Your Short Cut to Knowledge

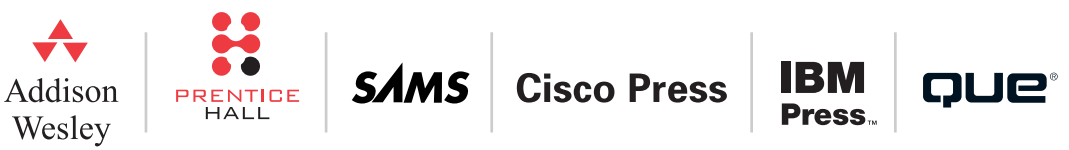
The following is an excerpt from a Short Cut published by one of the Pearson Education imprints.

Short Cuts are short, concise, PDF documents designed specifically for busy technical professionals like you.

We've provided this excerpt to help you review the product before you purchase. Please note, the hyperlinks contained within this excerpt have been deactivated.

Tap into learning—NOW!

Visit **www.informit.com/shortcuts** for a complete list of Short Cuts.



Installation of a Typical Sensor

The Command-Line Interface (CLI)

The CLI is much like the IOS version, but with fewer commands and different modes. You can access the CLI using

- Telnet (disabled by default)
- SSH
- The 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

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, you use the command **service** *service-name logical-instance-name*.

 Please see page 52 for more details.

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 ACLs 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.

Common CLI Configuration Tasks

Here are some common commands that are 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*

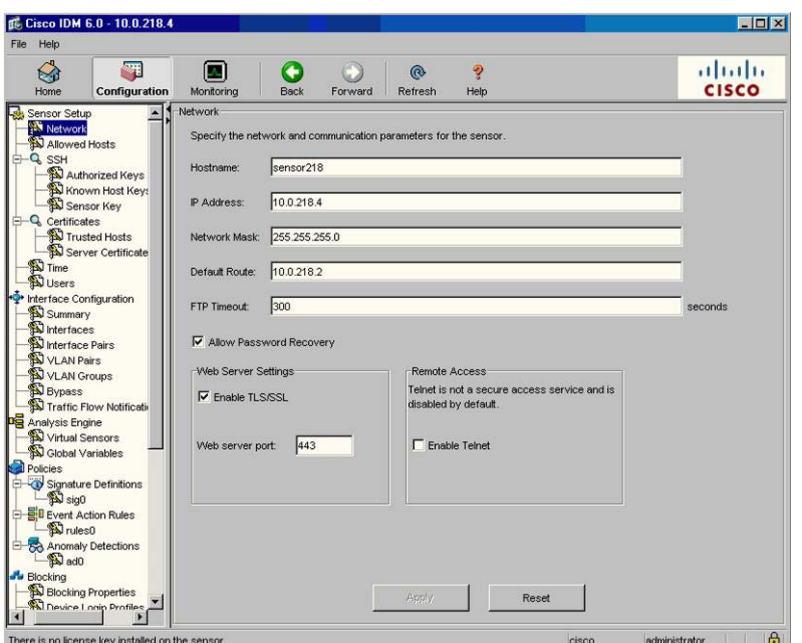
 Please see page 52 for more details.

- **copy /erase** *backup-config current-config*
- **more** *keyword*: Displays configs.
- **show settings**
- **show events**

Using the Intrusion Prevention System Device Manager

The Cisco IDM, shown in Figure 3, is a superb web-based graphical user interface for managing the IPS device. To maintain security, the IDM and the client engage in TLS and 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.

FIGURE 3
Cisco IDM



 Please see page 52 for more details.

The version 6.0 sensor software 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 software version 6 provides an application programming interface (API) for the sensor itself. SDEE is an enhancement to the earlier RDEP.

The Cisco IDM runs on the following:

- Windows 2000, XP: Internet Explorer 6 with Java Plug-in 1.5, Netscape 7.1 with Java Plug-in 1.5
- Sun SPARC Solaris 2.8 or 2.9: Mozilla 1.7
- Red Hat 9.0 or Red Hat Enterprise Linux WS, version 3 running GNOME or KDE: Mozilla 1.7

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.

Configuring Basic Sensor Settings

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

 Please see page 52 for more details.

Configuring Allowed Hosts

To configure the hosts that are allowed to access the sensor for management and configuration, choose **Configuration > Sensor Setup > Allowed Hosts**.

Setting the Time

It is very important to ensure that the sensor knows the correct time. This way, event information is more valuable. For a sensor, use 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.

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.

 Please see page 52 for more details.