



Configuring SSH and Certificates

This chapter describes how to configure SSH and certificates for your sensor, and it contains the following sections:

- [Understanding SSH, page 14-1](#)
- [Configuring Authorized RSA Keys, page 14-2](#)
- [Configuring Authorized RSA1 Keys, page 14-4](#)
- [Configuring Known Host RSA Keys, page 14-6](#)
- [Configuring Known Host RSA1 Keys, page 14-8](#)
- [Generating the Sensor Key, page 14-10](#)
- [Understanding Certificates, page 14-11](#)
- [Configuring Trusted Hosts, page 14-12](#)
- [Adding Trusted Root Certificates, page 14-14](#)
- [Generating the Server Certificate, page 14-16](#)

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. The IPS supports a management through both SSHv1 and SSHv2.

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

- Password
- User RSA public key



Note SSH never sends passwords in clear text.

SSH protects against the following:

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



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

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

Configuring Authorized RSA Keys

This section describes how to configure authorized RSA keys for the sensor, and contains the following topics:

- [Authorized RSA Keys Pane, page 14-2](#)
- [Authorized RSA Keys Pane Field Definitions, page 14-2](#)
- [Add and Edit Authorized RSA Key Dialog Boxes Field Definitions, page 14-3](#)
- [Defining Authorized RSA Keys, page 14-3](#)

Authorized RSA Keys Pane

**Note**

You must be administrator to add or edit authorized RSA 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 RSA Keys pane to manage public keys for SSHv2 clients allowed to use RSA authentication to log in to the local SSH server. The Authorized RSA Keys pane displays the public keys of all SSH clients allowed to access the sensor. You can view only your key and not the keys of other users.

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 SSHv2 to log in to the sensor, you can use RSA authentication rather than using passwords.

Authorized RSA Keys Pane Field Definitions

The following fields are found in the Authorized RSA Keys pane:

- ID—Specifies 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.
- Public Key—Specifies the public key of the SSHv2 client.






Add and Edit Authorized RSA Key Dialog Boxes Field Definitions

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

- **ID**—Specifies 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.
- **Public Key**—Specifies the public key of the SSHv2 client.

Defining Authorized RSA Keys

To define public RSA keys, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > Sensor Management > SSH > Authorized RSA Keys**, and then click **Add** to add a public key to the list. You can add a maximum of 50 SSHv2 authorized keys.
- Step 3** In the ID field, enter a unique ID to identify the key.
- Step 4** In the Public Key field, enter the public key.
-  **Note** You generate the key on the SSH client and enter it in the Public Key field.
-
-  **Tip** To discard your changes and close the Add Authorized RSA Key dialog box, click **Cancel**.
-
- Step 5** Click **OK**. The new key appears in the authorized keys list in the Authorized RSA Keys pane.
- Step 6** To edit an existing entry in the authorized keys list, select it, and click **Edit**.
- Step 7** Edit the ID and Public Key fields.
-  **Caution** You cannot modify the ID field after you have created an entry.
-
-  **Tip** To discard your changes and close the Edit Authorized RSA Key dialog box, click **Cancel**.
-
- Step 8** Click **OK**. The edited key appears in the authorized keys list in the Authorized RSA Keys pane.
- Step 9** 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 RSA Keys pane.
-  **Tip** To discard your changes, click **Reset**.
-
- Step 10** Click **Apply** to apply your changes and save the revised configuration.
-

Configuring Authorized RSA1 Keys

This section describes how to configure authorized RSA1 keys for the sensor, and contains the following topics:

- [Authorized RSA1 Keys Pane, page 14-4](#)
- [Authorized RSA1 Keys Pane Field Definitions, page 14-4](#)
- [Add and Edit Authorized RSA1 Key Dialog Boxes Field Definitions, page 14-5](#)
- [Defining Authorized RSA1 Keys, page 14-5](#)

Authorized RSA1 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 RSA1 Keys pane to specify SSHv1 public keys for a client allowed to use RSA authentication to log in to the local SSH server. The Authorized RSA1 Keys pane displays the public keys of all SSH clients allowed to access the sensor. You can view only your key and not the keys of other users.

