



CHAPTER 2

Setting Up the Sensor

This chapter describes how to set up the sensor, and contains the following sections:

- [Understanding Setup, page 2-1](#)
- [Configuring Network Settings, page 2-1](#)
- [Configuring Allowed Hosts, page 2-4](#)
- [Configuring SSH, page 2-7](#)
- [Configuring Certificates, page 2-15](#)
- [Configuring Time, page 2-18](#)
- [Configuring Users, page 2-25](#)

Understanding Setup

After you have installed 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, time settings, and assign and enable interfaces. After you have initialized the sensor, you can communicate with it over the network. You are then ready to configure intrusion prevention.



Caution

You must initialize the sensor before you can use Configuration > Sensor Setup in IDM to further configure the sensor. For the procedure, see [Initializing the Sensor, page 1-4](#).

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:

- [Overview, page 2-2](#)
- [Supported User Role, page 2-2](#)

- [Field Definitions, page 2-2](#)
- [Configuring Network Settings, page 2-3](#)

Overview

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 on the Network pane. If you need to change these parameters, you can do so from the Network pane.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure network settings.

Field Definitions

The following fields and buttons are found on the Network pane.

Field Descriptions:

- **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.
- **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.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

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**.
The Network pane appears.
 - 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 enable or disable TLS/SSL, check or uncheck Enable TLS/SSL.



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 9** 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 10** 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 11 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:

- [Overview, page 2-4](#)
- [Supported User Role, page 2-5](#)
- [Field Definitions, page 2-5](#)
- [Configuring Allowed Hosts, page 2-6](#)

Overview

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 on the Allowed Hosts pane. If you need to change these parameters, you can do so from 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 will not be able to 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure allowed hosts and networks.

Field Definitions

This section lists the field definitions for allowed hosts, and contains the following topics:

- [Allowed Hosts Pane, page 2-5](#)
- [Add and Edit Allowed Host Dialog Boxes, page 2-5](#)

Allowed Hosts Pane

The following fields are found on the Allowed Hosts pane:

Field Descriptions:

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

Button Functions:

- Add—Opens the Add Allowed Host dialog box.
From this dialog box, you can add a host or network to the list of allowed hosts.
- Edit—Opens the Edit Allowed Host dialog box.
From this dialog box, you can change the values associated with this host or network.
- Delete—Removes this host or network from the list of allowed hosts.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Allowed Host Dialog Boxes

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

Field Descriptions:

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

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

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**.
The Allowed Hosts pane appears.
- Step 3** Click **Add** to add a host or network to the list.
The Add Allowed Host dialog box appears.
You can add a maximum of 512 allowed hosts.
- Step 4** Enter the IP address of the host or network in the IP Address field.
You receive an error message if the IP address is already included as part of an existing list entry.
- Step 5** Enter the network mask of the host or network in the Network Mask field or select 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 6** Click **OK**.
The new host or network appears in the allowed hosts list on the Allowed Hosts pane.
- Step 7** To edit an existing entry in the allowed hosts list, select it, and click **Edit**.
The Edit Allowed Host dialog box appears.
- Step 8** Edit the IP address of the host or network in the IP Address field.
- Step 9** Edit the network mask of the host or network in the Network Mask field.
- Step 10** Click **OK**.
The edited host or network appears in the allowed hosts list on the Allowed Hosts pane.
- Step 11** To delete a host or network from the list, select it, and click **Delete**.
The host no longer appears in the allowed hosts list on 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 12** Click **Apply** to apply your changes and save the revised configuration.
-

Configuring 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.

**Note**

SSH never sends passwords in clear text.

This section contains the following topics:

- [Defining Authorized Keys, page 2-7](#)
- [Defining Known Host Keys, page 2-10](#)
- [Displaying and Generating the Server Certificate, page 2-17](#)

Defining Authorized Keys

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

- [Overview, page 2-7](#)
- [Supported User Role, page 2-8](#)
- [Field Definitions, page 2-8](#)
- [Defining Authorized Keys, page 2-7](#)

Overview

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

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.

Field Definitions

This section lists the field definitions for authorized keys, and contains the following topics:

- [Authorized Keys Pane, page 2-8](#)
- [Add and Edit Authorized Key Dialog Boxes, page 2-9](#)

Authorized Keys Pane

The following fields and buttons are found on the Authorized Keys pane.

Field Descriptions:

- 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 $(2^{\text{length}} < \text{modulus} < (2^{\text{length} + 1}))$). 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]*$`.

