



CHAPTER 4

Setting Up the Sensor

This chapter contains procedures for the setting up the sensor, such as changing sensor initialization information, adding and deleting users, configuring authentication, configuring time and setting up NTP, creating a service account, configuring SSH and TLS, and installing the license key. It contains the following sections:

- [Changing Network Settings, page 4-1](#)
- [Changing Web Server Settings, page 4-11](#)
- [Configuring Authentication and User Parameters, page 4-13](#)
- [Configuring Time, page 4-29](#)
- [Configuring SSH, page 4-41](#)
- [Configuring TLS, page 4-45](#)
- [Installing the License Key, page 4-48](#)

Changing Network Settings

After you initialize your sensor, you may need to change some of the network settings that you configured when you ran the **setup** command. This section describes how to change network settings, and contains the following topics:

- [Changing the Hostname, page 4-2](#)
- [Changing the IP Address, Netmask, and Gateway, page 4-3](#)
- [Enabling and Disabling Telnet, page 4-4](#)
- [Changing the Access List, page 4-5](#)
- [Changing the FTP Timeout, page 4-7](#)
- [Adding a Login Banner, page 4-8](#)
- [Configuring the DNS and Proxy Servers for Global Correlation, page 4-9](#)

Changing the Hostname

Use the **host-name** *host_name* command in the service host submode to change the hostname of the sensor after you have run the **setup** command. The default is sensor.



Note

The CLI prompt of the current session and other existing sessions will not be updated with the new hostname. Subsequent CLI login sessions will reflect the new hostname in the prompt.

To change the sensor hostname, follow these steps:

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

Step 2 Enter network settings submode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
```

Step 3 Change the sensor hostname.

```
sensor(config-hos-net)# host-name firesafe
```

Step 4 Verify the new hostname.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.130.108/23,10.89.130.1 default:
10.1.9.201/24,10.1.9.1
host-name: firesafe default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----

ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
sensor(config-hos-net)#
```

Step 5 To change the hostname back to the default setting, use the **default** form of the command.

```
sensor(config-hos-net)# default host-name
```

Step 6 Verify the change to the default hostname sensor.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.130.108/23,10.89.130.1 default:
10.1.9.201/24,10.1.9.1
host-name: sensor <defaulted>
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----
```

```

ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
sensor(config-hos-net)#

```

Step 7 Exit network settings mode.

```

sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:[yes]:

```

Step 8 Press **Enter** to apply the changes or enter **no** to discard them.

Changing the IP Address, Netmask, and Gateway

Use the **host-ip** *ip_address/netmask,default_gateway* command in the service host submode to change the IP address, netmask, and default gateway after you have run the **setup** command. The default is 10.1.9.201/24,10.1.9.1.

The **host-ip** is in the form of IP Address/Netmask/Gateway: X.X.X.X/nn,Y.Y.Y.Y, where X.X.X.X specifies the sensor IP address as a 32-bit address written as 4 octets separated by periods where X = 0-255, nn specifies the number of bits in the netmask, and Y.Y.Y.Y specifies the default gateway as a 32-bit address written as 4 octets separated by periods where Y = 0-255.

To change the sensor IP address, netmask, and default gateway, follow these steps:

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

Step 2 Enter network settings mode.

```

sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings

```

Step 3 Change the sensor IP address, netmask, and default gateway.

```

sensor(config-hos-net)# host-ip 10.89.146.110/24,10.89.146.254

```



Note The default gateway must be in the same subnet as the IP address of the sensor or the sensor generates an error and does not accept the configuration change.

Step 4 Verify the new information.

```

sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.146.110/24,10.89.146.254
default: 10.1.9.201/24,10.1.9.1
host-name: sensor default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----

```

```
ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
```

Step 5 To change the information back to the default setting, use the **default** form of the command.

```
sensor(config-hos-net)# default host-ip
```

Step 6 Verify that the host IP is now the default of 10.1.9.201/24,10.1.9.1.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.1.9.201/24,10.1.9.1 <defaulted>
host-name: sensor default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----
ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
sensor(config-hos-net)#
```

Step 7 Exit network settings mode.

```
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:[yes]:
```

Step 8 Press **Enter** to apply the changes or enter **no** to discard them.

Enabling and Disabling Telnet



Caution

Telnet is not a secure access service and therefore is disabled by default. However, SSH is always running on the sensor and it is a secure service.

Use the **telnet-option {enabled | disabled}** command in the service host submode to enable Telnet for remote access to the sensor. The default is disabled.

To enable or disable Telnet services, follow these steps:

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

Step 2 Enter network settings mode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
```

Step 3 Enable Telnet services.

```
sensor(config-hos-net)# telnet-option enabled
sensor(config-hos-net)#
```

Step 4 Verify that Telnet is enabled.

```

sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.130.108/23,10.89.130.1
default: 10.1.9.201/24,10.1.9.1
host-name: sensor default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----

ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
sensor(config-hos-net)#

```

Step 5 Exit network settings mode.

```

sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:[yes]:

```

Step 6 Press **Enter** to apply the changes or enter **no** to discard them.**Note**

To Telnet to the sensor, you must enable Telnet and configure the access list to allow the Telnet clients to connect.

For More Information

For the procedure for configuring the access list, see [Changing the Access List, page 4-5](#).

Changing the Access List

Use the **access-list** *ip_address/netmask* command in the service host submode to configure the access list, the list of hosts or networks that you want to have access to your sensor. Use the **no** form of the command to remove an entry from the list. The default access list is empty.

The following hosts must have an entry in the access list:

- Hosts that need to Telnet to your sensor.
- Hosts that need to use SSH with your sensor.
- Hosts, such as IDM and IME, that need to access your sensor from a web browser.
- Management stations, such as CSM, that need access to your sensor.
- If your sensor is a master blocking sensor, the IP addresses of the blocking forwarding sensors must have an entry in the list.

To modify the access list, follow these steps:

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

Step 2 Enter network settings mode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
```

Step 3 Add an entry to the access list.

```
sensor(config-hos-net)# access-list 10.89.146.110/32
```

The netmask for a single host is 32.

Step 4 Verify the change you made to the access-list.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.1.9.201/24,10.1.9.1 <defaulted>
host-name: sensor <defaulted>
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 2)
-----
network-address: 10.1.9.0/24
-----
network-address: 10.89.146.110/32
-----
ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
```

Step 5 Remove the entry from the access list.

```
sensor(config-hos-net)# no access-list 10.89.146.110/32
```

Step 6 Verify the entry has been removed.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.1.9.201/24,10.1.9.1 <defaulted>
host-name: sensor <defaulted>
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 10.1.9.0/24
-----
ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
sensor(config-hos-net)#
```

The host is no longer in the list.

Step 7 Change the value back to the default.

```
sensor(config-hos-net)# default access-list
```

Step 8 Verify the value has been set back to the default.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.130.108/23,10.89.130.1
default: 10.1.9.201/24,10.1.9.1
```

```

host-name: sensor <defaulted>
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 0)
-----
ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
sensor(config-hos-net)#

```

There are no hosts or networks in the list.

Step 9 Exit network settings mode.

```

sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:[yes]:

```

Step 10 Press **Enter** to apply the changes or enter **no** to discard them.

Changing the FTP Timeout



Note

You can use the FTP client for downloading updates and configuration files from your FTP server.

Use the **ftp-timeout** command in the service host submode to change the number of seconds that the FTP client waits before timing out when the sensor is communicating with an FTP server. The default is 300 seconds.

To change the FTP timeout, follow these steps:

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

Step 2 Enter network settings mode.

```

sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings

```

Step 3 Change the number of seconds of the FTP timeout.

```

sensor(config-hos-net)# ftp-timeout 500

```

Step 4 Verify the FTP timeout change.

```

sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.130.108/23,10.89.130.1
default: 10.1.9.201/24,10.1.9.1
host-name: sensor default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----

ftp-timeout: 500 seconds default: 300
login-banner-text: <defaulted>

```

```
-----
sensor(config-hos-net)#
```

Step 5 Change the value back to the default.

```
sensor(config-hos-net)# default ftp-timeout
```

Step 6 Verify the value has been set back to the default.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.130.108/23,10.89.130.1
default: 10.1.9.201/24,10.1.9.1
host-name: sensor default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----

ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
sensor(config-hos-net)#
```

Step 7 Exit network settings mode.

```
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:
```

Step 8 Press **Enter** to apply the changes or enter **no** to discard them.

Adding a Login Banner

Use the **login-banner-text** *text_message* command to add a login banner that the user sees during login. There is no default. When you want to start a new line in your message, press **Ctrl-V Enter**.

To add a login banner, follow these steps:

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

Step 2 Enter network settings mode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
```

Step 3 Add the banner login text.

```
sensor(config-hos-net)# login-banner-text This is the banner login text message.
```

Step 4 Verify the banner login text message.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.130.108/23,10.89.130.1
default: 10.1.9.201/24,10.1.9.1
host-name: sensor default: sensor
```

```

telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----
ftp-timeout: 300 seconds <defaulted>
login-banner-text: This is the banner login text message. default:
-----
sensor(config-hos-net)#

```

Step 5 To remove the login banner text, use the **no** form of the command.

```
sensor(config-hos-net)# no login-banner-text
```

Step 6 Verify the login text has been removed.

```

sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.130.108/23,10.89.130.1
default: 10.1.9.201/24,10.1.9.1
host-name: sensor default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----
ftp-timeout: 300 seconds <defaulted>
login-banner-text: default:
-----
sensor(config-hos-net)#

```

Step 7 Exit network settings mode.

```

sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:[yes]:

```

Step 8 Press **Enter** to apply the changes or enter **no** to discard them.

Configuring the DNS and Proxy Servers for Global Correlation



Caution

For global correlation to function, you must have either a DNS server or an HTTP proxy server configured at all times.



Caution

DNS resolution is supported only for accessing the global correlation update server.

You must configure either an HTTP proxy server or DNS server to support global correlation. You may need an HTTP proxy server to download global correlation updates if you use proxy in your network. If you are using a DNS server, you must configure at least one DNS server and it must be reachable for

global correlation updates to be successful. You can configure other DNS servers as backup servers. DNS queries are sent to the first server in the list. If it is unreachable, DNS queries are sent to the next configured DNS server.

