CHAPTER 2

Logging In to the Sensor

This chapter explains how to log in to the sensor. It contains the following sections:

Overview

The number of concurrent CLI sessions is limited based on the platform. The IDS 4215 and the NM CIDS are limited to three concurrent CLI sessions. All other platforms allow ten concurrent sessions.

Supported User Roles

You can log in with the following user privileges:

- Administrator
- Operator
- Viewer
- Service

  The service role does not have direct access to the CLI. Service account users are logged directly in to a bash shell. Use this account for support and troubleshooting purposes only. Unauthorized modifications are not supported and will require the sensor to be reimaged to guarantee proper operation. You can create only one user with the service role.

When you log in to the service account, you receive the following warning:

```
****************************** WARNING ************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
*******************************************************************************
```

Note The service role is a special role that allows you to bypass the CLI if needed. Only a user with administrator privileges can edit the service account.

Note For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.

For More Information

For the procedure for creating the service account, see Creating the Service Account, page 4-13.

Logging In to the Appliance

You can log in to the appliance from a console port or by connecting a monitor and keyboard to the sensor.

Note You must initialize the appliance (run the **setup** command) from the console. After networking is configured, SSH and Telnet are available.

To log in to the appliance, follow these steps:

Step 1 Log in to the appliance:

- Connect a console port to the sensor.
- Connect a monitor and a keyboard to the sensor.

Step 2 Enter your username and password at the login prompt:

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the appliance.You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
```

```
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
ips-4240#
```

For More Information

- For the procedure for using the **setup** command to initialize the appliance, see Initializing the Appliance, page 3-4.
- For the procedure for connecting an appliance to a terminal server, see Connecting an Appliance to a Terminal Server, page 2-3.

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For IDS 4215, IPS 4240, IPS 4255, IPS 4260, and IPS 4270-20:
  - For terminal servers with RJ-45 connections, connect a 180 rollover cable from the console port on the appliance to a port on the terminal server.
  - For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.
- For all other appliances, connect the M.A.S.H. adapter (part number 29-4077-01) to COM1 on the appliance and:
  - For terminal servers with RJ-45 connections, connect a 180 rollover cable from the M.A.S.H. adapter to a port on the terminal server.
  - For hydra cable assemblies, connect a straight-through patch cable from the M.A.S.H. adapter to a port on the terminal server.

Step 2 Configure the line and port on the terminal server as follows:

a. In enable mode, enter the following configuration, where # is the line number of the port to be configured:

```
config t
line #
login
transport input all
```

```
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

b. If you are configuring a terminal server for an IDS 4215, IPS 4240, IPS 4255, IPS 4260, or IPS 4270-20, go to Step 3.

   Otherwise, for all other supported appliances, to direct all output to the terminal server, log in to the CLI and enter the following commands:

```
sensor# configure terminal
sensor(config)# display-serial
```

   Output is directed to the serial port. Use the **no display-serial** command to redirect output to the keyboard and monitor.

Note You can set up a terminal server and use the **display-serial** command to direct all output from the appliance to the serial port. This option lets you view system messages on a console connected to the serial port, even during the boot process. When you use this option, all output is directed to the serial port and any local keyboard and monitor connection is disabled. However, BIOS and POST messages are still displayed on the local keyboard and monitor.

Note There are no keyboard or monitor ports on an IDS-4215, IPS-4240, or IPS-4255. Keyboard and monitor ports are not supported on IPS-4260 or IPS 4270-20. Therefore, the **display-serial** and **no display-serial** commands do not apply to those platforms.

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance.

If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

For More Information

For the procedure for viewing appliance output, see Directing Output to a Serial Connection, page 2-5.

Directing Output to a Serial Connection

Use the **display-serial** command to direct all output to a serial connection. This lets you view system messages on a remote console (using the serial port) during the boot process. The local console is not available as long as this option is enabled. Use the **no display-serial** command to reset the output to the local terminal.

Caution If you are connected to the serial port, you will not get any feedback until Linux has fully booted and enabled support for the serial connection.

