Manage Certificate Revocation Lists (CRLs)

Manage Certificate Revocation Lists

Certificate revocation list files (CRLs) are used by the Expressway to validate certificates presented by client browsers and external systems that communicate with the Expressway over TLS/HTTPS. A CRL identifies those certificates that have been revoked and can no longer be used to communicate with the Expressway.

We recommend that you upload CRL data for the CAs that sign TLS/HTTPS client and server certificates. When enabled, CRL checking is applied for every CA in the chain of trust.

Certificate Revocation Sources

The Expressway can obtain certificate revocation information from multiple sources:

- Automatic downloads of CRL data from CRL distribution points.
- Through OCSP (Online Certificate Status Protocol) responder URIs in the certificate to be checked (SIP TLS only).
- Manual upload of CRL data.
- CRL data embedded within the Expressway's **Trusted CA certificate** file.

Limitations and Usage Guidelines

The following limitations and usage guidelines apply:

- When establishing SIP TLS connections, the CRL data sources are subject to the **Certificate revocation checking** settings on the **SIP configuration** page.

- Automatically downloaded CRL files override any manually loaded CRL files (except for when verifying SIP TLS connections, when both manually uploaded or automatically downloaded CRL data may be used).
- When validating certificates presented by external policy servers, the Expressway uses manually loaded CRLs only.
- When validating TLS connections with an LDAP server for remote login account authentication, the Expressway only uses CRL data that has been embedded into the **Trusted CA certificate** (**Tools** > **Security** > **Trusted CA certificate**).

  For LDAP connections, Expressway does not download the CRL from Certificate Distribution Point URLs in the server or issuing CA certificates. Also, it does not use the manual or automatic update settings on the **CRL management** page.

Automatic CRL Updates

We recommend you to configure the Expressway for automatic CRL updates. This ensures that the latest CRLs are available for certificate validation.

To configure the Expressway for automatic CRL updates:

Procedure

Step 1 Go to **Maintenance** > **Security** > **CRL management**.

Step 2 Set **Automatic CRL updates** to *Enabled*

Step 3 Enter the set of **HTTP(S) distribution points** from where the Expressway can obtain CRL files.

- you must specify each distribution point on a new line
- only HTTP(S) distribution points are supported; if HTTPS is used, the distribution point server itself must have a valid certificate
- PEM and DER encoded CRL files are supported
- the distribution point may point directly to a CRL file or to ZIP and GZIP archives containing multiple CRL files
- the file extensions in the URL or on any files unpacked from a downloaded archive do not matter as the Expressway will determine the underlying file type for itself; however, typical URLs could be in the format:
  - http://example.com/crl.pem
  - http://example.com/crl.der
  - http://example.com/ca.crl
  - https://example.com/allcrls.zip
  - https://example.com/allcrls.gz

Step 4 Enter the **Daily update time** (in UTC). This is the approximate time of day when the Expressway will attempt to update its CRLs from the distribution points.

Step 5 Click **Save**.

Manual CRL Updates

You can upload CRL files manually to the Expressway. Certificates presented by external policy servers can only be validated against manually loaded CRLs.

To upload a CRL file:

Procedure

Step 1 Go to **Maintenence** > **Security** > **CRL management**.

Step 2 Click **Browse** and select the required file from your file system. It must be in PEM encoded format.

Step 3 Click **Upload CRL file**.

This uploads the selected file and replaces any previously uploaded CRL file.

Click **Remove revocation list** if you want to remove the manually uploaded file from the Expressway.

If a certificate authority's CRL expires, all certificates issued by that CA will be treated as revoked.

Online Certificate Status Protocol (OCSP)

The Expressway can establish a connection with an OCSP responder to query the status of a particular certificate.The Expressway determines the OCSP responder to use from the responder URI listed in the certificate being verified. The OCSP responder sends a status of “good”, “revoked” or “unknown” for the certificate.

The benefit of OCSP is that there is no need to download an entire revocation list. OCSP is supported for SIP TLS connections only.

Outbound communication from the Expressway-E is required for the connection to the OCSP responder. Check the port number of the OCSP responder you are using (port 80 or 443) and ensure that outbound communication is allowed to that port from the Expressway-E.

Configure Revocation Checking for SIP TLS Connections

You must configure how certificate revocation checking is managed for SIP TLS connections.

Procedure

Step 1 Go to **Configuration** > **SIP**.

Step 2 Scroll down to the **Certificate revocation checking** section and configure the settings accordingly:

Field	Description	Usage tips
Certificate revocation checking mode	Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment.	We recommend that revocation checking is enabled.
Use OCSP	Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking.	To use OCSP: • The X.509 certificate to be checked must contain an OCSP responder URI. • The OCSP responder must support the SHA-256 hash algorithm. If it is not supported, the OCSP revocation check and the certificate validation will fail.
Use CRLs	Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking.	CRLs can be used if the certificate does not support OCSP.
Allow CRL downloads from CDPs	Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed.	
Fallback behavior	Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted. *Treat as revoked*: treat the certificate as revoked (and thus do not allow the TLS connection). *Treat as not revoked*: treat the certificate as not revoked. Default: Treat as not revoked	*Treat as not revoked* ensures that your system continues to operate in a normal manner if the revocation source cannot be contacted, however it does potentially mean that revoked certificates are accepted.