CHAPTER 5

IDS Device Manager Administration Tasks

The Administration tab enables you to perform the following tasks:

Viewing Diagnostics

You can obtain diagnostics information on your sensors for troubleshooting purposes.

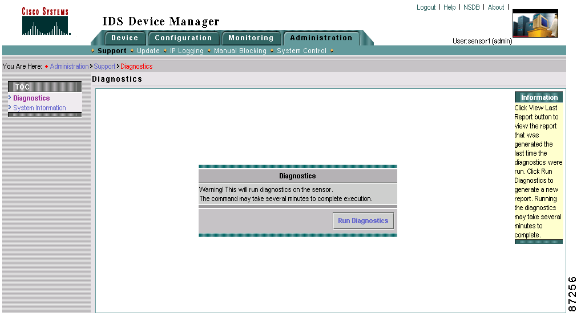
Note Running diagnostics takes several minutes to complete.

To run diagnostics, follow these steps:

Step 1 Select **Administration > Support > Diagnostics**.

The Diagnostics page appears.

Figure 5-1 Diagnostics Page



Warning! This will run diagnostics on the sensor.
The command may take several minutes to complete execution.

Click View Last Report button to view the report that was generated the last time the diagnostics were run. Click Run Diagnostics to generate a new report. Running the diagnostics may take several minutes to complete.

Step 2 Click **Run Diagnostics**.

The Cancel Diagnostics Command page appears. Then, the View Diagnostics Result page appears.

Step 3 Click **View Results** to see the diagnostics report.

The IDS 4.0 System Status Report appears in another window in HTML format.

Note The next time you open the Diagnostics page, there is an additional button, View Last Report. Click **View Last Report** to view the most recent report. This report is deleted when you run a new one.

Viewing System Information

The System Information page displays the following information:

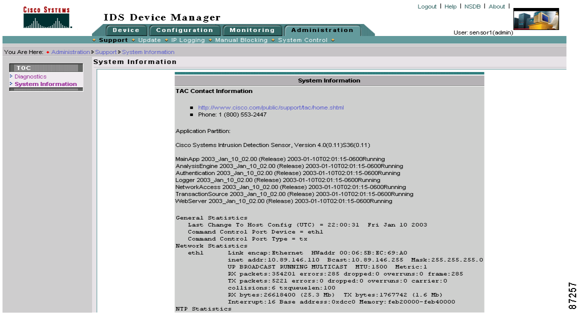
- TAC contact information.
- Software version.
- Status of applications.
- Interface information.
- Resource usage.

To view system information, follow these steps:

Step 1 Select **Administration > Support > System Information**.

The System Information page appears.

Figure 5-2 System Information Page



System Information

System Information

TAC Contact Information

- http://www.cisco.com/public/support/tac/home.shtml
- Phone: 1 (800) 553-2447

Application Partition:

Cisco Systems Intrusion Detection Sensor, Version 4.0(0.11)S36(0.11)

MainApp 2003_Jan_10_02.00 (Release) 2003-01-10T02:01:15-0600Running
AnalysisEngine 2003_Jan_10_02.00 (Release) 2003-01-10T02:01:15-0600Running
Authentication 2003_Jan_10_02.00 (Release) 2003-01-10T02:01:15-0600Running
Logger 2003_Jan_10_02.00 (Release) 2003-01-10T02:01:15-0600Running
NetworkAccess 2003_Jan_10_02.00 (Release) 2003-01-10T02:01:15-0600Running
TransactionSource 2003_Jan_10_02.00 (Release) 2003-01-10T02:01:15-0600Running
WebServer 2003_Jan_10_02.00 (Release) 2003-01-10T02:01:15-0600Running

```
General Statistics
   Last Change To Host Config (UTC) = 22:00:31  Fri Jan 10 2003
   Command Control Port Device = eth1
   Command Control Port Type = tx
Network Statistics
   eth1      Link encap:Ethernet  HWaddr 00:06:5B:EC:69:A0
             inet addr:10.89.146.110  Bcast:10.89.146.255  Mask:255.255.255.0
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:354201 errors:285 dropped:0 overruns:0 frame:285
             TX packets:5221 errors:0 dropped:0 overruns:0 carrier:0
             collisions:6 txqueuelen:100
             RX bytes:26618400 (25.3 Mb)  TX bytes:1767742 (1.6 Mb)
             Interrupt:16 Base address:0xdcc0 Memory:feb20000-feb40000
NTP Statistics
```

Step 2 To access the Cisco Technical Support Website, click the following link:

http://www.cisco.com/en/US/support/index.html

Applying Service Pack and Signature Updates

The Update page enables you to immediately apply service pack and signature updates.