Button Functions:

- Add—Opens the Add Authorized Key dialog box. From this dialog box, you can add a new authorized key.
- Edit—Opens the Edit Authorized Key dialog box. From this dialog box, you can change the values associated with this authorized key.
- Delete—Removes this authorized key from the list.

- **Apply**—Applies your changes and saves the revised configuration.
- **Reset**—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Authorized Key Dialog Boxes

The following fields and buttons are found in the Add and Edit Authorized Key dialog boxes.

Field Descriptions:

- **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 $(2^{\text{length}}) < \text{modulus} < (2^{(\text{length} + 1)})$). 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]*$`.

Button Functions:

- **OK**—Accepts your changes and closes the dialog box.
- **Cancel**—Discards your changes and closes the dialog box.
- **Help**—Displays the help topic for this feature.

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**.
The Authorized Keys pane appears.
 - Step 3** Click **Add** to add a public key to the list.
The Add Authorized Key dialog box appears.
You can add a maximum 50 SSH authorized keys.
 - Step 4** Enter a unique ID to identify the key in the **ID** field.
 - Step 5** Enter an integer in the Modulus Length field.
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 6** Enter an integer in the Public Exponent field.
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 7** Enter a value in the Public Modulus field.
The public modulus is a string value of numbers (where modulus is $(2^{\text{length}} < \text{modulus} < (2^{\text{length} + 1}))$).
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 8** Click **OK**.
The new key appears in the authorized keys list on the Authorized Keys pane.
- Step 9** To edit an existing entry in the authorized keys list, select it, and click **Edit**.
The Edit Authorized Key dialog box appears.
- 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 authorized keys list on the Authorized Keys pane.
- Step 12** To delete a public key from the list, select it, and click **Delete**.
The key no longer appears in the authorized keys list on the Authorized Keys pane.



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

- Step 13** 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:

- [Overview, page 2-11](#)
- [Supported User Role, page 2-11](#)
- [Field Definitions, page 2-11](#)
- [Defining Known Host Keys, page 2-12](#)

Overview

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to add or edit known host keys.

Field Definitions

This section lists the field definitions for known host keys, and contains the following topics:

- [Known Host Keys Pane, page 2-11](#)
- [Add and Edit Known Host Key Dialog Boxes, page 2-12](#)

Known Host Keys Pane

The following fields and buttons are found on the Known Host Keys pane.

Field Descriptions:

- 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 $(2^{\text{length}} < \text{modulus} < (2^{\text{length} + 1}))$). 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]*$`.

Button Functions:

- Add—Opens the Add Known Host Key dialog box. From this dialog box, you can add a new known host key.
- Edit—Opens the Edit Known Host Key dialog box. From this dialog box, you can change the values associated with this known host key.
- Delete—Removes this known host key from the list.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Known Host Key Dialog Boxes

The following fields and buttons are found in the Add and Edit Known Host Key dialog boxes.

Field Descriptions:

- **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 $(2^{\text{length}} < \text{modulus} < (2^{\text{length} + 1}))$). 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]*$`.

Button Functions:

- **Retrieve Host Key**—IDM attempts to retrieve the known host key from the host specified by the IP address. If successful, IDM populates the Add Known Host Key pane with the key.
Available only in the Add dialog box. You receive an error message if the IP address is invalid.
- **OK**—Accepts your changes and closes the dialog box.
- **Cancel**—Discards your changes and closes the dialog box.
- **Help**—Displays the help topic for this feature.

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**.

The Known Host Keys pane appears.

Step 3 Click **Add** to add a known host key to the list.

The Add Known Host Key dialog box appears.

Step 4 Enter the IP address of the host you are adding keys for in the IP Address field.

Step 5 Click **Retrieve Host Key**.

The Device Manager attempts to retrieve the key from the host whose IP address you entered in Step 3. If the attempt is successful, go to Step 8. If the attempt is not successful complete Steps 5 through 7.



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 6 Enter an integer in the Modulus Length field.

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 7** Enter an integer in the Public Exponent field.
The RSA algorithm uses the public exponent to encrypt data.
- Step 8** Enter a value in the Public Modulus field.
The public modulus is a string value of numbers (where modulus is $(2^{\text{length}} < \text{modulus} < (2^{\text{length} + 1}))$).
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 9** Click **OK**.
The new key appears in the known host keys list on the Known Host Keys pane.
- Step 10** To edit an existing entry in the authorized keys list, select it, and click **Edit**.
The Edit Authorized Key dialog box appears.
- Step 11** Edit the Modulus Length, Public Exponent, and Public Modulus fields.



