CHAPTER 2

Setting Up the Sensor

This chapter provides information for setting up the sensor, and contains the following sections:

Understanding the setup Command

After you install the sensor on your network, you must use the **setup** command to initialize it. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, Telnet server, web server port, access control lists, and time settings, and you assign and enable virtual sensors and interfaces. After you initialize the sensor, you can communicate with it over the network. You are now ready to configure intrusion prevention.

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

After you initialize the sensor, you can make any changes and configure other network parameters in Sensor Setup.

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.

Use the Network pane to specify network and communication parameters for the sensor.

Note 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 10.1.9.201.

- Network Mask—Mask corresponding to the IP address.

  The default is 255.255.255.0.

- Default Route—Default gateway address.

  The default is 10.1.9.1.

- FTP Timeout—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. 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. You receive an error message if you enter a value out of the range of 1 to 65535.

- 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.

For More Information

For more information on the password recovery mechanism, see Configuring Allowed Hosts, page 2-4.

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 format `https://`*sensor_ip_address:port_number* (for example, `https://10.1.9.201:1040`).

Step 11 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 discard your changes, click **Reset**.

Step 12 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

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

Allowed Hosts Pane

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

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

Note After you use the **setup** command to initialize the sensor, the allowed hosts parameter values appear in the Allowed Hosts pane. If you need to change these parameters, you can do so in the Allowed Hosts pane.

By default, there are no entries in the list, and therefore no hosts are permitted until you add them.

Note You must add the management host, such as ASDM, IDM, IDS MC and the monitoring host, such as IDS Security Monitor, 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 Host Pane and Add and Edit Allowed Host Dialog Boxes Field Definitions

The following fields are found in the Allowed Hosts pane and in the 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

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**, and then click **Add**.

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.

Step 5 Click **OK**.

The new host or network appears in the allowed hosts list in the Allowed Hosts pane.

Step 6 To edit an existing entry in the allowed hosts 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.

Step 9 Click **OK**.

The edited host or network appears in the allowed hosts list in the Allowed Hosts pane.

Step 10 To delete a host or network from the list, select it, and click **Delete**.

The host no longer appears in the allowed hosts list in the Allowed Hosts 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 SSH

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

Understanding SSH

SSH provides strong authentication and secure communications over channels that are not secure.

SSH encrypts your connection to the sensor and provides a key so you can validate that you are connecting to the correct sensor. SSH also provides authenticated and encrypted access to other devices that the sensor connects to for blocking.

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

- Password
- User RSA public key

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.

Note SSH never sends passwords in clear text.

Defining Authorized Keys

This section describes how to define public keys, and contains the following topics:

Authorized Keys Pane

Note You must be administrator to add or edit authorized keys. If you have operator or viewer privileges and you try to add or edit an authorized key, you receive the `Delivery Failed` message.

Use the Authorized Keys pane to define public keys for a client allowed to use RSA authentication to log in to the local SSH server. The Authorized Keys pane displays the public keys of all SSH clients allowed to access the sensor.

Each user who can log in to the sensor has a list of authorized keys compiled from each client the user logs in with. When using SSH to log in to the sensor, you can use the RSA authentication rather than using passwords.

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 in the fields on the Authorized Keys pane.

You can view only your key and not the keys of other users.

Authorized Keys Pane and Add and Edit Authorized Key Dialog Boxes Field Definitions

The following fields are found in the Authorized Keys pane and in the Add and Edit Authorized Key dialog boxes:

- ID—A unique string (1 to 256 characters) to identify the key.

  You receive an error message if the ID contains a space or exceeds 256 alphanumeric characters.
- Modulus Length—Number of significant bits (511 to 2048) in the modulus.

  You receive an error message if the length is out of range.
- Public Exponent—Used by the RSA algorithm to encrypt data.

