Setup Certificate Validation

Cisco UC Integration for Microsoft Lync uses certificate validation to establish secure connections with servers.

Servers present Cisco UC Integration for Microsoft Lync with certificates when attempting to establish secure connections. Cisco UC Integration for Microsoft Lync validates those certificates against certificates in the Microsoft Windows certificate store. If the client cannot validate a certificate, it prompts the user to confirm if they want to accept the certificate.

- Required Certificates, on page 1
- Get Certificates Signed by Certificate Authority, on page 1
- Server Identity in Certificates, on page 2
- Import Root Certificates on Client Computers, on page 3

Required Certificates

The following certificates are presented to establish a secure connection.

Server	Certificate
Cisco Unified Communications Manager	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)

Important Notes

- Every node in a cluster, including both subscribers and publishers, run a Tomcat service and can present the client with an HTTP certificate. You should plan to sign the certificates for each node in the cluster.
- To secure SIP signaling between the client and Cisco Unified Communications Manager, you should use Certification Authority Proxy Function (CAPF) enrollment.

Get Certificates Signed by Certificate Authority

Cisco recommends using server certificates that are signed by one of the following types of Certificate Authority (CA):

- **Public CA**

A third-party company verifies the server identity and issues a trusted certificate.

- **Private CA**

  You create and manage a local CA and issue trusted certificates.

The signing process varies for each server and can vary between server versions. It is beyond the scope of this document to provide detailed steps for every version of each server. You should consult the appropriate server documentation for detailed instructions on how to get certificates signed by a CA. However, the following steps provide a high-level overview of the procedure.

Procedure

Step 1 Generate a Certificate Signing Request (CSR) on each server that can present a certificate to the client.

Step 2 Submit each CSR to the CA.

Step 3 Upload the certificates that the CA issues to each server.

Certificate Signing Request Forms and Requirements

Public CAs typically require CSRs to conform to specific formats. For example, a public CA might only accept CSRs that:

- Are Base64-encoded.
- Do not contain certain characters, such as @&! , in the Organization, OU, or other fields.
- Use specific bit lengths in the server's public key.

Likewise, if you submit CSRs from multiple nodes, public CAs might require that the information is consistent in all CSRs.

To prevent issues with your CSRs, you should review the format requirements from the public CA to which you plan to submit the CSRs. You should then ensure that the information you enter when configuring your server conforms to the format that the public CA requires.

One Certificate Per FQDN: Some public CAs sign only one certificate per fully qualified domain name (FQDN).

Server Identity in Certificates

The CA specifies the server identity in the certificate as part of the signing process. When the client validates that certificate, it checks that:

- A trusted authority has issued the certificate.
- The identity of the server that presents the certificate matches the identity of the server specified in the certificate.

Note Public CAs generally require a fully qualified domain name (FQDN) as the server identity, not an IP address.

Identifier Fields

The client checks the following identifier fields in server certificates for an identity match:

- **HTTP certificates**
  - SubjectAltName\dnsNames
  - Subject CN

Tip The Subject CN field can contain a wildcard (*) as the leftmost character, for example, *.cisco.com.

Prevent Identity Mismatch

If users attempt to connect to a server with an IP address, and the server certificate identifies the server with an FQDN, the client cannot identify the server as trusted and prompts the user.

If your server certificates identify the servers with FQDNs, you should plan to specify each server name as FQDN throughout your environment.

Import Root Certificates on Client Computers

Every server certificate should have an associated root certificate present in the trust store on client computers. Cisco UC Integration for Microsoft Lync validates the certificates that servers present against the root certificates in the trust store.

If you get server certificates signed by a public CA, the public CA should already have a root certificate present in the trust store on the client computer. In this case, you do not need to import root certificates on the client computers.

You should import root certificates into the Microsoft Windows certificate store if:

- The certificates are signed by a CA that does not already exist in the trust store, such as a private CA.
  - Import the private CA certificate to the Trusted Root Certification Authorities store.
- The certificates are self-signed.
  - Import self-signed certificates to the Enterprise Trust store.

Important If root certificates are not present in the trust store, Cisco UC Integration for Microsoft Lync prompts users to accept certificates from each server in your environment.

When the client prompts users to accept a certificate, users can:

- **Accept the certificate**
  - The client saves the certificate to the Enterprise Trust store.
- **Decline the certificate**
  - The client
    - Does not save the certificate.

- Does not connect to the server.
- Displays an error notification.

When users restart the client, it prompts them to accept the certificate again.

You can use any appropriate method to import certificates into the Microsoft Windows certificate store, including the following. For detailed instructions on importing certificates, refer to the appropriate Microsoft documentation.

- Use the Certificate Import Wizard to import certificates individually.
- Deploy certificates to users with the CertMgr.exe command line tool on Microsoft Windows Server.

Note This option requires you to use the Certificate Manager tool, CertMgr.exe, not the Certificates Microsoft Management Console, CertMgr.msc.

- Deploy certificates to users with a Group Policy object (GPO) on Microsoft Windows Server.