This chapter covers the following subjects:

- Cisco IPS Device Manager
- System Requirements for IDM
- Navigating IDM
- Configuring Communication Parameters by Using IDM

CHAPTER 3

Cisco IPS Device Manager (IDM)

The Cisco IPS Device Manager (IDM) is a tool that enables you to configure and manage a single Cisco network sensor. This Java-based web tool provides you with a graphical interface to manipulate the operation of your sensor. Each IPS appliance running on your network has its own web server that provides access to the IDM application on the sensor.

Accurately configuring your Cisco IPS devices is vital to efficiently protecting your network. This chapter explains how to navigate the graphical configuration tool that comes with each sensor. Beginning with Cisco IPS version 5.0, the IDM interface has been completely revamped. Reviewing this chapter will provide you with information on how the new interface is structured. This information will be important for you to follow the configuration examples used throughout the rest of the book.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide if you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 10-question quiz, derived from the major sections in the "Foundation and Supplemental Topics" portion of the chapter, helps you determine how to spend your limited study time.

Table 3-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 3-1 *"Do I Know This Already?" Foundation and Supplemental Topics Mapping*

Foundation or Supplemental Topic	Questions Covering This Topic
System Requirements for IDM	1, 4, 5
Navigating IDM	3, 6, 8, 10
Configuring Communication Parameters by using IDM	2, 7, 9

> **CAUTION** The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which version of Linux is supported for use with IDM?

- **a.** Red Hat
- **b.** Debian
- **c.** Slackware
- **d.** Mandrake
- **e.** SUSE

2. Which of the following is a configurable sensor communication parameter?

- **a.** Changing the TLS/SSL port
- **b.** Changing the Telnet port
- **c.** Changing SSH port
- **d.** Changing the TLS/SSL port and the Telnet port
- **e.** None of these

3. Which of the following is not a configuration category in IDM?

- **a.** Sensor Setup
- **b.** Analysis Engine
- **c.** SNMP
- **d.** IP Logging
- **e.** Event Action Rules

4. Which of the following Solaris versions is supported for use with IDM?

- **a.** Version 2.6
- **b.** Version 2.7
- **c.** Version 2.9
- **d.** Version 2.5

5. Which web browser is supported on Microsoft Windows 2000 for access to IDM?

- **a.** Opera 7.54u1
- **b.** Internet Explorer 5.5
- **c.** Netscape 7.1
- **d.** Netscape 6.0
- **e.** Firefox 1.0

6. Which of the following is not a monitoring category in IDM?

- **a.** Blocking
- **b.** Denied Attackers
- **c.** IP Logging
- **d.** Events
- **e.** Network Blocks

7. Which of the following is not a configurable sensor communication parameter?

- **a.** Telnet port
- **b.** TLS/SSL port
- **c.** Default route
- **d.** IP address
- **e.** Host name

8. Where are the configuration options on the IDM screen?

- **a.** The location of the options is configurable.
- **b.** The options are listed on the right side of the screen.
- **c.** The options are accessed via pull-down menus.
- **d.** The options are listed across the top of the screen.
- **e.** The options are listed on the left of the screen.

9. Where should you configure the sensor communication parameters?

- **a.** **Sensor Setup>Network**
- **b.** **Interface Configuration>Interfaces**
- **c.** **Sensor Setup>Allowed Hosts**
- **d.** **Analysis Engine>Virtual Sensor**
- **e.** **Analysis Engine>Global Variables**

10. Which Simple Network Management Protocol (SNMP) operations are supported by Cisco IPS version 5.0?

   a. Get only

   b. Set only

   c. Trap only

   d. Get, Set, and Trap

   e. SNMP is not supported

The answers to the "Do I Know This Already?" quiz are found in the appendix. The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. This includes the "Foundation and Supplemental Topics," "Foundation Summary," and Q&A sections.

- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the Q&A section. Otherwise, move to the next chapter.

Foundation and Supplemental Topics

Cisco IPS Device Manager

The Cisco IDM is a Java-based web interface that enables you to configure and manipulate the operation of your Cisco network sensors. Each IPS appliance running on your network has its own web server that provides access to the IDM application on the sensor. The web server uses Transport Layer Security (TLS) to encrypt the traffic to and from the sensor to prevent an attacker from viewing sensitive management traffic. The web server is also hardened to minimize an attacker's ability to disrupt or compromise its operation.

This chapter focuses on the following topics:

- System requirements for IDM
- Navigating IDM
- Configuring communication parameters by using IDM

System Requirements for IDM

Because the IDS Device Manager is a web-based application, the major system requirement is a web browser. Having sufficient memory and screen resolution also promotes effective operation of IDM. The recommended memory and screen resolution are as follows:

- 256 MB memory (minimum)
- 1024 x 768 resolution and 256 colors (minimum)

Cisco has identified system requirements based on the following three operating systems for use with IDM:

- Microsoft Windows
- Sun Solaris
- Red Hat Linux

The recommended configuration for using Windows is as follows:

- Microsoft Windows 2000 or Windows XP

- Internet Explorer 6.0 with Java Plug-in 1.4.1 or 1.4.2, or Netscape 7.1 with Java Plug-in 1.4.1 or 1.4.2
- Pentium III or equivalent, running at 450 MHz or higher

The recommended configuration for using Solaris is as follows:

- Sun Solaris 2.8 or 2.9
- Mozilla 1.7

The recommended configuration for using Red Hat is as follows:

- Red Hat Linux 9.0 or Red Hat Enterprise Linux WS version 3, running GNOME or KDE
- Mozilla 1.7

NOTE Although any web browser may work with IDM, Cisco supports only the browsers and system configurations mentioned here.

