



Cisco Expressway Certificate Creation and Use

Deployment Guide

Cisco Expressway X8.5.2

April 2015

Contents

Introduction	3
PKI introduction	3
Overview of certificate use on the Expressway	3
Certificate generation overview	4
Generating a certificate signing request (CSR)	5
Creating a CSR using Expressway	5
Server certificates and clustered systems	6
Server certificate requirements for Unified Communications	7
Cisco Unified Communications Manager certificates	7
Expressway certificates	7
Authorizing a request and generating a certificate using Microsoft Certification Authority	10
Loading certificates and keys onto Expressway	12
Loading a server certificate and private key onto Expressway	12
Managing the trusted CA certificate list	13
Managing certificate revocation lists (CRLs)	14
Certificate revocation sources	14
Automatic CRL updates	14
Manual CRL updates	15
Online Certificate Status Protocol (OCSP)	15
Configuring revocation checking for SIP TLS connections	15
Appendix 1: Troubleshooting	17
SIP TLS negotiation failures on neighbor and traversal zones	17
Subject Alternative Name fields longer than 999 characters	17
Certificates with key length of 8192 bits	17
Service failures when using mobile and remote access	17
Issues with ssh failures and unsupported OIDs	17
Appendix 2: Certificate generation using OpenSSL only	19
Creating a certificate request using OpenSSL	19
Operating as a Certificate Authority using OpenSSL	21
Configuring OpenSSL to act as a CA	21
Creating a Certificate Authority using OpenSSL	21
Creating a signed certificate using OpenSSL	22
Creating self-signed certificates using OpenSSL	23
Appendix 3: Converting a DER certificate file to PEM format	24
Appendix 4: Decoding certificates	27
Appendix 5: Configuring Windows Server Manager with a "client and server" certificate template	28
Document revision history	31

Introduction

This deployment guide provides instructions on how to create X.509 cryptographic certificates for use with the Cisco Expressway (Expressway), and how to load them into Expressway.

PKI introduction

Public Key Infrastructure (PKI) provides the mechanisms through which communications can be secured (encrypted and integrity protected) and identities can be verified. Underlying PKI is:

- **A public/private key pair:** a public key is used to encrypt data sent to a server, but only the private key (kept secret by the server) can be used to decrypt it.
- **Signatures of data:** data can be “signed” by a server, by using a combination of a cryptographic hash of the data and the server’s private key. A client can verify the signature by using the server’s public key and verifying the same hash. This ensures the data has been sent from the expected server, and has not been tampered with.
- **Certificates:** a certificate is a wrapper around a public key, and provides information about the owner of the key. This metadata is provided in X.509 format, and typically includes the server name and contact details for the owner.
- **A certificate chain:** a certificate can be signed by a Certificate Authority (CA) using its own private key. In turn, therefore, a certificate can be verified as being signed by a CA by checking the signature against the CA’s certificate (public key). Web browsers and other clients have a list of CA certificates that they trust, and can thus verify the certificates of individual servers.

Transport Layer Security (TLS) is the standard mechanism for securing a TCP connection between hosts on a TCP/IP network. For example, secure HTTP (HTTPS) uses TLS to encrypt and verify traffic. To establish a TLS connection:

1. An initial TCP connection is made, and the client sends its capabilities (including cipher suites) and a random number.
2. The sever responds with its choice of those capabilities, another random number, and its certificate.
3. The client verifies that the server certificate was issued (signed) by a CA that it trusts, and has not been revoked.
4. The client sends a “pre-master secret”, encrypted with the server’s public key.
5. This pre-master secret, combined with the exchanged random numbers (to prevent replay attacks), is used to generate a “master secret”, with which the remaining communications of this TLS session are encrypted between the client and server.

The following sections describe how these PKI components can be used with the Expressway.

Overview of certificate use on the Expressway

Expressway needs certificates for:

- Secure HTTP with TLS (HTTPS) connectivity
- TLS connectivity for SIP signaling, endpoints and neighbor zones
- Connections to other systems such as Unified CM, Cisco TMS, LDAP servers and syslog servers

It uses its list of trusted Certificate Authority (CA) certificates and associated certificate revocation lists (CRLs) to validate other devices connecting to it.

It uses the Server Certificate and the Private key to provide a signed certificate to provide evidence that the Expressway is the device it says it is. This can be used with neighboring devices such as Microsoft Lync or Unified CM, as well as administrators using the web interface.

A certificate identifies the Expressway. It contains names by which it is known and to which traffic is routed. If the Expressway is known by multiple names for these purposes, such as if it is part of a cluster, this must be represented in the X.509 subject data, according to the guidance of RFC5922. The certificate must contain the FQDN of both the Expressway itself and of the cluster. If a certificate is shared across cluster peers, it must list all possible peer FQDNs. The following lists show what must be included in the X.509 subject, depending on the deployment model chosen.

If the Expressway is not clustered:

- Subject Common Name = FQDN of Expressway
- Subject Alternate Names = leave blank

If the Expressway is clustered, with individual certificates per Expressway:

- Subject Common Name = FQDN of Expressway
- Subject Alternate Names = FQDN of Expressway, FQDN of cluster

Wildcard certificates manage multiple subdomains and the services names they support, they can be less secure than SAN (Subject Alternate Name) certificates. Expressway does not support wildcard certificates.

Certificate generation overview

X.509 certificates may be supplied from a third party, or may be generated by a certificate generator such as OpenSSL or a tool available in applications such as Microsoft Certification Authority. Third-party certificates supplied by recognized certificate authorities are recommended, although Expressway deployments in controlled or test environments can use internally generated certificates.

Certificate generation is usually a 3-stage process:

- Stage 1: generate a private key
- Stage 2: create a certificate request
- Stage 3: authorize and create the certificate

This document presents alternative methods of generating the root certificate, client/server certificate for the Expressway, and private key:

- [Generating a certificate signing request \(CSR\) \[p.5\]](#) describes how to use the Expressway itself to generate the private key and certificate request.
- [Appendix 2: Certificate generation using OpenSSL only \[p.19\]](#) documents the OpenSSL-only process, which could be used with a third party or internally managed CA.

For mutual TLS authentication the Expressway **Server** certificate must be capable of being used as a **Client** certificate as well, thus allowing the Expressway to authenticate as a client device to a neighboring server (see [Appendix 5: Configuring Windows Server Manager with a "client and server" certificate template \[p.28\]](#)).

Note: It is worth noting that changes are being introduced to the way that dates are handled from 2050, and certificates that have expiry dates beyond that can cause operational issues.

Generating a certificate signing request (CSR)

A 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 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:

1. Go to **Maintenance > Security certificates > Server certificate**.
2. Click **Generate CSR** to go to the **Generate CSR** page.
3. Enter the required properties for the certificate.
 - See [Server certificates and clustered systems \[p.6\]](#) if your Expressway is part of a cluster.
 - See [Server certificate requirements for Unified Communications \[p.7\]](#) if this Expressway is part of a Unified Communications solution.
 - The certificate request includes automatically the public key that will be used in the certificate, and the client and server authentication Enhanced Key Usage (EKU) extension.
4. Click **Generate CSR**. The system will produce 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.
5. You are returned to the **Server certificate** page. From here you can:
 - **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).
 - 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).

