Generating a Certificate Signing Request

Generating a CSR

A Certificate Signing Request (CSR) contains the identity information about the owner of a private key. It can be passed to a third-party or internal certification authority for generating a signed certificate, or it can be used in conjunction with an application such as ACME, Microsoft Certification Authority, or OpenSSL.

Creating a CSR Using Expressway

The Expressway can generate server certificate signing requests. This removes the need to use an external mechanism to generate and obtain certificate requests.

To generate a CSR:

Step 1 Go to **Maintenance** > **Security** > **Server certificate**.

Step 2 Click **Generate CSR** to go to the **Generate CSR** page.

Step 3 Enter the required properties for the certificate:

a. See Server Certificates and Clustered Systems, if your Expressway is part of a cluster.

b. See the "Server Certificates Requirements for Unified Communications" section, if this Expressway is part of a Unified Communications solution.

c. The certificate request includes, automatically, the public key that is used in the certificate and, the client and server authentication Enhanced Key Usage (EKU) extension.

Step 4 Click **Generate CSR**. The system produces a signing request and an associated private key. The private key is stored securely on the Expressway and cannot be viewed or downloaded. You must never disclose your private key, not even to the certificate authority.

Step 5 You are returned to the **Server certificate** page. From here you can:

a. **Download** the request to your local file system so that it can be sent to a certificate authority. You are prompted to save the file (the exact wording depends on your browser).

b. View the current request (click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format).

c. Use ACME to manually or automatically submit the CSR to a CA that signs ACME certificates.

Note

- Only one signing request can be in progress at any point of time. This is because the Expressway has to keep track of the private key file associated with the current request. To discard the current request and start a new request, click **Discard CSR**.
- From version X8.5.1 the user interface provides an option to set the Digest algorithm. The default is set to SHA-256, with options to change to SHA-1, SHA-384, or SHA-512.
- From version X8.10, you cannot select SHA-1.
- The Issuer and Subject fields of certificates returned by Let's Encrypt do not include attributes like State, Country, and Organisation. The Expressway UI still requires you to complete these fields in the CSR, even though the authority ignores them.

You must now use CSR to generate a signed PEM certificate file. You can pass it to a third-party or internal certification authority, or use it in conjunction with an application such as Microsoft Certification Authority (see Appendix 6: Authorize a Request and Generate a Certificate using Microsoft Certification Authority) or OpenSSL (see Operate as a Certificate Authority Using OpenSSL).

If you have multiple entries or FQDNs in the SAN (such as for MRA deployments), ensure that you ask for a multi-domain / multi-SAN certificate from your certificate authority, not a single certificate. Some authorities do not suggest this option unless you specifically request it.

When the signed server certificate is received back from the certificate authority, upload it to the Expressway as described in Load Certificates and Keys Onto Expressway.

Server Certificates and Clustered Systems

When a CSR is generated, a single request and private key combination is generated for that peer only.

If you have a cluster of Expressways, you must generate a separate signing request on each peer. Those requests must then be sent to the certificate authority and the returned server certificates uploaded to each relevant peer.

You must ensure that the correct server certificate is uploaded to the appropriate peer, otherwise the stored private key on each peer will not correspond to the uploaded certificate.