Use the following options in network-settings submode to configure servers to support the global correlation features:

The following options apply:

- **http-proxy {no-proxy | proxy-sensor}**
 - **address** *ip_address*
 - **port** *port_number*
- **dns-primary-server {enabled | disabled}**
 - **address** *ip_address*
- **dns-secondary-server {enabled | disabled}**
 - **address** *ip_address*
- **dns-tertiary-server {enabled | disabled}**
 - **address** *ip_address*

To configure DNS and HTTP proxy servers to support global correlation, follow these steps:

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

Step 2 Enter network settings submode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
```

Step 3 Enable a proxy or DNS server to support global correlation:

a. Enable an HTTP proxy server.

```
sensor(config-hos-net)# http-proxy proxy-server
sensor(config-hos-net-pro)# address 10.10.10.1
sensor(config-hos-net-pro)# port 65
sensor(config-hos-net-pro)#
```

b. Enable a DNS server.

```
sensor(config-hos-net)# dns-primary-server enabled
sensor(config-hos-net-ena)# address 10.10.10.1
sensor(config-hos-net-ena)#
```

Step 4 Verify the settings.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 10.89.147.24/25,10.89.147.126 default: 192.168.1.2/24,192.168.1.1
host-name: sensor <defaulted>
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 1)
-----
network-address: 0.0.0.0/0
-----
ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
```

```

dns-primary-server
-----
enabled
-----
address: 10.10.10.1
-----
dns-secondary-server
-----
disabled
-----
-----
dns-tertiary-server
-----
disabled
-----
-----
http-proxy
-----
proxy-server
-----
address: 10.10.10.1
port: 65
-----
-----
sensor(config-hos-net) #

```

Step 5 Exit network settings mode.

```

sensor(config-hos-net) # exit
sensor(config-hos) # exit
Apply Changes:[yes]:

```

Step 6 Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

For more information on global correlation features, see [Chapter 10, “Configuring Global Correlation.”](#)

Changing Web Server Settings



Note

The default Web Server port is 443 if TLS is enabled and 80 if TLS is disabled.

After you run the **setup** command, you can change the following Web Server settings: the Web Server port, whether TLS encryption is being used, and the HTTP server header message.

HTTP is the protocol that web clients use to make requests from Web servers. The HTTP specification requires a server to identify itself in each response. Attackers sometimes exploit this protocol feature to perform reconnaissance. If the IPS Web Server identified itself by providing a predictable response, an attacker might learn that an IPS sensor is present.

We recommend that you not reveal to attackers that you have an IPS sensor. Change the **server-id** to anything that does not reveal any information, especially if your Web Server is available to the Internet. For example, if you forward a port through a firewall so you can monitor a sensor remotely, you need to set the **server-id**.

To change the Web Server settings, follow these steps:

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

Step 2 Enter web server mode.

```
sensor# configure terminal
sensor(config)# service web-server
```

Step 3 Change the port number.

```
sensor(config-web)# port 8080
```

If you change the port number from the default of 443 to 8080, you receive this message.

Warning: The web server's listening port number has changed from 443 to 8080. This change will not take effect until the web server is re-started

Step 4 Enable or disable TLS.

```
sensor(config-web)# enable-tls {true | false}
```

If you disable TLS, you receive this message.

Warning: TLS protocol support has been disabled. This change will not take effect until the web server is re-started.

Step 5 Change the HTTP server header.

```
sensor(config-web)# server-id Nothing to see here. Move along.
```

Step 6 Verify the Web Server changes.

```
sensor(config-web)# show settings
  enable-tls: true default: true
  port: 8001 default: 443
  server-id: Nothing to see here. Move along. default: HTTP/1.1 compliant
sensor(config-web)#
```

Step 7 To revert to the defaults, use the **default** form of the commands.

```
sensor(config-web)# default port
sensor(config-web)# default enable-tls
sensor(config-web)# default server-id
```

Step 8 Verify the defaults have been replaced.

```
sensor(config-web)# show settings
  enable-tls: true <defaulted>
  port: 443 <defaulted>
  server-id: HTTP/1.1 compliant <defaulted>
  configurable-service (min: 0, max: 99, current: 1)
  -----
  <protected entry>
  service-name: rdep-event-server
  -----
```

```

        enabled: true default: false
        file-name: event-server <protected>
-----
sensor(config-web)#

```

Step 9 Exit web server submode.

```

sensor(config-web)# exit
Apply Changes:[yes]:

```

Step 10 Press **Enter** to apply the changes or enter **no** to discard them.



Note

If you change the port or enable TLS settings, you must reset the sensor to make the Web Server use the new settings.

For More Information

- For the procedure for resetting the appliance, see [Resetting the Appliance, page 17-41](#).
- For the procedure for resetting the AIM IPS, see [Rebooting, Resetting, and Shutting Down the AIM IPS, page 18-18](#).
- For the procedure for resetting the AIP SSM, see [Reloading, Shutting Down, Resetting, and Recovering the AIP SSM, page 19-11](#).
- For the procedure for resetting the IDSM2, see [Resetting the IDSM2, page 20-41](#).
- For the procedure for resetting the NME IPS, see [Rebooting, Resetting, and Shutting Down the NME IPS, page 21-12](#).

Configuring Authentication and User Parameters

The following section explains how to create users, configure RADIUS authentication, create the service account, configure passwords, specify privilege level, view a list of users, configure the password policy, and lock and unlock user accounts. It contains the following topics:

- [Adding and Removing Users, page 4-14](#)
- [Configuring Authentication, page 4-15](#)
- [Creating the Service Account, page 4-21](#)
- [The Service Account and RADIUS Authentication, page 4-23](#)
- [RADIUS Authentication Functionality and Limitations, page 4-23](#)
- [Configuring Passwords, page 4-23](#)
- [Changing User Privilege Levels, page 4-24](#)
- [Showing User Status, page 4-25](#)
- [Configuring the Password Policy, page 4-26](#)
- [Configuring Account Locking, page 4-27](#)
- [Unlocking Locked Accounts, page 4-28](#)

Adding and Removing Users

Use the **username** command to create users on the local system. You can add a new user, set the privilege level—administrator, operator, viewer—and set the password for the new user. Use the **no** form of this command to remove a user from the system. This removes the user from CLI and web access.



Caution

The **username** command provides username and password authentication for login purposes only. You cannot use this command to remove a user who is logged in to the system. You cannot use this command to remove yourself from the system.

If you do not specify a password, the system prompts you for one. Use the **password** command to change the password for existing users. Use the **privilege** command to change the privilege for existing users.

The username follows the pattern `^[A-Za-z0-9()+,./-]+$`, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and `_`, and can contain 1 to 64 characters. The password must conform to the requirements set by the sensor administrator.

You receive the following error messages if you do not create a valid password:

- `Error: setEnableAuthenticationTokenStatus : The password is too short.`
- `Error: setEnableAuthenticationTokenStatus : Failure setting the account's password: it does not contain enough DIFFERENT characters`



Note

You cannot use the **privilege** command to give a user service privileges. If you want to give an existing user service privileges, you must remove that user and then use the **username** command to create the service account.

To add and remove users, follow these steps:

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

Step 2 Enter configuration mode.

```
sensor# configure terminal
```

Step 3 Specify the parameters for the user.

```
sensor(config)# username username password password privilege  
administrator/operator/viewer
```



Note

The username follows the pattern `^[A-Za-z0-9()+,./-]+$`, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and `_`, and can contain 1 to 64 characters. The password must conform to the requirements set by the sensor administrator.

For example, to add the user “tester” with a privilege level of administrator and the password “testpassword,” enter the following command.



Note

If you do not want to see the password in clear text, wait for the password prompt. Do not enter the password along with the username and privilege.

```

sensor(config)# username tester privilege administrator
Enter Login Password: *****
Re-enter Login Password: *****
sensor(config)#

```



Note If you do not specify a privilege level for the user, the user is assigned the default viewer privilege.

Step 4 Verify that the user has been added.

```

sensor(config)# exit
sensor# show users all
   CLI ID  User          Privilege
*   13491  cisco         administrator
           jsmith        operator
           jtaylor       service
           jroberts     viewer

sensor#

```

A list of users is displayed.

Step 5 To remove a user, use the **no** form of the command.

```

sensor# configure terminal
sensor(config)# no username jsmith

```



Note You cannot use this command to remove yourself from the system

Step 6 Verify that the user has been removed.

```

sensor(config)# exit
sensor# show users all
   CLI ID  User          Privilege
*   13491  cisco         administrator
           jtaylor       service
           jroberts     viewer

sensor#

```

The user `jsmith` has been removed.

For More Information

- For the procedure for creating the service account, see [Creating the Service Account, page 4-21](#).
- For the procedure for configuring local or RADIUS authentication, see [Configuring Authentication, page 4-15](#).

Configuring Authentication



Caution

Make sure you have a RADIUS server already configured before you configure RADIUS authentication on the sensor. IPS 7.0(4) has been tested with CiscoSecure ACS 4.2 servers. Refer to your RADIUS server documentation for information on how to set up a RADIUS server.

You can create and remove users from the local sensor. You can only modify one user account at a time. Each user is associated with a role that controls what that user can and cannot modify. The requirements that must be used for user passwords are set with the **password** command.

Users are authenticated through AAA either locally or through RADIUS servers. Local authentication is enabled by default. You must configure RADIUS authentication before it is active.

You must specify the user role that is authenticated through RADIUS either by configuring the user role on the RADIUS server or specifying a default user role. The username and password are sent in an authentication request to the configured RADIUS server. The response of the server determines whether the login is authenticated.

**Note**

If the sensor is not configured to use a default user role and the sensor user role information is not in the Accept Message of the CiscoSecure ACS server, the sensor rejects RADIUS authentication even if the CiscoSecure ACS server accepts the username and password.

You can configure a primary RADIUS server and a secondary RADIUS server. The secondary RADIUS server authenticates and authorizes users if the primary RADIUS server is unresponsive.

You can also configure the sensor to use local authentication (local fallback) if no RADIUS servers are responding. In this case, the sensor authenticates against the locally configured user accounts. The sensor will only use local authentication if the RADIUS servers are not available, not if the RADIUS server rejects the authentication requests of the user.

You can also configure how users connected through the console port are authenticated—through local user accounts, through RADIUS first and if that fails through local user accounts, or through RADIUS alone. If you have local fallback enabled, the SSH and Telnet sessions try to authenticate as local accounts. If you have local fallback disabled, the SSH and Telnet sessions fail.

To configure a RADIUS server on the Authentication pane, you must have the IP address, port, and shared secret of the RADIUS server. You must also either have the NAS-ID of the RADIUS server, or have the RADIUS server configured to authenticate clients without a NAS-ID or with the default IPS NAS-ID of `cisco-ips`.

