Chapter 2
Installation of a Typical Sensor

Command-Line Interface

The command-line interface (CLI) of a Cisco IPS sensor is much like an IOS router, but with fewer commands and different modes. You can access the CLI using

- Telnet (disabled by default)
- Secure Shell (SSH)
- Serial interface

The default username is **cisco**, with a default password of **cisco**. You are prompted to change these upon the first login.

The CLI can be used to

- Initialize the sensor
- Configure
- Administer
- Troubleshoot
- Monitor

 Please see page 62 for more details.

Two modes of the CLI differ from a router:

- **Service mode:** Used to edit a service. You enter it using the command **service** *service-name*.
- **Multi-instance service mode:** Some of the services are multi-instance services to support virtualization. To enter this mode, use the command **service** *service-name logical-instance-name*.

Initializing the Sensor

The **setup** command at the CLI walks you through initialization. You can do the following:

- Assign a hostname to the sensor. This is case sensitive. It defaults to sensor.
- Assign an IP address to the command and control interface. The default is 10.1.9.201/24.
- Assign a default gateway. The default is 10.1.9.1.
- Enable or disable the Telnet server. Telnet is disabled by default.
- Specify the web server port. The default is 443.
- Create network access control lists (ACL) that can access the sensor for management.
- Configure the date and time.
- Configure the sensor interfaces.
- Configure virtual sensors. This enables the configuration of promiscuous and inline interface pairs.
- Configure threat prevention. An event action override denies high-risk network traffic with a risk rating of 90 to 100. This option lets you disable this feature.

 Please see page 62 for more details.

Common CLI Configuration Tasks

Here are some common commands available for use at the CLI:

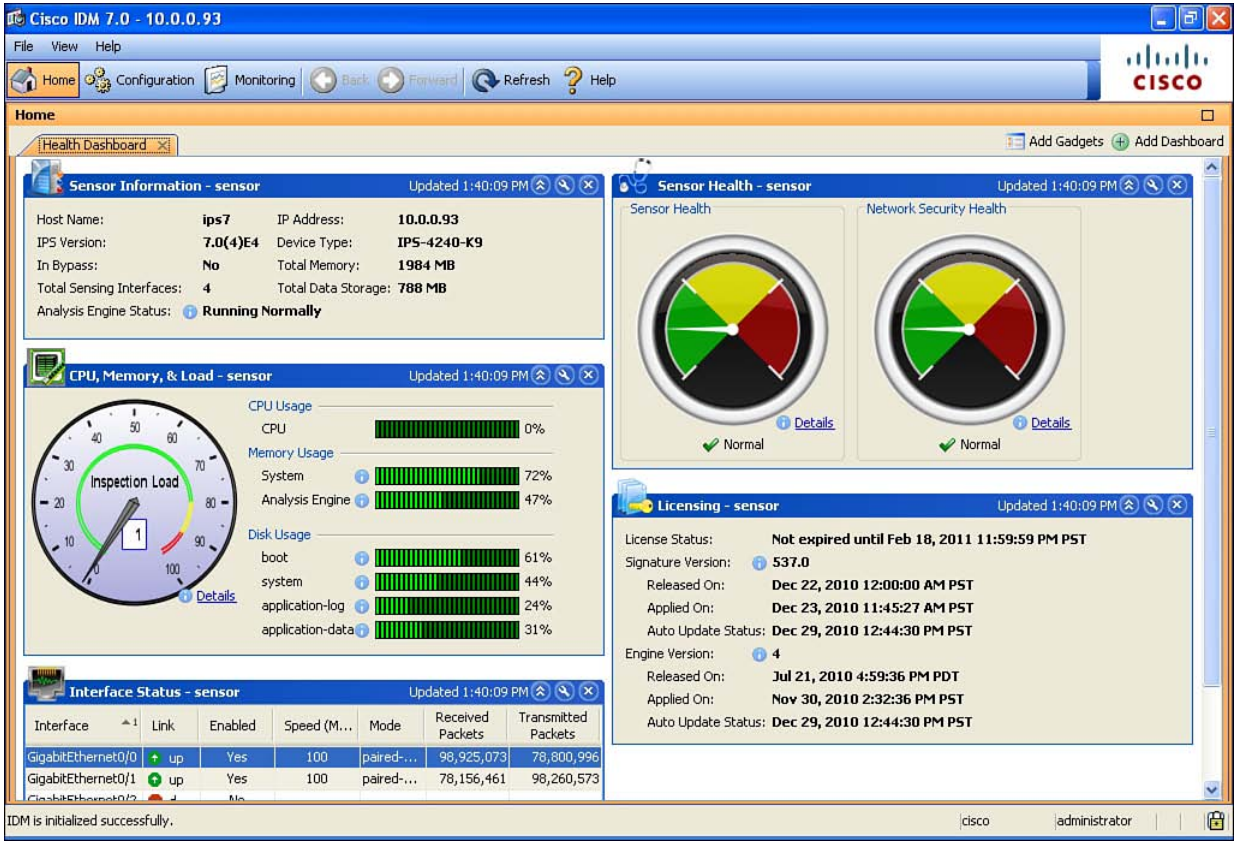
- **ping**
- **trace**
- **banner login**
- **show version**
- **copy /erase** *source-url destination-url* (The **erase** option erases the destination file before copying.)
- **copy current-config backup-config**
- **copy /erase backup-config current-config**
- **more** *keyword* (Displays configs.)
- **show settings**
- **show events**

