Set Up Certificate Validation

- Certificate Validation for Cloud Deployments, on page 1

Certificate Validation for Cloud Deployments

Cisco Webex Messenger and Cisco Webex Meetings Center present the following certificates to the client by default:

- CAS
- WAPI

Note Cisco Webex certificates are signed by a public Certificate Authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

Cisco Jabber validates the following XMPP certificates received from Cisco Webex Messenger. If these certificates are not included in your operating system, you must provide them.

- VeriSign Class 3 Public Primary Certification Authority - G5 — This certificate is stored in the Trusted Root Certificate Authority
- VeriSign Class 3 Secure Server CA - G3 —This certificate validates the Webex Messenger server identity and is stored in the Intermediate Certificate Authority.
- AddTrust External CA Root
- GoDaddy Class 2 Certification Authority Root Certificate

For more information about root certificates for Cisco Jabber for Windows, see https://www.identrust.co.uk/certificates/trustid/install-nes36.html.

For more information about root certificates for Cisco Jabber for Mac, see 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 Webexcertificate.
- 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 WebexAdministration 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.