Loading Certificates and Keys Onto Expressway

The Expressway uses standard X.509 certificates. The certificate information must be supplied to the Expressway in PEM format. Typically three elements are loaded:

- The server certificate (which is generated by the certificate authority, identifying the ID of the certificate holder, and should be able to act as both a client and server certificate).
- The private key (used to sign data sent to the client, and decrypt data sent from the client, encrypted with the public key in the server certificate). This must only be kept on the Expressway and backed up in a safe place – security of the TLS communications relies upon this being kept secret.
- A list of certificates of trusted certificate authorities.

Note New installations of Expressway software (from X8.1 onwards) ship with a temporary trusted CA, and a server certificate issued by that temporary CA. We strongly recommend that you replace the server certificate with one generated by a trusted certificate authority, and that you install CA certificates for the authorities that you trust.

Note On Expressway-C and Expressway-E, we recommend that you do not upload multiple CA certificates with the same common name. This is because the endpoints may fail to log in if Expressway is configured to authenticate endpoints using an external IdP.

Warning Warning messages that may be displayed

From X8.10, the upload mechanism for server certificates (**Maintenance** > **Security** > **Server certificate**) displays a warning if the certificate fails to meet certain criteria. Cases when the warning is displayed include:

- Certificate does not have an acceptable level of security.
- Certificate is missing a common name (CN) attribute. An alarm is also raised in this case. Because some Expressway services don't work without the common name (MRA, Jabber Guest, and the Web Proxy for Cisco Meeting Server).
- The certification authority (CA) or certificate revocation list (CRL) is not recognized.

The certificate upload is not prevented.

This chapter explains the following:

Loading a Server Certificate and Private Key Onto Expressway

The Expressway's server certificate is used to identify the Expressway when it communicates with client systems using TLS encryption, and with web browsers over HTTPS.

As well as these instructions, a video demonstration of the process provided by Cisco TAC engineers is available on the Expressway/VCS Screencast Video List page.

Note We recommend you install the CA certificate first before installing the server certificate. Otherwise, the server certificate will fail to load.

To upload a server certificate:

1. Go to **Maintenance** > **Security** > **Server certificate**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the **server certificate** PEM file.

Note Make sure to upload the Server certificate file with a valid FQDN.

   a. If you upload a certificate with a hostname or IP in the SAN field, the upload fails with the error "File upload failed.: Subject alternative name must be a valid FQDN".

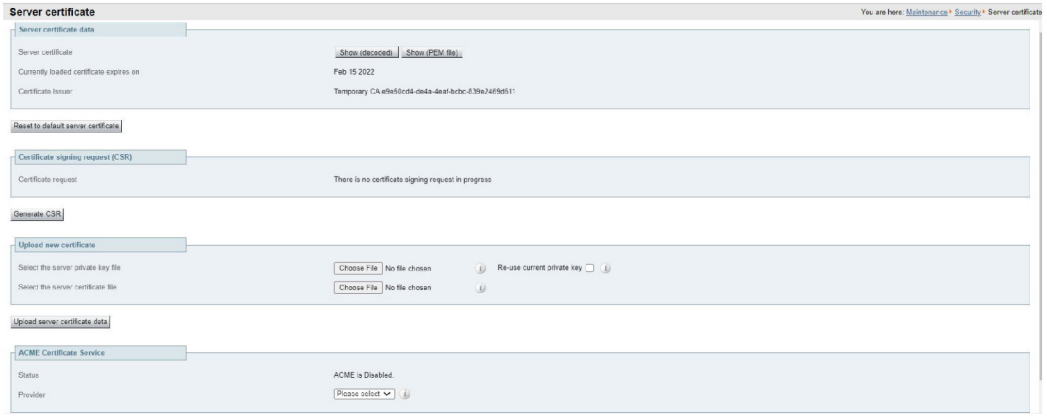
   b. If you upload a certificate with a hostname or IP in the CN (common name) field, the upload fails with the error "File upload failed.: Common name must be a valid FQDN".

3. If you used an external system to generate the Certificate Signing Request (CSR) you must also upload the **server private key** PEM file that was used to encrypt the server certificate. (The private key file will have been automatically generated and stored earlier if the Expressway was used to produce the CSR for this server certificate.)
   - The **server private key** PEM file must not be password protected.
   - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload server certificate data.**
   - When you generate a CSR in X7, the application puts **csr.pem** and **privkey_csr.pem** into **/tandberg/persistent/certs**.
   - When you generate a CSR in X8, the application puts **csr.pem** and **privkey.pem** into **/tandberg/persistent/certs/generated_csr**.