Note:

- Only one signing request can be in progress at any one 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.
- The certificate signing request storage location changed in X8.
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**.
If you want to upgrade from X7 and have an unsubmitted CSR, then we recommend discarding the CSR before upgrade, and then regenerating the CSR after upgrade.

You must now authorize the request and 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 [Authorizing a request and generating a certificate using Microsoft Certification Authority \[p.10\]](#)) or OpenSSL (see [Operating as a Certificate Authority using OpenSSL \[p.21\]](#)).

When the signed server certificate is received back from the certificate authority, it must be uploaded to the Expressway as described in [Loading certificates and keys onto Expressway \[p. 12\]](#).

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.

Server certificate requirements for Unified Communications

Cisco Unified Communications Manager certificates

The two Cisco Unified Communications Manager certificates that are significant for Mobile and Remote Access are the *CallManager* certificate and the *tomcat* certificate. These are automatically installed on the Cisco Unified Communications Manager and by default they are self-signed and have the same common name (CN).

We recommend using externally-signed certificates for best end-to-end security between external endpoints and internal endpoints. However, if you do use self-signed certificates, the two certificates must have different common names. This is because the Expressway does not allow two self-signed certificates with the same CN. If the *CallManager* and *tomcat* self-signed certs have the same CN in the Expressway's trusted CA list, then it can only trust one of them. This means that either secure HTTP or secure SIP, between Expressway-C and Cisco Unified Communications Manager, will fail.

Expressway certificates

The Expressway certificate signing request (CSR) tool prompts for and incorporates the relevant subject alternate name (SAN) entries as appropriate for the Unified Communications features that are supported on that Expressway.

The following table shows which CSR alternative name elements apply to which Unified Communications features:

CSR SAN element	Mobile and remote access	Jabber Guest	XMPP federation
Unified CM registrations domains	✓ (Expressway-E only)	X	X
XMPP federation domains	X	X	✓ (Expressway-E only)
IM and Presence chat node aliases (federated group chat)	X	X	✓
Unified CM phone security profile names	✓ (Expressway-C only)	X	X

Note:

- A new Expressway-C certificate may need to be produced for the Expressway-C if chat node aliases are added or renamed, such as when an IM and Presence node is added or renamed, or if new TLS phone security profiles are added.
- A new Expressway-E certificate must be produced if new chat node aliases are added to the system, or if the Unified CM or XMPP federation domains are modified.
- You must restart the Expressway for any new uploaded server certificate to take effect.

More details about the individual feature requirements per Expressway-C / Expressway-E are described below.

Expressway-C server certificate requirements

The Expressway-C server certificate needs to include the following elements in its list of subject alternate names:

- Unified CM phone security profile names:** the names of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.

Having the secure phone profiles as alternative names means that Unified CM can communicate via TLS with the Expressway-C when it is forwarding messages from devices that use those profiles.
- IM and Presence chat node aliases (federated group chat):** the **Chat Node Aliases** (e.g. chatroom1.example.com) that are configured on the IM and Presence servers. These are required only for Unified Communications XMPP federation deployments that intend to support group chat over TLS with federated contacts.

The Expressway-C automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM&P servers.

We recommend that you use DNS format for the chat node aliases when generating the CSR. You must include the same chat node aliases in the Expressway-E server certificate's alternative names.

Figure 1: Entering subject alternative names for security profiles and chat node aliases on the Expressway-C's CSR generator

The screenshot shows a web interface for configuring subject alternative names. It includes a title bar 'Alternative name' and four input fields with corresponding labels and information icons:

- Additional alternative names (comma separated):** An empty text input field.
- IM and Presence chat node aliases (federated group chat):** A text input field containing 'chatnode1.xmpp.example.com,chatnode2.xmpp.example.com' and a 'Format' dropdown menu set to 'DNS'.
- Unified CM phone security profile names:** A text input field containing 'DX80TLSprofile.example.com'.
- Alternative name as it will appear:** A list of four entries: 'DNS:vcsc.example.com', 'DNS:chatnode1.xmpp.example.com', 'DNS:chatnode2.xmpp.example.com', and 'DNS:DX80TLSprofile.example.com'.

Expressway-E server certificate requirements

The Expressway-E server certificate needs to include the following elements in its list of subject alternate names:

- Unified CM registrations domains:** all of the domains which are configured on the Expressway-C for Unified CM registrations. They are required for secure communications between endpoint devices and Expressway-E.

Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. You may select *CollabEdgeDNS* format instead, which simply adds the prefix **co1lab-edge.** to the domain that you enter. This format is recommended if you do not want to include your top level domain as a SAN (see example in following screenshot).
- XMPP federation domains:** the domains used for point-to-point XMPP federation. These are configured on the IM&P servers and should also be configured on the Expressway-C as domains for XMPP federation.

Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the Expressway software.
- IM and Presence chat node aliases (federated group chat):** the same set of **Chat Node Aliases** as entered on the Expressway-C's certificate. They are only required for voice and presence deployments

which will support group chat over TLS with federated contacts.

Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the Expressway software.

Note that you can copy the list of chat node aliases from the equivalent [Generate CSR](#) page on the Expressway-C.

Figure 2: Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator

Alternative name	
Additional alternative names (comma separated)	<input type="text"/> ?
Unified CM registrations domains	<input type="text" value="example.com"/> Format: CollabEdgeDNS ?
XMPP federation domains	<input type="text" value="xmpp.example.com"/> Format: DNS ?
IM and Presence chat node aliases (federated group chat)	<input type="text" value="chatnode1.xmpp.example.com,chatnode2.xmpp.example.com"/> Format: DNS ?
Alternative name as it will appear	DNS:vcse.example.com DNS:collab-edge.example.com DNS:xmpp.example.com DNS:chatnode1.xmpp.example.com DNS:chatnode2.xmpp.example.com

Authorizing a request and generating a certificate using Microsoft Certification Authority

This section describes how to authorize a certificate request and generate a PEM certificate file using Microsoft Certification Authority.