**Note**

Enabling RADIUS authentication on the sensor does not disconnect already established connections. RADIUS authentication is only enforced for new connections to the sensor. Existing CLI, IDM, and IME connections remain established with the login credentials used prior to configuring RADIUS authentication. To force disconnection of these established connections, you must reset the sensor after RADIUS is configured.

RADIUS Authentication Options

Use the **aaa** command in service `aaa` submode to configure either local authentication or authentication using a RADIUS server.

The following options apply:

- **local**—Lets you specify local authentication. To continue to create users, use the **password** command.
- **radius**—Lets you specify RADIUS as the method of authentication:
 - **nas-id**—Identifies the service requesting authentication. The value can be **no nas-id**, **cisco-ips**, or a NAS-ID already configured on the RADIUS server. The default is **cisco-ips**.

- **default-user-role**—Lets you assign a default user role on the sensor that is only applied when there is NOT a Cisco av pair specifying the user role. The value can be **unspecified**, **viewer**, **operator**, or **administrator**. Service cannot be the default role. The default is **unspecified**.

If you do not want to configure a default user role on the sensor that is applied in the absence of a Cisco av pair, you need to configure the Cisco IOS/PIX 6.x RADIUS Attributes [009\001] cisco-av-pair under the group or user profile with one of the following options:

ips-role=viewer, **ips-role=operator**, **ips-role=administrator**, or **ips-role=service**.



Note If the sensor is not configured to use a default user role and the sensor user role information is not in the Accept Message of the CiscoSecure ACS server, the sensor rejects RADIUS authentication even if the CiscoSecure ACS server accepts the username and password.



Note The default user role is used only when the user has not been configured with a specific role on the ACS server. Local users are always configured with a specific role so the default user role will never apply to locally authenticated users.

- **local-fallback {enabled | disabled}**—Lets you default to local authentication if the RADIUS servers are not responding. The default is **enabled**.
- **primary-server**—Lets you configure the main RADIUS server:
 - **server-address**—The IP address of the RADIUS server.
 - **server-port**—The port of the RADIUS server. If not specified, the default RADIUS port is used.
 - **timeout** (seconds)—Specifies the number of seconds the sensor waits for a response from a RADIUS server before it considers the server to be unresponsive.
 - **shared-secret**—The secret value configured on the RADIUS server. You must obtain the secret value of the RADIUS server to enter with the **shared-secret** command.



Note You must have the same secret value configured on both the RADIUS server and the IPS sensor so that the server can authenticate the requests of the client and the client can authenticate the responses of the server.

- **secondary-server {enabled | disabled}** (optional)—Lets you configure a secondary RADIUS server:
 - **server-address**—The IP address of the RADIUS server.
 - **server-port**—Port of the RADIUS server. If not specified, the default RADIUS port is used.
 - **timeout** (seconds)—Specifies the number of seconds the sensor waits for a response from a RADIUS server before it considers the server to be unresponsive.
 - **shared-secret**—The secret value configured on the RADIUS server. You must obtain the secret value of the RADIUS server to enter with the **shared-secret** command.



Note You must have the same secret value configured on both the RADIUS server and the IPS sensor so that the server can authenticate the requests of the client and the client can authenticate the responses of the server.

- **console-authentication**—Lets you choose how users connected through the console port are authenticated:



Note Login sessions created with the ASA **session** command are authenticated as console logins.

- **local**—Users connected through the console port are authenticated through local user accounts.
- **radius-and-local**—Users connected through the console port are authenticated through RADIUS first. If RADIUS fails, local authentication is attempted. This is the default.
- **radius**—Users connected through the console port are authenticated by RADIUS. If you also have **local-fallback** enabled, users can also be authenticated through the local user accounts.

Configuring Local or RADIUS Authentication



Caution

Make sure you have a RADIUS server already configured before you configure RADIUS authentication on the sensor. IPS 7.0(4) has been tested with CiscoSecure ACS 4.2 servers. Refer to your RADIUS server documentation for information on how to set up a RADIUS server.



Note

Enabling RADIUS authentication on the sensor does not disconnect already established connections. RADIUS authentication is only enforced for new connections to the sensor. Existing CLI, IDM, and IME connections remain established with the login credentials used prior to configuring RADIUS authentication. To force disconnection of these established connections, you must reset the sensor after RADIUS is configured.

To configure local or RADIUS authentication on the sensor, follow these steps:

-
- Step 1** Log in to the CLI using an account with administrator privileges.
- Step 2** Enter configuration mode.
- ```
sensor# configure terminal
```
- Step 3** Enter AAA submode.
- ```
sensor(config)# service aaa
sensor(config-aaa)#
```
- Step 4** Configure local authentication. To continue to create users on the local system, enter **yes** to save your configuration, and use the **username** command in configure terminal mode. To configure AAA RADIUS authentication, go to Step 5.
- ```
sensor(config-aaa)# aaa local
sensor(config-aaa)# exit
Apply Changes?[yes]:yes
```
- Step 5** Configure AAA RADIUS authentication:
- Enter RADIUS authentication submode.
- ```
sensor(config-aaa)# aaa radius
sensor(config-aaa-rad)#
```

- b. Enter the Network Access ID. The NAS-ID is an identifier that clients send to servers to communicate the type of service they are attempting to authenticate. The value can be **no nas-id**, **cisco-ips**, or a NAS-ID already configured on the RADIUS server. The default is **cisco-ips**.

```
sensor(config-aaa-rad) # nas-id cisco-ips
sensor(config-aaa-rad) #
```

- c. (Optional) Configure a default user role if you are not configuring a Cisco av pair. You can configure a default user role on the sensor that is only applied when there is NOT a Cisco av pair specifying the user role. The values are **unspecified**, **viewer**, **operator**, or **administrator**. The default is **unspecified**.

```
sensor(config-aaa-rad) # default-user-role operator
sensor(config-aaa-rad) #
```



Note Service cannot be the default user role.

- d. Configure a Cisco av pair. If you do not want to configure a default user role on the sensor that is applied in the absence of a Cisco av pair, you need to configure the Cisco IOS/PIX 6.x RADIUS Attributes [009\001] cisco-av-pair under the group or user profile with one of the following options:
- **ips-role=viewer**
 - **ips-role=operator**
 - **ips-role=administrator**
 - **ips-role=service**



Note If the sensor is not configured to use a default user role and the sensor user role information is not in the Accept Message of the CiscoSecure ACS server, the sensor rejects RADIUS authentication even if the CiscoSecure ACS server accepts the username and password.



Note The default user role is used only when the user has not been configured with a specific role on the ACS server. Local users are always configured with a specific role so the default user role will never apply to locally authenticated users.

- e. Configure the sensor to switch over to local authentication if the RADIUS server becomes unresponsive.

```
sensor(config-aaa-rad) # local-fallback enabled
sensor(config-aaa-rad) #
```

Step 6 Configure the primary RADIUS server:

- a. Enter primary server submode.

```
sensor(config-aaa-rad) # primary-server
sensor(config-aaa-rad-pri) #
```

- b. Enter the RADIUS server IP address.

```
sensor(config-aaa-rad-pri) # server-address 10.1.2.3
sensor(config-aaa-rad-pri) #
```

- c. Enter the RADIUS server port. If not specified, the default RADIUS port is used.

```
sensor(config-aaa-rad-pri)# server-port 1812
sensor(config-aaa-rad-pri)#
```

- d. Enter the amount of time in seconds you want to wait for the RADIUS server to respond.

```
sensor(config-aaa-rad-pri)# time-out 5
sensor(config-aaa-rad-pri)#
```

- e. Enter the secret value that you obtained from the RADIUS server. The shared secret is a piece of data known only to the parties involved in a secure communication.

```
sensor(config-aaa-rad-pri)# shared-secret mysharedsecret
sensor(config-aaa-rad-pri)#
```



Note You must have the same secret value configured on both the RADIUS server and the IPS sensor so that the server can authenticate the requests of the client and the client can authenticate the responses of the server.

- Step 7** (Optional) Enable a secondary RADIUS server to perform authentication in case the primary RADIUS server is not responsive:

- a. Enter secondary server submode.

```
sensor(config-aaa-rad)# secondary-server enabled
sensor(config-aaa-rad-sec)#
```

- b. Enter the IP address of the second RADIUS server.

```
sensor(config-aaa-rad-sec)# server-address 10.4.5.6
sensor(config-aaa-rad-sec)#
```

- c. Enter the RADIUS server port. If not specified, the default RADIUS port is used.

```
sensor(config-aaa-rad-sec)# server-port 1812
sensor(config-aaa-rad-sec)#
```

- d. Enter the amount of time in seconds you want to wait for the RADIUS server to respond.

```
sensor(config-aaa-rad-sec)# time-out 8
sensor(config-aaa-rad-sec)#
```

- e. Enter the secret value you obtained for this RADIUS server. The shared secret is a piece of data known only to the parties involved in a secure communication.

```
sensor(config-aaa-rad-sec)# shared-secret mysharedsecret
sensor(config-aaa-rad-sec)#
```



Note You must have the same secret value configured on both the RADIUS server and the IPS sensor so that the server can authenticate the requests of the client and the client can authenticate the responses of the server.

- Step 8** Specify the type of console authentication. You can choose local, local and RADIUS, or RADIUS.



Note Login sessions created with the ASA **session** command are authenticated as console logins.

```
sensor(config-aaa-rad)# console-authentication radius-and-local
```

```
sensor(config-aaa-rad)#
```

Step 9 Verify the settings:

```
sensor(config-aaa-rad)# show settings
radius
-----
primary-server
-----
server-address: 10.1.2.3
server-port: 1812 <defaulted>
shared-secret: mysharedsecret
timeout: 3 <defaulted>
-----
secondary-server
-----
enabled
-----
server-address: 10.4.5.6
server-port: 1816 default: 1812
shared-secret: mysharedsecret
timeout: 8 default: 3
-----
nas-id: cisco-ips default: cisco-ips
local-fallback: enabled default: enabled
console-authentication: radius-and-local <defaulted>
default-user-role: operator default: unspecified
-----
sensor(config-aaa-rad)#
```

Step 10 Exit AAA mode.

```
sensor(config-aaa-rad)# exit
sensor(config-aaa)# exit
Apply Changes:[yes]:
```

Step 11 Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

- For the procedure for adding and removing users, see [Adding and Removing Users, page 4-14](#).
- For the procedure for configuring passwords, see [Configuring Passwords, page 4-23](#).
- For the procedure for specifying password requirements, see [Configuring the Password Policy, page 4-26](#).
- For detailed information on RADIUS and the service account, see [The Service Account and RADIUS Authentication, page 4-23](#).