Navigating IDM

Starting with Cisco IPS version 5.0, the IDM interface has been completely restructured. The new graphical interface (see Figure 3-1) contains an icon bar with the following options:

- Configuration
- Monitoring
- Back
- Forward
- Refresh
- Help

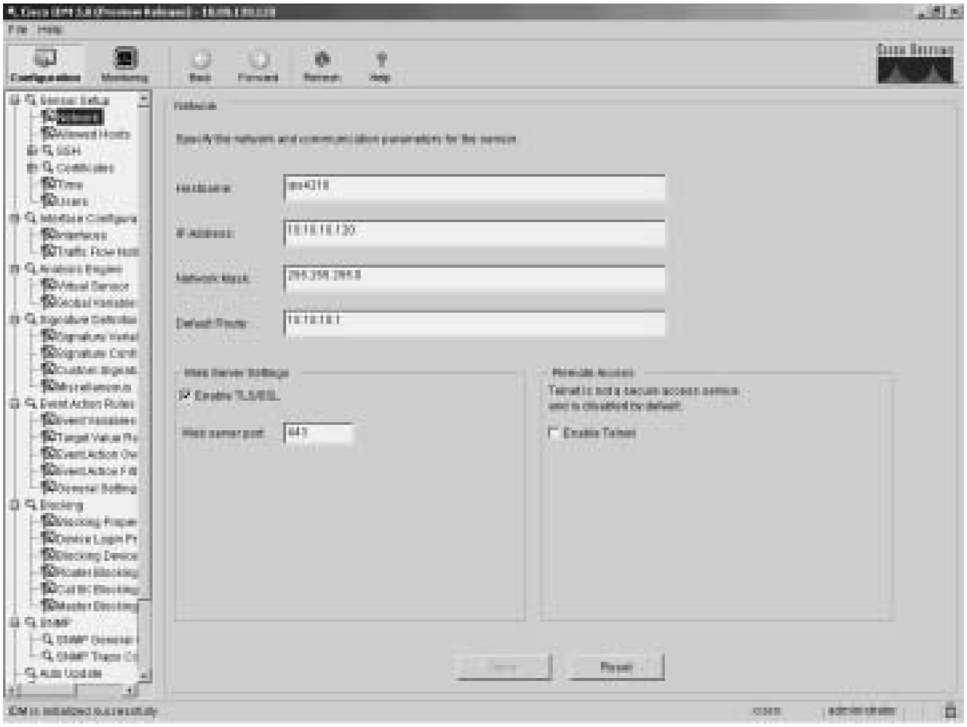
Configuration

Configuring the operational characteristics of the sensor is the main functionality provided by IDM. By clicking on the **Configuration** icon (located on the top menu bar), you can display a list of configurable items down the left side of the screen (see Figure 3-1). These items are divided into the following operational categories:

- Sensor Setup
- Interface Configuration

- Analysis Engine
- Signature Definition
- Event Action Rules
- Blocking
- SNMP
- Auto Update

Figure 3-1 *Main IDM Screen*



Network

Specify the network and communication parameters for the sensor.

Hostname: ids4210

IP Address: 10.10.10.120

Network Mask: 255.255.255.0

Default Route: 10.10.10.1

Web Server Settings

☑ Enable TLS/SSL

Web server port: 443

Remote Access

Telnet is not a secure access service and is disabled by default.

☐ Enable Telnet

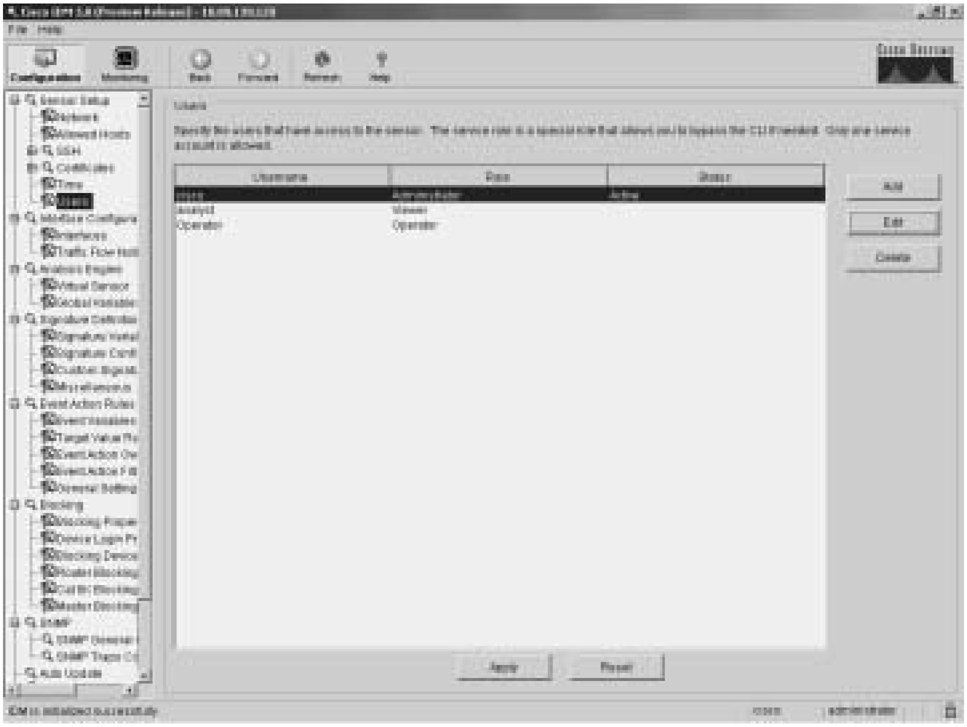
These operational categories are explained in the following sections.

