



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:

- [Supported User Roles, page 19-1](#)
- [Logging In to the Appliance, page 19-2](#)
- [Connecting an Appliance to a Terminal Server, page 19-3](#)
- [Logging In to the ASA 5500-X IPS SSP, page 19-4](#)
- [Logging In to the ASA 5585-X IPS SSP, page 19-5](#)
- [Using Telnet or SSH to Log In, page 19-6](#)

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 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.

For More Information

- For more information on the service account, see [Understanding the Service Account, page 4-18](#).
- For the procedures for adding and deleting users, see [Adding, Editing, Deleting Users, and Creating Accounts, page 4-23](#).

Logging In to the Appliance

**Note**

You can log in to the appliance from a console port. The currently supported Cisco IPS appliances are the IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL.

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.
 sensor#

For More Information

- For the procedure for connecting an appliance to a terminal server, see [Connecting an Appliance to a Terminal Server, page 19-3](#).
- For the procedure for using the **setup** command to initialize the appliance, see [Chapter 20, “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 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 the ASA 5500-X IPS SSP

You log in to the ASA 5500-X IPS SSP from the adaptive security appliance.

To session in to the ASA 5500-X IPS SSP from the adaptive security appliance, follow these steps:

Step 1 Log in to the adaptive security appliance.



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

```
asa# session ips
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

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 module. 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 this IPS platform.
The system will continue to operate with the currently installed
signature set. A valid license must be obtained in order to apply
signature updates. Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.

asa-ips#
```

Step 4 To escape from a session and return to the 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 ASA 5500-X IPS SSP, see [ASA 5500-X IPS SSP Advanced Setup, page 20-13](#).

Logging In to the ASA 5585-X IPS SSP

You log in to the ASA 5585-X IPS SSP from the adaptive security appliance.

To session in to the ASA 5585-X IPS SSP from the adaptive security appliance, follow these steps:

Step 1 Log in to the adaptive security appliance.



Note If the 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 ASA 5585-X IPS SSP. You have 60 seconds to log in before the session times out.

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

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 module. 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.
ips-ssp#
```

Step 4 To escape from a session and return to the 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 ASA 5585-X IPS SSP, see [ASA 5585-X IPS SSP Advanced Setup, page 20-17](#).

Using Telnet or SSH to Log In

**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 using Telnet or SSH, 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#
```

For More Information

For the procedure for initializing the sensor, see [Basic Sensor Setup, page 20-4](#).