  The valid range is 3 to 2147483647. You receive an error message if the exponent is out of range.
- Public Modulus—Used by the RSA algorithm to encrypt data. The public modulus is a string of 1 to 2048 numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). You receive an error message if the modulus is out of range or if you use characters rather than numbers. The numbers must match the following pattern: ^[0-9][0-9]*$.

Defining Authorized Keys

To define public keys, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > SSH > Authorized Keys**, and then click **Add**. You can add a maximum of 50 SSH authorized keys.

Step 3 In the ID field, enter a unique ID to identify the key.

Step 4 In the Modulus Length field, enter an integer. The modulus length is the number of significant bits in the modulus. The strength of an RSA key relies on the size of the modulus. The more bits the modulus has, the stronger the key.

Note If you do not know the modulus length, public exponent, and public modulus, use an RSA key generation tool on the client where the private key is going to reside. Display the generated public key as a set of three numbers (modulus length, public exponent, and public modulus) and enter those numbers in Steps 5 through 7.

Step 5 In the Public Exponent field, enter an integer. The RSA algorithm uses the public exponent to encrypt data. The valid value for the public exponent is a number between 3 and 2147483647.

Step 6 In the Public Modulus field, enter a value. The public modulus is a string value of numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). The RSA algorithm uses the public modulus to encrypt data.

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

Step 7 Click **OK**. The new key appears in the authorized keys list in the Authorized Keys pane.

Step 8 To edit an existing entry in the authorized keys list, select it, and click **Edit**.

Step 9 Edit the Modulus Length, Public Exponent, and Public Modulus fields.

Caution You cannot modify the ID field after you have created an entry.

Step 10 Click **OK**. The edited key appears in the authorized keys list in the Authorized Keys pane.

Step 11 To delete a public key from the list, select it, and click **Delete**. The key no longer appears in the authorized keys list in the Authorized Keys pane.

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

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

Defining Known Host Keys

This section describes how to define known host keys, and contains the following topics:

Known Host Keys Pane

Note You must be administrator to add or edit known host keys.

Use the Known Host Keys pane to define public keys for the blocking devices that the sensor manages, and for SSH (SCP) servers that are used for downloading updates or copying files. You must get each device and server to report its public key so that you have the information you need to configure the Known Host Keys pane. If you cannot obtain the public key in the correct format, click **Retrieve Host Key** in the Add Known Host Keys dialog box.

Known Host Key Pane and Add and Edit Known Host Key Dialog Boxes Field Definitions

The following fields are found in the Known Host Keys pane and in the Add and Edit Known Host Key dialog boxes:

- IP Address—IP address of the host you are adding keys for.
- Modulus Length—Number of significant bits (511 to 2048) in the modulus.

  You receive an error message if the length is out of range.
- Public Exponent—Used by the RSA algorithm to encrypt data.

  The valid range is 3 to 2147483647. You receive an error message if the exponent is out of range.
- Public Modulus—Used by the RSA algorithm to encrypt data. The public modulus is a string of 1 to 2048 numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). You receive an error message if the modulus is out of range or if you use characters rather than numbers. The numbers must match the following pattern: ^[0-9][0-9]*$.

Defining Known Host Keys

To define known host keys, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > SSH > Known Host Keys**, and then click **Add**.

Step 3 In the IP Address field, enter the IP address of the host you are adding keys for.

Step 4 Click **Retrieve Host Key**. IDM attempts to retrieve the key from the host whose IP address you entered in Step 4. If the attempt is successful, go to Step 9. If the attempt is not successful, complete Steps 6 through 8.

Caution Validate that the key that was retrieved is correct for the specified address to make sure the server IP address is not being spoofed.

Step 5 In the Modulus Length field, enter an integer. The modulus length is the number of significant bits in the modulus. The strength of an RSA key relies on the size of the modulus. The more bits the modulus has, the stronger the key.

Step 6 In the Public Exponent field, enter an integer. The RSA algorithm uses the public exponent to encrypt data.