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 SSHv1 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 RSA1 Keys pane.

Authorized RSA1 Keys Pane Field Definitions

The following fields are found in the Authorized RSA1 Keys pane:

- **ID**—Specifies 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**—Specifies the 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]*$`.

Add and Edit Authorized RSA1 Key Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Authorized RSA1 Key dialog boxes:

- **ID**—Specifies 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**—Specifies the 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]*$`.

Defining Authorized RSA1 Keys

To define public RSA1 keys, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > Sensor Management > SSH > Authorized RSA1 Keys**, and then click **Add** to add a public key to the list. 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 4 through 6.

- 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 $(2^{\text{length}} < \text{modulus} < (2^{\text{length} + 1}))$). The RSA algorithm uses the public modulus to encrypt data.



Tip To discard your changes and close the Add Authorized RSA1 Key dialog box, click **Cancel**.

- Step 7** Click **OK**. The new key appears in the authorized keys list in the Authorized RSA1 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.

**Tip**

To discard your changes and close the Edit Authorized RSA1 Key dialog box, click **Cancel**.

Step 10 Click **OK**. The edited key appears in the authorized keys list in the Authorized RSA1 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 RSA1 Keys pane.

**Tip**

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

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

Configuring Known Host RSA Keys

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

- [Known Host RSA Keys Pane, page 14-6](#)
- [Known Host RSA Keys Pane Field Definitions, page 14-7](#)
- [Add and Edit Known Host RSA Key Dialog Boxes Field Definitions, page 14-7](#)
- [Defining Known Host RSA Keys, page 14-7](#)

Known Host RSA Keys Pane

**Note**

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

Use the Known Host RSA 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 RSA Keys pane. If you cannot obtain the public key in the correct format, click **Retrieve Host Key** in the Add Known Host RSA Keys dialog box.

The IME attempts to retrieve the known host key from the host specified by the IP address. If successful, The IME populates the Add Known Host RSA Key pane with the key.

**Note**

Retrieve Host Key is available only in the Add dialog box. You receive an error message if the IP address is invalid.

Known Host RSA Keys Pane Field Definitions

The following fields are found in the Known Host RSA Keys pane:

- IP Address—Specifies the IP address of the host for which you are adding keys.
- Public Key—Specifies the RSA host key.

Add and Edit Known Host RSA Key Dialog Boxes Field Definitions

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

- IP Address—Specifies the IP address of the host for which you are adding keys.
- Public Key—Specifies the RSA host key.
- Retrieve Host Key—Lets the IME try to retrieve the known host key from the host specified by the IP address. If successful, The IME populates the Add Known Host RSA Key pane with the key.



Note **Retrieve Host Key** is available only in the Add dialog box. You receive an error message if the IP address is invalid.

Defining Known Host RSA Keys

To define known host RSA keys, follow these steps:

- Step 1** Log in to the IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > Sensor Management > SSH > Known Host RSA Keys**, and then click **Add** to add a known host RSA key to the list.
- Step 3** In the IP Address field, enter the IP address of the host for which you are adding a key.
- Step 4** If you know the public key, enter it in the Public key field, or click **Retrieve Host Key** to obtain the known host key. The IME attempts to retrieve the key from the host whose IP address you entered in Step 3. If the attempt is successful, go to Step 5.



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.



Tip

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

- Step 5** Click **OK**. The new key appears in the known host keys list in the Known Host RSA Keys pane.
- Step 6** To edit an existing entry in the authorized keys list, select it, and click **Edit**.
- Step 7** Edit the ID and the Public Key fields.



Caution

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



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

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

Step 9 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 RSA Keys pane.



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

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

Configuring Known Host RSA1 Keys

This section describes how to configure known host RSA1 keys, and contains the following topics:

- [Known Host RSA1 Keys Pane, page 14-8](#)
- [Known Host RSA1 Keys Pane Field Definitions, page 14-9](#)
- [Add and Edit Known Host RSA1 Key Dialog Boxes Field Definitions, page 14-9](#)
- [Defining Known Host RSA1 Keys, page 14-9](#)

Known Host RSA1 Keys Pane



Note You must be administrator to add or edit known host RSA1 keys.

