Working With Trusted TLS Certificates

Viewing and Removing Trusted TLS Certificates

Restriction

Trusted TLS certificates cannot be edited.

Procedure

Step 1 Select **System > Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page with the following information:

- Label
- Owner
- Issuer

Step 2 To add a trusted TLS certificate, click **Add**. See Adding a Trusted TLS Certificate.

Step 3 To see more information about a trusted TLS certificate, click the underlined name of the certificate. See Viewing a Trusted TLS Certificate.

Step 4 To remove a trusted TLS certificate, do the following:

a. Select the check box next to the trusted TLS certificate to remove.

b. Click **Remove**.

Related Topics

- Back to the Working With Trusted TLS Certificates menu page
- Adding a Trusted TLS Certificate
- Viewing a Trusted TLS Certificate

Adding a Trusted TLS Certificate

Add a trusted TLS certificate either by uploading a file or by uploading text.

Before You Begin

If uploading a file, upload the trusted TLS certificate to a location where you can find it easily.

Restriction

TLS certificates that you paste into the text window must be in PEM format. Certificate files that you upload to Cisco Unified SRST Manager may be in PEM or DER format.

Procedure

Step 1 Select **System > Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page.

Step 2 Click **Add**.

The system displays the Add Trusted TLS Certificate page.

Step 3 Enter the keystore label for this trusted TLS certificate. This is a unique identifier for this certificate.

Step 4 Select **Certificate File** if the trusted TLS certificate will be a file or select **Certificate Text** if the certificate will be uploaded as plain text.

Step 5 Do one of the following:

- If you selected Certificate File, click **Browse**. Navigate to the file, highlight it, and click **Open**.
- If you selected Certificate Text, paste the contents of the trusted TLS certificate in the text box.

Step 6 Click **Update**.

Related Topics

- Back to the Working With Trusted TLS Certificates menu page
- Viewing and Removing Trusted TLS Certificates
- Viewing a Trusted TLS Certificate

Viewing a Trusted TLS Certificate

Procedure

Step 1 Select **System > Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page.

Step 2 To see more information about a trusted TLS certificate, click the underlined name of the certificate. The system displays the <*name_of_trusted_TLS_certificate*> Trusted Certificate Entry page with the following information:

Parameter	Description
Owner Info	
Common Name (CN)	The X.500 common name attribute, which contains the name of an object. If the object corresponds to a person, it is typically the person's full name. This is usually the hostname of the server to which you are talking.
Organization (O)	The name of an organization.
Organization (OU)	The name of an organizational unit.
Location (L)	The name of a locality, such as a city, county or other geographic region.
State (ST)	The full name of a state or province.
Country (C)	The country name. A two-letter ISO 3166 country code.
Issuer Info—The entity that verified the information and issued the certificate.	
Common Name (CN)	The X.500 common name attribute, which contains the name of an object. If the object corresponds to a person, it is typically the person's full name. This is usually the hostname of the server to which you are talking.
Organization (O)	The name of an organization.
Organization (OU)	The name of an organizational unit.
Location (L)	The name of a locality, such as a city, county or other geographic region.
State (ST)	The full name of a state or province.
Country (C)	The country name. A two-letter ISO 3166 country code.
Validity	
Valid From	The date from which the certificate is first valid.
Expires On	The date on which the certificate expires.

Parameter	Description
Fingerprint	
MD5	The fingerprint (also known as thumbprint) is a cryptographic hash value that uniquely identifies the certificate. The MD5 message-digest algorithm is a widely used cryptographic hash function with a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.

Step 3 To return to the Trusted TLS Certificates page, click **Back**.

Related Topics

- Back to the Working With Trusted TLS Certificates menu page
- Viewing and Removing Trusted TLS Certificates
- Adding a Trusted TLS Certificate