NOTE Most operational categories have multiple options. If the individual options (for a specific category) are not shown, click on the plus sign on the left of the category name. This will expand that category and show all of the next-level options. Clicking on the minus sign (to the left of a category name) collapses the individual options under the category name.

NOTE The configuration options displayed vary depending on the privilege level of the user who logs in to IDM.

Clicking on one of the configuration options (shown on the left side of the IDM interface) displays the configuration information for that option in the main portion of the screen. For example, Figure 3-2 shows the configuration screen displayed when you select **Sensor Setup>Users**.

Figure 3-2 *Sensor Setup Users Screen*



Users

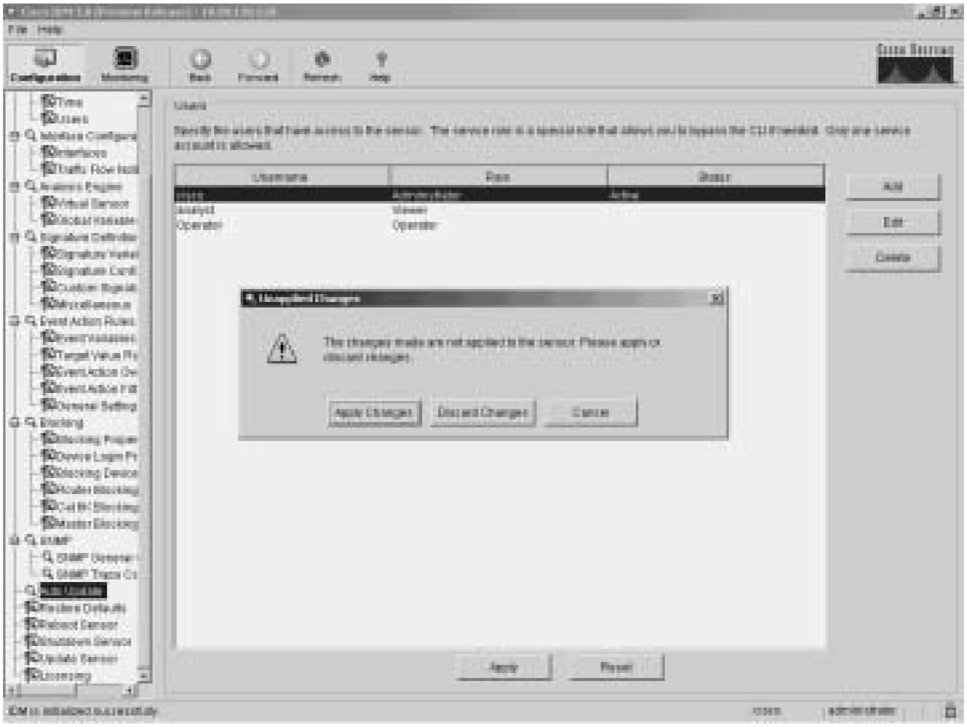
Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
cisco	Administrator	Active
analyst	Viewer	
Operator	Operator	

When you make changes to a configuration screen, the **Apply** icon is no longer grayed out. To save the changes, click on the **Apply** button at the bottom of the configuration screen. Clicking on the **Reset** button removes your changes (restoring the original configuration values).

NOTE When you make changes to a configuration screen and then attempt to move to another configuration screen (without clicking on either the **Apply** icon or the **Reset** button), the popup window shown in Figure 3-3 appears. To save your changes, simply click on **Apply Changes**. To discard the changes, click on **Discard Changes**. Clicking on **Cancel** causes you to remain at the current configuration screen without applying changes or restoring them to their original values.

Figure 3-3 *Accept Changes Popup Window*



Users

Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
cisco	Administrator	Active
analyst	Viewer	
Operator	Operator	

The changes made are not applied to the sensor. Please apply or discard changes.

IDM is initialized successfully.