Re-use current private key check box - According to your local security requirements, check the **Re-use current private key** check box if you don't want a new private key. You may want to do this if you are extending the validity of your current certificate or re-issuing a previously generated CSR.

5. Use the **Provider** drop-down list in the **ACME Certificate Service** section to select trusted ACME clients used for signing of CSRs.

If you want to upgrade from X7 and have an unsubmitted CSR, then we recommend you to discard the CSR before upgrade, and then regenerate the CSR after upgrade.

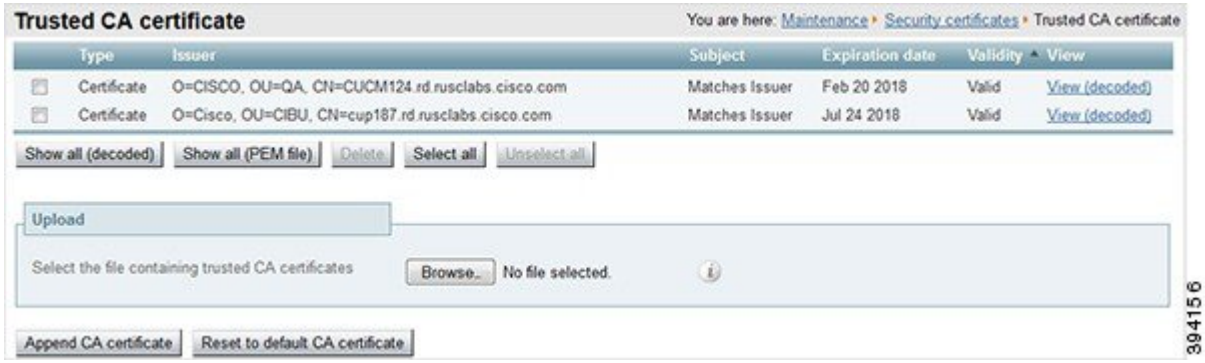


456940

Managing the Trusted CA Certificate List

The Trusted CA certificate page (**Maintenance** > **Security** > **Trusted CA certificate**) allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway. When a TLS connection to Expressway mandates certificate verification, the certificate presented to the Expressway must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

- To upload a new file containing one or more CA certificates, **Browse** to the required PEM file and click **Append CA certificate**. This will append any new certificates to the existing list of CA certificates. If you are replacing existing certificates for a particular issuer and subject, you have to manually delete the previous certificates.
- To replace all of the currently uploaded CA certificates with the system's original list of trusted CA certificates, click **Reset to default CA certificate**.
- To view the entire list of currently uploaded trusted CA certificates, click **Show all (decoded)** to view it in a human-readable form, or click **Show all (PEM file)** to view the file in its raw format.
- To view an individual trusted CA certificate, click **View (decoded)** in the row for the specific CA certificate.
- To delete one or more CA certificates, tick the box(es) next to the relevant CA certificate(s) and click **Delete**.



Note this Recommendation

The maximum number of Certificate Authority (CAs) that can be uploaded/supported to the Expressway *trust store* is 1000.

Changing an Existing Server Certificate

Important This procedure on “Changing an Existing Server Certificate” does not apply to server certificates generated through “Let's Encrypt” certificate authority.

Before you begin

Generate Certificate Signing Request (CSR) before changing the server certificate. For more information, see Generating a Certificate Signing Request.

Note Set the Transport Line Signaling (TLS) verify mode to *Permissive* before changing the server certificate. This will protect against any errors encountered during certificate changes. Revert the TLS verify mode to *Enforce* after the changes.

Procedure

Step 1 Add the new Trusted CA certificate on all nodes in the cluster.

Step 2 If "TLS Verification mode" in **System** > **Clustering** is set to *Enforce*, change the "TLS Verification mode" to *Permissive*. Click **Save**.

Step 3 Update the Server Certificate on all the nodes in the cluster.

Step 4 Restart the nodes one at a time.

Note Allow each node to recover before restarting the next node.

Step 5 If you change the "TLS Verification mode" from *Enforce* to *Permissive* in **step 2**, change it back to *Enforce*.

Step 6 Delete any unwanted CA certificates if they are no longer required.