CHAPTER 4

Setting Up the Sensor

This chapter provides information for setting up the sensor. It contains the following sections:

Understanding Sensor Setup

Caution You must initialize the sensor before you can choose **Configuration > Sensor Setup** in IDM to further configure the sensor.

After you install the sensor on your network, you must use the **setup** command to initialize it so that you can communicate with it over the network. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, access control lists, and time settings. You can continue using Advanced Setup in the CLI to enable Telnet, configure the Web server, and assign and enable virtual sensors and interfaces, or you can use the Startup Wizard in IDM. After you initialize the sensor, you can make any changes and configure other network parameters in Sensor Setup.

For More Information

For the procedure for running the **setup** command, see Chapter 17, "Initializing the Sensor."

Configuring Network Settings

This section describes how to change the network settings, and contains the following topics:

Network Pane

Note You must be administrator to configure network settings.

After you use the **setup** command to initialize the sensor, the network and communication parameter values appear in the Network pane. If you need to change these parameters, you can do so in the Network pane.

Network Pane Field Definitions

The following fields are found in the Network pane:

- Hostname—Name of the sensor. The hostname can be a string of 1 to 64 characters that matches the pattern ^[A-Za-z0-9_/-]+$. The default is sensor. You receive an error message if the name contains a space or exceeds 64 alphanumeric characters.
- IP Address—IP address of the sensor. The default is 192.168.1.2.
- Network Mask—Mask corresponding to the IP address. The default is 255.255.255.0.
- Default Route—Default gateway address. The default is 192.168.1.1.
- FTP Timeout (seconds)—Sets the amount of time in seconds that the FTP client waits before timing out when the sensor is communicating with an FTP server. The valid range is 1 to 86400 seconds. The default is 300 seconds.
- Allow Password Recovery—Enables password recovery. The default is enabled.
- Web Server Settings—Sets the web server security level and port.
  - Enable TLS/SSL—Enables TLS and SSL in the web server. The default is enabled.

    Note We strongly recommend that you enable TLS and SSL.

  - Web server port—TCP port used by the web server. The default is 443 for HTTPS.

    Note You receive an error message if you enter a value out of the range of 1 to 65535.

  - Enable RDEP Event Server Subscriptions—Enable if you are using a third-party event client that is only able to parse IDS 4.*x* alerts.

    Note The RDEP event interface was deprecated in Cisco IPS 5.0 and replaced by SDEE/CIDEE.

- Remote Access—Enables the sensor for remote access.
  - Enable Telnet—Enables or disables Telnet for remote access to the sensor.

    Note Telnet is not a secure access service and therefore is disabled by default.

Configuring Network Settings

To configure network settings, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Network**.

Step 3 To edit the sensor hostname, enter the new name in the Hostname field.

Step 4 To change the sensor IP address, enter the new address in the IP Address field.

Step 5 To change the network mask, enter the new mask in the Network Mask field.

Step 6 To change the default gateway, enter the new address in the Default Route field.

Step 7 To change the amount of FTP timeout, enter the new amount in the FTP Timeout field.

Step 8 To allow password recovery, check the **Allow Password Recovery** check box.

Note We strongly recommend that you enable password recover. Otherwise, you must reimage your sensor to gain access if you have a password problem.

Step 9 To enable or disable TLS/SSL, check the **Enable TLS/SSL** check box.

Note We strongly recommend that you enable TLS/SSL.

Note TLS and SSL are protocols that enable encrypted communications between a web browser and a web server. When TLS/SSL is enabled, you connect to IDM using `https://sensor_ip_address`. If you disable TLS/SSL, connect to IDM using `http://sensor_ip_address:port_number`.

Step 10 To change the web server port, enter the new port number in the Web server port field.

Note If you change the web server port, you must specify the port in the URL address of your browser when you connect to IDM Use the following format: `https://sensor_ip_address:port_number` (for example, `https://10.1.9.201:1040`).

Step 11 To enable or disable RDEP Event Server Subscriptions, check the **Enable RDEP Event Server Subscriptions** check box.

Note If you are using a third-party event client that can only parse IDS 4.*x* alerts, you need to enable RDEP Event Server Subscriptions.

Step 12 To enable or disable remote access, check the **Enable Telnet** check box.

Note 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.

Tip To undo your changes, click **Reset**.

Step 13 Click **Apply** to apply your changes and save the revised configuration.