Sensor Setup

When configuring access to your sensor, you will use the options available in the Sensor Setup category. These include configuring the sensor's IP address, the users on the system, and the sensor's time parameters. Through the Sensor Setup options, you can also configure access to the sensor for Secure Shell (SSH) and secure web access (using HTTPS). The Sensor Setup category is divided into the following options:

- Network
- Allowed Hosts
- SSH>Authorized Keys
- SSH>Known Host Keys
- SSH>Sensor Key
- Certificates>Trusted Hosts
- Certificates>Server Certificate

- Time
- Users

The Network option enables you to configure the basic sensor network properties such as IP address, default gateway, network mask, and host name. The Allowed Hosts option enables you to define which IP addresses are allowed to access the sensor via its management interface.

The SSH options enable you to define the authorized host keys for systems that you want to connect to from the sensor (such as when using Secure Copy [SCP] to upgrade the sensor's software) as well as the public keys for SSH clients that are allowed to connect to the sensor. Similarly, the two Certificates options enable you to define the trusted certificates for systems that the sensor needs to connect to via HTTPS. This would commonly apply to master blocking sensors and other IPS devices to which your sensor connects by using Remote Data Exchange Protocol (RDEP).

The Time option enables you to define the time settings on the sensor. This includes specifying a Network Time Protocol (NTP) server, time zone settings, and summertime parameters. Finally, the Users option enables you to view the currently configured users, add users, and change users' passwords (if you log in via a privileged account). If you log in to a nonprivileged account, you will be able to change only your own password.

Interface Configuration

Each time your sensor is powered on; it automatically detects the interface modules that are installed in the sensor. The network interfaces enable your sensor to monitor network traffic, using either promiscuous or inline modes of operation. Before monitoring traffic, the interfaces need to be configured.

The command and control interface enables you to access your sensor. This interface is permanently mapped to a specific physical interface (depending on the model of the sensor).

The Interface Configuration category includes the following options:

- Interfaces
- Interface Pairs*
- Bypass*
- Traffic Flow Notifications

NOTE The selections marked with an asterisk (*) may not be shown if your sensor does not have enough interfaces to support inline mode. Inline mode requires at least two interfaces in addition to the command and control interface.

The Interfaces option enables you to configure basic interface properties, such as speed and whether the interface is enabled. The Interface Pairs option enables you to define pairs of interfaces that will be used for inline monitoring. When using inline mode, you may also need to use the Bypass option to configure the software bypass mode, which determines how network traffic is handled during operational disruptions in the sensor's inspection applications.

The Traffic Flow Notifications option enables you to configure the following parameters:

- Missed Packet Threshold
- Notification Interval
- Interface Idle Threshold

These parameters determine when event notifications are generated based on the flow of traffic across the sensor's interfaces. For more information on Traffic Flow Notifications, refer to Chapter 4, "Basic Sensor Configuration."

Analysis Engine

The analysis engine performs packet analysis and alert detection. It monitors traffic that flows through the specified interfaces and interface pairs.

The Analysis Engine category provides the following options:

- Virtual Sensor
- Global Variables

To use the any of the sensor's interfaces to analyze network traffic, you must assign it to a virtual sensor. The Virtual Sensor option enables you to assign or remove sensor interfaces from a virtual sensor.

> **NOTE** Currently, sensor software supports only a single virtual sensor (vs0). In the future, however, Cisco IPS sensors may support multiple virtual sensors. These virtual sensors would enable you to make one physical sensor appear to be multiple sensors, each with unique configuration settings. This concept is similar to that of virtual firewalls, where a single physical firewall can be configured (via software) to operate as multiple virtual firewalls that each have unique configuration parameters.

The Global Variables option enables you to configure the maximum number of IP log files that the sensor will support.

Signature Definition

Network intrusions are attacks and other misuses of network resources. A signature is a set of rules that a sensor uses to detect intrusive activity. As the sensor scans network traffic, it searches for matches to the signatures that it is configured to detect. When a match to a signature is found, the sensor takes the action that you have configured for that signature.

The Signature Definition category has the following options:

- Signature Variables
- Signature Configuration
- Custom Signature Wizard
- Miscellaneous

Using the Signature Variables option, you can configure signature variables that define ranges of IP addresses. You can then use these signature variables when defining signatures. When you change the value of the variable, the change is automatically replicated to all of the signatures where it is referenced. You can also change the predefined signature variable that determines which ports are examined during web analysis.

Using the Signature Configuration option, you can view the available signatures and their properties. You can enable and disable signatures as well as adding new signatures and editing the properties of existing signatures.

Using the Custom Signature Wizard option, you can create custom signatures by using a menu-driven interface that simplifies the creation process.

The Miscellaneous option enables you to configure specific global sensor parameters for the following aspects of the sensor's operation:

- Application policy settings
- Fragment reassembly settings
- Stream reassembly settings
- IP log settings

For more information on configuring these options, refer to Chapter 8, "Sensor Tuning."