Creating the Service Account

You can create a service account for TAC to use during troubleshooting. Although more than one user can have access to the sensor, only one user can have service privileges on a sensor. The service account is for support purposes only.

**Caution**

Do not make modifications to the sensor through the service account except under the direction of TAC. If you use the service account to configure the sensor, your configuration is not supported by TAC. Adding services to the operating system through the service account affects proper performance and functioning of the other IPS services. TAC does not support a sensor on which additional services have been added.

**Note**

The root user password is synchronized to the service account password when the service account is created. To gain root access you must log in with the service account and switch to user root with the **su - root** command.

**Caution**

You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

**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.

To create the service account, follow these steps:

-
- Step 1** Log in to the CLI using an account with administrator privileges.
- Step 2** Enter configuration mode.
- ```
sensor# configure terminal
```
- Step 3** Specify the parameters for the service account. The username follows the pattern `^[A-Za-z0-9()+,._/-]+$`, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and \_, and can contain 1 to 64 characters.
- ```
sensor(config)# user username privilege service
```
- Step 4** Specify a password when prompted. The password must conform to the requirements set by the sensor administrator. If a service account already exists for this sensor, the following error is displayed and no service account is created.
- ```
Error: Only one service account may exist
```
- Step 5** Exit configuration mode.
- ```
sensor(config)# exit
sensor#
```

When you use the service account to log in to the CLI, you receive this 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 reimaged to guarantee proper operation.
*****
```

The Service Account and RADIUS Authentication

If you are using RADIUS authentication and want to create and use a service account, you must create the service account both on your sensor and on the RADIUS server.

You must use local authentication to access the service account on the sensor. The service account must be created manually as a local account on the sensor. Then when you configure RADIUS authentication, the service account must also be configured manually on the RADIUS server with the accept message set to `ip-role=service`.

When you log in to the service account, you are authenticated against both the sensor account and the RADIUS server account. By whatever method you use to access the service account—serial console port, direct monitor/keyboard (for sensors that support it), or a network connection, such as SSH or Telnet—you have to log in using local authentication.

RADIUS Authentication Functionality and Limitations

The current AAA RADIUS implementation has the following functionality and limitations:

- Authentication with a RADIUS server

However, you cannot change the password of the RADIUS server from the IPS.

- Authorization

You can perform role-based authorization by specifying the IPS role of the user on the RADIUS server.

- Accounting

The login attempts of the user and the configuration changes are logged as events locally on the IPS. However, these account messages are not communicated to the RADIUS server.

Configuring Passwords

Use the `password` command to update the password on the local sensor. You can also use this command to change the password for an existing user or to reset the password for a locked account. A valid password is 8 to 32 characters long. All characters except space are allowed.

To change the password, follow these steps:

Step 1 To change the password for another user or reset the password for a locked account, follow these steps:

- a. Log in to the CLI using an account with administrator privileges.
- b. Enter configuration mode.

```
sensor# configure terminal
```

- c. Change the password for a specific user.

```
sensor(config)# password tester
Enter New Login Password: *****
Re-enter New Login Password: *****
```



Note This example modifies the password for the user “tester.”

- Step 2** To change your password, follow these steps:

- a. Log in to the CLI.
b. Enter configuration mode.

```
sensor# configure terminal
```

- c. Change your password.

```
sensor(config)# password
Enter Old Login Password:*****
Enter New Login Password: *****
Re-enter New Login Password: *****
```

Changing User Privilege Levels



Note

You cannot use the **privilege** command to give a user service privileges. If you want to give an existing user service privileges, you must remove that user and then use the **username** command to create the service account. There can only be one person with service privileges.

Use the **privilege** command to change the privilege level—administrator, operator, viewer—for a user.

To change the privilege level for a user, follow these steps:

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

- Step 2** Verify the current privilege of the user *jsmith*.

```
sensor# show users all
  CLI ID  User      Privilege
*   13491  cisco    administrator
          jsmith   viewer
          operator operator
          service service
          viewer  viewer
sensor#
```

- Step 3** Change the privilege level from viewer to operator.

```
sensor# configure terminal
sensor(config)# privilege user jsmith operator
Warning: The privilege change does not apply to current CLI sessions. It will be applied
to subsequent logins.
sensor(config)#
```

- Step 4** Verify that the privilege of the user has been changed. The privilege of the user jsmith has been changed from viewer to operator.

```
sensor(config)# exit
sensor# show users all

      CLI ID  User      Privilege
*   13491   cisco    administrator
      jsmith   operator
      operator operator
      service  service
      viewer   viewer

sensor#
```

- Step 5** Display your current level of privilege.

```
sensor# show privilege
Current privilege level is administrator
```

For More Information

For the procedure for creating the service account, see [Creating the Service Account, page 4-21](#).

Showing User Status



Note All IPS platforms allow ten concurrent log in sessions.

Use the **show users** command to view information about the username and privilege of all users logged in to the sensor, and all user accounts on the sensor regardless of login status.

An * indicates the current user. If an account is locked, the username is surrounded by parentheses. A locked account means that the user failed to enter the correct password after the configured attempts.

To show user information, follow these steps:

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

- Step 2** Verify the users logged in to the sensor.

```
sensor# show users

      CLI ID  User      Privilege
*   13491   cisco    administrator

sensor#
```

- Step 3** Verify all users.

```
sensor# show users all

      CLI ID  User      Privilege
*   13491   cisco    administrator
      5824   (jsmith) viewer
      9802   tester   operator

sensor#
```

The account of the user jsmith is locked.

- Step 4** To unlock the account of jsmith, reset the password.

```
sensor# configure terminal
```

```
sensor(config)# password jsmith
Enter New Login Password: *****
Re-enter New Login Password: *****
```

Configuring the Password Policy



Caution

If the password policy includes minimum numbers of character sets, such as upper case or number characters, the sum of the minimum number of required character sets cannot exceed the minimum password size. For example, you cannot set a minimum password size of eight and also require that passwords must contain at least five lowercase and five uppercase characters.

As sensor administrator, you can configure how passwords are created. All user-created passwords must conform to the policy that you set up. For example, you can set a policy where passwords must have at least 10 characters and no more than 40, and must have a minimum of 2 upper case and 2 numeric characters. Once that policy is set, every password configured for each user account must conform to this password policy.

You can set login attempts and the size and minimum characters requirements for a password. The minimum password length is eight characters.

If you forget your password, there are various ways to recover the password depending on your sensor platform.

To set up a password policy, follow these steps:

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

Step 2 Enter password strength authentication submode.

```
sensor# configure terminal
sensor(config)# service authentication
sensor(config-aut)# password-strength
```

Step 3 Set the minimum number of numeric digits that must be in a password. The range is 0 to 64.

```
sensor(config-aut-pas)# digits-min 6
```

Step 4 Set the minimum number of nonalphanumeric printable characters that must be in a password. The range is 0 to 64.

```
sensor(config-aut-pas)# other-min 3
```

Step 5 Set the minimum number of uppercase alphabet characters that must be in a password. The range is 0 to 64.

```
sensor(config-aut-pas)# uppercase-min 3
```

Step 6 Set the minimum number of lower-case alphabet characters that must be in a password.

```
sensor(config-aut-pas)# lowercase-min 3
```

Step 7 Set the number of old passwords to remember for each account.

```
sensor(config-aut-pas)# number-old-passwords 3
```

A new password cannot match any of the old passwords of an account.

Step 8 Check your new setting.

```

sensor(config-aut-pas)# show settings
password-strength
-----
size: 8-64 <defaulted>
digits-min: 6 default: 0
uppercase-min: 3 default: 0
lowercase-min: 3 default: 0
other-min: 3 default: 0
number-old-passwords: 3 default: 0
-----
sensor(config-aut-pas)#

```

For More Information

For the procedures for recovering the sensor password, see [Configuring Time, page 4-29](#).

Configuring Account Locking

**Note**

When you configure account locking, local authentication, as well as RADIUS authentication, is affected. After a specified number of failed attempts to log in locally or in to a RADIUS account, the account is locked locally on the sensor.

Use the **attemptLimit** *number* command in authentication submode to lock accounts so that users cannot keep trying to log in after a certain number of failed attempts. The default is 0, which indicates unlimited authentication attempts. For security purposes, you should change this number.

To configure account locking, follow these steps:

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

Step 2 Enter service authentication submode.

```

sensor# configure terminal
sensor(config)# service authentication

```

Step 3 Set the number of attempts users will have to log in to accounts.

```

sensor(config-aut)# attemptLimit 3

```

Step 4 Check your new setting.

```

sensor(config-aut)# show settings
attemptLimit: 3 defaulted: 0
sensor(config-aut)#

```

Step 5 To set the value back to the system default setting:

```

sensor(config-aut)# default attemptLimit

```

Step 6 Check that the setting has returned to the default.

```

sensor(config-aut)# show settings
attemptLimit: 0 <defaulted>
sensor(config-aut)#

```

Step 7 Check to see if any users have locked accounts.



Note When you apply a configuration that contains a non-zero value for `attemptLimit`, a change is made in the SSH server that may subsequently impact your ability to connect with the sensor. When `attemptLimit` is non-zero, the SSH server requires the client to support challenge-response authentication. If you experience problems after your SSH client connects but before it prompts for a password, you need to enable challenge-response authentication. Refer to the documentation for your SSH client for instructions.

```
sensor(config-aut)# exit
sensor(config)# exit
sensor# show users all
  CLI ID   User      Privilege
*  1349    cisco     administrator
   5824    (jsmith)  viewer
   9802    tester    operator
```

The account of the user `jsmith` is locked as indicated by the parenthesis.

Step 8 To unlock the account of `jsmith`, reset the password or use the **unlock user** *username* command.