Note The sensor cannot download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

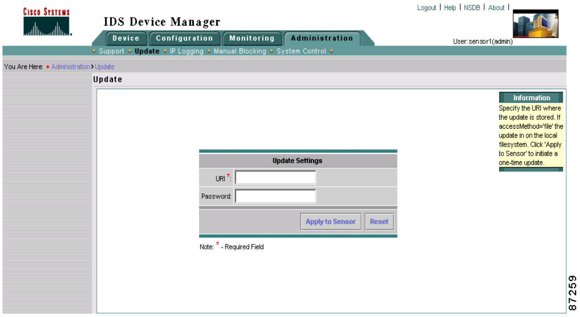
See Supported FTP Servers, page 3-37, for a list of supported servers.

To immediately apply a service pack and signature update, follow these steps:

Step 1 Select **Administration > Update**.

The Update page appears.

Figure 5-3 Update Page



Specify the URI where the update is stored. If accessMethod='file' the update in on the local filesystem. Click 'Apply to Sensor' to initiate a one-time update.

Note: * - Required Field

Step 2 In the URL field, enter the URL where the update can be found.

For example:

```
URL: ftp://user@10.1.1.1/UPDATES/IDS-K9-sp-4.0-1.1-S36-0.1-.rpm.pkg
```

Note You must have already downloaded the update from Cisco.com and put it on the FTP server.

Step 3 In the Password field, enter the particular transport protocol password.

Note You can use the following transport protocols: SCP, FTP, HTTP, or HTTPS.

Note To reset the form, click **Reset**.

Step 4 Click **Apply to Sensor** to apply the update.

Note To schedule regular updates, see Configuring Automatic Updates, page 3-35.

Configuring IP Logging

You can configure the sensor to catch all IP traffic associated with the hosts you specify by IP address.

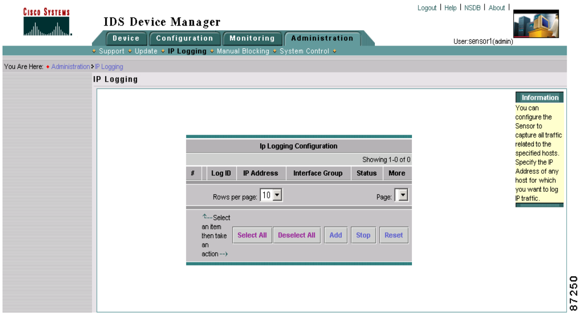
Note IP Logging requires that event logging be enabled with Informational as the severity level. See Configuring Signatures, page 3-1, for more information.

To generate logs files for specific IP addresses, follow these steps:

Step 1 Select **Administration > IP Logging**.

The Ip Logging Configuration page appears.

Figure 5-4 Ip Logging Configuration Page



You can configure the Sensor to capture all traffic related to the specified hosts. Specify the IP Address of any host for which you want to log IP traffic.

Ip Logging Configuration

Showing 1-0 of 0

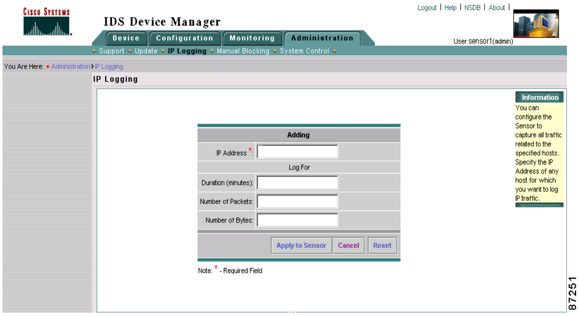
#		Log ID	IP Address	Interface Group	Status	More

←--Select an item then take an action -->

Step 2 Click **Add** to add the IP addresses of the hosts whose IP traffic you want to log.

The Adding page appears.

Figure 5-5 Adding Page



You can configure the Sensor to capture all traffic related to the specified hosts. Specify the IP Address of any host for which you want to log IP traffic.

Adding

IP Address *:

Log For

Duration (minutes):

Number of Packets:

Number of Bytes:

Note: * - Required Field

Step 3 In the IP address field, enter the source IP address of the host whose IP traffic you want to log.

Step 4 In the Duration field, enter the number of minutes you want to the sensor to log IP traffic (optional).

Step 5 In the Number of Packets field, enter the number of packets you want the sensor to count (optional).

Step 6 In the Number of Bytes field, enter the number of bytes you want to log (optional).