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

- Step 12** Click **OK**.
The edited key appears in the known host keys list on the Known Host Keys pane.
- Step 13** To delete a public key from the list, select it, and click **Delete**.
The key no longer appears in the known host keys list on the Known Host Keys pane.



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

- Step 14** 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:

- [Overview, page 2-14](#)
- [Supported User Role, page 2-14](#)
- [Field Definitions, page 2-14](#)
- [Displaying and Generating the Sensor SSH Host Key, page 2-14](#)

Overview

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 on the Sensor Key pane. Click **Generate Key** to replace that key with a new key.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to generate sensor SSH host keys.

Field Definitions

The Sensor Key pane displays the sensor SSH host key. 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 Key pane appears.

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

For more information on the sensor and certificates, see [IDM and Certificates, page 1-15](#). This section contains the following topics:

- [Adding Trusted Hosts, page 2-15](#)
- [Displaying and Generating the Server Certificate, page 2-17](#)

Adding Trusted Hosts

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

- [Overview, page 2-15](#)
- [Supported User Role, page 2-15](#)
- [Field Definitions, page 2-15](#)
- [Adding Trusted Hosts, page 2-16](#)

Overview

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.

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to add trusted hosts.

Field Definitions

This section lists field definitions for trusted hosts, and contains the following topics:

- [Trusted Hosts Pane, page 2-16](#)
- [Add Trusted Host Dialog Box, page 2-16](#)

Trusted Hosts Pane

The following fields and buttons are found on the Trusted Hosts pane.

Field Descriptions:

- 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.

Button Functions:

- Add—Opens the Add Trusted Host dialog box. From this dialog box, you can add a new trusted host.
- View—Opens the View Trusted Host dialog box. From this dialog box, you can view the certificate data associated with this trusted host.
- Delete—Removes this trusted host from the list.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add Trusted Host Dialog Box

The following fields and buttons are found on the Add Trusted Host dialog box.

Field Descriptions:

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

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

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**.
The Trusted Hosts pane appears.
 - Step 3** Click **Add** to add a trusted host to the list.
The Add Trusted Host dialog box appears.
 - Step 4** Enter the IP address of the trusted host you are adding in the IP Address field.
 - Step 5** Enter a port number in the **Port** field if the sensor is using a port other than 443.

- Step 6** Click **OK**.
- IDM retrieves the certificate from the host whose IP address you entered in Step 3. The new trusted host appears in the trusted hosts list on 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 7** 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. See Step 7. If you find any discrepancies, delete the trusted host immediately. See Step 8.
- Step 8** 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 9** Click **OK**.
- Step 10** To delete a trusted host from the list, select it, and click **Delete**.
- The trusted host no longer appears in the trusted hosts list on the Trusted Hosts pane.
- 
Tip To discard your changes, click **Reset**.
- Step 11** 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:

- [Overview, page 2-17](#)
- [Supported User Role, page 2-18](#)
- [Field Definitions, page 2-18](#)
- [Displaying and Generating the Server Certificate, page 2-18](#)

Overview

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.



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

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to generate server certificates.

Field Definitions

The Server Certificate pane displays the sensor server X.509 certificate. Clicking Generate Certificate generates 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 Server Certificate pane appears.
- 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:

- [Overview, page 2-19](#)
- [Time Sources and the Sensor, page 2-19](#)
- [Supported User Role, page 2-21](#)
- [Field Definitions, page 2-21](#)

- [Configuring Time on the Sensor, page 2-23](#)
- [Correcting Time on the Sensor, page 2-24](#)

Overview

Use the Time pane to configure the 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's 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. For more information, see [Initializing the Sensor, page 1-4](#).

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, refer to [Manually Setting the Clock](#).

- Use NTP

You can configure the appliance to get its time from an NTP time synchronization source. For the procedure, refer to [Configuring a Cisco Router to be an NTP Server](#). 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. The local time of IDSM-2 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. For the procedure, refer to [Configuring a Cisco Router to be an NTP Server](#). 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. The local time of NM-CIDS 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. For the procedure, refer to [Configuring a Cisco Router to be an NTP Server](#). 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. The local time of AIP-SSM 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. For the procedure, refer to [Configuring a Cisco Router to be an NTP Server](#). 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure time settings.

Field Definitions

This section lists the field definitions for time, and contains the following topics:

- [Time Pane, page 2-21](#)
- [Configure Summertime Dialog Box, page 2-22](#)

Time Pane

The following fields and buttons are found on the Time pane.

Field Descriptions:

- **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.
 - 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.
- Summertime—Lets you enable and configure summertime settings.
 - Enable Summertime—Click to enable summertime mode.
The default is disabled.