Event Action Rules

Event action rules define how your sensor will process specific events when it detects them on the network. Event action rules define the following functionality on the sensor:

- Calculating the Risk Rating
- Adding event-action overrides

- Filtering event action
- Executing the resulting event action
- Summarizing and aggregating events
- Maintaining a list of denied attackers

The Event Action Rules category provides the following options:

- Event Variables
- Target Value Rating
- Event Action Overrides
- Event Action Filters
- General Settings

Using the Event Variables option, you can define variables that you use when defining event filters. These variables identify lists or ranges of IP address. By defining event variables (instead of using the actual addresses in the filters), you can more easily update IP addresses. Whenever you need to add or remove an address, you just change the event variable definition.

The Target Value Rating enables you to configure an asset rating for specific IP address ranges. The asset rating can be one of the following values:

- No value
- Low
- Medium
- High
- Mission critical

The Event Action Overrides option defines when actions are automatically assigned to events based on the value of the Risk Rating. You can assign an event action override for each of the actions that you can normally assign to a signature.

The Event Action Filters option enables you to define event action filters. These filters prevent (or filter) configured actions from being applied to specific events. Filters can be based on numerous factors such as IP address, signature ID, and Risk Rating.

The General Settings option enables you to define general settings that apply to event action rules. These include the following parameters, as well as the ability to enable and disable the meta-event generator and summarizer:

- Deny attacker duration
- Block action duration
- Maximum denied attackers

Blocking

One of the actions that you can configure your sensor to take when a signature triggers is to block traffic from the system that initiated the intrusive traffic. The two types of blocking actions that you can configure are as follows:

- Host block
- Connection block

When you configure a signature to block a connection, it blocks only traffic from the host that triggered the signature to the destination port, the protocol (such as TCP or UDP), and the destination IP address that triggered the signature. Therefore, the blocking decision is based on the following parameters:

- Source IP address
- Destination IP address
- Destination port
- Protocol

A host block, on the other hand, blocks all traffic from the attacking host regardless of the destination port, protocol, or destination IP address.

The Blocking category has the following configuration options:

- Blocking Properties
- Device Login Profiles
- Blocking Devices
- Router Blocking Device Interfaces

- Cat6k Blocking Device Interfaces
- Master Blocking Sensor

Using the Block Properties option, you can configure the basic blocking properties along with the IP addresses that the blocking devices should never block. The Device Login Profiles option defines the credentials necessary for the sensor to access the blocking devices that you add by using the Blocking Devices option. To block network traffic, the blocking device applies an access control list (ACL) to one of its interfaces. You configure which interface the blocking ACL will be applied to on routers by using the Router Blocking Device Interfaces option. Similarly, you configure which interface the blocking ACL will be applied to on Catalyst 6000 switches by using Cat6k Blocking Device Interfaces.

NOTE For Cisco PIX and ASA blocking devices, you do not need to configure a specific interface since each uses the device's **shun** command to block the traffic.

The Master Blocking Sensor option enables you define which sensors will serve as master blocking sensors. A master blocking sensor initiates IP blocking for another sensor, since only one sensor can initiate IP blocking on a specific blocking device.

Simple Network Management Protocol

Beginning with Cisco IPS version 5.0, sensor software supports Simple Network Management Protocol (SNMP) functionality (see RFC 1157, "Simple Network Management Protocol [SNMP]"). SNMP facilitates the exchange of management information between network devices, enabling network administrators to manage network performance as well as find and solve network problems. Using SNMP, management stations can efficiently monitor the health and status of many types of network devices, including switches, routers, and sensors.

NOTE SNMP is a simple protocol in which the network-management system issues a request, and managed devices return responses. This interaction is implemented by using one of the following four operations:

- Get—Retrieves information for a specific SNMP field
- GetNext—Retrieves the next SNMP field
- Set—Sets the value for a specific SNMP field
- Trap—Configures SNMP to generate a SNMP response when a certain event occurs

Besides polling for SNMP responses, your can configure your sensors to generate SNMP traps. In this situation, the management station does not poll the sensor for information. Instead, when a specific event occurs, the sensor sends an unsolicited message to the management system. SNMP traps are effective in environments where it is impractical to constantly poll every device on the network.

The SNMP category provides the following options:

- SNMP General Configuration
- SNMP Traps Configuration

SNMP Gets, Sets, and Traps are disabled by default. To use these features to manage your sensor, you need to enable them.

Auto Update

To maintain the latest software images on your sensors, you can configure your sensor to automatically load service pack and signature updates from a central FTP or SCP server. Selecting Auto Update displays the configuration values that your sensor will use to automatically update software.

NOTE Your sensor cannot automatically load service pack and signature updates from Cisco.com. You need to download them to your FTP or SCP server, from which your sensors can automatically retrieve them. Furthermore, if you need to downgrade the software (return to a previous software version) on your sensor, you can use the **downgrade** global configuration command via the sensor CLI.

NOTE FTP transmits login credentials in the clear (in other words, the traffic is not encrypted). Therefore, the FTP server should be on a separate management network since it will be a prime target for attack. At minimum, the user account used to retrieve sensor software images needs to have minimal privileges on the FTP server.