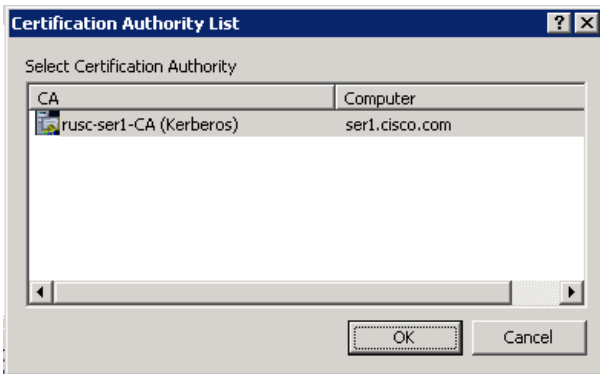
1. Copy the certificate request file (for example, **certcsr.der** if generated via OpenSSL) to a location, such as the desktop, on the server where the Microsoft Certification Authority application is installed.
2. Submit the certificate request from a command prompt:
 - To generate a certificate with Server Authentication and Client Authentication, which is required if you want to configure a neighbor or traversal zone with mutual authentication (**TLS verify mode**), type:


```
certreq -submit -attrib "CertificateTemplate:Webclientandserver"
C:\Users\\Desktop\certcsr.der
```

 See [Appendix 5: Configuring Windows Server Manager with a "client and server" certificate template \[p.28\]](#) for details about how to set up the **Webclientandserver** certificate template.
 - To generate a certificate with Server Authentication only, type:


```
certreq -submit -attrib "CertificateTemplate:WebServer"
C:\Users\\Desktop\certcsr.der
```

This triggers the Certification Authority window to open:

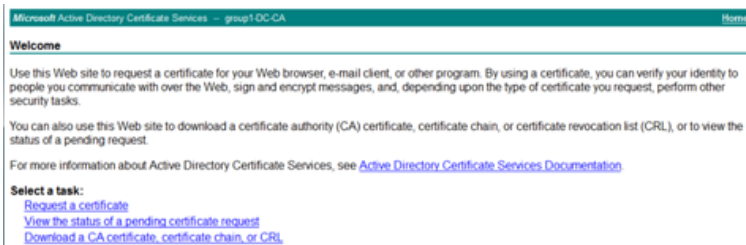


Note that the command must be run as the administrator user.

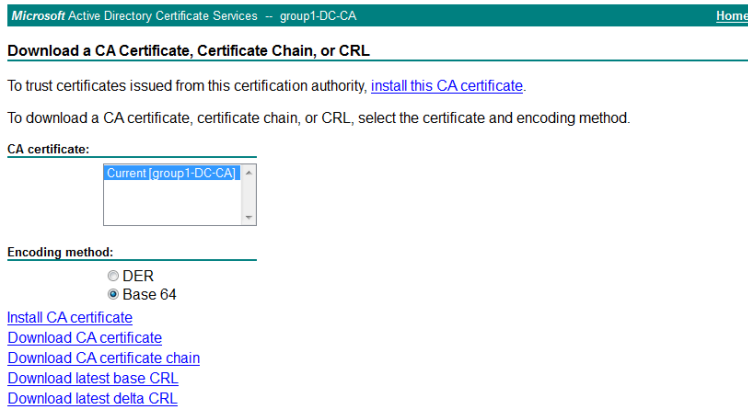
3. Select the **Certification Authority** to use (typically only one is offered) and click **OK**.
4. When requested, save the certificate (browse to the required folder if the default **Libraries > Documents** folder is not to be used) calling it **server.cer** for example.
5. Rename **server.cer** to **server.pem** for use with the Expressway.

Get the Microsoft CA certificate

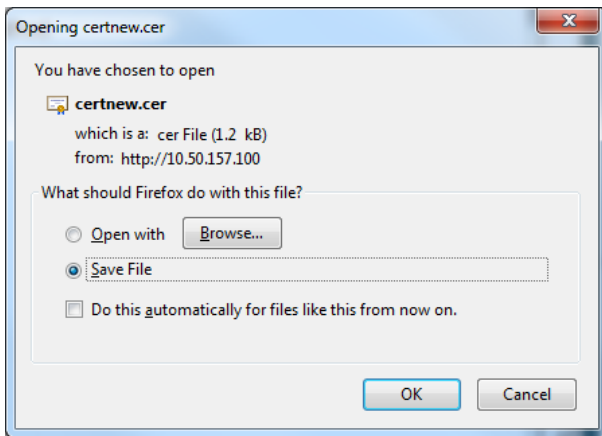
1. In your web browser, go to <IP or URL of the Microsoft Certificate Server>/certsrv and log in.



2. Select **Download a CA certificate, certificate chain or CRL**.



3. Select **Base 64**.
4. Select **Download CA certificate**.



5. Choose **Save File** and click **OK**.
6. Rename **certnew.cer** to **certnew.pem**.

Files **server.pem** and **certnew.pem** are now available.

Go to the [Loading certificates and keys onto Expressway \[p. 12\]](#) section in this document and upload **server.pem** and **certnew.pem** to Expressway.

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 3 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.

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.

To upload a server certificate:

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

The certificate signing request storage location changed in X8.

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**.

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

Server certificate You are here: [Maintenance](#) > [Security certificates](#) > [Server certificate](#)

Server certificate data

Server certificate PEM File [Show server certificate](#)

Currently loaded certificate expires on Aug 28 2029

[Reset to default server certificate](#)

Certificate signing request (CSR)

Certificate request PEM File [View](#) [Download](#)

Generated on May 23 2012

[Discard CSR](#)

Upload new certificate

Select the server private key file System will use the private key file generated at the same time as the CSR.

Select the server certificate file [Browse...](#) [?](#)

[Upload server certificate data](#)

Managing the trusted CA certificate list

The **Trusted CA certificate** page ([Maintenance > Security certificates > 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 on **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**.

Trusted CA certificate You are here: [Maintenance](#) > [Security certificates](#) > [Trusted CA certificate](#)

Type	Issuer	Subject	Expiration date	Validity	View	
<input type="checkbox"/>	Certificate	O=CISCO, OU=QA, CN=CUCM124.rd.rusclabs.cisco.com	Matches Issuer	Feb 20 2018	Valid	View (decoded)
<input type="checkbox"/>	Certificate	O=Cisco, OU=CIBU, CN=cup187.rd.rusclabs.cisco.com	Matches Issuer	Jul 24 2018	Valid	View (decoded)

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)

Upload

Select the file containing trusted CA certificates [Browse...](#) No file selected. [?](#)

[Append CA certificate](#) [Reset to default CA certificate](#)

Managing certificate revocation lists (CRLs)

Certificate revocation list (CRL) files 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

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 uses CRL data within the **Trusted CA certificate** only

Automatic CRL updates

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

To configure the Expressway to use automatic CRL updates:

1. Go to **Maintenance > Security certificates > CRL management**.
2. Set **Automatic CRL updates** to *Enabled*.
3. Enter the set of **HTTP(S) distribution points** from where the Expressway can obtain CRL files.

Note:

- 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>
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.
 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:

1. Go to **Maintenance > Security certificates > CRL management**.
2. Click **Browse** and select the required file from your file system. It must be in PEM encoded format.
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. See below for information on how to enable OCSP.

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 (typically this is port 80 or 443) and ensure that outbound communication is allowed to that port from the Expressway-E.

Configuring revocation checking for SIP TLS connections

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

1. Go to **Configuration > SIP**.
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.
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	<p>Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted.</p> <p><i>Treat as revoked</i>: treat the certificate as revoked (and thus do not allow the TLS connection).</p> <p><i>Treat as not revoked</i>: treat the certificate as not revoked.</p> <p>Default: <i>Treat as not revoked</i></p>	<i>Treat as not revoked</i> 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 will be accepted.

