



CHAPTER 4

Initial Configuration Tasks

This chapter contains procedures for the initial configuration tasks, such as changing sensor setup information, adding and deleting users, configuring time and setting up NTP, creating a service account, configuring SSH and TLS, and installing the license key.

This chapter contains the following sections:

- [Changing Network Settings, page 4-1](#)
- [Changing Web Server Settings, page 4-9](#)
- [Configuring User Parameters, page 4-11](#)
- [Configuring Time, page 4-18](#)
- [Configuring SSH, page 4-30](#)
- [Configuring TLS, page 4-34](#)
- [Installing the License Key, page 4-37](#)

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 configure the 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](#)

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 type **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 sensor's IP address or the sensor will generate an error and 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 type **no** to discard them.

Enabling and Disabling Telnet

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.



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.

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
```

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 type **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 the procedure, 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, that need to access your sensor from a web browser.
- Management stations, such as VMS, 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 type **no** to discard them.

Changing the FTP Timeout

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.



Note

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

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 type **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 type **no** to discard them.

Changing Web Server Settings

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.



Note

The default web server port is 443 if TLS is enabled and 80 if TLS is disabled.

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 the following 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 the following 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>
sensor(config-web)#
```

Step 9 Exit web server submenu:

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

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

**Note**

If you changed the port or enable TLS settings, you must reset the sensor to make the web server use the new settings.

Configuring User Parameters

The following section explains how to create the service account, create users, change passwords, specify privilege level, and view a list of users. It contains the following topics:

- [Adding and Removing Users, page 4-11](#)
- [Password Recovery, page 4-13](#)
- [Creating the Service Account, page 4-13](#)
- [Configuring Passwords, page 4-14](#)
- [Changing User Privilege Levels, page 4-15](#)
- [Viewing User Status, page 4-16](#)
- [Configuring Account Locking, page 4-17](#)

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.

A valid password is 6 to 32 characters long. All characters except space and '?' are allowed.

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

- `Error: setEnableAuthenticationTokenStatus : Failure setting the account's password: it's WAY 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. For the procedure, see [Creating the Service Account, page 4-13](#).

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 A valid username contains 1 to 64 alphanumeric characters. You can also use an underscore (_) or dash (-) in the username. A valid password is 6 to 32 characters long. All characters except space and '?' are allowed.

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



Note If you do not want to see the password in clear text, wait for the password prompt. Do not type 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
```

Step 6 Verify that the user has been removed:

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

The user `jsmith` has been removed.



Note

You cannot use this command to remove yourself from the system

Password Recovery

The following password recovery options exist:

- If another Administrator account exists, the other Administrator can change the password.
- If a Service account exists, you can log in to the service account and switch to user root using the command `su - root`. Use the `password` command to change the CLI Administrator account's password. For example, if the Administrator password is "adminu," the command is `password adminu`. You are prompted to enter the new password twice. For more information, see [Creating the Service Account, page 4-13](#).

You can reimage the sensor using either the recovery partition or a system image file. For more information, see [Chapter 17, "Upgrading, Downgrading, and Installing System Images."](#)

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

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 new password if the Administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.



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's password is synchronized to the service account's 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.

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:

```
sensor(config)# user username privilege service
```

A valid username contains 1 to 64 alphanumeric characters. You can also use an underscore (_) or dash (-) in the username.

Step 4 Specify a password when prompted.

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 allowed in UserAccount document
```

Step 5 Exit configuration mode:

```
sensor(config)# exit  
sensor#
```

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

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

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 6 to 32 characters long. All characters except space and '?' 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

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



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. For the procedure, see [Creating the Service Account, page 4-13](#).

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 user's privilege has been changed:

```

sensor(config)# exit
sensor# show users all

      CLI ID  User      Privilege
*   13491    cisco    administrator
      5824    jsmith   operator
      9802    operator operator
      5824    service  service
      9802    viewer   viewer

sensor#

```

The privilege of the user `jsmith` has been changed from `viewer` to `operator`.

Step 5 Display your current level of privilege:

```

sensor# show privilege
Current privilege level is administrator

```

Viewing User Status

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.



Note The number of concurrent CLI sessions is limited based on platform. IDS-4210, IDS-4215, and NM-CIDS are limited to 3 concurrent sessions. All other platforms allow 10 sessions.

