



## Introduction

---

- [Introduction, on page 1](#)
- [Information Not Covered in this Guide, on page 1](#)
- [PKI Introduction, on page 2](#)
- [Certificate Use on the Expressway Overview, on page 2](#)
- [Certificate Generation Overview, on page 3](#)
- [Points to be Aware, on page 4](#)

## Introduction



---

### Important

New features in software version X12.5 and later are not supported for the Cisco TelePresence Video Communication Server (VCS) product. They apply only to the Cisco Expressway Series (Expressway) product. This software version is provided to VCS for maintenance and bug fixing purposes only.

---

From version X12.5 onwards, this guide applies only to the Cisco Expressway Series (Expressway) product and no longer applies to the Cisco TelePresence Video Communication Server (VCS) product. Older VCS guides on [Cisco.com](https://www.cisco.com) are still valid for the VCS versions they apply to—as specified on the title page of each guide.

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.

## Information Not Covered in this Guide

This document does not cover the following Expressway configuration topics, which are instead covered in the *Expressway Administrator Guide*:

- How to enable certificate-based authentication on Expressway
- Details of root CAs pre-installed in Expressway
- How to configure minimum TLS versions and cipher suites
- How to test client certificates

- Managing mTLS certificates (Mobile and Remote Access deployments)
- Domain certificates and Server Name Indication for multitenancy (Hosted Collaboration Solution deployments)

## PKI Introduction

Public Key Infrastructure (PKI) provides the mechanisms through which you can secure communications (encrypted and integrity protected) and verify the identities. Underlying PKI is:

- **A public/private key pair:** a public key is used to encrypt data that is sent to a server, but only the private key (kept secret by the server) can be used to decrypt it.
- **Signatures of data:** server “signs” data using a combination of a cryptographic hash of the data and the server’s private key. A client can verify the signature using server’s public key and the same hash. This ensures that the data is sent from the expected server, and is not tampered with.
- **Certificates:** a certificate is a wrapper around a public key, and provides information about the owner of the key in X.509 format, and typically includes server name and contact details.
- **A certificate chain:** Certificate Authority (CA) signs a certificate using its own private key. In turn, you can verify a certificate as signed 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. The client sends its capabilities (including cipher suites) and a random number to make an initial TCP connection.
2. The server responds with its choice of those capabilities, another random number, and its certificate.
3. The client verifies that the server certificate is issued (signed) by a CA that it trusts, and it is not revoked.
4. The client sends a “pre secret”, encrypted with the server’s public key.
5. This pre secret, combined with the exchanged random numbers (to prevent replay attacks), is used to generate a “shared secret”. This shared secret keeps the remaining communications of this TLS session encrypted between the client and server.

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

## Certificate Use on the Expressway Overview

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.

The Expressway 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. 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 cluster
- Subject Alternate Name = FQDN of Expressway peer, FQDN of cluster\*

You manage the Cisco Expressway's server certificate through the Server certificate page (**Maintenance > Security > Server certificate**). This certificate is used to identify the Expressway when it communicates with client systems using TLS encryption, and with web browsers over HTTPS. You can use the Server certificate page to:

- View details about the currently loaded certificate.
- Generate a certificate signing request.
- Upload a new server certificate.

## 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.

The Expressway also supports the Automated Certificate Management Environment (ACME), and you can configure it to automatically request and deploy certificates signed by the *Let's Encrypt*<sup>®</sup> certificate authority.

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:

- [Generate a Certificate Signing Request \(CSR\)](#), describes how to use the Expressway itself to generate the private key and certificate request.
- [Appendix 2: Certificate Generation using OpenSSL Only](#), 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: Enable AD CS to Issue "Client and Server" Certificates](#)).

## Points to be Aware

- Some deployments rely on SANs (Subject Alternate Names) to implement TLS connections to other Cisco or third-party infrastructure. You need to check the documentation for your deployment before you order the certificate.
- When you generate a CSR using external systems, ensure that the CSR does not contain any unsupported OIDs. Currently, only the following Extended Validation OIDs are supported.
  - 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

For more information on how to verify if there are unsupported OIDs in the certificate, see the section [Issues with SSH Failures and Unsupported OIDs](#).

- Wildcard certificates manage multiple subdomains and the services names they support. They can be less secure than SAN certificates and are not supported by Expressway.
- 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.
- The Expressway mechanism for CA certificate checking, requires the BasicConstraints extension to be present.
- We highly recommend using certificates based on RSA keys. Other types of certificate, such as those based on DSA keys, are not tested and may not work with the Expressway in all scenarios.
- Do not allow your server certificate to expire as this may cause other external systems to reject your certificate and prevent the Expressway from being able to connect to those systems.