Appendix 1: Troubleshooting

SIP TLS negotiation failures on neighbor and traversal zones

If **TLS verify mode** is enabled, the neighbor system's FQDN or IP address, as specified in the **Peer address** field of the zone's configuration, is used to verify against the certificate holder's name contained within the X.509 certificate presented by that system. (The name has to be contained in either the Subject Common Name or the Subject Alternative Name attributes of the certificate.) The certificate itself must also be valid and signed by a trusted certificate authority.

Therefore when certificates have been generated with peer or cluster FQDNs, ensure that the zone's **Peer address** fields are configured with FQDNs rather than IP addresses.

Subject Alternative Name fields longer than 999 characters

If a secure traversal zone or Unified Communications zone fails to come up because of a TLS negotiation error, check the certificate for a long SAN field.

The Expressway does not parse SANs beyond 999 characters. So, if there are many alternative names on the certificate, the Expressway-E's FQDN may be outside of the portion that is read by the Expressway-C.

To avoid or workaround this issue, you need to make sure that any SANs that Expressway needs to trust are fully within the first 999 characters of the `subjectAltName`.

Certificates with key length of 8192 bits

SIP TLS zones may fail to become active if certificates with a key length of 8192 bits are used. We recommend using certificates with a key length of 4096 bits.

Service failures when using mobile and remote access

Unified Communications mobile and remote access services can fail due to certificate errors if you have uploaded a private key file that does not contain a trailing newline character.

Ensure that the private key file contains a trailing newline character.

Issues with ssh failures and unsupported OIDs

If you experience unknown ssh failures such as ssh tunnels failing to establish, please verify there are no unknown OIDs in the certificate. This can be done by checking that there are no undecoded numerical entries in the CN of the Issuer & Subject fields (from the GUI: **Maintenance** -> **Security Certificates** -> **Server Certificate** -> **Show(decoded)**) or from the console: `'openssl x509 -text -noout -in /tandberg/persistent/certs/server.pem'`

```
Invalid
```

```
subject=CN=blahdeblah,OU=IT
```

```
Security,O=BigBang,L=Washington,ST=District of
```

```
Columbia,C=US,1.3.6.1.4.1.6449.1.2.1.5.1 = #060C2B06010401B2310102010501
```

Valid

subject=CN=blahdeblah,OU=IT

Security,O=BigBang,L=Washington,ST=District of

Columbia,C=US,jurisdictionOfIncorporationLocalityName=Dover

For instance, currently, the only supported Extended Validation OIDs are:

- 1.3.6.1.4.1.311.60.2.1.1 jurisdictionOfIncorporationLocalityName
- 1.3.6.1.4.1.311.60.2.1.2 jurisdictionOfIncorporationStateOrProvinceName
- 1.3.6.1.4.1.311.60.2.1.3 jurisdictionOfIncorporationCountryName.

Appendix 2: Certificate generation using OpenSSL only

This section describes the process for generating a private key and certificate request for the Expressway using OpenSSL. This is a generic process that relies only on the free OpenSSL package and not on any other software. It is appropriate when certificates are required for interfacing with neighboring devices for test purposes, and for providing output to interact with Certificate Authorities.

The output for the certificate request generation process can be given to a Certificate Authority which may be internal or external to the organization, and which can be used to produce the X.509 certificates required by the Expressway to authenticate itself with neighboring devices.

This section also briefly describes how OpenSSL could be used to manage a private Certificate Authority, but does not intend to be comprehensive. Various components of these processes can be used when interfacing with third party CAs.

OpenSSL and Mac OS X or Linux

OpenSSL is already installed on Mac OS X, and is usually installed on Linux.

OpenSSL and Windows

If you do not have OpenSSL already installed, this is available as a free download from <http://www.openssl.org/related/binaries.html>.

Choose the relevant 32 bit or 64 bit OpenSSL - the 'Light' version is all that is needed.

If you receive a warning while installing OpenSSL that C++ files cannot be found, load the "Visual C++ Redistributables" also available on this site and then re-load the OpenSSL software.

Creating a certificate request using OpenSSL

This process creates a private key and certificate request for the server that can then be validated by a CA. This could be a CA that has been created and managed locally, or a third-party CA.

Note:

- This method to create a CSR should only be used if you have a good knowledge of working with OpenSSL as there is a potential for entering incorrect commands (especially with numerous SAN entries). Missing relevant SAN entries would require recreating the certificate at a later date.
- 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.

To generate the CSR from the command line with OpenSSL use these instructions:

1. SSH to the Expressway and log in as root.
2. Make a new directory to do the work in - `mkdir /tmp/certtemp`
3. Move in to this directory - `cd /tmp/certtemp`
4. Copy the Open SSL configuration file we use for CSR to this directory, as we need to edit it (**Note: Keep the dot at the end**) - `cp /etc/openssl/csrreq.cnf .`
5. Open the file for editing – `vi csrreq.cnf`

6. Find the line “`default_md = sha1`” and edit it so that it reads “`default_md = sha256`”
7. Uncomment the line “`# req_extensions = v3_req`” by removing the # at the start of it
8. Make sure that the line “`extendedKeyUsage=serverAuth, clientAuth`” is present within the section [v3_req].
9. Find the line “`subjectAltName = ${ENV::CSR_ALT_NAME}`” and replace it such that it lists what you want in the Subject Alternative Names in the certificate e.g. “`subjectAltName = DNS:peer1vcs.example.com,DNS:peer2vcs.example.com,DNS:ClusterFQDN.example.com`”. Make sure you add all the additional relevant entries. For MRA this may comprise:
 - a. **Expressway E:** `DNS:<CM domain name>, DNS:<XMPP federation domain>, DNS:<federation chat alias 1>, DNS:<federation chat alias 2>`, etc.
 - b. **Expressway C:** `DNS:<secure profile name 1>, DNS:<secure profile name 2>`, etc.
10. Now save the file and exit.
11. Run the following OpenSSL command to generate a new CSR and Private key for the VCS “`openssl req -nodes -newkey rsa:4096 -keyout privatekey.pem -out myrequest.csr -config csrreq.cnf`” changing the `rsa:nnnn` if required. (nnnn = keylength, recommended number is 4096).
12. On the screen you will get output similar to what follows, some things can & should be left blank. When this is complete, there will be two new files, **myrequest.csr** and **privatekey.pem**. The required fields that should be completed are:
 - Country
 - State and province
 - Locality name
 - Organization name
 - Common name - this is the Expressway cluster FQDN if the certificate is for a cluster of Expressways or it is the FQDN of the Expressway if the certificate is for a single Expressway
 - Email address - optional, can leave blank
 - A challenge password - optional, can leave blank
 - An optional company name - optional, can leave blank

Generating a 4096 bit RSA private key

```
.....++
.....++
writing new private key to 'privatekey.pem'
```

```
-----
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