To view 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 jsmith's account, reset the password:

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

Configuring Account Locking

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 mode:

```
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 `jsmith`'s account, reset the password:

```

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

```

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 4-18](#)
- [Correcting Time on the Sensor, page 4-20](#)
- [Configuring Time on the Sensor, page 4-21](#)
- [Configuring NTP, page 4-27](#)

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. For more information, see [Initializing the Sensor, page 3-2](#).

Here is a summary of ways to set the time on sensors:

- For appliances
 - Use the **clock set** command to set the time. This is the default.
For the procedure, see [Manually Setting the System Clock, page 4-22](#).

- Use NTP

You can configure the appliance to get its time from an NTP time synchronization source. See [Configuring a Cisco Router to be an NTP Server, page 4-27](#). You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can set up NTP on the appliance during initialization or you can configure NTP through the CLI, IDM, or ASDM.



Note We recommend that you use an NTP time synchronization source.

- For IDSM-2
 - The IDSM-2 can automatically synchronize its clock with the switch time. This is the default.



Note The UTC time is synchronized between the switch and the IDSM-2. The time zone and summertime settings are not synchronized between the switch and the IDSM-2.

**Caution**

Be sure to set the time zone and summertime settings on both the switch and IDSM-2 to ensure that the UTC time settings are correct. IDSM-2's local time could be incorrect if the time zone and/or summertime settings do not match between IDSM-2 and the switch.

- Use NTP

You can configure IDSM-2 to get its time from an NTP time synchronization source. See [Configuring a Cisco Router to be an NTP Server, page 4-27](#). You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure IDSM-2 to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.



Note We recommend that you use an NTP time synchronization source.

- For NM-CIDS
 - NM-CIDS can automatically synchronize its clock with the clock in the router chassis in which it is installed (parent router). This is the default.



Note The UTC time is synchronized between the parent router and NM-CIDS. The time zone and summertime settings are not synchronized between the parent router and NM-CIDS.

**Caution**

Be sure to set the time zone and summertime settings on both the parent router and NM-CIDS to ensure that the UTC time settings are correct. NM-CIDS's local time could be incorrect if the time zone and/or summertime settings do not match between NM-CIDS and the router.

- Use NTP

You can configure NM-CIDS to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. See [Configuring a Cisco Router to be an NTP Server, page 4-27](#). You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure NM-CIDS to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.



Note We recommend that you use an NTP time synchronization source.

- For AIP-SSM:
 - AIP-SSM can automatically synchronize its clock with the clock in the ASA in which it is installed. This is the default.



Note The UTC time is synchronized between ASA and AIP-SSM. The time zone and summertime settings are not synchronized between ASA and AIP-SSM.



Caution

Be sure to set the time zone and summertime settings on both ASA and AIP-SSM to ensure that the UTC time settings are correct. AIP-SSM's local time could be incorrect if the time zone and/or summertime settings do not match between AIP-SSM and ASA.

- Use NTP

You can configure AIP-SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. See [Configuring a Cisco Router to be an NTP Server, page 4-27](#). You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure AIP-SSM to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.



Note We recommend that you use an NTP time synchronization source.

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. For more information on the **clear events** command, see [Clearing Events from the Event Store, page 13-7](#).



Caution

You cannot remove individual events.

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:

- [System Clock, page 4-21](#)
- [Configuring Summertime Settings, page 4-22](#)
- [Configuring Timezones Settings, page 4-27](#)

System Clock

This section describes how to display and manually set the system clock and, contains the following topics:

- [Displaying the System Clock, page 4-21](#)
- [Manually Setting the System Clock, page 4-22](#)

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.

| 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:

```
sensor# show clock
22:39:21 UTC Sat Jan 25 2003
```

Step 3 Display the system clock with details:

```
sensor# show clock detail
22:39:21 CST Sat Jan 25 2003
Time source is NTP
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

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

```
sensor# show clock detail
*12:19:22 CST Sat Dec 04 2004
No time source
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

This indicates that no time source is configured.

Manually Setting the System Clock

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.



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.

For the procedure for configuring NTP, see [Configuring NTP, page 4-27](#). See [Time Sources and the Sensor, page 4-18](#), for an explanation of the importance of having a valid time source for the sensor. For an explanation of what to do if you set the clock incorrectly, see [Correcting Time on the Sensor, page 4-20](#).

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

- IDSM-2
- NM-CIDS
- AIP-SSM-10
- AIP-SSM-20

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 July 29 2004
```



Note

The time format is 24-hour time.

