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. IDS-4210, IDS-4215, and NM-CIDS are limited to three concurrent CLI session. All other platforms allow ten concurrent sessions.

Supported User Role

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 into 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.

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 sensor (run the **setup** command) from the console. After networking is configured, SSH and Telnet are available. For the procedure, see Logging In to the Sensor, page 2-8.

To log in to the appliance, follow these steps:

Step 1 Log in to the appliance:

- Connect a console port to the sensor.

  For the procedure, see Connecting an Appliance to a Terminal Server, page 2-3.
- 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#
```

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, and IPS-4260:
  - For 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 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/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, or IPS-4260, skip 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/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/monitor connection is disabled. However, BIOS and POST messages are still displayed on the local keyboard/monitor. For the procedure, see Directing Output to a Serial Connection, page 13-21.

Note There is only one console port on an IDS-4215, IPS-4240, IPS-4255, and IPS-4260; 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.

Logging In to IDSM-2

You can log in to IDSM-2 from the switch.

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

To session in to IDSM-2, follow these steps

Step 1 Session to IDSM-2 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 IDSM-2.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#
```

Logging In to NM-CIDS

You cannot access 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 NM-CIDS, you receive an error message.

After you assign the IP address, you can log in to NM-CIDS from the router console.

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

To session to 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 NM-CIDS through the router console:

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 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.

Logging In to AIP-SSM

You can log in to AIP-SSM from ASA.

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

To log in to AIP-SSM from ASA, follow these steps:

Step 1 Log in to ASA.

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

Step 2 Session to 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 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 prompt, do one of the following:

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

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.

To log in to the sensor, follow these steps:

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#
```