Button Functions:

- Configure Summertime—Click to open the Configure Summertime dialog box.
You can only open the Configure Summertime box if you have Enable Summertime selected.
- Apply—Applies your changes and saves the revised configuration.
Apply is enabled if any other settings on the Time pane are modified (such as NTP, summertime, and standard time zone settings). Apply corresponds to all other fields on the Time pane except the date and time.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.
- Apply Time to Sensor—Sets the date and time on the sensor.
Apply Time to Sensor is only enabled when you change the date and time. If you want the modified date and time to be saved to the sensor, you must click **Apply Time to Sensor**.

Configure Summertime Dialog Box

The following fields and buttons are found on the Configure Summertime dialog box.

Field Descriptions:

- 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 select a predefined time zone, this field is populated automatically.



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

- 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.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

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**.

The Time pane appears.

Step 3 Under Date, choose the current date from the drop down boxes.

Date indicates the date on the local host.

Step 4 Under 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 will have the wrong time stamp. You must clear the events. For more information, see [Correcting Time on the Sensor, page 2-24](#).



Note

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

Step 5 Under Standard Time Zone:

- a. Select a time zone from the drop down box in the Zone Name field or enter one that you have created.

This is the time zone to be displayed when summertime hours are not in effect.

- b. Enter the offset in minutes from UTC in the UTC Offset field.

If you select 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:

- a. The IP address of the NTP server in the IP Address field

- b. The key of the NTP server in the Key field
- c. The key ID of the NTP server in the Key ID field



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 Under Summertime, check the **Enable Summertime** check box to enable daylight saving time.

Step 8 Click **Configure Summertime**.

The Configure Summertime dialog box appears.

Step 9 Select the Summer Zone Name from the drop down box or enter one that you have created.

This is the name to be displayed when daylight saving time is in effect.

Step 10 Enter the number of minutes to add during summertime.

If you select a predefined summer zone name, this field is automatically populated.

Step 11 Enter the time to apply summertime settings in the Start Time field.

Step 12 Enter the time to remove summertime settings in the End Time field.

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—Select the Start and End times from the drop down boxes.
The default is the first Sunday in April and the last Sunday in October.
- b. Date—Select the Start and End time from the drop down boxes.
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 1 and 2), 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. For more information on the **clear events** command refer to [Clearing Events from Event Store](#).

**Caution**

You cannot remove individual events.

Configuring Users

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

- [Overview, page 2-25](#)
- [Supported User Role, page 2-26](#)
- [Field Definitions, page 2-26](#)
- [Configuring Users, page 2-28](#)

Overview

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 new 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to add and edit users.

Field Definitions

This section lists the field definitions for users, and contains the following topics:

- [Users Pane, page 2-27](#)
- [Add and Edit User Dialog Boxes, page 2-27](#)

Users Pane

The following fields and buttons are found on the Users pane.

Field Descriptions:

- **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.

Button Functions:

- **Add**—Opens the Add User dialog box. From this dialog box, you can add a user to the list of users.
- **Edit**—Opens the Edit User dialog box. From this dialog box, you can edit a user in the list of users.
- **Delete**—Removes this user from the list of users.
- **Apply**—Applies your changes and saves the revised configuration.
- **Reset**—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit User Dialog Boxes

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

Field Descriptions:

- **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.
The password must contain a minimum of eight characters. 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 user's password.
Only available in the Edit dialog box.

Button Functions:

- **OK**—Accepts your changes and closes the dialog box.
- **Cancel**—Discards your changes and closes the dialog box.
- **Help**—Displays the help topic for this feature.

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**.
The Users pane appears.
- Step 3** Click **Add** to add a user.
The Add User dialog box appears.
- Step 4** Enter the user name in the Username field.
- Step 5** Select one of the following user roles from the drop-down list in the User Role field:
- Administrator
 - Operator
 - Viewer
 - Service
- Step 6** Enter the new password for that user in the Password field.
- Step 7** Confirm the new password for that user in the Confirm Password field.
- Step 8** Click **OK**.
The new user appears in the users list on the Users pane.
- Step 9** To edit a user, select the user in the users list, and click **Edit**.
The Edit User dialog box appears.
- Step 10** Check the **Change the password to access the sensor** check box.
- Step 11** Make any changes you need to in the User Role and Password fields.
- Step 12** Click **OK**.
The edited user appears in the users list on the Users pane.
- Step 13** To delete a user from the user list, select the user, and click **Delete**.
That user is no longer in the users list on the User pane.



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

- Step 14** Click **Apply** to apply your changes and save the revised configuration.
-