Monitoring

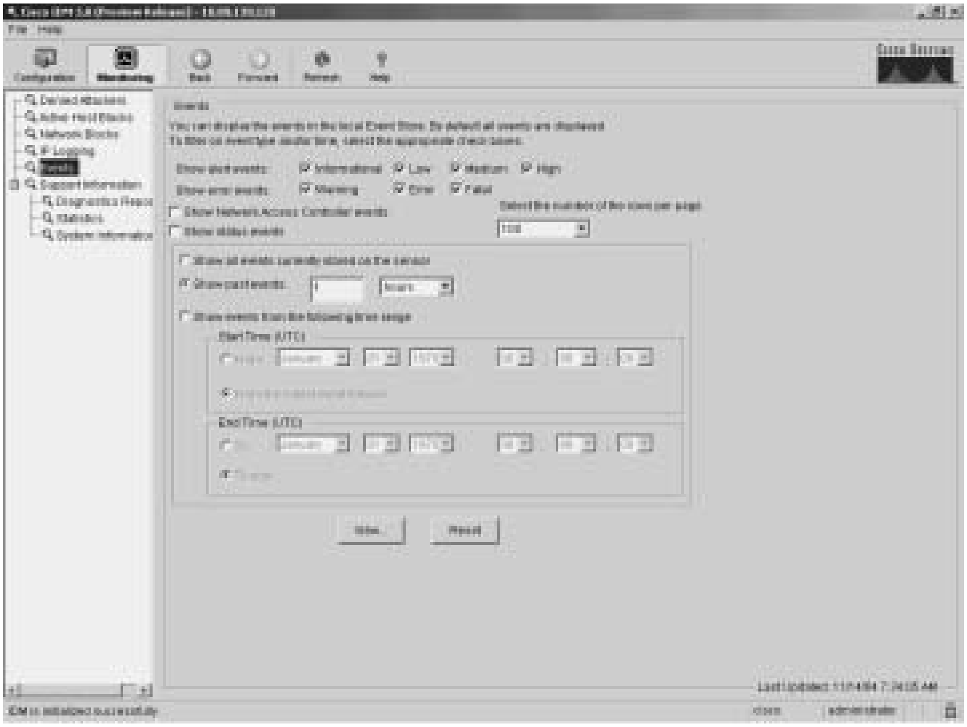
Besides helping you configure your sensor, IDM also provides the ability to monitor the status and operation of the sensor. The monitoring functionality is divided into the following options (see Figure 3-4):

- Denied Attackers
- Active Host Blocks
- Network Blocks
- IP Logging
- Events
- Support Information>Diagnostic Report

- Support Information>Statistics
- Support Information>System Information

> **NOTE** The monitoring options displayed vary depending on the privilege level of the user who logs in to IDM.

Figure 3-4 *IDM Monitoring Functionality*



Show alert events: ☑ Informational ☑ Low ☑ Medium ☑ High

Show error events: ☑ Warning ☑ Error ☑ Fatal

□ Show Network Access Controller events

□ Show status events

Select the number of the rows per page: 100

○ Show all events currently stored on the sensor

● Show past events: 1 hours

○ Show events from the following time range

Start Time (UTC)

End Time (UTC)

The Denied Attackers option enables you to view the IP addresses that are currently blocked by the sensor. The Active Host Blocks option enables you to manually block specific hosts for a specified duration. Similarly, the Network Blocks option enables you to manually establish a block for an entire network. Using the IP Logging option, you can manually log traffic from a specified host.

Using the Events option, you can view events generated by the sensor. Monitoring events provides a basic mechanism that you can use to examine the events that your sensor is generating.

The Support Information options provide information useful in debugging the operation of the sensor. Refer to Chapter 12, "Verifying System Configuration," for more information on debugging the operation of your sensor.

Back

As you move through the various configuration and monitoring screens, IDM keeps track of the options you have selected. Clicking on the **Back** icon enables you to return to one of previous configuration screens that you were modifying or viewing (the **Back** icon is similar to your browser's **Back** button). Each click on the **Back** icon takes you back one screen in the list of configuration screens that you have visited.

For instance, suppose that you view the following configuration screens for the sensor:

- Blocking > Blocking Properties
- Sensor Setup > Users
- Interface Configuration > Interfaces

Clicking on the **Back** icon returns you to the Sensor Setup Users configuration screen. Clicking on the **Back** icon a second time will return you to the Blocking Blocking Properties configuration screen.

Forward

As you move through the various configuration and monitoring screens, IDM keeps track of the options that you have selected. Clicking on the **Forward** icon enables you to move forward through this list of your selections. The functionality provided by the **Forward** icon is the opposite of the functionality provided by the **Back** icon.

For instance, suppose that you view the following configuration screens for the sensor:

- Blocking>Blocking Properties
- Sensor Setup>Users
- Interface Configuration>Interfaces

Clicking on the **Back** icon returns you to the Sensor Setup Users configuration screen. Clicking on the **Forward** icon returns you to the Interface Configuration>Interfaces configuration screen.