Configuring Summertime Settings

You can configure summertime settings if you did not do so during initialization of the sensor. Or you can change them after initialization.



Note

Summertime is a term for daylight saving time.

This section contains the following topics:

- [Configuring Recurring Summertime Settings, page 4-23](#)
- [Configuring Non-recurring Summertime Settings, page 4-25](#)

Configuring Recurring Summertime Settings

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:

d. Type the day of the week you want to start summertime settings:

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

e. Type the month you want to start summertime settings:

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

f. Type the time of day you want to start summertime settings:

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

The format is hh:mm:ss.

g. Type the week of the month you want to start summertime settings:

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

The values are first through fifth, or last.

h. 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. Type the day of the week you want to end summertime settings:

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

- b. Type the month you want to end summertime settings:

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

- c. Type the time of day you want to end summertime settings:

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

The format is hh:mm:ss.

- d. Type 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
```

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 type **no** to discard them.

Configuring Non-recurring Summertime Settings

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. Type the date you want to start summertime settings:

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

The format is yyyy-mm-dd.

- b. Type the time you want to start summertime settings:

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

The format is hh:mm:ss.

- 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. Type the date you want to end summertime settings:

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

The format is yyyy-mm-dd.

b. Type the time you want to end summertime settings:

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

The format is hh:mm:ss.

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
```

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 type **no** to discard them.

Configuring Timezones Settings

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

To configure the timezone settings on the sensor, follow these steps:

-
- Step 1** Log in to the sensor using an account with administrator privileges.
- Step 2** Enter timezone settings submode:
- ```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# time-zone-settings
```
- Step 3** Configure the timezone 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
```
- 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 timezone settings submode:
- ```
sensor(config-hos-tim)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:
```
- Step 7** Press **Enter** to apply the changes or type **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 4-27](#)
- [Configuring the Sensor to Use an NTP Time Source, page 4-29](#)

### Configuring a Cisco Router to be an NTP Server

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.

**Note**

Remember the NTP server's key ID and key values. You will need them along with the NTP server's IP address when you configure the sensor to use the NTP server as its time source. For the procedure, see [Configuring the Sensor to Use an NTP Time Source, page 4-29](#).

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:

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

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):

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

The trusted key ID is the same number as the key ID in Step 3.

Example:

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

**Step 5** Specify the interface on the router that the sensor will communicate with:

```
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:

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

Example:

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

The NTP master stratum number identifies the server's relative position in the NTP hierarchy. You can choose a number between 1 and 15. It is not important to the sensor which number you choose.

## Configuring the Sensor to Use an NTP Time Source

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.



### Note

You must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server. For more information, see [Configuring a Cisco Router to be an NTP Server, page 4-27](#).

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** Enter NTP configuration mode:

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

**Step 5** Type the NTP server IP address and key ID:

```
sensor(config-hos-ena)# ntp-servers ip_address key-id 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. See Step 3 of [Configuring a Cisco Router to be an NTP Server, page 4-27](#).

Example:

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

**Step 6** Type the NTP server's key value:

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

The key value is text (numeric or character). This is the key value that you already set up on the NTP server. See Step 3 of [Configuring a Cisco Router to be an NTP Server, page 4-27](#).

Example:

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

**Step 7** 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 8** Exit NTP configuration mode:

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

**Step 9** Press **Enter** to apply the changes or type **no** to discard them.

---

## Configuring SSH

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

- [About SSH, page 4-30](#)
- [Adding Hosts to the Known Hosts List, page 4-31](#)
- [Adding SSH Authorized Public Keys, page 4-32](#)
- [Generating a New SSH Server Key, page 4-34](#)

## About 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 more of the following:

- Password
- User RSA public key

SSH protects against the following:

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

SSH never sends passwords in clear text.

## Adding Hosts to the 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 an attacker's key.



### 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, the following message appears:

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

**Step 4** Type **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
60106861481274996959351374059833139315488498830230218292235335152653860589163651944997842
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
```

The host is removed from the SSH known hosts list.

**Step 8** Verify the host was removed:

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

The IP address no longer appears in the list.

