Set Up Certificate Validation

About Certificate Validation

Cisco Jabber uses certificate validation to establish secure connections with servers.

When attempting to establish secure connections, servers present Cisco Jabber with certificates.

Cisco Jabber for Mac validates those certificates against certificates in the Keychain.

If the client cannot validate a certificate, it prompts the user to confirm if they want to accept the certificate.

In Expressway for Mobile and Remote Access deployment, when using an online certificate status protocol (OCSP) or online certificate revocation lists (CRL) to obtain the revocation status of the certificates, the Cisco Jabber client expects a response time of less than 5 seconds. Connections will fail if the response time is greater than the expected 5 seconds.

On-Premises Servers

Review which certificates on-premises servers present to the client and the tasks involved in getting those certificates signed.

Required Certificates for On-Premises Servers

On-premises servers present the following certificates to establish a secure connection with Cisco Jabber:

Server	Certificate
Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP (Tomcat) and CallManager certificate (secure SIP call signaling for secure phone)
Cisco Unity Connection	HTTP (Tomcat)

Server	Certificate
Cisco WebEx Meetings Server	HTTP (Tomcat)
Cisco VCS Expressway Cisco Expressway-E	Server certificate (used for HTTP, XMPP, and SIP call signaling)

Important Notes

- Security Assertion Markup Language (SAML) single sign-on (SSO) and the Identity Provider (IdP) require an X.509 certificate.
- You should apply the most recent Service Update (SU) for Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service before you begin the certificate signing process.
- The required certificates apply to all server versions.
- Each cluster node, subscriber, and publisher, runs 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.
If the process your company uses means you must wait for the CSRs to be sent back to you before you can apply them, then you may wish to configure your services now while you wait for the CSRs. Then you can apply the certificates after the service configuration is complete, prior to deployment.

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

Certificate Signing Request Formats and Requirements

A public certificate authority (CA) typically requires a certificate signing request (CSR) to conform to specific formats. For example, a public CA might only accept CSRs that have the following requirements:

- 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.

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).

For example, to sign the HTTP and XMPP certificates for a single Cisco Unified Communications Manager IM and Presence Service node, you might need to submit each CSR to different public CAs.

Revocation Servers

To validate certificates, the certificate must contain an HTTP URL in the **CDP** or **AIA** fields for a reachable server that can provide revocation information. If a certificate authority (CA) revokes a certificate, the client does not allow users to connect to that server.

Users are not notified of the following outcomes:

- The certificates do not contain revocation information.
- The revocation server cannot be reached.

To ensure that your certificates are validated when you get a certificate issued by a CA, you must meet one of the following requirements:

- Ensure that the **CRL Distribution Point** (CDP) field contains an HTTP URL to a certificate revocation list (CRL) on a revocation server.
- Ensure that the **Authority Information Access** (AIA) field contains an HTTP URL for an Online Certificate Status Protocol (OCSP) server.

Server Identity in Certificates

As part of the signing process, the CA specifies the server identity in the certificate. 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:

- XMPP certificates
  - `SubjectAltName\OtherName\xmppAddr`
  - `SubjectAltName\OtherName\srvName`
  - `SubjectAltName\dnsNames`
  - `Subject CN`
- 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.

Provide XMPP Domain to Clients

This task is not required if you are using Cisco Unified Communications Manager IM and Presence Service version 10.0 or later.

The client identifies `XMPP` certificates using the XMPP domain, rather than the FQDN. The `XMPP` certificates must contain the XMPP domain in an identifier field.

When the client attempts to connect to the presence server, the presence server provides the XMPP domain to the client. The client can then validate the identity of the presence server against the `XMPP` certificate.

Complete the following steps to ensure the presence server provides the XMPP domain to the client:

Procedure

Step 1 Open the administration interface for your presence server, as follows:

- Cisco Unified Communications Manager IM and Presence Service — Open the **Cisco Unified CM IM and Presence Administration** interface.
- Cisco Unified Presence — Open the **Cisco Unified Presence Administration** interface.

Step 2 Select **System** > **Security** > **Settings**.

Step 3 Locate the **XMPP Certificate Settings** section.