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

The Ip Logging Configuration page now displays the new Log ID.

Note The sensor begins logging and creates a log file that you can view by selecting **Monitoring > IP Logs**. See Downloading IP Logs, page 4-1, for more information.

Step 8 To discontinue logging IP traffic, select the check box next to the log ID, and then click **Stop**.

Note The IP log is overwritten when the sensor uses up its allocated space for IP logging.

Blocking Hosts Manually

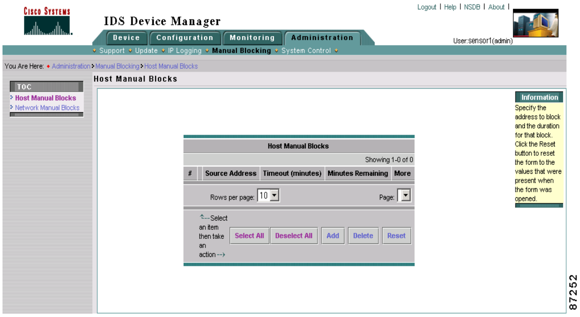
On occasion, you may want to block a host for a short time. From the Host Manual Blocks page, you can configure which host is blocked and for how long, and you can view a list of hosts that are being blocked.

To set up the manual blocking of a host, follow these steps:

Step 1 Select **Administration > Manual Blocking > Host Manual Blocks**.

The Host Manual Blocks page appears.

Figure 5-6 Host Manual Blocks Page



User:sensor1(admin)

You Are Here: Administration > Manual Blocking > Host Manual Blocks

Host Manual Blocks

Information: Specify the address to block and the duration for that block. Click the Reset button to reset the form to the values that were present when the form was opened.

Host Manual Blocks

Showing 1-0 of 0

#	Source Address	Timeout (minutes)	Minutes Remaining	More

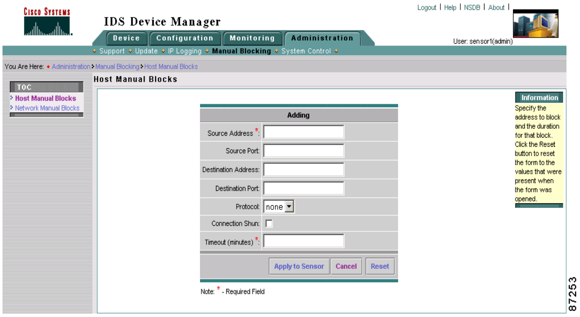
Rows per page: 10 Page:

Select an item then take an action -->

Step 2 Click **Add** to add a host to block.

The Adding Page appears.

Figure 5-7 Adding Page



User: sensor1(admin)

You Are Here: Administration > Manual Blocking > Host Manual Blocks

Host Manual Blocks

Information: Specify the address to block and the duration for that block. Click the Reset button to reset the form to the values that were present when the form was opened.

Adding

Source Address *:	
Source Port:	
Destination Address:	
Destination Port:	
Protocol:	none
Connection Shun:	□
Timeout (minutes) *:	

Note: * - Required Field

Step 3 In the Source Address field, enter the IP address of the host you want to block.

Step 4 In the Source Port field, enter the port you want to use to block the host (optional).

Step 5 In the Destination Address field, enter the destination address (optional).

Step 6 From the Protocol list box, select one of these options (optional):

- None
- tcp
- udp

Step 7 Select the **Connection Shun** check box to block only those connections that have the source IP address, destination IP address, destination port, or protocol specified (optional).

Note If you select the Connection Shun check box, the attacking host is free to connect to other hosts or to other services on the protected host. If destination port and protocol are not specified, the attacking host cannot send packets to the protected host at all, but can access other hosts on the network.

Step 8 In the Timeout field, enter the number of minutes you want the block to last.

Note To create a permanent block, enter **-1**.

Note To reset the form, click **Reset**.

Step 9 Click **Apply to Sensor** to save your changes.

The Host Manual Blocks page lists the hosts that you are blocking and the time remaining.

Step 10 To see how many minutes have passed for a specific block, select the check box next to the host you want to check and click **Host Manual Blocks** again. The page is refreshed and the remaining block time is shown.

Step 11 To delete a block, select the check box next to the host you want to discontinue the block for, and then click **Delete**.

The host is no longer in the list of blocked hosts.