## 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, 2<sup>32</sup>].
- *public-modulus*—An ASCII decimal integer, *x*, such that (2<sup>(key-modulus-length-1)</sup>) < *x* < (2<sup>(key-modulus-length)</sup>).

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 passphrase on a local file system. To minimize password or passphrase 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
```

The key is removed from the SSH authorized keys list.

**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 type 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. For the procedure, see [Adding Hosts to the Known Hosts List, page 4-31](#).

**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#
```

---

## Configuring TLS

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

- [About TLS, page 4-34](#)
- [Adding TLS Trusted Hosts, page 4-35](#)
- [Displaying and Generating the Server Certificate, page 4-37](#)

## About TLS

IPS 5.0 contains a web server that is running the IDM and ASDM and that the management stations, such as VMS, connect to. 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 and ASDM because it does not trust the CA.

---

**Note**

---

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

---

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 or ASDM, 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 or ASDM, you will receive the manual override dialog boxes. You must perform the certificate fingerprint validation again for Internet Explorer, Netscape, and Mozilla.

---

## Adding TLS Trusted Hosts

In certain situations, the sensor uses TLS and 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 remote web servers' TLS certificates. 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 [port port]** command to add a trusted host to the trusted hosts list. This command retrieves the TLS certificate from the specified host and 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 an attacker's certificate

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** Type **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
```

The host is removed from the trusted hosts list.

**Step 7** Verify the entry was removed from the trusted host list:

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

The IP address no longer appears in the list:

---

## 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 sensor's IP address is included in the certificate. If you change the sensor's 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. For the procedure, see [Adding TLS Trusted Hosts, page 4-35](#). 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
```

**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#
```

---

## Installing the License Key

Although the sensor functions without the license, you must have a license to obtain signature updates. To obtain a license, you must have a Cisco Service for IPS contract. Contact your reseller, Cisco service or product sales to purchase a contract.

**Note**

You can install the first few signature updates for 5.0 without a license. This gives you time to get your sensor licensed. If you are unable to get your sensor licensed because of confusion with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

You can view the status of the IPS subscription license key on the Licensing panel in IDM or ASDM. You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the sensor license key from a license key provided in a local file.

You must know your IPS device serial number to obtain a license key. You can find the IPS device serial number in IDM by clicking Configuration > Licensing, in the ASDM by clicking Configuration > Features > IPS > Licensing, or through the CLI by using the **show version** command.

Whenever you start IDM or ASDM, a dialog box informs you 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 and ASDM, but you cannot download signature updates.

When you enter the CLI, you receive the following message if there is no license installed:

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

You will continue to see this message until you have installed a license. Go to <http://www.cisco.com/go/license> and click IPS Signature Subscription Service to apply for a license.

Use the **copy source-url license\_file\_name license-key** command to copy the license file 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.

**Note**

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

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
- **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 FTP or SCP, you are prompted for a password.



**Note** If you use SCP, the remote host must be on the SSH known hosts list. For the procedure, see [Adding Hosts to the Known Hosts List, page 4-31](#).



**Note** If you use HTTPS, the remote host must be a TLS trusted host. For the procedure, see [Adding TLS Trusted Hosts, page 4-35](#).

To install the license key, follow these steps:

**Step 1** Apply for the license key at this URL: [www.cisco.com/go/license](http://www.cisco.com/go/license)

**Step 2** Fill in the required fields.



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

Your Cisco IPS Signature Subscription Service license key will be sent by e-mail to the e-mail address you specified.

**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@10.89.147.3://tftpboot/dev.lic license-key
Password: *****
```

**Step 6** Verify the sensor is licensed:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R0JS
Licensed, expires: 19-Dec-2005 UTC
Sensor up-time is 2 days.
Using 706699264 out of 3974291456 bytes of available memory (17% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.5M out of 166.8M bytes of available disk space (23% usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)

MainApp 2005_Feb_18_03.00 (Release) 2005-02-18T03:13:47-0600 Running
AnalysisEngine 2005_Feb_15_03.00 (QATest) 2005-02-15T12:59:35-0600 Running
CLI 2005_Feb_18_03.00 (Release) 2005-02-18T03:13:47-0600
```

Upgrade History:

IDS-K9-maj-5.0-1- 14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149

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@10.89.147.3://tftpboot/dev.lic
Password: *****
sensor#
```

---