Step 7 In the Public Modulus field, enter a value. The public modulus is a string value of numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). The RSA algorithm uses the public modulus to encrypt data.

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

Step 8 Click **OK**. The new key appears in the known host keys list in the Known Host Keys pane.

Step 9 To edit an existing entry in the authorized keys list, select it, and click **Edit**.

Step 10 Edit the Modulus Length, Public Exponent, and Public Modulus fields.

Caution You cannot modify the ID field after you have created an entry.

Step 11 Click **OK**. The edited key appears in the known host keys list in the Known Host Keys pane.

Step 12 To delete a public key from the list, select it, and click **Delete**. The key no longer appears in the known host keys list in the Known Host Keys pane.

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

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

Displaying and Generating the Sensor SSH Host Key

This section describes how to display and generate the Sensor SSH host key, and contains the following topics:

Sensor Key Pane

Note You must be administrator to generate sensor SSH host keys.

The server uses the SSH host key to prove its identity. Clients know they have contacted the correct server when they see a known key.

The sensor generates an SSH host key the first time it starts up. It is displayed in the Sensor Key pane. Click **Generate Key** to replace that key with a new key.

Sensor Key Pane Field Definitions

The Sensor Key pane displays the sensor SSH host key. Pressing the **Generate Key** button generates a new sensor SSH host key.

Displaying and Generating the Sensor SSH Host Key

To display and generate sensor SSH host keys, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > SSH > Sensor Key**. The sensor SSH host key is displayed.

Step 3 To generate a new sensor SSH host key, click **Generate Key**. A dialog box displays the following warning:

```
Generating a new SSH host key requires you to update the known hosts tables on remote
systems with the new key so that future connections succeed. Do you want to continue?
```

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.

Step 4 Click **OK** to continue. A new host key is generated and the old host key is deleted. A status message states the key was updated successfully.

Configuring Certificates

This section describes certificates, and contains the following topics:

Understanding Certificates

IPS 6.0 contains a web server that is running IDM 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 in to the web browser that starts with `https://`*ip_address*, the web browser responds by using either TLS or SSL protocol to negotiate an encrypted session with the host.

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

Note IDM is 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, the certificate that is returned fails because the sensor issues its own certificate (the sensor is its own CA) and the sensor is not already in the list of CAs trusted by your browser.

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

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

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

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

For More Information

For more information on the sensor and certificates, see Validating the CA, page 1-48.

Adding Trusted Hosts

This section describes how to add trusted hosts, and contains the following topics:

Trusted Hosts Pane

Note You must be administrator to add trusted hosts.

Use the Trusted Hosts pane to add certificates for master blocking sensors and for TLS and SSL servers that the sensor uses for downloading updates. You can also use it to add the IP addresses of external product interfaces, such as CSA MC, that the sensor communicates with.

The Trusted Hosts pane lists all trusted host certificates that you have added. You can add certificates by entering an IP address. IDM retrieves the certificate and displays its fingerprint. If you accept the fingerprint, the certificate is trusted. You can add and delete entries from the list, but you cannot edit them.

For More Information

For more information on external product interfaces, see Adding, Editing, and Deleting External Product Interfaces and Posture ACLs, page 10-7.

Trusted Hosts Pane Field Definitions

The following fields are found in the Trusted Hosts pane:

- IP Address—IP address of the trusted host.
- MD5—Message Digest 5 encryption.

  MD5 is an algorithm used to compute the 128-bit hash of a message.
- SHA1—Secure Hash Algorithm.

  SHA1 is a cryptographic message digest algorithm.

Add Trusted Host Dialog Box Field Definitions

The following fields are found in the Add Trusted Host dialog box:

- IP Address—IP address of the trusted host.
- Port—(Optional) Specifies the port number of where to obtain the host certificate.

Adding Trusted Hosts

To add trusted hosts, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Certificate > Trusted Hosts**, and then click **Add**.