Using Cisco IPS Device Manager

The Cisco IPS Device Manager (IDM), shown in Figure 2-1, is a superb web-based graphical user interface (GUI) for managing a single IPS device. To maintain security, the IDM and the client engage in Transport Layer Security (TLS) and Secure Sockets Layer (SSL). The server uses a trusted host certificate to verify the identity of the management workstation. The client uses a server certificate to ensure the identity of the IPS device.

 Please see page 62 for more details.

FIGURE 2-1
Cisco IDM



The Cisco IPS Sensor Software Version 7.0 uses Security Device Event Exchange (SDEE) for communication, but it still relies on Remote Data Exchange Protocol (RDEP2) to communicate configuration and IP log information.

SDEE is an IPS communications protocol developed by Cisco. Through SDEE, IPS Sensor Software Version 7.0 provides an application programming interface (API) for the sensor itself. SDEE is an enhancement to the earlier RDEP.

 Please see page 62 for more details.

The Cisco IDM runs on the following:

- Windows XP Professional (32 bit)
- Windows Vista, Business and Ultimate (32 bit)
- Windows 2003 Server
- U.S. or Japanese versions of the previously listed Windows versions
- Red Hat Linux Desktop Version 4
- Red Hat Enterprise Linux Server Version 4
- Java SE 5.0 or 6.0
- Internet Explorer 6.0 or 7.0, or Firefox 2.0

To log in to the IDM, enter **https://***sensor_ip_address*. The default address is 10.1.9.201 if you did not provide one during setup.

After you are in the IDM, you can configure the general network settings (such as hostname and IP address) by choosing **Configuration, Sensor Setup, Network**.

To display or re-create the sensor's SSH host key, choose **Configuration, Sensor Setup, SSH, Sensor Key**.

To reboot the sensor, choose **Configuration, Reboot**.