Blocking Networks Manually

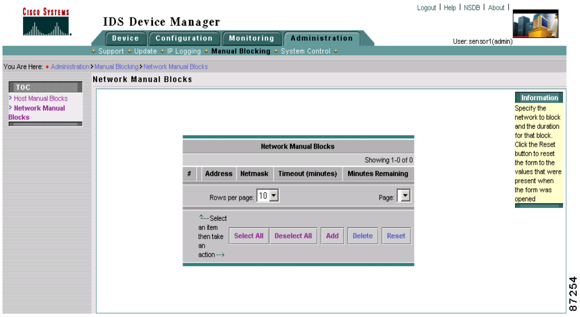
On occasion, you may want to block a network for a short time. From the Network Manual Blocks page, you can configure which network is blocked and for how long, and you can view a list of networks that are being blocked.

To set up manual blocking of a network, follow these steps:

Step 1 Select **Administration > Manual Blocking > Network Manual Blocks**.

The Network Manual Blocks page appears.

Figure 5-8 Network Manual Blocks Page



You Are Here: Administration > Manual Blocking > Network Manual Blocks

Network Manual Blocks

Information

Specify the network to block and the duration for that block. Click the Reset button to reset the form to the values that were present when the form was opened

Network Manual Blocks

Showing 1-0 of 0

#	Address	Netmask	Timeout (minutes)	Minutes Remaining

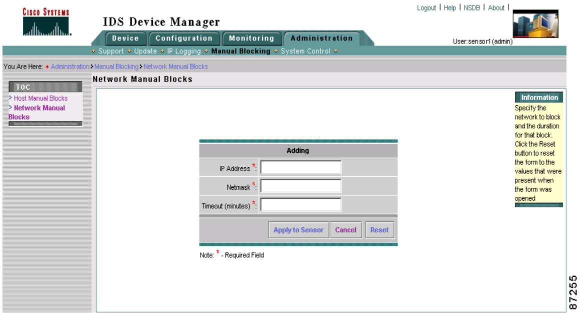
Rows per page: 10 Page:

←--Select an item then take an action -->

Step 2 Click **Add** to add a network to block.

The Adding page appears.

Figure 5-9 Adding Page



Specify the network to block and the duration for that block. Click the Reset button to reset the form to the values that were present when the form was opened

Note: * - Required Field

Step 3 In the IP Address field, enter the IP address of the network you want to block.

Step 4 In the Netmask field, enter the netmask of the network you want to block.

Step 5 In the Timeout field, enter the number of minutes you want the block to last.

Note To create a permanent block, enter **-1**.

Note To reset the form, click **Reset**.

Step 6 Click **Apply to Sensor** to save your changes.

The Network Manual Blocks page lists the networks that you are blocking and the time remaining.

Step 7 To see how many minutes have passed for a specific block, select the check box next to the network you want to check, and then click **Network Manual Blocks**. The page is refreshed and the remaining block time is shown.

Step 8 To delete a block, select the check box next to the network you want to discontinue a block for, and then click **Delete**.

The network is no longer in the list of blocked networks.

Resetting and Powering Down the Sensor

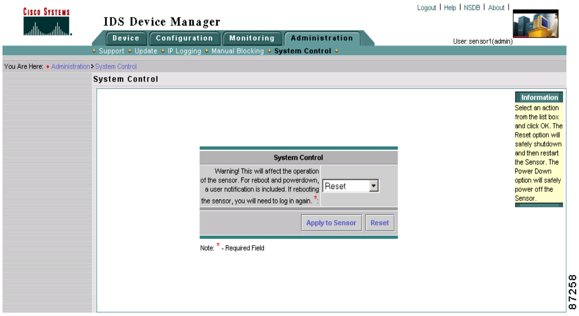
You can reset and power down the sensor from the System Control page. Reset shuts down the sensor safely and then restarts the sensor. Power Down safely shuts down the sensor.

To reset or power down the sensor, follow these steps:

Step 1 Select **Administration > System Control**.

The System Control page appears.

Figure 5-10 System Control Page



System Control

Warning! This will affect the operation of the sensor. For reboot and powerdown, a user notification is included. If rebooting the sensor, you will need to log in again. *: Reset

Note: * - Required Field

Select an action from the list box and click OK. The Reset option will safely shutdown and then restart the Sensor. The Power Down option will safely power off the Sensor.

Step 2 Select one of the following options from the list box:

- **Reset**—Shuts down the IDS applications and the sensor, and then reboots. After the reboot, you must log in again.

  Note There is a 30-second delay during which users who are currently logged in to the CLI are notified that the IDS applications and sensor are going to shut down.

- **Power Down**—Shuts down the IDS applications and then shuts off the sensor.

Note There is a 30-second delay during which users who are currently logged in to the CLI are notified that the IDS applications and the sensor are going to shut down.