Step 3 In the IP Address field, enter the IP address of the trusted host you are adding.

Step 4 In the Port field, enter a port number if the sensor is using a port other than 443.

Step 5 Click **OK**. IDM retrieves the certificate from the host whose IP address you entered in Step 4. The new trusted host appears in the trusted hosts list in the Trusted Hosts pane.

A dialog box informs you that IDM is communicating with the sensor:

```
Communicating with the sensor, please wait ...
```

A dialog box provides status about whether IDM was successful in adding a trusted host:

```
The new host was added successfully.
```

Step 6 Verify that the fingerprint is correct by comparing the displayed values with a securely obtained value, such as through direct terminal connection or on the console. If you find any discrepancies, delete the trusted host immediately.

Step 7 To view an existing entry in the trusted hosts list, select it, and click **View**.

The View Trusted Host dialog box appears. The certificate data is displayed. Data displayed in this dialog box is read-only.

Step 8 Click **OK**.

Step 9 To delete a trusted host from the list, select it, and click **Delete**. The trusted host no longer appears in the trusted hosts list in the Trusted Hosts pane.

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

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Displaying and Generating the Server Certificate

This section describes how to display and generate a server certificate, and contains the following topics:

Server Certificate Pane

Note You must be administrator to generate server certificates.

The Server Certificate pane displays the sensor server X.509 certificate. You can generate a new server self-signed X.509 certificate from this pane. A certificate is generated when the sensor is first started. Click **Generate Certificate** to generate a new host certificate.

Caution The sensor IP address is included in the certificate. If you change the sensor IP address, you must generate a new certificate.

Server Certificate Pane Field Definitions

The Server Certificate pane displays the sensor server X.509 certificate. Click **Generate Certificate** to generate a new sensor X.509 certificate.

Displaying and Generating the Server Certificate

To display and generate the sensor server X.509 certificate, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Certificate > Server Certificate**. The sensor server X.509 certificate is displayed.

Step 3 To generate a new sensor server X.509 certificate, click **Generate Certificate**. A dialog box displays the following warning:

```
Generating a new server certificate requires you to verify the new fingerprint the next
time you connect or when you add the sensor as a trusted host. Do you want to continue?
```

Caution Write down the new fingerprint. Later you will need it to verify what is displayed in your web browser when you connect, or when you are adding the sensor as a trusted host. If the sensor is a master blocking sensor, you must update the trusted hosts table on the remote sensors that are sending blocks to the master blocking sensor.

Step 4 Click **OK** to continue. A new server certificate is generated and the old server certificate is deleted.

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 time synchronization source.

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. You 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.
- For 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 IDSM2 to ensure that the UTC time settings are correct. The local time of IDSM2 could be incorrect if the time zone and/or summertime settings do not match between IDSM2 and the switch.

  - Use NTP—You can configure IDSM2 to get its time from an NTP time synchronization source. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure IDSM2 to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

- For NM- CIDS and AIM IPS
  - NM- CIDS and AIM 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 NM CIDS and AIM IPS. The time zone and summertime settings are not synchronized between the parent router and NM CIDS and AIM IPS.

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

  - Use NTP—You can configure NM CIDS and AIM IPS to get their time from an NTP time synchronization source, such as a Cisco router other than the parent router. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure NM CIDS and AIM IPS to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.
- For AIP SSM
  - AIP SSM can automatically synchronize its clock with the clock in the adaptive security appliance in which it is installed. This is the default. The UTC time is synchronized between the adaptive security appliance and AIP SSM. The time zone and summertime settings are not synchronized between the adaptive security appliance and AIP SSM.

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

  - 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. You 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.

For More Information

- For the procedure for using the **setup** command to initialize the sensor, see Initializing the Sensor, page 1-3.
- For the procedure for using the **clock set** command to set the time, see Manually Setting the System Clock, page 2-24.
- For the procedure for configuring a Cisco router to be an NTP server, see Configuring a Cisco Router to be an NTP Server, page 2-21.
- For more information about how to synchronize module clocks with parent device clocks, see Synchronizing IPS Module System Clocks with Parent Device System Clocks, page 2-18.