Use the Known Host RSA1 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 RSA1 Keys pane. If you cannot obtain the public key in the correct format, click **Retrieve Host Key** in the Add Known Host RSA1 Keys dialog box.

The IME attempts to retrieve the known host key from the host specified by the IP address. If successful, The IME populates the Add Known Host RSA1 Key pane with the key.



Note **Retrieve Host Key** is available only in the Add dialog box. You receive an error message if the IP address is invalid.

Known Host RSA1 Keys Pane Field Definitions

The following fields are found in the Known Host RSA1 Keys pane:

- IP Address—Specifies the IP address of the host for which you are adding keys.
- Modulus Length—Specifies the 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]*$`.

Add and Edit Known Host RSA1 Key Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Known Host RSA1 Key dialog boxes:

- IP Address—Specifies the IP address of the host for which you are adding keys.
- Modulus Length—Specifies the 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]*$`.
- Retrieve Host Key—Lets the IME try to retrieve the known host key from the host specified by the IP address. If successful, The IME populates the Add Known Host RSA Key pane with the key.



Note **Retrieve Host Key** is available only in the Add dialog box. You receive an error message if the IP address is invalid.

Defining Known Host RSA1 Keys

To define known host RSA1 keys, follow these steps:

- Step 1** Log in to the IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > Sensor Management > SSH > Known Host RSA1 Keys**, and then click **Add** to add a known host key to the list.
- Step 3** In the IP Address field, enter the IP address of the host for which you are adding a key.
- Step 4** Click **Retrieve Host Key**. The IME 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 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 $(2^{\text{length}} < \text{modulus} < (2^{\text{length} + 1}))$). The RSA algorithm uses the public modulus to encrypt data.

**Tip**

To discard your changes and close the Add Known Host RSA1 Key dialog box, click **Cancel**.

Step 8 Click **OK**. The new key appears in the known host keys list in the Known Host RSA1 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.

**Tip**

To discard your changes and close the Edit Known Host RSA1 Key dialog box, click **Cancel**.

Step 11 Click **OK**. The edited key appears in the known host keys list in the Known Host RSA1 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 RSA1 Keys pane.

**Tip**

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

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

Generating the Sensor Key

**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 SSHv1 or SSHv2 host key the first time it starts up. It is displayed in the Sensor Key pane along with the Bubble Babble. Click **Generate Key** to replace that key with a new key.

**Note**

If you generate a new key, you must update the known hosts tables on remote systems with the new key to prevent connection failures.

Field Definitions

The Sensor Key pane displays the current sensor RSA1 (SSHv1) and RSA (SSHv2) host keys. Press **Generate Key** to generate a new sensor SSH host key.

Displaying and Generating the Sensor SSH Host Key**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.

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

- Step 1** Log in to the IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > Sensor Management > 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?
- 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.

Understanding Certificates

**Note**

The IDM configuration component is embedded in the IME.

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

**Caution**

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

**Note**

The 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 the 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 the 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 about the master blocking sensor, see [Configuring the Master Blocking Sensor, page 15-24](#).

Configuring Trusted Hosts

This section describes how to configure trusted hosts, and contains the following sections.

- [Trusted Hosts Pane, page 14-13](#)
- [Trusted Hosts Pane Field Definitions, page 14-13](#)
- [Add Trusted Host Dialog Box Field Definitions, page 14-13](#)
- [Adding Trusted Hosts, page 14-13](#)

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. The IME 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.

Trusted Hosts Pane Field Definitions

The following fields are found in the Trusted Hosts pane:

- IP Address—Specifies the IP address of the trusted host.
- SHA1—Specifies the 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—Specifies the 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 the IME using an account with administrator privileges.
- Step 2** Choose **Configuration** > *sensor_name* > **Sensor Management** > **Certificates** > **Trusted Hosts**, and then click **Add** to add a trusted host to the list.
- 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.