Note Changing the network settings may disrupt your connection to the sensor and force you to reconnect with the new address.

Configuring Allowed Hosts/Networks

This section describes how to add allowed hosts and networks to the system, and contains the following topics:

Allowed Hosts/Networks Pane

Note You must be administrator to configure allowed hosts and networks.

Use the Allowed Hosts/Networks pane to specify hosts or networks that have permission to access the sensor.

After you use the **setup** command to initialize the sensor, the allowed hosts parameter values appear in the Allowed Hosts/Networks pane. By default, there are no entries in the list, and therefore no hosts are permitted until you add them. If you need to change these parameters, you can do so in the Allowed Hosts/Networks pane.

Note You must add the management host, such as ASDM, IDM, IME, Cisco Security Manager and the monitoring host, such as Cisco Security Mars, to the allowed hosts list, otherwise they cannot communicate with the sensor.

Caution When adding, editing, or deleting allowed hosts, make sure that you do not delete the IP address used for remote management of the sensor.

Allowed Hosts/Network Pane and Add and Edit Allowed Host Dialog Boxes Field Definitions

The following fields are found in the Allowed Hosts/Networks pane and Add and Edit Allowed Host dialog boxes:

- IP Address—IP address of the host allowed to access the sensor.
- Network Mask—Mask corresponding to the IP address of the host.

Configuring Allowed Hosts/Networks

To specify hosts and networks that have permission to access your sensor, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Allowed Hosts/Networks**, and then click **Add** to add a host or network to the list. You can add a maximum of 512 allowed hosts.

Step 3 In the IP Address field, enter the IP address of the host or network. You receive an error message if the IP address is already included as part of an existing list entry.

Step 4 In the Network Mask field, enter the network mask of the host or network, or choose a network mask from the drop-down list. IDM requires that a netmask always be provided, whether the IP address is a host or a network. If you do not specify a netmask, you receive the following error: `Network Mask is not valid`.

You also receive an error message if the network mask does not match the IP address.

Tip To discard your changes and close the Add Allowed Host dialog box, click **Cancel**.

Step 5 Click **OK**. The new host or network appears in the list in the Allowed Hosts/Networks pane.

Step 6 To edit an existing entry in the list, select it, and click **Edit**.

Step 7 In the IP Address field, edit the IP address of the host or network.

Step 8 In the Network Mask field, edit the network mask of the host or network.

Tip To discard your changes and close the Edit Allowed Host dialog box, click **Cancel**.

Step 9 Click **OK**. The edited host or network appears in the list in the Allowed Hosts/Networks pane.

Step 10 To delete a host or network from the list, select it, and click **Delete**. The host no longer appears in the list in the Allowed Hosts/Networks pane.

Caution All future network connections from the host that you deleted will be denied.

Tip To discard your changes, click **Reset**.

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring Time

This section describes time sources and the sensor, and contains the following topics:

Time Pane

Note You must be administrator to configure time settings.

Use the Time pane to configure the sensor local date, time, time zone, summertime (DST), and whether the sensor will use an NTP server for its time source.

Note We recommend that you use an NTP server as the sensor time source.

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.

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.

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.
  - Use NTP—You can configure the appliance to get its time from an NTP time synchronization source.
- For the 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.

  - Use NTP—You can configure the IDSM2 to get its time from an NTP time synchronization source.
- For the AIM IPS and the NME IPS
  - The AIM IPS and the 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 the AIM IPS and the NME IPS. The time zone and summertime settings are not synchronized between the parent router and the AIM IPS and the NME IPS.

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

  - Use NTP—You can configure the AIM IPS and the NME IPS to get their time from an NTP time synchronization source, such as a Cisco router, other than the parent router.
- For the AIP SSM and AIP SSC-5
  - The AIP SSM and AIP SSC-5 can automatically synchronize their clocks with the clock in the adaptive security appliance in which they are installed. This is the default. The UTC time is synchronized between the adaptive security appliance and the AIP SSM and AIP SSC-5. The time zone and summertime settings are not synchronized between the adaptive security appliance and the AIP SSM and AIP SSC-5.

    Note Be sure to set the time zone and summertime settings on both the adaptive security appliance and the AIP SSM and AIP SSC-5 to ensure that the UTC time settings are correct. The local time of the AIP SSM and AIP SSC-5 could be incorrect if the time zone and/or summertime settings do not match between the AIP SSM and AIP SSC-5 and the adaptive security appliance.