```
sensor# configure terminal
sensor(config)# password jsmith
Enter New Login Password: *****
Re-enter New Login Password: *****
```

For More Information

For the procedure to use the **unlock user** *username* command to unlock a locked account, see [Unlocking Locked Accounts](#), page 4-28.

Unlocking Locked Accounts



Note When you configure account locking, local authentication as well as RADIUS authentication is affected. After a specified number of failed attempts to log in locally or into a RADIUS account, the account is locked locally on the sensor. For local accounts, you can reset the password or use the **unlock user** *username* command to unlock the account. For RADIUS user accounts, you must use the **unlock user** *username* command to unlock the account.

Use the **unlock user** *username* command in global configuration mode to unlock local and RADIUS accounts after users have been locked out after a certain number of failed attempts.



Note The **unlock** command is only supported in IPS 7.0(4)E4 and later and does not work in earlier IPS software versions.

To configure account unlocking, follow these steps:

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

Step 2 Check to see if any users have locked accounts.

```
sensor# show users all
  CLI ID  User      Privilege
*   1349  cisco    administrator
    5824  (jsmith) viewer
    9802  tester   operator
```

The account of the user `jsmith` is locked as indicated by the parenthesis.

Step 3 Enter global configuration mode.

```
sensor# configure terminal
sensor(config)#
```

Step 4 Unlock the account.

```
sensor(config)# unlock user jsmith
```

Step 5 Check your new setting.

```
sensor# show users all
  CLI ID  User      Privilege
*   1349  cisco    administrator
    5824  jsmith   viewer
    9802  tester   operator
```

The account of the user `jsmith` is now unlocked as indicated by the lack of parenthesis.

Configuring Time

This section describes the importance of having a reliable time source for the sensor. It contains the following topics:

- [Time Sources and the Sensor, page 4-29](#)
- [Synchronizing IPS Module System Clocks with the Parent Device System Clock, page 4-31](#)
- [Correcting Time on the Sensor, page 4-31](#)
- [Configuring Time on the Sensor, page 4-31](#)
- [Configuring NTP, page 4-38](#)

Time Sources and the Sensor

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings. This section provides a summary of the various ways to set the time on sensors.



Note We recommend that you use an NTP server. You can use authenticated or unauthenticated NTP. For authenticated NTP, you must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server. You can set up NTP during initialization or you can configure NTP through the CLI, IDM, IME, or ASDM.

Appliances

- Use the **clock set** command to set the time. This is the default.
- Configure the appliance to get its time from an NTP time synchronization source.

IDSM2

- The IDSM2 can automatically synchronize its clock with the switch time. This is the default. The UTC time is synchronized between the switch and the IDSM2. The time zone and summertime settings are not synchronized between the switch and the IDSM2.



Note Be sure to set the time zone and summertime settings on both the switch and the IDSM2 to ensure that the UTC time settings are correct. The local time of the IDSM2 could be incorrect if the time zone and/or summertime settings do not match between the IDSM2 and the switch.

- Configure the IDSM2 to get its time from an NTP time synchronization source.

AIM IPS and the NME IPS

- AIM IPS and NME IPS can automatically synchronize their clock with the clock in the router chassis in which they are installed (parent router). This is the default. The UTC time is synchronized between the parent router and AIM IPS and NME IPS. The time zone and summertime settings are not synchronized between the parent router and AIM IPS and NME IPS.



Note Be sure to set the time zone and summertime settings on both the parent router and AIM IPS and NME IPS to ensure that the UTC time settings are correct. The local time of AIM IPS and NME IPS could be incorrect if the time zone and/or summertime settings do not match between AIM IPS and NME IPS and the router.

- Configure the AIM IPS and NME IPS to get their time from an NTP time synchronization source, such as a Cisco router, other than the parent router.

AIP SSM

- The AIP SSM automatically synchronizes its clock with the clock in the adaptive security appliance in which it is installed. This is the default.
- Configure the AIP SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router.

For More Information

For the procedure for configuring NTP, see [Configuring NTP, page 4-38](#).

Synchronizing IPS Module System Clocks with the Parent Device System Clock

All IPS modules (AIM IPS, AIP SSM, IDSM2, and NME IPS) synchronize their system clocks to the parent chassis clock (switch, router, or security appliance) each time the module boots up and any time the parent chassis clock is set. The module clock and parent chassis clock tend to drift apart over time. The difference can be as much as several seconds per day. To avoid this problem, make sure that both the module clock and the parent clock are synchronized to an external NTP server. If only the module clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs.

Correcting Time on the Sensor

If you set the time incorrectly, your stored events will have the incorrect time because they are stamped with the time the event was created. The Event Store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command.

**Note**

You cannot remove individual events.

For More Information

For the procedure for clearing events, see [Clearing Events from Event Store, page 7-42](#).

Configuring Time on the Sensor

This section describes how to configure time on the sensor so that your events are time-stamped correctly. It contains the following topics:

- [Displaying the System Clock, page 4-32](#)
- [Manually Setting the System Clock, page 4-32](#)
- [Configuring Recurring Summertime Settings, page 4-33](#)
- [Configuring Nonrecurring Summertime Settings, page 4-35](#)
- [Configuring Time Zones Settings, page 4-37](#)

Displaying the System Clock

Use the **show clock [detail]** command to display the system clock. You can use the **detail** option to indicate the clock source (NTP or system) and the current summertime setting (if any). The system clock keeps an authoritative flag that indicates whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source, such as NTP, the flag is set.

Table 4-1 lists the system clock flags.

Table 4-1 System Clock Flags

Symbol	Description
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but NTP is not synchronized.

To display the system clock, follow these steps:

-
- Step 1** Log in to the CLI.
- Step 2** Display the system clock.
- Step 3** Display the system clock with details.

```
sensor# show clock
*19:04:52 UTC Thu Apr 03 2008
```

```
sensor# show clock detail
20:09:43 UTC Thu Apr 03 2008
Time source is NTP
Summer time starts 03:00:00 UTC Sun Mar 09 2008
Summer time stops 01:00:00 UTC Sun Nov 02 2008
```

This indicates that the sensor is getting its time from NTP and that is configured and synchronized.

```
sensor# show clock detail
*20:09:43 UTC Thu Apr 03 2008
No time source
Summer time starts 03:00:00 UTC Sun Mar 09 2008
Summer time stops 01:00:00 UTC Sun Nov 02 2008
```

This indicates that no time source is configured.

Manually Setting the System Clock



Note

You do not need to set the system clock if your sensor is synchronized by a valid outside timing mechanism such as an NTP clock source.

Use the **clock set hh:mm [:ss] month day year** command to manually set the clock on the appliance. Use this command if no other time sources are available.

The **clock set** command does not apply to the following platforms:

- AIM IPS
- AIP SSM
- IDSM2
- NME IPS

To manually set the clock on the appliance, follow these steps:

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

Step 2 Set the clock manually.

```
sensor# clock set 13:21 Mar 29 2008
```



Note The time format is 24-hour time.

Configuring Recurring Summertime Settings



Note Summertime is a term for daylight saving time.

Use the **summertime-option recurring** command to configure the sensor to switch to summertime settings on a recurring basis. The default is recurring.

To configure the sensor to switch to summertime settings on a recurring basis, follow these steps:

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

Step 2 Enter summertime recurring submode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# summertime-option recurring
```

Step 3 Enter start summertime submode.

```
sensor(config-hos-rec)# start-summertime
```

Step 4 Configure the start summertime parameters:

- a. Enter the day of the week you want to start summertime settings.

```
sensor(config-hos-rec-sta)# day-of-week monday
```

- b. Enter the month you want to start summertime settings.

```
sensor(config-hos-rec-sta)# month april
```

- c. Enter the time of day you want to start summertime settings. The format is hh:mm:ss.

```
sensor(config-hos-rec-sta)# time-of-day 12:00:00
```

- d. Enter the week of the month you want to start summertime settings. The values are first through fifth, or last.

```
sensor(config-hos-rec-sta)# week-of-month first
```

- e. Verify your settings.

```
sensor(config-hos-rec-sta)# show settings
start-summertime
-----
month: april default: april
week-of-month: first default: first
day-of-week: monday default: sunday
time-of-day: 12:00:00 default: 02:00:00
-----
sensor(config-hos-rec-sta)#
```

- Step 5** Enter end summertime submode.

```
sensor(config-hos-rec-sta)# exit
sensor(config-hos-rec)# end-summertime
```

- Step 6** Configure the end summertime parameters:

- a. Enter the day of the week you want to end summertime settings.

```
sensor(config-hos-rec-end)# day-of-week friday
```

- b. Enter the month you want to end summertime settings.

```
sensor(config-hos-rec-end)# month october
```

- c. Enter the time of day you want to end summertime settings. The format is hh:mm:ss.

```
sensor(config-hos-rec-end)# time-of-day 05:15:00
```

- d. Enter the week of the month you want to end summertime settings.

```
sensor(config-hos-rec-end)# week-of-month last
```

The values are first through fifth, or last.

- e. Verify your settings.

```
sensor(config-hos-rec-end)# show settings
end-summertime
-----
month: october default: october
week-of-month: last default: last
day-of-week: friday default: sunday
time-of-day: 05:15:00 default: 02:00:00
-----
sensor(config-hos-rec-end)#
```

- Step 7** Specify the local time zone used during summertime.

```
sensor(config-hos-rec-end)# exit
sensor(config-hos-rec)# summertime-zone-name CDT
```

- Step 8** Specify the offset.

```
sensor(config-hos-rec)# offset 60
```



Note Changing the time zone offset requires the sensor to reboot.

Step 9 Verify your settings.

```

sensor(config-hos-rec)# show settings
recurring
-----
offset: 60 minutes default: 60
summertime-zone-name: CDT
start-summertime
-----
month: april default: april
week-of-month: first default: first
day-of-week: monday default: sunday
time-of-day: 12:00:00 default: 02:00:00
-----
end-summertime
-----
month: october default: october
week-of-month: last default: last
day-of-week: friday default: sunday
time-of-day: 05:15:00 default: 02:00:00
-----
-----

```

Step 10 Exit recurring summertime submode.

```

sensor(config-hos-rec)# exit
sensor(config-hos)# exit
Apply Changes:[yes]:

```

Step 11 Press **Enter** to apply the changes or enter **no** to discard them.

Configuring Nonrecurring Summertime Settings



Note Summertime is a term for daylight saving time.