**Tip**

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

- Step 5** Click **OK**. The IME retrieves the certificate from the host whose IP address you entered in Step 3. The new trusted host appears in the trusted hosts list in the Trusted Hosts pane. A dialog box informs you that the IME is communicating with the sensor:

Communicating with the sensor, please wait ...

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

The new host was added successfully.

Step 6 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 7 Click **OK**.

Step 8 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 9 Click **Apply** to apply your changes and save the revised configuration.

Adding Trusted Root Certificates



Note Support for trusted root certificates is valid for IPS 7.3(2)E4 and later.

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

- [Trusted Root Certificates Pane, page 14-14](#)
- [Trusted Root Certificates Field Definitions, page 14-15](#)
- [Add and Update Trusted Root Certificates Dialog Box Field Definitions, page 14-15](#)
- [Adding and Updating Trusted Root Certificates, page 14-15](#)

Trusted Root Certificates Pane

Use the Trusted Root Certificates pane to add trusted root certificates used to validate the root certificate chain of the updater server when updates are downloaded. The IPS validates whether the root certificate in the certificate chain is signed by a trusted root CA. For example, the TLS root certificates obtained during signature updates from the Cisco server and global correlation server will be validated.

In the Network pane, you can enable strict TLS certificate checking or you can disable it and the root certificate of the certificate chain will not be validated against the root certificate store. The default is disabled.

If the root CA validation fails, the TLS connection is not established and signature updates and global correlation updates are not downloaded from the update server.

The Trusted Root Certificates pane lists all trusted root certificates that you have added. You can use SCP or HTTPs protocol to add and update the trusted root certificates. Global correlation updates use SHA-384.



Note TLS root certificates installed on the sensor are preserved across software upgrades and recovery.

**Note**

You can add and update entries from the list, but you cannot delete them.

For More Information

For information on enabling strict TLS server validation, see [Configuring Network Settings, page 6-1](#).

Trusted Root Certificates Field Definitions

The following fields are found in the Trusted Root Certificates pane:

- **TLS Certificate Name**—Specifies the common name of the certificate.
- **Expiry Date**—Specifies the date the certificate expires.
- **Issued To**—Specifies the specific domain name to which the certificate is issued.
- **Issued By**—Specifies the entity that verified the information and issued the certificate.
- **SHA1-Fingerprint**—Specifies the Secure Hash Algorithm. SHA1 is a cryptographic message digest algorithm.
- **MD5-Fingerprint**—Specifies the Message Digest 5 encryption. MD5 is an algorithm used to compute the 128-bit hash of a message.

Add and Update Trusted Root Certificates Dialog Box Field Definitions

The following fields are found in the Add/Update Trusted Root Certificate dialog box:

- **URL**—Specifies the protocol and path from where the trusted root certificate can be downloaded.

**Note**

Make sure the sensor has access to the server.

- **Username**—Specifies the login name on the server where the certificate is located.

Password—Specifies the password of the user logging into the server where the certificate is located.

Adding and Updating Trusted Root Certificates

To add or update trusted root certificates, follow these steps:

- Step 1** Log in to the IDM using an account with administrator privileges.
- Step 2** Choose **Configuration > Sensor Management > Certificates > Trusted Root Certificates**, and then click **Add/Update** to add or update a trusted root certificate.
- Step 3** In the URL field, choose the protocol (SCP or HTTPs) and enter the path where the sensor can find the trusted root certificate.

**Note**

Make sure the sensor has access to the server.

- Step 4** In the Username field, enter the login name on the server where the certificate is located.

Step 5 In the Password field, enter the password of the username on the server where the certificate is located



Tip To discard your changes and close the Add/Update Trusted Root Certificate dialog box, click **Cancel**.

Step 6 Click **OK**. The new/updated trusted root certificate appears in the list.

Step 7 To refresh the list, click **Refresh**.

Generating the Server Certificate



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.

Field Definitions

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

Displaying and Generating the Server Certificate



Note 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.

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

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

Step 2 Choose **Configuration > sensor_name > 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?

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