



CHAPTER 22

Logging In to the Sensor



Note

All IPS platforms allow ten concurrent CLI sessions.

This chapter explains how to log in to the various Cisco IPS platforms, and contains the following sections:

- [Logging In to the Appliance, page 22-1](#)
- [Connecting an Appliance to a Terminal Server, page 22-2](#)
- [Logging In to AIM-IPS, page 22-3](#)
- [Logging In to AIP-SSM, page 22-6](#)
- [Logging In to IDSM-2, page 22-7](#)
- [Logging In to NME-IPS, page 22-8](#)
- [Logging In to the Sensor, page 22-10](#)

Logging In to the Appliance

You can log in to the appliance from a console port.



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 Connect a console port to the sensor to log in to the appliance.

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 connecting an appliance to a terminal server, see [Connecting an Appliance to a Terminal Server, page 22-2](#).
- For the procedure for using the **setup** command to initialize the appliance, see [Chapter 21, “Initializing the Sensor.”](#)

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 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.
- Step 2** Configure the line and port on the terminal server.

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
```

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 AIM-IPS

This section describes how to session to AIM-IPS, and contains the following topics:

- [AIM-IPS and the session Command, page 22-3](#)
- [Sessioning In to AIM-IPS, page 22-4](#)

AIM-IPS and the session Command

You session in to AIM-IPS from the router console.

Because AIM-IPS does not have an external console port, console access to 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 into 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 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 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 AIM-IPS is visible on the network through that routable IP address, meaning you can communicate with 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 AIM-IPS, and is isolated for the purposes of sessioning in to 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 setting up an unnumbered IP address, refer to [Using an Unnumbered IP Address Interface](#).

Sessioning In to AIM-IPS

**Note**

You must initialize AIM-IPS (run the **setup** command) from the 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 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 AIM-IPS, follow these steps:

- Step 1** Log in to the router.
- Step 2** Check the status of AIM-IPS to make sure it is running:

```
router# service-module ids-sensor 0/1 status
Service Module is Cisco IDS-Sensor0/1
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: 6.1(1)E1
  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 AIM-IPS:

```
router# service-module ids-sensor 0/1 session  
Trying 10.89.148.196, 2322 ... Open
```

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

- `sensor# exit`

**Note**

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

**Caution**

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

- To suspend and close the session to 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 initializing AIM-IPS, see [Advanced Setup for AIM-IPS, page 21-12](#).

Logging In to AIP-SSM

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


Note

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

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

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


Note

If the 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 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 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 AIP-SSM, see [Advanced Setup for AIP-SSM, page 21-15](#).

Logging In to IDSM-2

You log in to IDSM-2 from the switch.



Note

You must initialize IDSM-2 (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/wvl/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 IDSM-2, see [Advanced Setup for IDSM-2, page 21-20](#).

Logging In to NME-IPS

This section describes how to session to NME-IPS, and contains the following topics:

- [NME-IPS and the session Command, page 22-8](#)
- [Sessioning In to NME-IPS, page 22-9](#)

NME-IPS and the session Command

You session in to NME-IPS from the router console.

Because NME-IPS does not have an external console port, console access to NME-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 into the router with the slot number corresponding to the NME-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 NME-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 NME-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 NME-IPS is visible on the network through that routable IP address, meaning you can communicate with NME-IPS outside the router. To counter this vulnerability, assign an unnumbered IP address to the IDS-Sensor interface. Then the NME-IPS IP address is only used locally between the router and NME-IPS, and is isolated for the purposes of sessioning in to NME-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 setting up interfaces on NME-IPS and the router, refer to [Setting Up Interfaces on NME-IPS and the Router](#).

Sessioning In to NME-IPS

**Note**

You must initialize NME-IPS (run the **setup** command) from the 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 NME-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 NME-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 NME-IPS session, you should close the session rather than suspend it.

When you close a session, you are logged completely out of the NME-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 NME-IPS, follow these steps:

Step 1 Log in to the router.

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

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 130
Service Module is in Steady state
Service Module heartbeat-reset is disabled
Getting status from the Service Module, please wait..

Cisco Systems Intrusion Prevention System Network Module
  Software version: 6.1(1)E2
  Model: NME-IPS
  Memory: 443508 KB
  Mgmt IP addr: 10.89.148.195
  Mgmt web ports: 443
  Mgmt TLS enabled: true

router#
```

Step 3 Open a session from the router to NME-IPS:

```
router# service-module ids-sensor 1/0 session
Trying 10.89.148.195, 2322 ... Open
```

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

- `sensor# exit`



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



Caution

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

- To suspend and close the session to NME-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 initializing NME-IPS, see [Advanced Setup for NME-IPS, page 21-24](#).

Logging In to the Sensor



Note

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#