Refresh

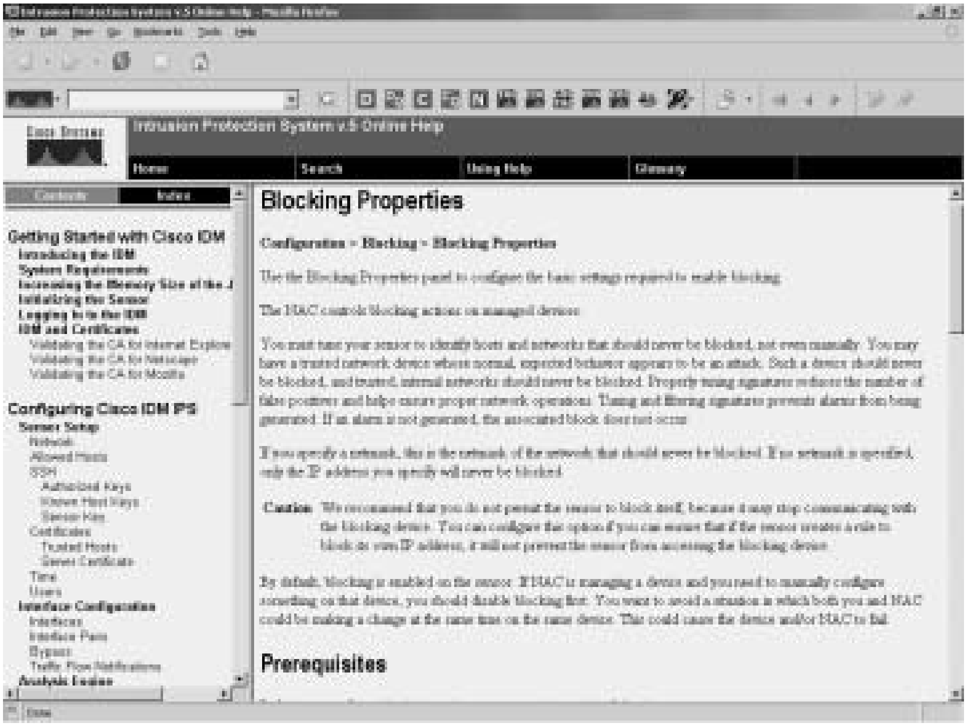
Clicking on the **Refresh** icon causes the current screen to update based on the configuration information stored on the sensor. If you try to refresh without applying changes that you have made, you will be prompted to either save the changes or discard them.

Help

Clicking on the **Help** icon brings up context-sensitive help in a separate browser window. Suppose that you are configuring the blocking properties for the sensor (via Blocking Blocking Properties).

Clicking on the **Help** icon brings up Help information on configuring the blocking properties (see Figure 3-5).

Figure 3-5 *IDM Help Screen*



Blocking Properties

Configuration > Blocking > Blocking Properties

Use the Blocking Properties panel to configure the basic settings required to enable blocking.

The NAC controls blocking actions on managed devices.

You must tune your sensor to identify hosts and networks that should never be blocked, not even manually. You may have a trusted network device whose normal, expected behavior appears to be an attack. Such a device should never be blocked, and trusted, internal networks should never be blocked. Properly tuning signatures reduces the number of false positives and helps ensure proper network operations. Tuning and filtering signatures prevents alarms from being generated. If an alarm is not generated, the associated block does not occur.

If you specify a netmask, this is the netmask of the network that should never be blocked. If no netmask is specified, only the IP address you specify will never be blocked.

Caution: We recommend that you do not permit the sensor to block itself, because it may stop communicating with the blocking device. You can configure this option if you can ensure that if the sensor creates a rule to block its own IP address, it will not prevent the sensor from accessing the blocking device.

By default, blocking is enabled on the sensor. If NAC is managing a device and you need to manually configure something on that device, you should disable blocking first. You want to avoid a situation in which both you and NAC could be making a change at the same time on the same device. This could cause the device and/or NAC to fail.

Prerequisites

Configuring Communication Parameters Using IDM

To configure the sensor communication parameters on your sensor, perform the following steps:

Step 1 Click on the **Configuration** icon located on the top IDM menu bar.

Step 2 If the **Sensor Setup** category is not expanded, click on the plus sign to the left of **Sensor Setup**.