– Use NTP—You can configure the AIP SSM and AIP SSC-5 to get their time from an NTP time synchronization source, such as a Cisco router other than the parent router.

Synchronizing IPS Module System Clocks with Parent Device System Clocks

All IPS modules (AIM IPS, AIP SSM, AIP SSC-5, 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.

Verifying the Sensor is Synchronized with the NTP Server

In Cisco IPS, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the **show statistics host** command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.

To verify the NTP configuration, follow these steps:

Step 1 Log in to the sensor.

Step 2 Generate the host statistics:

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
          2 10373  9014   yes   yes  none    reject   reachable  1
        status = Not Synchronized
     ...
```

Step 3 Generate the hosts statistics again after a few minutes:

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
        *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
         LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f624   yes   yes   ok   sys.peer   reachable  2
          2 10373  9024   yes   yes  none    reject   reachable  2
        status = Synchronized
```

Step 4 If the status continues to read `Not Synchronized`, check with the NTP server administrator to make sure the NTP server is configured correctly.

Time Pane Field Definitions

The following fields are found in the Time pane:

- Sensor Local Date—Current date on the sensor. The default is January 1, 1970. You receive an error message if the day value is out of range for the month.
- Sensor Local Time—Current time (hh:mm:ss) on the sensor. The default is 00:00:00. You receive an error message if the hours, minutes, or seconds are out of range.

  Note The date and time fields are disabled if the sensor does not support these fields, or if you have configured NTP settings on the sensor.

- Standard Time Zone—Lets you set the zone name and UTC offset.
  - Zone Name—Local time zone when summertime is not in effect. The default is UTC. You can choose from a predefined set of 37 time zones, or you can create a unique name (24 characters) in the following pattern: ^[A-Za-z0-9()+:,_/-]+$
  - UTC Offset—Local time zone offset in minutes. The default is 0. If you select a predefined time zone this field is populated automatically.

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

- NTP Server—Lets you configure the sensor to use an NTP server as its time source.
  - IP Address—IP address of the NTP server if you use this to set time on the sensor.
  - Authenticated NTP—Lets you use authenticated NTP, which requires a key and key ID.
  - Key—NTP MD5 key type.
  - Key ID—ID of the key (1 to 65535) used to authenticate on the NTP server. You receive an error message if the key ID is out of range.
  - Unauthenticated NTP—Lets you use NTP, but does not require authentication, therefore, no key or key ID.
- Summertime—Lets you enable and configure summertime settings.
  - Enable Summertime—Click to enable summertime mode. The default is disabled.

Configure Summertime Dialog Box Field Definitions

The following fields are found in the Configure Summertime dialog box:

- Summer Zone Name—Summertime zone name. The default is UTC. You can choose from a predefined set of 37 time zones, or you can create a unique name (24 characters) in the following pattern: ^[A-Za-z0-9()+:,_/-]+$
- Offset—The number of minutes to add during summertime. The default is 60. If you choose a predefined time zone, this field is populated automatically.
- Start Time—Summertime start time setting. The value is hh:mm. You receive an error message if the hours or minutes are out of range.
- End Time—Summertime end time setting. The value is hh:mm. You receive an error message if the hours or minutes are out of range.

- Summertime Duration—Lets you set whether the duration is recurring or a single date.
  - Recurring—Duration is in recurring mode.
  - Date—Duration is in nonrecurring mode.
  - Start—Start week, day, and month setting.
  - End—End week, day, and month setting.

Configuring Time on the Sensor

To configure time on the sensor, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Time**.

Step 3 Under Sensor Local Date, select the current date from the drop-down lists. Date indicates the date on the local host.

Step 4 Under Sensor Local Time, enter the current time (hh:mm:ss). Time indicates the time on the local host. To see the current time, click **Refresh**.

Caution If you accidentally specify the incorrect time, stored events have the wrong time stamp. You must clear the events.

Note You cannot change the date or time on modules or if you have configured NTP.

Step 5 Under Standard Time Zone configure the time zone and offset:

a. In the Zone Name field, choose a time zone from the drop- down list, or enter one that you have created. This is the time zone to be displayed when summertime hours are not in effect.

b. In the UTC Offset field, enter the offset in minutes from UTC. If you choose a predefined time zone name, this field is automatically populated.