Use the **summertime-option non-recurring** command to configure the sensor to switch to summer time settings on a one-time basis. The default is recurring. To configure the sensor to switch to summertime settings on a one-time basis, follow these steps:

Step 1 Log in to the sensor using an account with administrator privileges.**Step 2** Enter summertime non-recurring submode.

```

sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# summertime-option non-recurring

```

Step 3 Enter start summertime submode.

```

sensor(config-hos-non)# start-summertime

```

Step 4 Configure the start summertime parameters:

- a. Enter the date you want to start summertime settings. The format is yyyy-mm-dd.

```

sensor(config-hos-non-sta)# date 2004-05-15

```

- b. Enter the time you want to start summertime settings. The format is hh:mm:ss.

```
sensor(config-hos-non-sta)# time 12:00:00
```

- c. Verify your settings.

```
sensor(config-hos-non-sta)# show settings
start-summertime
-----
date: 2004-05-15
time: 12:00:00
-----
sensor(config-hos-non-sta)#
```

- Step 5** Enter end summertime submode.

```
sensor(config-hos-non-sta)# exit
sensor(config-hos-non)# end-summertime
```

- Step 6** Configure the end summertime parameters:

- a. Enter the date you want to end summertime settings. The format is yyyy-mm-dd.

```
sensor(config-hos-non-end)# date 2004-10-31
```

- b. Enter the time you want to end summertime settings. The format is hh:mm:ss.

```
sensor(config-hos-non-end)# time 12:00:00
```

- c. Verify your settings.

```
sensor(config-hos-non-end)# show settings
end-summertime
-----
date: 2004-10-31
time: 12:00:00
-----
sensor(config-hos-non-end)#
```

- Step 7** Specify the local time zone used during summertime.

```
sensor(config-hos-non-end)# exit
sensor(config-hos-non)# summertime-zone-name CDT
```

- Step 8** Specify the offset.

```
sensor(config-hos-non)# offset 60
```



Note Changing the time zone offset requires the sensor to reboot.

- Step 9** Verify your settings.

```
sensor(config-hos-non)# show settings
non-recurring
-----
offset: 60 minutes default: 60
summertime-zone-name: CDT
start-summertime
-----
date: 2004-05-15
time: 12:00:00
-----
end-summertime
-----
```

```

date: 2004-10-31
time: 12:00:00
-----
-----
sensor(config-hos-non)#

```

Step 10 Exit non-recurring summertime submode.

```

sensor(config-hos-non)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:

```

Step 11 Press **Enter** to apply the changes or enter **no** to discard them.

Configuring Time Zones Settings

Use the **time-zone-settings** command to configure the time zone settings on the sensor, such as the time zone name the sensor displays whenever summertime settings are not in effect and the offset. To configure the time zone settings on the sensor, follow these steps:

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

Step 2 Enter time zone settings submode.

```

sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# time-zone-settings

```

Step 3 Configure the time zone name that is displayed whenever summertime settings are not in effect. The default is UTC.

```

sensor(config-hos-tim)# standard-time-zone-name CST

```

Step 4 Configure the offset in minutes. The offset is the number of minutes you add to UTC to get the local time. The default is 0.

```

sensor(config-hos-tim)# offset -360

```



Note Changing the time zone offset requires the sensor to reboot.

Step 5 Verify your settings.

```

sensor(config-hos-tim)# show settings
time-zone-settings
-----
offset: -360 minutes default: 0
standard-time-zone-name: CST default: UTC
-----
sensor(config-hos-tim)#

```

Step 6 Exit time zone settings submode.

```

sensor(config-hos-tim)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:

```

Step 7 Press **Enter** to apply the changes or enter **no** to discard them.

Configuring NTP

This section describes how to configure a Cisco router to be an NTP server and how to configure the sensor to use an NTP server as its time source. It contains the following topics:

- [Configuring a Cisco Router to be an NTP Server, page 4-38](#)
- [Configuring the Sensor to Use an NTP Time Source, page 4-39](#)

Configuring a Cisco Router to be an NTP Server



Caution

The sensor NTP capability is designed to be compatible with Cisco routers acting as NTP servers. The sensor may work with other NTP servers, but is not tested or supported.



Note

Remember the NTP server key ID and key values. You need them along with the NTP server IP address when you configure the sensor to use the NTP server as its time source.

The sensor requires an authenticated connection with an NTP server if it is going to use the NTP server as its time source. The sensor supports only the MD5 hash algorithm for key encryption. Use the following procedure to activate a Cisco router to act as an NTP server and use its internal clock as the time source.

To set up a Cisco router to act as an NTP server, follow these steps:

Step 1 Log in to the router.

Step 2 Enter configuration mode.

```
router# configure terminal
```

Step 3 Create the key ID and key value. The key ID can be a number between 1 and 65535. The key value is text (numeric or character). It is encrypted later.

```
router(config)# ntp authentication-key key_ID md5 key_value
```

Example

```
router(config)# ntp authentication-key 100 md5 attack
```



Note

The sensor only supports MD5 keys.



Note

Keys may already exist on the router. Use the **show running configuration** command to check for other keys. You can use those values for the trusted key in Step 4.

- Step 4** Designate the key you just created in Step 3 as the trusted key (or use an existing key). The trusted key ID is the same number as the key ID in Step 3.

```
router(config)# ntp trusted-key key_ID
```

Example

```
router(config)# ntp trusted-key 100
```

- Step 5** Specify the interface on the router with which the sensor will communicate.

```
router(config)# ntp source interface_name
```

Example

```
router(config)# ntp source FastEthernet 1/0
```

- Step 6** Specify the NTP master stratum number to be assigned to the sensor. The NTP master stratum number identifies the relative position of the server in the NTP hierarchy. You can choose a number between 1 and 15. It is not important to the sensor which number you choose.

```
router(config)# ntp master stratum_number
```

Example

```
router(config)# ntp master 6
```

Configuring the Sensor to Use an NTP Time Source



Note

For authenticated NTP, you must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server.



Caution

The sensor NTP capability is designed to be compatible with Cisco routers acting as NTP servers. The sensor may work with other NTP servers, but is not tested or supported.

The sensor requires a consistent time source. We recommend that you use an NTP server. Use the following procedure to configure the sensor to use the NTP server as its time source. You can use authenticated or unauthenticated NTP.

To configure the sensor to use an NTP server as its time source, follow these steps:

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

- Step 2** Enter configuration mode.

```
sensor# configure terminal
```

- Step 3** Enter service host mode.

```
sensor(config)# service host
```

- Step 4** Configure unauthenticated NTP:

- a. Enter NTP configuration mode.

```
sensor(config-hos)# ntp-option enabled-ntp-unauthenticated
```

- b. Specify the NTP server IP address.

```
sensor(config-hos-ena)# ntp-server ip_address
```

- c. Verify the unauthenticated NTP settings.

```
sensor(config-hos-ena)# show settings
enabled-ntp-unauthenticated
-----
ntp-server: 10.89.147.45
-----
sensor(config-hos-ena)#
```

Step 5 Configure authenticated NTP:

- a. Enter NTP configuration mode.

```
sensor(config-hos)# ntp-option enable
```

- b. Specify the NTP server IP address and key ID. The key ID is a number between 1 and 65535. This is the key ID that you already set up on the NTP server.

```
sensor(config-hos-ena)# ntp-servers ip_address key-id key_ID
```

Example

```
sensor(config-hos-ena)# ntp-servers 10.16.0.0 key-id 100
```

- c. Specify the key value NTP server.

- d. The key value is text (numeric or character). This is the key value that you already set up on the NTP server.

```
sensor(config-hos-ena)# ntp-keys key_ID md5-key key_value
```

Example

```
sensor(config-hos-ena)# ntp-keys 100 md5-key attack
```

- e. Verify the NTP settings.

```
sensor(config-hos-ena)# show settings
enabled
-----
ntp-keys (min: 1, max: 1, current: 1)
-----
key-id: 100
-----
md5-key: attack
-----
ntp-servers (min: 1, max: 1, current: 1)
-----
ip-address: 10.16.0.0
key-id: 100
-----
sensor(config-hos-ena)#
```

Step 6 Exit NTP configuration mode.

```
sensor(config-hos-ena)# exit
sensor(config-hos)# exit
Apply Changes:[yes]
```

Step 7 Press **Enter** to apply the changes or enter **no** to discard them.

Configuring SSH

This section describes SSH on the sensor, and contains the following topics:

- [Understanding SSH, page 4-41](#)
- [Adding Hosts to the SSH Known Hosts List, page 4-41](#)
- [Adding SSH Authorized Public Keys, page 4-43](#)
- [Generating a New SSH Server Key, page 4-44](#)

Understanding SSH

SSH provides strong authentication and secure communications over channels that are not secure. SSH encrypts your connection to the sensor and provides a key so you can validate that you are connecting to the correct sensor. SSH also provides authenticated and encrypted access to other devices that the sensor connects to for blocking.

SSH authenticates the hosts or networks using one or both of the following:

- Password
- User RSA public key



Note SSH never sends passwords in clear text.

SSH protects against the following:

- IP spoofing—A remote host sends out packets pretending to come from another trusted host.



Note SSH even protects against a spoofer on the local network who can pretend he is your router to the outside.

- IP source routing—A host pretends an IP packet comes from another trusted host.
- DNS spoofing—An attacker forges name server records.
- Interception of clear text passwords and other data by intermediate hosts.
- Manipulation of data by those in control of intermediate hosts.
- Attacks based on listening to X authentication data and spoofed connection to the X11 server.

Adding Hosts to the SSH Known Hosts List

You must add hosts to the SSH known hosts list so that the sensor can recognize the hosts that it can communicate with through SSH. These hosts are SSH servers that the sensor needs to connect to for upgrades and file copying, and other hosts, such as Cisco routers, PIX Firewalls, and Catalyst switches that the sensor will connect to for blocking.

Use the **ssh host-key ip-address [key-modulus-length public-exponent public-modulus]** command to add an entry to the known hosts list. If you do not know the values for the modulus, exponent, and length, the system displays the MD5 fingerprint and bubble babble for the requested IP address. You can then select to add the key to the list.

**Caution**

When you use the **ssh host-key ip-address** command, the SSH server at the specified IP address is contacted to obtain the required key over the network. The specified host must be accessible at the moment the command is issued. If the host is unreachable, you must use the full form of the command, **ssh host-key ip-address [key-modulus-length public-exponent public-modulus]**, to confirm the fingerprint of the key displayed to protect yourself from accepting a key of an attacker.

**Note**

To modify a key for an IP address, the entry must be removed and recreated. Use the **no** form of the command to remove the entry.

