Configuring SSH and Certificates

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

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.

> **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.

✎
Note   SSH never sends passwords in clear text.

Configuring Authorized Keys

This section describes how to configure authorized keys for the sensor, 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 Field Definitions

The following fields are found in the Authorized Keys pane:

- 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]*$.

Add and Edit Authorized Key Dialog Boxes Field Definitions

The following fields are found 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 the IDM using an account with administrator privileges.

Step 2   Choose **Configuration > Sensor Management > SSH > Authorized 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 ^ 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.

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

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.

Configuring Known Host Keys

This section describes how to configure 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.

The IDM attempts to retrieve the known host key from the host specified by the IP address. If successful, the IDM populates the Add Known Host 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 Keys Pane Field Definitions

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

- 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 $(2 \wedge length) < modulus < (2 \wedge (length + 1))$). 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 Key Dialog Boxes Field Definitions

The following fields are found 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 $(2 \wedge length) < modulus < (2 \wedge (length + 1))$). 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 the IDM using an account with administrator privileges.

Step 2   Choose **Configuration > Sensor Management > SSH > Known Host 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 IDM 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 $(2 \wedge \text{length}) < \text{modulus} < (2 \wedge (\text{length} + 1)))$. 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 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.

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

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.

Generating the Sensor Key

This section describes how to obtain a sensor 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.

Field Definitions

The Sensor Key pane displays the sensor SSH host key. Press **Generate Key** to generate 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 the IDM using an account with administrator privileges.

Step 2   Choose **Configuration > 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?
```

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.

Understanding Certificates

⚠️

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

✎

Note   The IDM is enabled by default to use TLS and SSL. We highly recommend that you use TLS and SSL.

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.

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 on validating certificates, see Validating the CA, page 1-7.

Configuring Trusted Hosts

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

- Trusted Hosts Pane, page 12-9
- Trusted Hosts Pane Field Definitions, page 12-9
- Add Trusted Host Dialog Box Field Definitions, page 12-9
- Adding Trusted Hosts, page 12-10

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 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 adding external product interfaces, see Chapter 15, "Configuring External Product Interfaces."

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 the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > 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 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 in the Trusted Hosts pane. A dialog box informs you that the IDM is communicating with the sensor:

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

A dialog box provides status about whether the 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**. 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.

Generating the Server Certificate

This section describes how to generate the 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.

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 the 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.