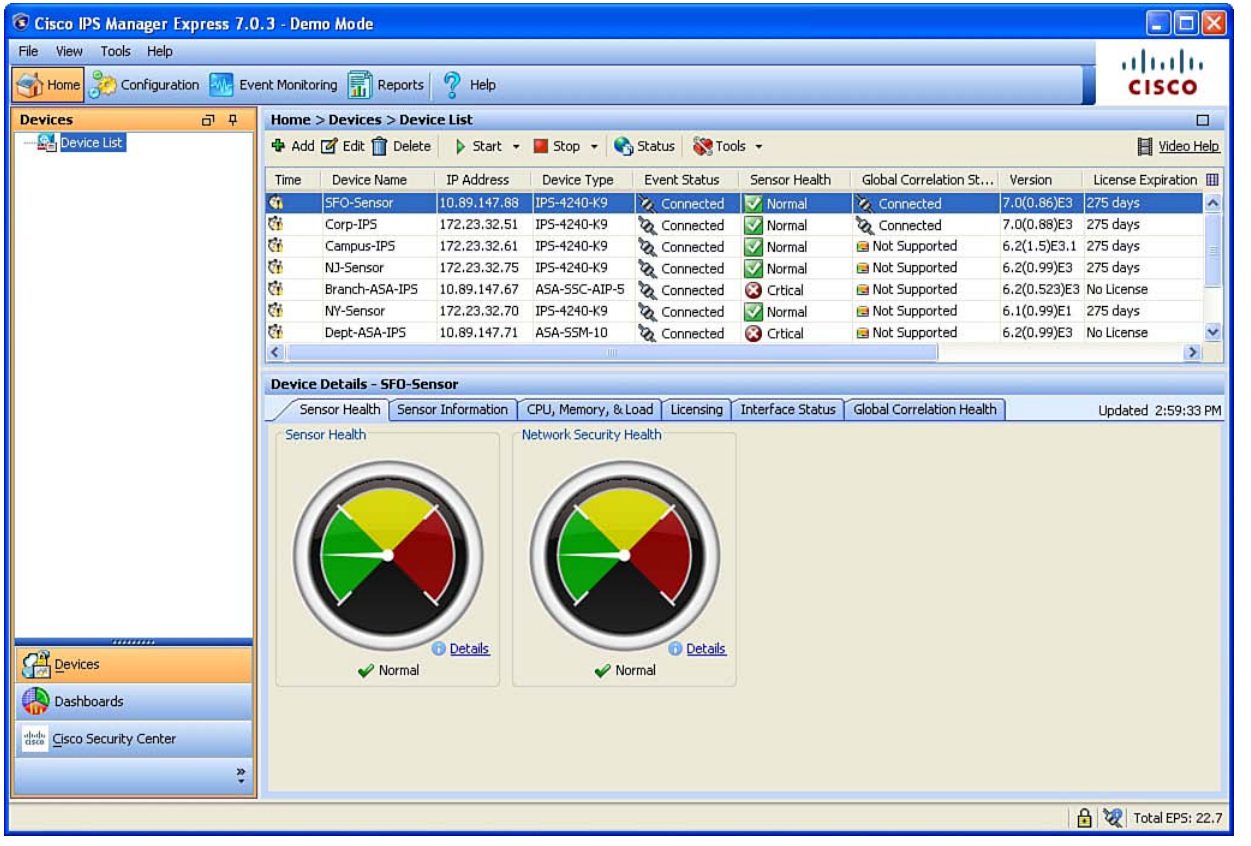
To shut down the sensor, choose **Configuration, Shut Down Sensor**. For both the reboot and shutdown, the sensor delays for 30 seconds. The logged-in users are notified that the sensor is shutting down.

Using Cisco IPS Manager Express

Cisco IPS Manager Express (IME), shown in Figure 2-2, is a free GUI for managing, monitoring, and reporting for up to ten IPS devices. It is installed onto a Windows computer and shares a common look and feel with IPS Device Manager. Like IDM, it also uses TLS and SSL for communication with the IPS sensors. The server uses a trusted host certificate to verify the identity of the management workstation. The client uses a server certificate to ensure the identity of the IPS device.

 Please see page 62 for more details.

FIGURE 2-2
Cisco IME



Cisco IPS Manager Express runs on the following:

- Windows XP (32 bit)
- Windows Vista, Business or Ultimate (32 bit)
- Windows 2003 Server

Cisco IME supports only the 32-bit U.S. version of Windows.

 Please see page 62 for more details.

Cisco IME is launched like any Windows application. When it is installed, it creates icons for both the regular version and a demo version. The demo version is useful for learning the application.

Configuring Basic Sensor Settings

This section provides guidance for completing the basic sensor setup. As soon as these tasks are complete, a basic sensor configuration will be in place in your network. The sensor generates alarms for potentially unsafe traffic that it sees. Although many of these tasks might have been completed using the **setup** command at the command line, this section focuses on using the IDM for sensor configuration.