Step 4 Specify the presence server domain in the following field: **Domain name for XMPP Server-to-Server Certificate Subject Alternative Name**.

Step 5 Select the following checkbox: **Use Domain Name for XMPP Certificate Subject Alternative Name**.

Step 6 Click **Save**.

Deploy Certificates on Client Computers

Every server certificate should have an associated certificate in the Keychain on the client computers. Cisco Jabber validates the certificates that the servers present against the certificates in the Keychain.

Important If root certificates are not present in the Keychain, Cisco Jabber prompts users to accept certificates from each server in your environment.

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

- Always trust *server name* — The client saves the certificate to the Keychain.
- Continue — The client will connect, but when the user restarts the client they are prompted to accept the certificate again.
- Cancel — The client:
  - Does not save the certificate.
  - Does not connect to the server.

Prevent the warning dialogs by downloading the certificates from the **Cisco Unified OS Administration** interface. Complete the following steps to deploy self-signed certificates to the user.

Procedure

Step 1 For each Cisco node, download the corresponding “tomcat-trust” certificate from the **Cisco Unified OS Administration** interface. Select **Security** > **Certificate Management**.

Step 2 Concatenate the certificates into a single file with the extension **.pem** (for example, “companyABCcertificates.pem”).

Step 3 Send the file to your Cisco Jabber users and ask them to double-click it. Doing so launches the Keychain Access application and imports the certificates.

Note The operating system requires that the user enter the Mac OS X administration password for each certificate that is being imported.

Certificate Requirements for Cloud-Based Servers

Cisco WebEx Messenger and Cisco WebEx Meeting Center present the following certificates to the client:

- Central Authentication Service (CAS)
- WLAN Authentication and Privacy Infrastructure (WAPI)

Important Cisco WebEx certificates are signed by a public certificate authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

As of Cisco Jabber for Windows 9.7.2 and Cisco Jabber for Mac 9.6.1, Cisco Jabber validates the XMPP certificate received from Cisco WebEx Messenger. If your operating system does not contain the following certificates for Cisco WebEx Messenger, you must provide them:

- VeriSign Class 3 Public Primary Certification Authority—G5 (stored in the Trusted Root Certificate Authority)
- VeriSign Class 3 Secure Server CA—G3 (stored in the Intermediate Certificate Authority)

The same set of certificates are applicable for Cisco Jabber for Android, iPhone and iPad.

The certificate that is stored in the Intermediate Certificate Authority validates the Cisco WebEx Messenger server identity.

For Cisco Jabber for Windows 9.7.2 or later, you can find more information and installation instructions for the root certificate at http://www.identrust.co.uk/certificates/trustid/install-nes36.html.

For Cisco Jabber for Mac 9.6.1 or later and iOS, you can find more information for the root certificate on the Apple support website at https://support.apple.com.

Update Profile Photo URLs

In cloud-based deployments, Cisco WebEx assigns unique URLs to profile photos when you add or import users. When Cisco Jabber resolves contact information, it retrieves the profile photo from Cisco WebEx at the URL where the photo is hosted.

Profile photo URLs use HTTP Secure (`https://server_name/`) and present certificates to the client. If the server name in the URL is:

- A fully qualified domain name (FQDN) that contains the Cisco WebEx domain — The client can validate the web server that is hosting the profile photo against the Cisco WebEx certificate.
- An IP address — The client cannot validate the web server that is hosting the profile photo against the Cisco WebEx certificate. In this case, the client prompts users to accept certificates whenever they look up contacts with an IP address in their profile photo URLs.

Important

- We recommend that you update all profile photo URLs that contain an IP address as the server name. Replace the IP address with the FQDN that contains the Cisco WebEx domain to ensure that the client does not prompt users to accept certificates.
- When you update a photo, the photo can take up to 24 hours to refresh in the client.

The following steps describe how to update profile photo URLs. Refer to the appropriate Cisco WebEx documentation for detailed instructions.

Procedure

Step 1 Export user contact data in CSV file format with the Cisco WebEx Administration Tool.

Step 2 In the **userProfilePhotoURL** field, replace IP addresses with the Cisco WebEx domain.

Step 3 Save the CSV file.

Step 4 Import the CSV file with the Cisco WebEx Administration Tool.