```
-----
```

```
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:Berkshire
Locality Name (eg, city) []:Reading
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:CIBU
Common Name (eg, YOUR name) []:rusc01-et-xm030.rusclabs.cisco.com
Email Address []:
```

13. (Optional) If you want to validate the DNS entries have been entered correctly into the request, the **myrequest.csr** file can be decoded using the command: `openssl req -text -noout -in myrequest.csr`
14. Submit the CSR to your chosen Certificate Authority, who will provide the public certificate.
15. Upload the public certificate to the VCS via the **Maintenance > Security certificates > Server certificate** webpage, “**Select the server certificate file**” entry box.
16. Upload the **privatekey.pem** to the VCS via the **Maintenance > Security certificates > Server certificate** webpage, “**Select the server private key file**” entry box.

The **privatekey.pem** should be kept safe.

Operating as a Certificate Authority using OpenSSL

A major deployment is likely to make use of a third-party certificate authority, or already have one internal to an organization’s IT department. However, you can use OpenSSL to manage certificates in a private certificate authority as outlined below.

If you have already configured OpenSSL to act as a CA, go to section [Creating a signed certificate using OpenSSL \[p.22\]](#).

Configuring OpenSSL to act as a CA

OpenSSL is powerful software, and when operating as a CA, requires a number of directories and databases to be configured for tracking issued certificates.

The list of directories and files can be found in the openssl configuration file under the section [**CA_default**]. By default, the files/directories required to be created are:

- A **demoCA** directory in the current directory, with 3 subdirectories **certs**, **newcerts** and **private**.
- An empty file called **index.txt** in the **demoCA** directory.
- A file called **serial** in the **demoCA** directory, storing a 2-digit number, such as “10”.

For example, use the commands:

```
mkdir demoCA
cd demoCA
mkdir certs
mkdir newcerts
mkdir private
touch index.txt
echo 10 > serial
```

Creating a Certificate Authority using OpenSSL

This process creates a private key and certificate of a Certificate Authority (CA), which can then be used to validate other certificates. Note that this will not be trusted by devices outside of those on which it is explicitly installed.

From a command prompt:

1. Ensure that you are in the **demoCA** directory.
2. For Windows: copy **openssl.cfg** from the directory where OpenSSL is installed to the **demoCA** directory and rename it as **openssl_local.cfg**.

For Mac OS X: copy `/System/Library/OpenSSL/openssl.cnf` to the **demoCA** directory and rename it as **openssl_local.cfg**.

3. Use a text editor to edit the **openssl_local.cfg** file that was created by the above copy command. Make the following modifications to the `[CA_default]` section:
 - a. Ensure that the line `copy_extensions = copy` does not have a `#` at the beginning of the line. Delete the `#` if it is there. If the line remains commented out, it will strip attributes in the CSR and the SSL Server and SSL Client attributes will not appear in the certificate.
 - b. Change `policy = policy_match` to `policy = policy_anything`
 - c. Change `dir = ./demoCA` to `dir = .`
 - d. Optionally, change `default_days = 365` (1 year validity of the generated certificate) to `default_days = 3650` (10 years, or choose another suitable value).
 - e. Save the file.
4. Generate a private key for the CA by running the following command:


```
openssl genrsa -aes256 -out private/cakey.pem 4096
```

 This will prompt for a password with which to encrypt the private key: choose a strong password and record it in a safe place. The `cakey.pem` file will be used to create the CA certificate and to sign other certificates and must also be kept secure.
5. Generate the CA certificate by running the following command.

For Windows: `openssl req -new -x509 -days 3650 -key private/cakey.pem -config openssl_local.cfg -sha1 -extensions v3_ca -out cacert.pem`

For OS X: `openssl req -new -x509 -days 3650 -key private/cakey.pem -config openssl_local.cfg -sha1 -extensions v3_ca -out cacert.pem`
6. Enter a passphrase for the key, and then enter the data requested, including:
 - Country
 - State or province
 - Locality name
 - Organization name
 - Organizational unit
 - Common name – this is typically the name of a contact person for this CA
 - Email address – optional, can leave blank

After entering the requested data, the operation completes and the certificate authority certificate **cacert.pem** is now available.

Creating a signed certificate using OpenSSL

This process signs the server certificate with the generated CA key, using the previously generated certificate request.

From a command prompt:

1. Ensure that you are in the **demoCA** directory.
2. Ensure that the certificate request file (**certcsr.pem**) is available:
 - If the certificate request was created using the Expressway (recommended process): Copy the file downloaded from the Expressway into the **demoCA** directory and rename it as **certcsr.pem**.
 - If the certificate request was created using OpenSSL: Copy the previously generated certificate request into the **demoCA** directory and then convert it to PEM format by running the following command:


```
openssl req -in certcsr.der -inform DER -out certcsr.pem -outform PEM
```

3. Generate a signed server certificate by running the following command:

```
openssl ca -config openssl_local.cfg -cert cacert.pem -keyfile  
private/cakey.pem -in certcsr.pem -out certs/server.pem -md sha1
```

If you receive a "failed to update database TXT_DB error number 2" error message, you can remove the contents of the **index.txt** file and then rerun the command.
4. You will be prompted to enter the password for the CA's private key.

The signed certificate for the server is now available as **demoCA/certs/server.pem**.

Creating self-signed certificates using OpenSSL

We do not recommend creating self-signed certificates. They will not work in Unified Communications deployments.

Instead you should create a Certificate Authority using OpenSSL as described above.

Appendix 3: Converting a DER certificate file to PEM format

A private key, root (CA) certificate and the server / client certificate can be generated using third-party tools (or purchased from a certificate authority), and may be generated as PEM (required format, extension .pem) or DER (extension .cer) format files.

Certificates must be in PEM format for use on the Expressway. Conversion from DER to PEM format can be done in one of two ways, either using OpenSSL or Windows, as documented in the following sections.

Converting a DER certificate file to a PEM file using OpenSSL

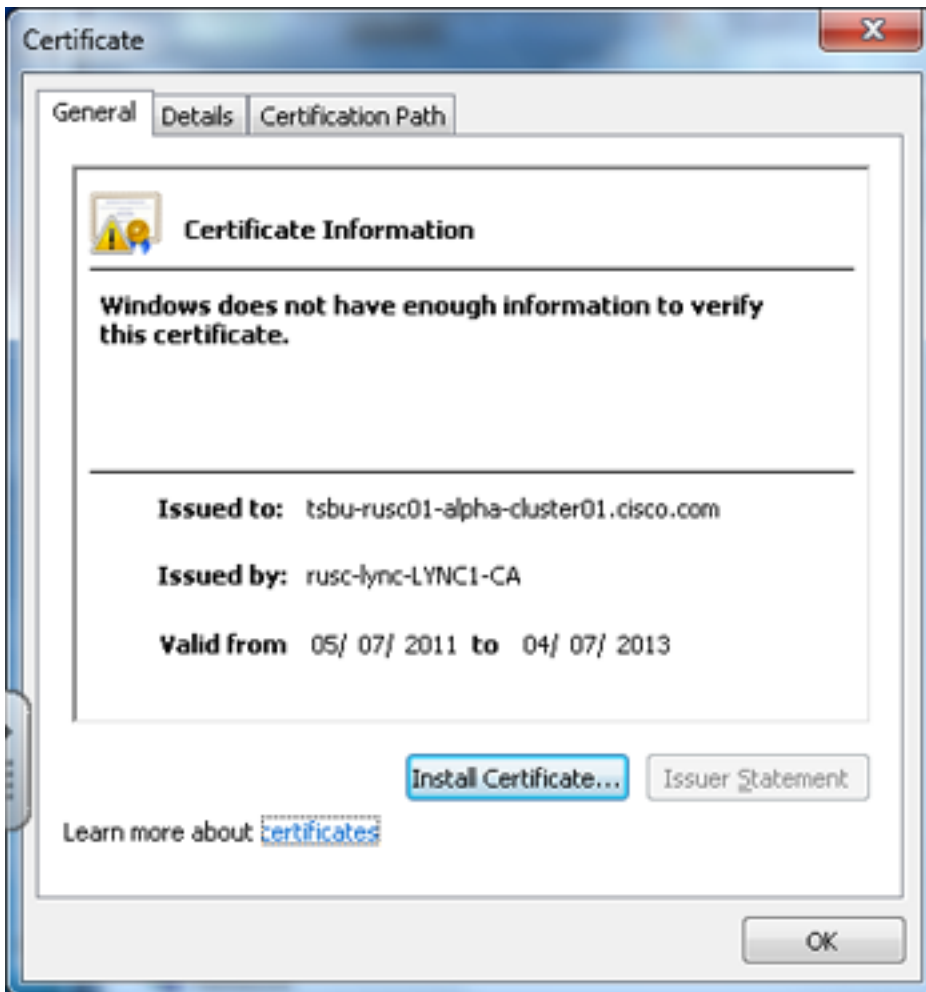
To convert from DER to PEM format, on a system running openssl, execute the command:

```
openssl x509 -in <filename>.cer -inform DER -out <filename>.pem -outform PEM
```

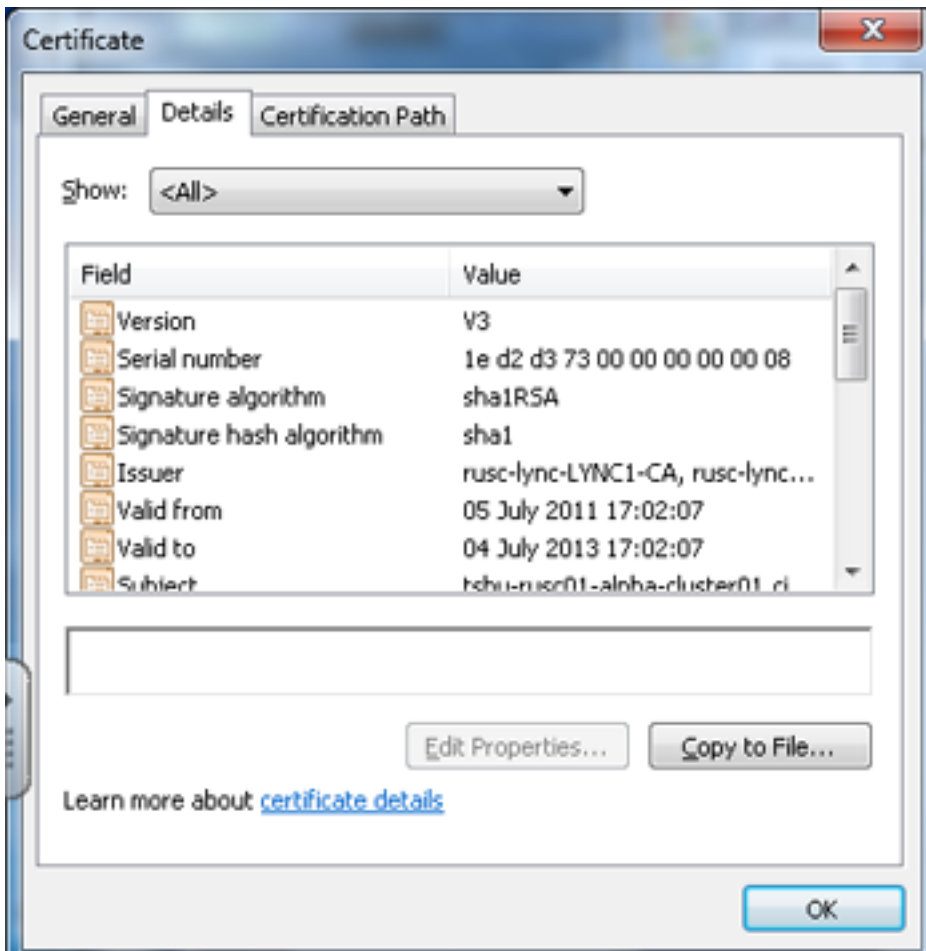
Converting a DER certificate file to a PEM file using Microsoft Windows

To convert from DER to PEM format using Microsoft Windows:

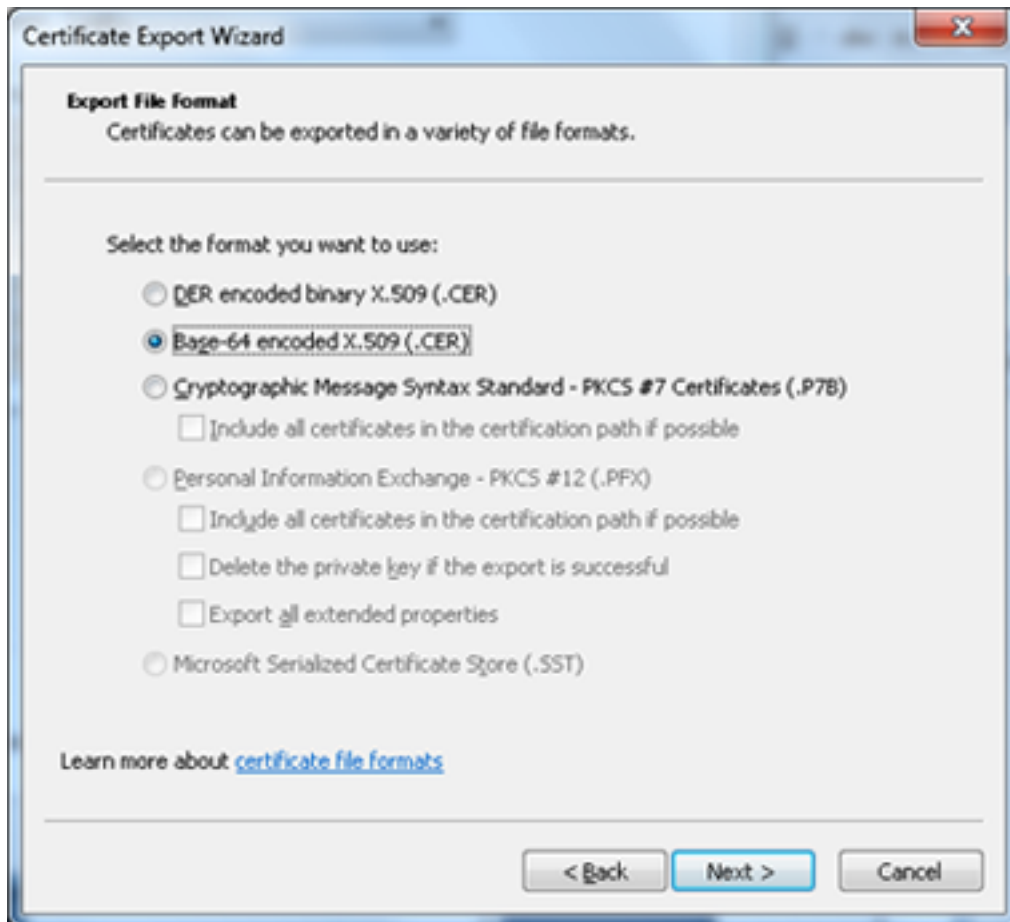
1. Double click on the DER file to convert (this will likely have a '.cer' extension).



2. Select the **Details** tab.



3. Click **Copy to File...**
4. On the **Welcome** page, click **Next**.
5. Select *Base-64 encoded X.509 (.CER)* and click **Next**.



6. Click **Browse** and select required destination for file (e.g. **server.pem**) and then click **Next**.
7. Click **Finish**.
8. Change the filename from **server.pem.cer** to **server.pem**.
9. This will be used in the [Loading certificates and keys onto Expressway \[p. 12\]](#) section of this document.

Appendix 4: Decoding certificates

This section describes some methods for decoding and viewing the content of certificates.

OpenSSL

A PEM file (e.g. **cert.pem**) can be decoded by the following command:

```
openssl x509 -text -in cert.pem
```

A DER file (e.g. **cert.cer**) can be decoded by the following command:

```
openssl x509 -text -inform DER -in cert.cer
```

Firefox

The certificate in use for a website being visited can be viewed in Firefox by clicking on the security information button on the address bar, and then clicking **More Information** followed by **View Certificate**.

Internet Explorer

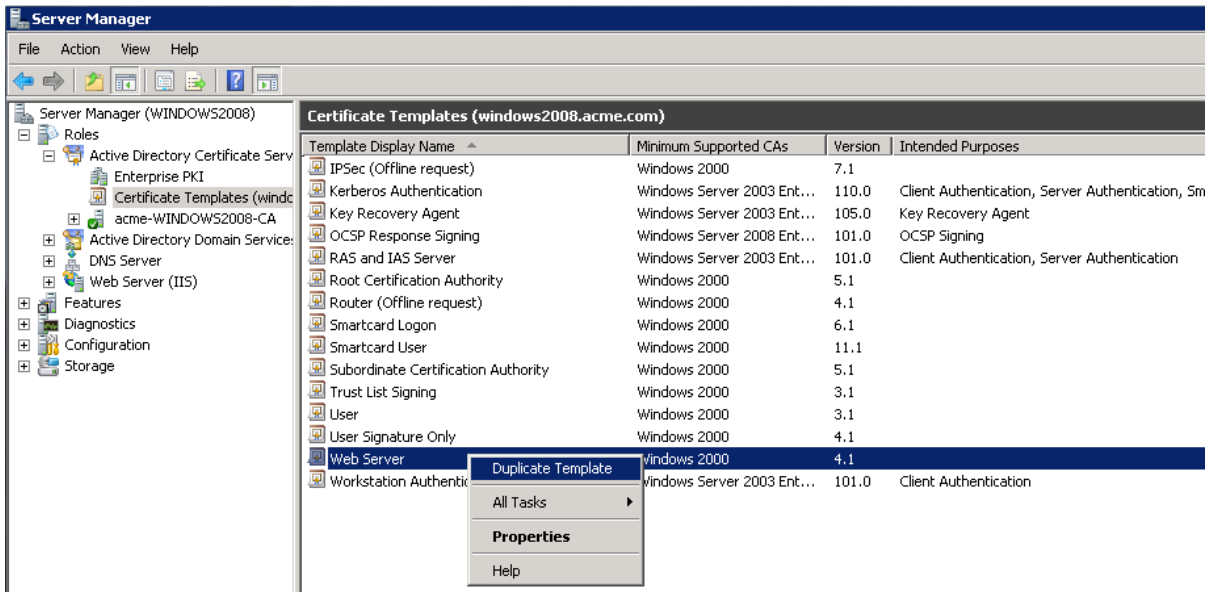
The certificate in use for a website being visited can be viewed in Internet Explorer by clicking the lock icon to the right of the address bar. A **Website Identification** dialog will appear. Click the **View Certificates** link at the bottom.

Appendix 5: Configuring Windows Server Manager with a "client and server" certificate template

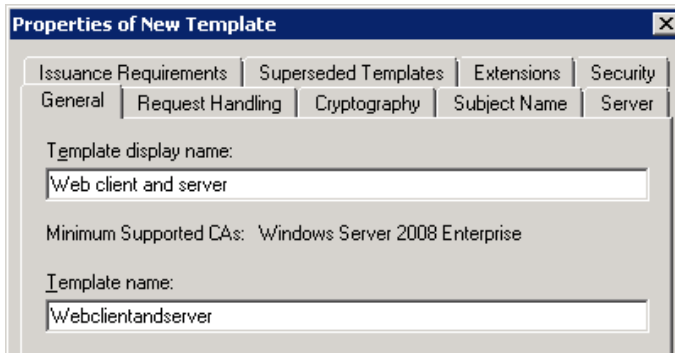
The default "Web Server" certificate template used by the Microsoft Certification Authority application will only create a certificate for Server Authentication. The server certificate for the Expressway also needs Client Authentication if you want to configure a neighbor or traversal zone with mutual authentication (where **TLS verify mode** is enabled).

To set up a certificate template with Server and Client Authentication:

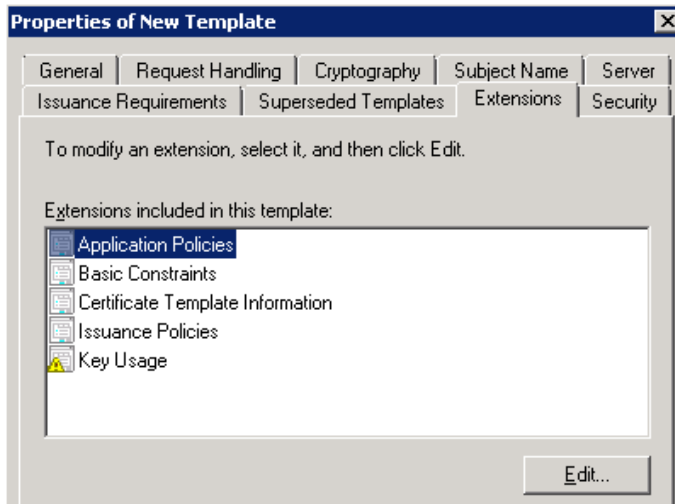
1. In Windows, launch **Server Manager** (**Start > Administrative Tools > Server Manager**). (Server Manager is a feature included with server editions of Windows.)
2. Expand the **Server Manager** navigation tree to **Roles > Active Directory Certificate Services > Certificate Templates (<domain>)**.
3. Right-click on **Web Server** and select **Duplicate Template**.



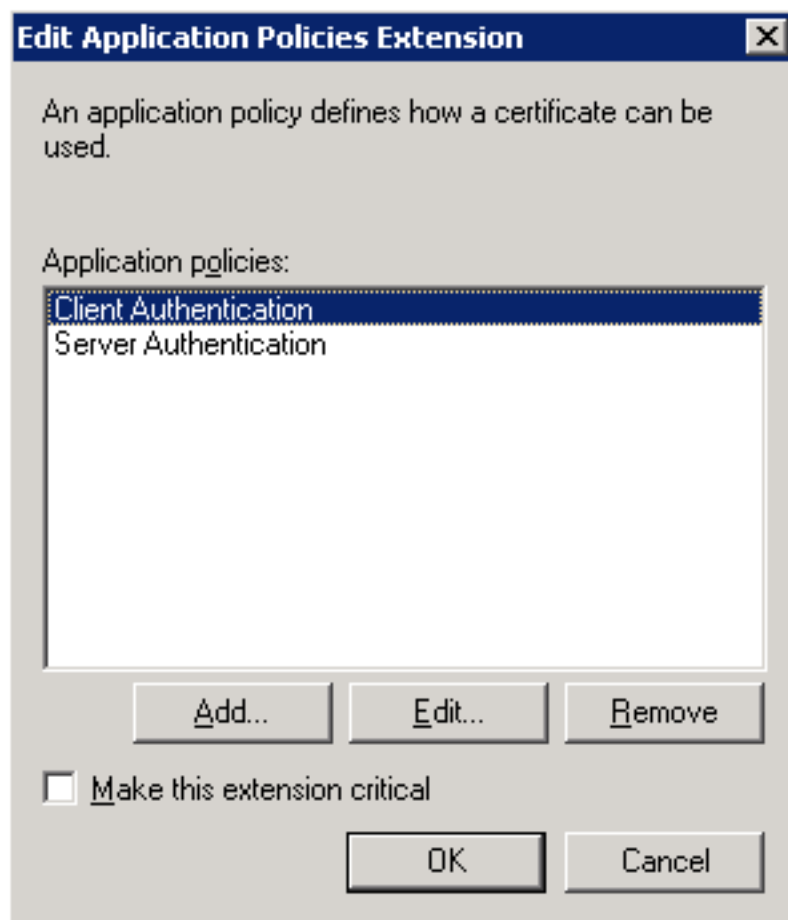
4. Select **Windows Server 2003 Enterprise** and click **OK**.
