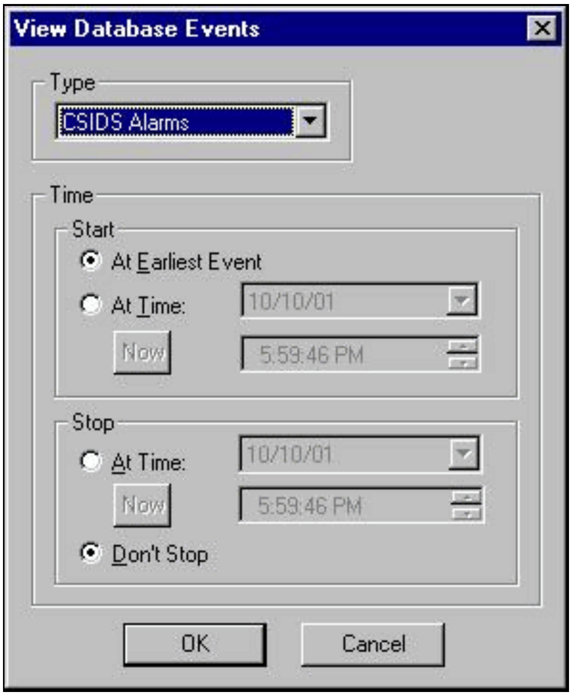
Status: Upload 1 completed (no errors)

Policy 1

Commands/Messages

```
#
# Start of Sensor Configuration
#
```

After this is complete, you can look for alarms that the Sensor sends to the CSPM host in the event viewer. To view the event viewer, from the CSPM main menu select **Tools** > **View Sensor Events** > **Database**.



View Database Events

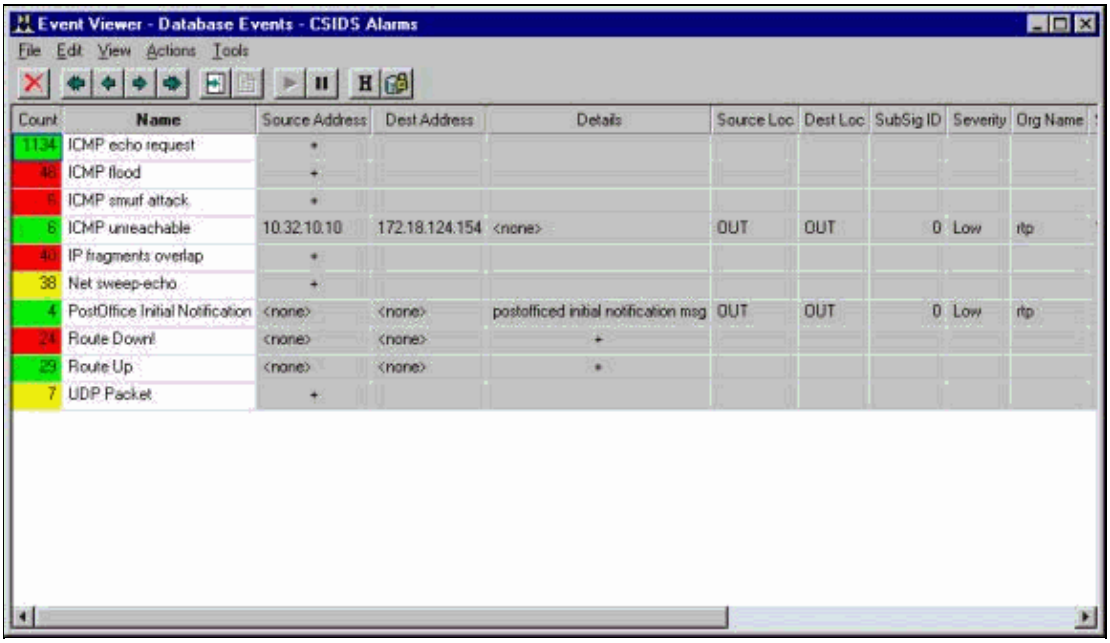
Type: CSIDS Alarms

Time

Start
- ● At Earliest Event
- ○ At Time: 10/10/01 5:59:46 PM

Stop
- ○ At Time: 10/10/01 5:59:46 PM
- ● Don't Stop

Click **OK** to display the events database window. Your screen will vary depending on the alarms that you may be getting.



Count	Name	Source Address	Dest Address	Details	Source Loc	Dest Loc	SubSig ID	Severity	Org Name
1134	ICMP echo request	+							
48	ICMP flood	+							
6	ICMP smurf attack	+							
6	ICMP unreachable	10.32.10.10	172.18.124.154	<none>	OUT	OUT	0	Low	rtp
40	IP fragments overlap	+							
38	Net sweep-echo	+							
4	PostOffice Initial Notification	<none>	<none>	postofficed initial notification msg	OUT	OUT	0	Low	rtp
24	Route Down	<none>	<none>	+					
29	Route Up	<none>	<none>	+					
7	UDP Packet	+							

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 19, 2006 Document ID: 6117