The **display-serial** command does not apply to the following IPS platforms:

- AIP SSM-10
- AIP SSM-20
- AIP SSM-40
- AIM IPS
- IDS 4215
- IDSM2
- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- NM CIDS

To direct output to the serial port, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Direct the output to the serial port:

```
sensor# configure terminal
sensor(config)# display-serial
```

The default is not to direct the output to a serial connection.

Step 3 Reset the output to the local console:

```
sensor(config)# no display-serial
```

Logging In to the IDSM2

You can log in to the IDSM2 from the switch.

Note You must initialize the IDSM2 (run the **setup** command) from the switch. After networking is configured, SSH and Telnet are available.

To session in to the IDSM2, follow these steps:

Step 1 Session to the IDSM2 from the switch:

- For Catalyst Software:

```
console> (enable) session slot_number
```

- For Cisco IOS software:

```
router# session slot_number processor 1
```

Step 2 Enter your username and password at the login prompt:

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the IDSM2.You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
idsm-2#
```

For More Information

For the procedure for using the **setup** command to initialize the IDSM2, see Initializing the IDSM2, page 3-12.

Logging In to the NM CIDS

You cannot access the NM CIDS through the router using the **session** command until you assign the internal management port an IP address. You can do this either by assigning an IP address directly to the IDS interface or by assigning an unnumbered loopback interface. If you do not set an IP address before you session to the NM CIDS, you receive an error message. After you assign the IP address, you can log in to the NM CIDS from the router console.

Note You must initialize the NM CIDS (run the **setup** command) from the router. After networking is configured, SSH and Telnet are available.

To session to the NM CIDS, follow these steps:

Step 1 Assign an IP address to the management port:

a. Assign an IP address directly to the IDS interface:

```
router(config)# interface IDS-Sensor1/0
router(config-if)# ip unnumbered Loopback0
router(config-if)# exit
```

b. Assign an unnumbered loopback interface:

```
router(config)# interface Loopback0
router(config-if)# ip address 1.2.3.4 255.255.255.255
router(config-if)# exit
```

The IP address can be any address that is not used anywhere else in the network.

Step 2 Session to the NM CIDS through the router console:

```
router# service-module IDS-Sensor slot_number/0 session
```

Step 3 Enter your username and password at the login prompt:

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the NM CIDS. You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
nm-cids#
```

Step 4 Press **Ctrl-Shift-6**, then **x** to get back to the router prompt if you sessioned to the router.

For More Information

For the procedure for using the **setup** command to initialize the NM CIDS, see Initializing NM CIDS, page 3-31.

Logging In to the AIM IPS

This section describes how to use the **session** command to log in to the AIM IPS. It contains the following topics:

Overview

Because the AIM IPS does not have an external console port, console access to the AIM IPS is enabled when you issue the **service-module ids-sensor** *slot*/*port* **session** command on the router, or when you initiate a Telnet connection in to the router with the slot number corresponding to the AIM IPS port number. The lack of an external console port means that the initial bootup configuration is possible only through the router.

When you issue the **service-module ids-sensor** *slot*/*port* **session** command, you create a console session with the AIM IPS, in which you can issue any IPS configuration commands. After completing work in the session and exiting the IPS CLI, you are returned to the Cisco IOS CLI.

The **session** command starts a reverse Telnet connection using the IP address of the IDS-Sensor interface. The IDS-Sensor interface is an interface between the AIM IPS and the router. You must assign an IP address to the IDS-Sensor interface before invoking the **session** command. Assigning a routable IP address can make the IDS-Sensor interface itself vulnerable to attacks, because the AIM IPS is visible on the network through that routable IP address, meaning you can communicate with the AIM IPS outside the router. To counter this vulnerability, assign an unnumbered IP address to the IDS-Sensor interface. Then the AIM IPS IP address is only used locally between the router and the AIM IPS, and is isolated for the purposes of sessioning in to the AIM IPS.

Note Before you install your application software or reimage the module, opening a session brings up the bootloader. After you install the software, opening a session brings up the application.

Caution If you session to the module and perform large console transfers, character traffic may be lost unless the host console interface speed is set to 115200/bps or higher. Use the **show running config** command to check that the speed is set to 115200/bps.