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

Step 6 If you are using NTP synchronization, under NTP Server enter the following:

- The IP address of the NTP server in the IP Address field.
- If using authenticated NTP, check the **Authenticated NTP** check box, and then enter the key of the NTP server in the Key field, and the key ID of the NTP server in the Key ID field.
- If using unauthenticated NTP, check the **Unauthenticated NTP** check box.

Note If you define an NTP server, the sensor time is set by the NTP server. The CLI **clock set** command produces an error, but time zone and daylight saving time parameters are valid.

Step 7 To enable daylight saving time, check the **Enable Summertime** check box.

Step 8 Click **Configure Summertime**.

Step 9 Choose the Summer Zone Name from the drop-down list or enter one that you have created. This is the name to be displayed when daylight saving time is in effect.

Step 10 In the Offset field, enter the number of minutes to add during summertime. If you choose a predefined summer zone name, this field is automatically populated.

Step 11 In the Start Time field, enter the time to apply summertime settings.

Step 12 In the End Time field, enter the time to remove summertime settings.

Step 13 Under Summertime Duration, choose whether summertime settings will occur on specified days each year (recurring) or whether they will start and end on specific dates (date):

a. Recurring—Choose the Start and End times from the drop-down lists.

   The default is the second Sunday in March and the first Sunday in November.

b. Date—Choose the Start and End time from the drop-down lists.

   The default is January 1 for the start and end time.

Tip To discard your changes and close the Configure Summertime dialog box, click **Cancel**.

Step 14 Click **OK**.

Tip To discard your changes, click **Reset**.

Step 15 Click **Apply** to apply your changes and save the revised configuration.

Step 16 If you changed the time and date settings (Steps 3 and 4), you must also click **Apply Time to Sensor** to save the time and date settings on the sensor.

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 from Event Store, see Clearing Events, page 4-15.

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

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.

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.

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 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.

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. You can use authenticated or unauthenticated NTP.

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.

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 For 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 For authenticated NTP:

a. Enter NTP configuration mode.

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

b. Specify 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.

Example

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

c. Specify the key value NTP server.

```
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.

Example

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

d. 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.

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.

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

- AIM IPS
- AIP SSC-5
- 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.

Clearing Events

Use the **clear events** command to clear Event Store.

To clear events from Event Store, follow these steps:

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

Step 2 Clear Event Store.

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

Step 3 Enter **yes** to clear the events.

Configuring Users

This section describes how to add and remove users on the system, and contains the following topics:

Users Pane

Note You must be administrator to add and edit users.

IDM permits multiple users to log in at a time. 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.

Users Pane Field Definitions

The following fields are found in the Users pane:

- Username—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.
- Role—The user role. The values are administrator, operator, service, and viewer. The default is viewer.

  Note Only one user with the role of service is allowed.

- Status—Displays the current user account status, such as active, expired, or locked.

Add and Edit User Dialog Boxes Field Definitions

The following fields found in the Add and Edit User dialog boxes:

- Username—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.
- User Role—The user role. Valid values are administrator, operator, service, and viewer. The default is viewer.

  Note Only one user with the role of service is allowed.

- Password—The user password. The password must conform to the requirements set by the sensor administrator.

- Confirm Password—Lets you confirm the password. You receive an error message if the confirm password does not match the user password.
- Change the password to access the sensor—Lets you change the password of the user. Only available in the Edit dialog box.

Understanding 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.

Adding, Editing, Deleting Users and Creating Accounts

To configure users on the sensor, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Users**, and then click **Add** to add a user.

Step 3 In the Username field, enter the username.

Step 4 From the drop-down list in the User Role field, choose one of the following user roles:

- Administrator

- Operator
- Viewer
- Service

Note Only one user with the role of service is allowed.

Step 5 In the Password field, enter the new password for that user.

Step 6 In the Confirm Password field, enter the new password for that user.

Tip To discard your changes and close the Add User dialog box, click **Cancel**.

Step 7 Click **OK**. The new user appears in the users list in the Users pane.

Step 8 To edit a user, select the user in the users list, and click **Edit**.

Step 9 Make any changes you need to in the Username, User Role, and Password fields.

Tip To discard your changes and close the Edit User dialog box, click **Cancel**.

Step 10 Click **OK**. The edited user appears in the users list in the Users pane.

Step 11 To delete a user from the user list, select the user, and click **Delete**. That user is no longer in the users list in the User pane.

Tip To discard your changes, click **Reset**.

Step 12 Click **Apply** to apply your changes and save the revised configuration.