5. On the **General** tab, enter the **Template display name** and **Template name**, for example **web client and server** and **Webclientandserver**.



- On the **Extensions** tab, select **Application Policies** and click **Edit**.

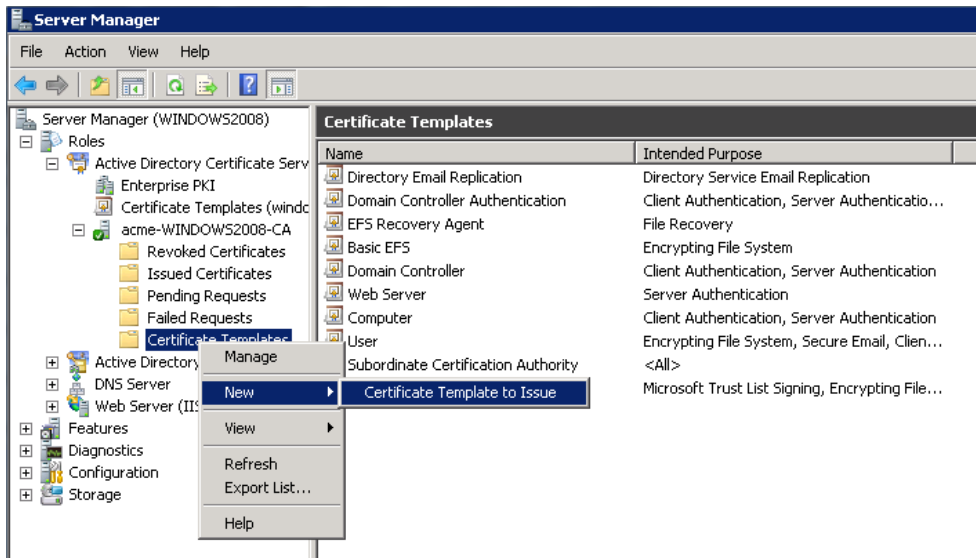


- Add **Client Authentication** to the set of application policies:
 - Click **Add**.
 - Select **Client Authentication** and click **OK**.
 - Click **OK**.

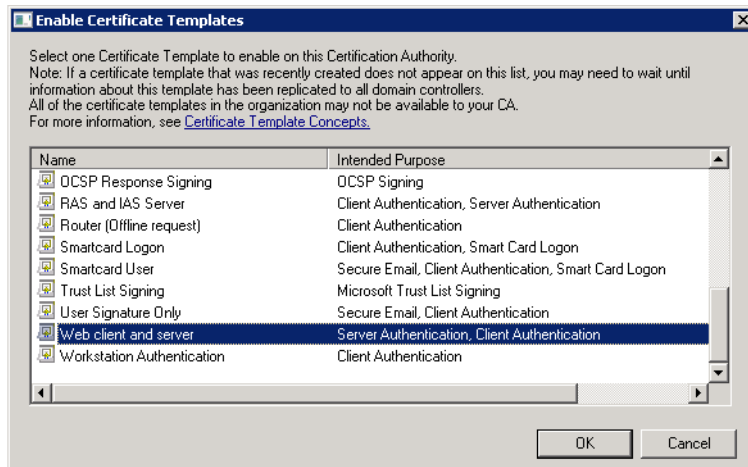


- Click **OK** to complete the addition of the new template.

9. Add the new template to the Certificate Authority:
 - a. Go to **Roles > Active Directory Certificate Services > <your certificate authority>**.
 - b. Right-click on **Certificate Templates** and select **New > Certificate Template to Issue**.



- c. Select your new **Web client and server** template and click **OK**.



The new **Web client and server** template can now be used when submitting a certificate request to that Microsoft Certification Authority.

Document revision history

The following table summarizes the changes that have been applied to this document.

Revision	Date	Description
6	April 2015	Update for X8.5.2. Changes to CRL information, CSR generation page defaults, 999 character limit on SANs.
5	January 2015	Update for X8.5.1. Introduced an option on the user interface to select the Digest algorithm . The default is set to SHA-256 (hash algorithm).
4	December 2014	Re-issued for X8.5. Notes inserted over 2050 date management, and unsupported OIDs. Changed instructions in Appendix 2 "Creating a certificate request using OpenSSL".
3	July 2014	Re-issued for X8.2. Recommended options changed for server certificate in Unified Communications deployments.
2	June 2014	Republished for X8.2. Enhanced the server certificate requirements for Unified Communications deployments.
1	December 2013	Initial release.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.