For More Information

For the procedure for configuring an unnumbered IP address interface for the AIM IPS, see Using an Unnumbered IP Address Interface, page 17-5.

Sessioning In to the AIM IPS

Note You must initialize the AIM IPS (run the **setup** command) from router. After networking is configured, SSH and Telnet are available.

Use the **service-module ids-sensor** *slot*/*port* **session** command to establish a session from the AIM IPS to the module. Press **Ctrl-Shift-6**, then **x**, to return a session prompt to a router prompt, that is, to go from the AIM IPS prompt back to the router prompt. Press **Enter** on a blank line to go back to the session prompt, which is also the router prompt. You should only suspend a session to the router if you will be returning to the session after executing router commands. If you do not plan on returning to the AIM IPS session, you should close the session rather than suspend it.

When you close a session, you are logged completely out of the AIM IPS CLI and a new session connection requires a username and password to log in. A suspended session leaves you logged in to the CLI. When you connect with the **session** command, you can go back to the same CLI without having to provide your username and password.

Note Telnet clients vary. In some cases, you may have to press **Ctrl-6 + x**. The control character is specified as ^^, Ctrl-^, or ASCII value 30 (hex 1E).

Caution If you use the **disconnect** command to leave the session, the session remains running. The open session can be exploited by someone wanting to take advantage of a connection that is still in place.

To open and close sessions to the AIM IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Check the status of the AIM IPS to make sure it is running:

```
router# service-module ids-sensor 0/0 status
Service Module is Cisco IDS-Sensor0/0
Service Module supports session via TTY line 322
Service Module is in Steady state
Getting status from the Service Module, please wait..
Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.0(0.527)E0.1
  Model:             AIM-IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.196
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

Step 3 Open a session from the router to the AIM IPS:

```
router# service-module ids-sensor 0/0 session
Trying 10.89.148.196, 2322 ... Open
```

Step 4 Exit, or suspend and close the module session.

a. `sensor# exit`

Note If you are in submodes of the IPS CLI, you must exit all submodes. Type **exit** until the sensor login prompt appears.

Failing to close a session properly makes it possible for others to exploit a connection that is still in place. Remember to type **exit** at the `router#` prompt to close the Cisco IOS session completely.

b. To suspend and close the session to the AIM IPS, press **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.

Note When you are finished with a session, you need to return to the router to establish the association between a session (the IPS application) and the router interfaces you want to monitor.

Step 5 Disconnect from the router:

```
router# disconnect
```

Step 6 Press **Enter** to confirm the disconnection:

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

For More Information

For the procedure for using the **setup** command to initialize the AIM IPS, see Initializing the AIM IPS, page 3-19.

Logging In to AIP SSM

You can log in to the AIP SSM from ASA 5500 series adaptive security appliance.

Note You must initialize the AIP SSM (run the **setup** command) from ASA 5500 series adaptive security appliance. After networking is configured, SSH and Telnet are available.

To session in to the AIP SSM from ASA 5500 series adaptive security appliance, follow these steps:

Step 1 Log in to ASA 5500 series adaptive security appliance.

Note If ASA 5500 series adaptive security appliance is operating in multi-mode, use the **change system** command to get to the system level prompt before continuing.

Step 2 Session to the AIP SSM:

```
asa# session 1
Opening command session with slot 1.
```

```
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

You have 60 seconds to log in before the session times out.

Step 3 Enter your username and password at the login prompt:

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the AIP SSM. You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
aip-ssm#
```

Step 4 To escape from a session and return to the ASA 5500 series adaptive security appliance prompt, do one of the following:

- Enter **exit**.
- Press **CTRL-Shift-6-x** (represented as **CTRL^X**).

For More Information

For the procedure for using the **setup** command to initialize the AIP SSM, see Initializing AIP SSM, page 3-24.

Logging In to the Sensor

After you have initialized the sensor using the **setup** command and enabled Telnet, you can use SSH or Telnet to log in to the sensor.

Step 1 To log in to the sensor over the network using SSH or Telnet:

```
ssh sensor_ip_address
telnet sensor_ip_address
```

Step 2 Enter your username and password at the login prompt:

```
login: ******
Password: ******
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
sensor#
```