To add a host to the SSH known hosts list, follow these steps:

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

Step 2 Enter configuration mode.

```
sensor# configure terminal
```

Step 3 Add an entry to the known hosts list.

```
sensor(config)# ssh host-key 10.16.0.0
MD5 fingerprint is F3:10:3E:BA:1E:AB:88:F8:F5:56:D3:A6:63:42:1C:11
Bubble Babble is xucis-hehon-kizog-nedeg-zunom-kolyn-syzec-zasyk-symuf-rykum-sexyx
Would you like to add this to the known hosts table for this host?[yes]
```

The MD5 fingerprint appears. You are prompted to add it to the known hosts list.

If the host is not accessible when the command is issued, this message appears.

```
Error: getHostSshKey : socket connect failed [4,111]
```

Step 4 Enter **yes** to have the fingerprint added to the known hosts list.

Step 5 Verify that the host was added.

```
sensor(config)# exit
sensor# show ssh host-keys
10.89.146.110
```

Step 6 View the key for a specific IP address.

```
sensor# show ssh host-keys 10.16.0.0
1024 35
139306213541835240385332922253968814685684523520064131997839905113640120217816869696708721
704631322844292073851730565044879082670677554157937058485203995572114631296604552161309712
601068614812749969593513740598331393154884988302302182922353335152653860589163651944997842
874583627883277460138506084043415861927
MD5: 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble: xebiz-vykyk-fekuh-rukuk-cabaz-paret-gosym-serum-korus-fypop-huxyx
sensor#
```

Step 7 Remove an entry.

```
sensor(config)# no ssh host-key 10.16.0.0
```

Step 8 Verify the host was removed. The IP address no longer appears in the list.

```
sensor(config)# exit
sensor# show ssh host-keys
```

Adding SSH Authorized Public Keys

Use the **ssh authorized-key** command to define public keys for a client allowed to use RSA authentication to log in to the local SSH server.

The following options apply:

- *id*—1 to 256-character string that uniquely identifies the authorized key. You can use numbers, “_,” and “-,” but spaces and “?” are not acceptable.
- *key-modulus-length*—An ASCII decimal integer in the range [511, 2048].
- *public-exponent*—An ASCII decimal integer in the range [3, 2³²].
- *public-modulus*—An ASCII decimal integer, *x*, such that $(2^{(\text{key-modulus-length}-1)}) < x < (2^{\text{key-modulus-length}})$.

Each user who can log in to the sensor has a list of authorized public keys. An SSH client with access to any of the corresponding RSA private keys can log in to the sensor as the user without entering a password.

Use an RSA key generation tool on the client where the private key is going to reside. Then, display the generated public key as a set of three numbers (modulus length, public exponent, public modulus) and enter those numbers as parameters for the **ssh authorized-key** command.



Note

You configure your own list of SSH authorized keys. An administrator cannot manage the list of SSH authorized keys for other users on the sensor.



Note

An SSH authorized key provides better security than passwords if the private key is adequately safeguarded. The best practice is to create the private key on the same host where it will be used and store it with a pass phrase on a local file system. To minimize password or pass phrase prompts, use a key agent.



Note

To modify an authorized key, you must remove and recreate the entry. Use the **no** form of the command to remove the entry. Users can only create and remove their own keys.

To add a key entry to the SSH authorized keys list for the current user, follow these steps:

Step 1 Log in to the CLI.

Step 2 Add a key to the authorized keys list for the current user.

```
sensor# configure terminal
```

```

sensor(config)# ssh authorized-key system1 1023 37
660222729556609833380897067163729433570828686860008172017802434921804214207813035920829509
101701358480525039993932112503147452768378620911189986653716089813147922086044739911341369
642870682319361928148521864094557416306138786468335115835910404940213136954353396163449793
49705016792583146548622146467421997057
sensor(config)#

```

Step 3 Verify that the key was added.

```

sensor(config)# exit
sensor# show ssh authorized-keys
system1
sensor#

```

Step 4 View the key for a specific ID.

```

sensor# show ssh authorized-keys system1
1023 37 660222729556609833380897067163729433570828686860008172017802434921804214
20781303592082950910170135848052503999393211250314745276837862091118998665371608
98131479220860447399113413696428706823193619281485218640945574163061387864683351
1583591040494021313695435339616344979349705016792583146548622146467421997057
sensor#

```

Step 5 Remove an entry from the list of SSH authorized keys.

```

sensor# configure terminal
sensor(config)# no ssh authorized-key system1

```

Step 6 Verify the entry was removed.

```

sensor(config)# exit
sensor# show ssh authorized-keys

```

The key system1 no longer appears in the list.

If you enter the former ID, you receive an error message.

```

sensor# show ssh authorized-keys system1
Error: Requested id does not exist for the current user.
sensor#

```

Generating a New SSH Server Key

Use the `ssh generate-key` command to change the SSH server host key. The displayed fingerprint matches the one displayed in the remote SSH client in future connections with this sensor if the remote client is using SSH 1.5.

To generate a new SSH server host key, follow these steps:

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

Step 2 Generate the new server host key.

```

sensor# ssh generate-key
MD5: 93:F5:51:58:C7:FD:40:8C:07:26:5E:29:13:C8:33:AE
Bubble Babble: ximal-sudez-kusot-gosym-levag-fegoc-holez-cakar-kunel-nylis-kyxox
sensor#

```

**Caution**

The new key replaces the existing key, which requires you to update the known hosts tables on remote systems with the new host key so that future connections succeed. You can update the known hosts tables on remote systems using the **ssh host-key** command.

Step 3 Display the current SSH server host key.

```
sensor# show ssh server-key
1024 35
137196765426571419509124895787229630062726389801071715581921573847280637533000158590028798
074385824867184332364758899959675370523879609376174812179228415215782949029183962207840731
771645803509837259475421477212459797170806510716077556010753169312675023860474987441651041
217710152766990480431898217878170000647
MD5: 93:F5:51:58:C7:FD:40:8C:07:26:5E:29:13:C8:33:AE
Bubble Babble: ximal-sudez-kusot-gosym-levag-fegoc-holez-cakar-kunel-nylis-kyxox
sensor#
```

For More Information

For the procedure for updating the known hosts table, see [Adding Hosts to the SSH Known Hosts List, page 4-41](#).

Configuring TLS

This section describes TLS on the sensor, and contains the following topics:

- [Understanding TLS, page 4-45](#)
- [Adding TLS Trusted Hosts, page 4-46](#)
- [Displaying and Generating the Server Certificate, page 4-48](#)

Understanding TLS

**Note**

IDM is enabled by default to use TLS and SSL. We highly recommend that you use TLS and SSL.

Cisco IPS contains a Web server that is running IDM. Management stations connect to this Web server. Blocking forwarding sensors also connect to the Web server of the master blocking sensor. To provide security, this Web server uses an encryption protocol known as TLS, which is closely related to SSL protocol. When you enter a URL into the web browser that starts with `https://ip_address`, the web browser responds by using either TLS or SSL protocol to negotiate an encrypted session with the host.

**Caution**

The web browser initially rejects the certificate presented by IDM because it does not trust the CA.

The process of negotiating an encrypted session in TLS is called “handshaking,” because it involves a number of coordinated exchanges between client and server. The server sends its certificate to the client. The client performs the following three-part test on this certificate:

1. Is the issuer identified in the certificate trusted?

Every web browser ships with a list of trusted third-party CAs. If the issuer identified in the certificate is among the list of CAs trusted by your browser, the first test is passed.

2. Is the date within the range of dates during which the certificate is considered valid?

Each certificate contains a Validity field, which is a pair of dates. If the date falls within this range of dates, the second test is passed.

3. Does the common name of the subject identified in the certificate match the URL hostname?

The URL hostname is compared with the subject common name. If they match, the third test is passed.

When you direct your web browser to connect with IDM, the certificate that is returned fails because the sensor issues its own certificate (the sensor is its own CA) and the sensor is not already in the list of CAs trusted by your browser.

When you receive an error message from your browser, you have three options:

- Disconnect from the site immediately.
- Accept the certificate for the remainder of the web browsing session.
- Add the issuer identified in the certificate to the list of trusted CAs of the web browser and trust the certificate until it expires.

The most convenient option is to permanently trust the issuer. However, before you add the issuer, use out-of-band methods to examine the fingerprint of the certificate. This prevents you from being victimized by an attacker posing as a sensor. Confirm that the fingerprint of the certificate appearing in your web browser is the same as the one on your sensor.



Caution

If you change the organization name or hostname of the sensor, a new certificate is generated the next time the sensor is rebooted. The next time your web browser connects to IDM, you will receive the manual override dialog boxes. You must perform the certificate fingerprint validation again for Internet Explorer and Firefox.

Adding TLS Trusted Hosts

In certain situations, the sensor uses TLS/SSL to protect a session it establishes with a remote Web server. For these sessions to be secure from man-in-the-middle attacks you must establish trust of the TLS certificates of the remote Web servers. A copy of the TLS certificate of each trusted remote host is stored in the trusted hosts list.

Use the **tls trusted-host ip-address ip-address [port port]** command to add a trusted host to the trusted hosts list. This command retrieves the TLS certificate from the specified host/port and displays its fingerprint. You can accept or reject the fingerprint based on information retrieved directly from the host you are requesting to add. The default port is 443.

Each certificate is stored with an identifier field (**id**). For the IP address and default port, the identifier field is **ipaddress**. For the IP address and specified port, the identifier field is **ipaddress:port**.

**Caution**

TLS at the specified IP address is contacted to obtain the required fingerprint over the network. The specified host must be accessible at the moment the command is issued. Use an alternate method to confirm the fingerprint to protect yourself from accepting a certificate of an attacker.

To add a trusted host to the trusted hosts list, follow these steps:

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

Step 2 Add the trusted host.

```
sensor# configure terminal
sensor(config)# tls trusted-host ip-address 10.16.0.0
Certificate MD5 fingerprint is 4F:BA:15:67:D3:E6:FB:51:8A:C4:57:93:4D:F2:83:FE
Certificate SHA1 fingerprint is B1:6F:F5:DA:F3:7A:FB:FB:93:E9:2D:39:B9:99:08:D4:
47:02:F6:12
Would you like to add this to the trusted certificate table for this host?[yes]:
```

The MD5 and SHA1 fingerprints appear. You are prompted to add the trusted host.

If the connection cannot be established, the transaction fails.

```
sensor(config)# tls trusted-host ip-address 10.89.146.110 port 8000
Error: getHostCertificate : socket connect failed [4,111]
```

Step 3 Enter **yes** to accept the fingerprint.

```
Certificate ID: 10.89.146.110 successfully added to the TLS trusted host table.
sensor(config)#
```

The host has been added to the TLS trusted host list. The Certificate ID stored for the requested certificate is displayed when the command is successful.