Synchronizing IPS Module System Clocks with Parent Device System Clocks

All IPS modules (IDSM2, NM CIDS, AIP SSM, and AIM 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.

For More Information

- For more information on NTP, see Configuring NTP, page 2-21.
- For more information on verifying that the module and NTP server are synchronized, see Verifying the Sensor is Synchronized with the NTP Server, page A-19.

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 TNP, 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 is needed.
- 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:

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 NPT, check the **Unauthenticated NTP** check box.

Note If you define an NTP server, the time of 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 first Sunday in April and the last Sunday in October.

b. Date—Choose the Start and End time from the drop-down lists. The default is January 1 for the start and end time.

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.

For More Information

- For more information on correcting the time on the sensor, see Correcting Time on the Sensor, page 2-21.
- For the procedure for clearing events, see Clearing Events, page 2-25.

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.

Caution You cannot remove individual events.

For More Information

For more information on the **clear events** command, see Clearing Events, page 2-25.

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 2-21
- Configuring the Sensor to Use an NTP Time Source, page 2-23

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.

For More Information

For the procedure for configuring the sensor to use NTP, see Configuring the Sensor to Use an NTP Time Source, page 2-23.

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.

For More Information

For the procedure for configuring a Cisco router to be an NTP server, see Configuring a Cisco Router to be an NTP Server, page 2-21.

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:

- IDSM2
- NM CIDS
- AIM IPS
- AIP SSM-10
- AIP SSM-20
- AIP SSM-40

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.

For More Information

- For the procedure for configuring NTP, see Configuring a Cisco Router to be an NTP Server, page 2-21 and Configuring the Sensor to Use an NTP Time Source, page 2-23.
- For an explanation of the importance of having a valid time source for the sensor, see Time Sources and the Sensor, page 2-16.
- For an explanation of what to do if you set the clock incorrectly, see Correcting Time on the Sensor, page 2-21.

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:

Understanding User Roles

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.

There are four user roles:

- Viewers—Can view configuration and events, but cannot modify any configuration data except their user passwords.
- Operators—Can view everything and can modify the following options:
  - Signature tuning (priority, disable or enable)
  - Virtual sensor definition
  - Managed routers
  - Their user passwords
- Administrators—Can view everything and can modify all options that operators can modify in addition to the following:
  - Sensor addressing configuration
  - List of hosts allowed to connect as configuration or viewing agents
  - Assignment of physical sensing interfaces
  - Enable or disable control of physical interfaces
  - Add and delete users and passwords
  - Generate new SSH host keys and server certificates
- Service—Only one user with service privileges can exist on a sensor. The service user cannot log in to IDM. The service user logs in to a bash shell rather than the CLI.

Note The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed. You should only create an account with the service role for troubleshooting purposes. Only a user with administrator privileges can edit the service account.

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.

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

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

Note 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.

User Pane Field Definitions

The following fields are found in the Users pane:

- Username—The 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.

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

Add and Edit User Dialog Boxes Field Definitions

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

- Username—The 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.

- Password—The user password.

  A valid password is 8 to 32 characters long. All characters except space are allowed.

- 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.

Configuring Users

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**.

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

Step 5 Check the **Change the password to access the sensor** check box.

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

Step 7 In the Confirm Password field, enter the new password for that user.

Step 8 Click **OK**. The new user appears in the users list in the Users pane.

Step 9 To edit a user, select the user in the users list, and click **Edit**.

Step 10 Make any changes you need to in the Username, User Role, and Password fields.

Step 11 Click **OK**. The edited user appears in the users list in the Users pane.

Step 12 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 13 Click **Apply** to apply your changes and save the revised configuration.