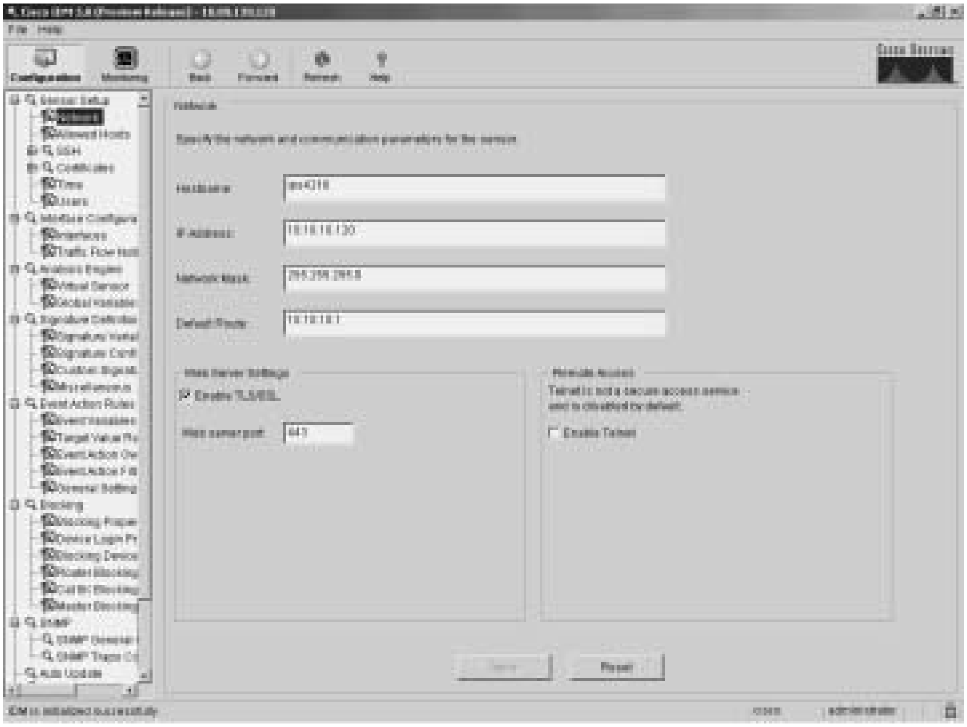
Step 3 Click on **Sensor Setup>Network**. This will display the sensor's current communication parameters (see Figure 3-6).

Step 4 Enter the host name to be used for the sensor in the **Hostname** field.

Step 5 Enter the IP address of the sensor in the **IP Address** field.

Step 6 Enter the network mask in the **Network Mask** field.

Figure 3-6 *Sensor Communication Parameters Screen*



Network

Specify the network and communication parameters for the sensor.

Hostname: ids4210

IP Address: 10.10.10.120

Network Mask: 255.255.255.0

Default Route: 10.10.10.1

Web Server Settings

☑ Enable TLS/SSL

Web server port: 443

Remote Access

Telnet is not a secure access service and is disabled by default.

☐ Enable Telnet

Step 7 Enter the default route that the sensor will use for command and control traffic by specifying the IP address of the default router in the **Default Route** field.

Step 8 To enable secure web access, click on the **Enable TLS/SSL** check box. You can also specify the port for secure web access by specifying a port number in the **Web server port** field (the default is 443).

NOTE Many tools automatically target systems based on default ports (such as port 443 for TLS/SSL). Changing the web server port may make it more difficult for an attacker to directly attack your web server since doing so requires the attacker to scan the network first to determine the new port assigned to TLS/SSL.

Step 9 To enable Telnet access to the sensor, click on the **Enable Telnet** check box (the default is for Telnet access to be disabled because it is an insecure management protocol since it does not encrypt the traffic).

Step 10 Click on the **Apply** button to save the changes to the communication parameters.

Foundation Summary

The Cisco IPS Device Manager (IDM) provides a graphical interface that enables you to configure the operational characteristics of a single sensor on your network. IDM is a Java-based web application that should work with most web browsers.

The recommended memory and screen resolution are as follows:

- 256 MB memory (minimum)
- 1024 x 768 resolution and 256 colors (minimum)

Cisco has identified system requirements based on the following operating systems for use with IDM:

- Microsoft Windows 2000 and Windows XP
- Sun Solaris 2.8 and 2.9
- Red Hat Linux 9.0 and Red Hat Enterprise Linux WS version, 3 running GNOME or KDE

The functionality provided by IDM is divided into the following two categories:

- Configuration
- Monitoring

The configuration tasks are divided into the following categories:

- Sensor Setup
- Interface Configuration
- Analysis Engine
- Signature Definition
- Event Action Rules
- Blocking
- SNMP
- Auto Update

Each of these categories provides one or more configuration screens that control the operation of the sensor. The monitoring functionality is divided into the following categories:

- Denied Attackers
- Active Host Blocks
- Network Blocks
- IP Logging
- Events
- Support Information>Diagnostic Report
- Support Information>Statistics
- Support Information>System Information

The monitoring categories provide you with information about the current operation of the sensor.

IDM provides online help and also supports **Back** and **Forward** icons (as in a browser) to help you operate more efficiently while using IDM to configure your sensor.

Q&A

You have two choices for review questions:

- The questions that follow give you a bigger challenge than the exam itself by using an open-ended question format. By reviewing now with this more difficult question format, you can exercise your memory better and prove your conceptual and factual knowledge of this chapter. The answers to these questions are found in the appendix.
- For more practice with exam-like question formats, use the exam engine on the CD-ROM.

1. Which Windows operating systems are supported for accessing IDM?
2. What is the minimum amount of RAM that is recommended for systems to run IDM?
3. Which fields can you configure when you access the **Sensor Setup>Network** option?
4. What SNMP functionality is available for Cisco IPS version 5.0?
5. Which web browsers are supported for IDM use on systems running Windows operating systems?
6. Which web browser is supported for accessing IDM from both Solaris and Linux operating systems?
7. Is Telnet access to the sensor enabled by default?
8. What two blocking actions can you configure on the sensor?
9. What versions of Solaris are supported for access to IDM?
10. What is the purpose of the **Back** icon?
11. What are the main categories of configuration options available to a user with Administrator privileges?
12. Is SSH access to the sensor enabled by default?