Step 4 Verify that the host was added.

```
sensor(config)# exit
sensor# show tls trusted-hosts
10.89.146.110
sensor#
```

Step 5 View the fingerprint for a specific host.

```
sensor# show tls trusted-hosts 10.89.146.110
MD5: 4F:BA:15:67:D3:E6:FB:51:8A:C4:57:93:4D:F2:83:FE
SHA1: B1:6F:F5:DA:F3:7A:FB:FB:93:E9:2D:39:B9:99:08:D4:47:02:F6:12
sensor#
```

Step 6 Remove an entry from the trusted hosts list.

```
sensor# configure terminal
sensor(config)# no tls trusted-host 10.89.146.110
```

Step 7 Verify the entry was removed from the trusted host list. The IP address no longer appears in the list.

```
sensor(config)# exit
sensor# show tls trusted-hosts
No entries
```

Displaying and Generating the Server Certificate

A TLS certificate is generated when the sensor is first started. Use the **tls generate-key** command to generate a new server self-signed X.509 certificate.

**Note**

The IP address of the sensor is included in the certificate. If you change the sensor IP address, the sensor automatically generates a new certificate.

**Caution**

The new certificate replaces the existing certificate, which requires you to update the trusted hosts lists on remote systems with the new certificate so that future connections succeed. You can update the trusted hosts lists on remote IPS sensors using the **tls trusted-host** command. If the sensor is a master blocking sensor, you must update the trusted hosts lists on the remote sensors that are sending block requests to the master blocking sensor.

To generate a new TLS certificate, follow these steps:

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

Step 2 Generate the new certificate.

```
sensor# tls generate-key
MD5 fingerprint is FD:83:6E:41:D3:88:48:1F:44:7F:AF:5D:52:60:89:DE
SHA1 fingerprint is 4A:2B:79:A0:82:8B:65:3A:83:B5:D9:50:C0:8E:F6:C6:B0:30:47:BB
sensor#
```

Step 3 Verify that the key was generated.

```
sensor# show tls fingerprint
MD5: FD:83:6E:41:D3:88:48:1F:44:7F:AF:5D:52:60:89:DE
SHA1: 4A:2B:79:A0:82:8B:65:3A:83:B5:D9:50:C0:8E:F6:C6:B0:30:47:BB
sensor#
```

For More Information

For the procedure for updating the trusted hosts lists on remote sensors, see [Adding TLS Trusted Hosts](#), page 4-46.

Installing the License Key

This section describes the IPS license key and how to install and uninstall it. It contains the following topics:

- [Understanding the License Key](#), page 4-49
- [Service Programs for IPS Products](#), page 4-49
- [Obtaining and Installing the License Key](#), page 4-50
- [Uninstalling the License Key](#), page 4-52

Understanding the License Key

Although the sensor functions without the license key, you must have a license key to obtain signature updates and use the global correlation features. To obtain a license key, you must have the following:

- Cisco Service for IPS service contract

Contact your reseller, Cisco service or product sales to purchase a contract.

- Your IPS device serial number

To find the IPS device serial number in IDM or IME, for IDM choose **Configuration > Sensor Management > Licensing**, and for IME choose **Configuration > sensor_name > Sensor Management > Licensing**, or in the CLI use the **show version** command.

- Valid Cisco.com username and password

Trial license keys are also available. If you cannot get your sensor licensed because of problems with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the license key from a license key provided in a local file. Go to <http://www.cisco.com/go/license> and click **IPS Signature Subscription Service** to apply for a license key.

You can view the status of the license key in these places:

- IDM Home window Licensing section on the Health tab
- IDM Licensing pane (**Configuration > Licensing**)
- IME Home page in the Device Details section on the Licensing tab
- License Notice at CLI login

Whenever you start IDM, IME, or the CLI, you are informed of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use IDM, IME, and the CLI, but you cannot download signature updates.

If you already have a valid license on the sensor, you can click **Download** on the License pane to download a copy of your license key to the computer that IDM or IME is running on and save it to a local file. You can then replace a lost or corrupted license, or reinstall your license after you have reimaged the sensor.

Service Programs for IPS Products

You must have a Cisco Services for IPS service contract for any IPS product so that you can download a license key and obtain the latest IPS signature updates. If you have a direct relationship with Cisco Systems, contact your account manager or service account manager to purchase the Cisco Services for IPS service contract. If you do not have a direct relationship with Cisco Systems, you can purchase the service account from a one-tier or two-tier partner.

When you purchase the following IPS products you must also purchase a Cisco Services for IPS service contract:

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20

- AIM IPS
- IDSM2
- NME IPS

When you purchase an ASA 5500 series adaptive security appliance product that does not contain IPS, you must purchase a SMARTnet contract.

**Note**

SMARTnet provides operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

When you purchase an ASA 5500 series adaptive security appliance product that ships with AIP SSM installed, or if you purchase an AIP SSM to add to your ASA 5500 series adaptive security appliance product, you must purchase the Cisco Services for IPS service contract.

**Note**

Cisco Services for IPS provides IPS signature updates, operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

For example, if you purchase an ASA 5510 and then later want to add IPS and purchase an ASA-SSM-AIP-10-K9, you must now purchase the Cisco Services for IPS service contract.

After you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key.

**Caution**

If you ever send your product for RMA, the serial number changes. You must then get a new license key for the new serial number.

Obtaining and Installing the License Key

**Note**

You cannot install an older license key over a newer license key.

Use the **copy source-url license_file_name license-key** command to copy the license key to your sensor.

The following options apply:

- *source-url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination-url*—The location of the destination file to be copied. It can be a URL or a keyword.
- **license-key**—The subscription license file.
- *license_file_name*—The name of the license file you receive.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- **ftp:**—Source or destination URL for an FTP network server. The syntax for this prefix is:
 ftp://[username@] location]/relativeDirectory]/filename
 ftp://[username@]location]//absoluteDirectory]/filename

- **scp:**—Source or destination URL for the SCP network server. The syntax for this prefix is:
 scp:[/[username@] location]/relativeDirectory]/filename
 scp:[/[username@] location]//absoluteDirectory]/filename



Note If you use FTP or SCP protocol, you are prompted for a password. If you use SCP protocol, you must add the remote host to the SSH known hosts list.

- **http:**—Source URL for the Web server. The syntax for this prefix is:
 http:[/[username@]location]/directory]/filename
- **https:**—Source URL for the Web server. The syntax for this prefix is:
 https:[/[username@]location]/directory]/filename



Note If you use HTTPS protocol, the remote host must be a TLS trusted host.

To install the license key, follow these steps:

Step 1 Apply for the license key at this URL: www.cisco.com/go/license.



Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

Step 2 Fill in the required fields. Your Cisco IPS Signature Subscription Service license key will be sent by e-mail to the e-mail address you specified.



Note You must have the correct IPS device serial number because the license key only functions on the device with that number.

Step 3 Save the license key to a system that has a Web server, FTP server, or SCP server.

Step 4 Log in to the CLI using an account with administrator privileges.

Step 5 Copy the license key to the sensor.

```
sensor# copy scp://user@10.10.110.3://tftpboot/dev.lic license-key
Password: *****
```

Step 6 Verify the sensor is licensed.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(7)E4

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S615.0                2012-01-03
OS Version:          2.4.30-IDS-smp-bigphys
Platform:            IPS-4260-K9
Serial Number:       P300000220
Sensor up-time is 3 days.
```

```
Using 1031888896 out of 2093682688 bytes of available memory (49% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 52.4M out of 166.6M bytes of available disk space (33% usage)
boot is using 37.8M out of 68.5M bytes of available disk space (58% usage)
```

```
MainApp          N-2007_JUN_19_16_45  (Release)  2007-06-19T17:10:20-0500  Running
AnalysisEngine  N-2007_JUN_19_16_45  (Release)  2007-06-19T17:10:20-0500  Running
CLI             N-2007_JUN_19_16_45  (Release)  2007-06-19T17:10:20-0500
```

Upgrade History:

```
IPS-K9-7.0-74-E4 15:36:05 UTC Thu Apr 24 2008
```

Recovery Partition Version 1.1 - 7.0(4)E4

Host Certificate Valid from: 22-Apr-2008 to 26-Apr-2010

sensor#

Step 7 Copy your license key from a sensor to a server to keep a backup copy of the license.

```
sensor# copy license-key scp://user@10.10.10.3://tftpboot/dev.lic
Password: *****
sensor#
```

Uninstalling the License Key

Use the **erase license-key** command to uninstall the license key on your sensor. This allows you to delete an installed license key from a sensor without restarting the sensor or logging into the sensor using the service account.

To uninstall the license key, follow these steps:

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

Step 2 Uninstall the license key on the sensor.

```
sensor# erase license-key
Warning: Executing this command will remove the license key installed on the sensor.
```

You must have a valid license key installed on the sensor to apply the Signature Updates and use the Global Correlation features.

```
Continue? []: yes
sensor#
```

Step 3 Verify the sensor key has been uninstalled.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(7)E4

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S615.0          2012-01-03
```

```
OS Version:          2.4.30-IDS-smp-bigphys
Platform:           IPS-4260-K9
Serial Number:      AZBW6460105
No license present
Sensor up-time is 5 days.
Using 1889390592 out of 4100345856 bytes of available memory (46% usage)
system is using 18.2M out of 38.5M bytes of available disk space (47% usage)
application-data is using 48.0M out of 166.8M bytes of available disk space (30% usage)
boot is using 46.1M out of 69.5M bytes of available disk space (70% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)
```

```
MainApp             B-2012_JAN_20_00_30_7_0_7 (Ipsbuild)  2012-01-20T00:32:
41-0600 Running
AnalysisEngine     B-2012_JAN_20_00_30_7_0_7 (Ipsbuild)  2012-01-20T00:32:
41-0600 Running
CollaborationApp  B-2012_JAN_20_00_30_7_0_7 (Ipsbuild)  2012-01-20T00:32:
41-0600 Running
CLI                B-2012_JAN_20_00_30_7_0_7 (Ipsbuild)  2012-01-20T00:32:
41-0600
```

Upgrade History:

```
IPS-K9-7.0-7-E4  00:44:07 UTC Fri Jan 20 2012
```

Recovery Partition Version 1.1 - 7.0(7)E4

Host Certificate Valid from: 22-Jan-2012 to 22-Jan-2014

sensor#