Configuring Allowed Hosts

To configure the hosts that are allowed to access the sensor for management and configuration, choose **Configuration, Sensor Setup, Allowed Hosts**. If a host is not listed as an Allowed Host, the sensor ignores all network traffic from it, including ping.

Setting the Time

It is important to ensure that the sensor knows the correct time. This way, event information is more valuable. For a sensor, use Network Time Protocol (NTP) or, if you must, set the time manually. For the Cisco Catalyst 6500 IDSM-2, use the parent device or NTP. For the AIP-SSM, use the parent device or NTP. For the sensor, choose **Configuration, Sensor Setup, Time** to find the time settings.

Configuring Certificates

The sensor uses certificates to prove its identity to other Cisco devices on the network, and also to verify the identity of those devices.

 Please see page 62 for more details.

The sensor generates a server certificate when it first starts. You can view this certificate and generate a new one by choosing **Configuration, Sensor Setup, Certificates, Server Certificate**.

The Trusted Hosts area lists all the trusted host certificates your sensor will accept from other Cisco devices. To modify this list, choose **Configuration, Sensor Setup, Certificates, Server Certificate** and **Configuration, Sensor Setup, Certificates, Trusted Hosts**.

User Accounts

When creating user accounts on the sensor for management, you can choose from one of four roles:

- Administrator is the highest level of privileges.
- Operator can view all configuration and events. Operator can also tune signatures and manage virtual sensors and routers.
- Viewer can view configuration and event data, but cannot modify any configuration except its own password.
- Service is a special role with access to the underlying Linux operating system. It is typically used only for troubleshooting by Technical Assistance Center (TAC). Only one service account can be created on each sensor.

Only one user at a time can log in to IDM.

Create users by choosing **Configuration, Sensor Setup, Users**.

Interface Roles

Each sensor has one command and control interface for management purposes. Depending on the sensor, you can configure multiple monitoring interfaces, depending on specific hardware being used. Interfaces can function as command and control, or monitoring, or alternate TCP reset interfaces. The alternate TCP reset interface is for when the interface is operating in promiscuous mode and cannot send TCP reset packets over the same interface where the attack was detected.

 Please see page 62 for more details.

Monitoring interfaces can operate in one of four modes:

- **Promiscuous mode:** In this mode, packets do not flow through the sensor. Instead, packets are copied to the interface from a network device. This is also known as IDS mode.
- **Inline Interface Pairing mode:** Traffic passes through the sensor, from one interface to another. Two monitoring interfaces must be configured as a pair. The sensor functions as a Layer 2 bridge for this traffic.
- **Inline VLAN Pairing mode:** Here, the monitoring interface acts as an 802.1Q trunk port. The sensor bridges between pairs of VLANs on the trunk.
- **VLAN Group mode:** Each physical interface can be divided into VLAN group subinterfaces. This enables you to use a sensor with only a few interfaces as if it had many interfaces.

Configuring Interfaces

To set up monitoring interfaces, choose **Configuration, Interface Configuration, Interfaces**.

Software and Hardware Bypass Mode

The software bypass feature allows the sensor to continue passing traffic even if the sensor software fails. You configure it by choosing **Configuration, Interface Configuration, Bypass**. The possible modes are Auto, Off, and On. Choosing On causes the sensor to simply act as a bridge and not inspect traffic. Choosing Off disables software bypass entirely.

Hardware bypass complements software bypass. The four-port Gigabit Ethernet bypass card, which is available for the IPS-4260 and IPS-4270 sensors, supports hardware bypass only between ports 0 and 1 and ports 2 and 3. Hardware bypass is available only when interfaces are configured in Inline Interface Pairing mode.

 Please see page 62 for more details.

Viewing Events

As you have learned, following the steps described in this chapter enables you to configure the basics on the sensor. The sensor now produces alerts based on its default signature settings. You can view the events triggered by signatures that are enabled easily in IDM or IME. To do this in IDM, choose **Monitoring, Events**. To view events in IME, click the **Event Monitoring** button.

 Please see page 62 for more details.