Set Up Certificate Validation

Configure Certificates for an On-Premises Deployment

Certificates are required for each service to which the Jabber clients connect.

Procedure

	Command or Action	Purpose
Step 1	If you have Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service, download the applicable HTTP (tomcat) and XMPP certificates.	For more information, see the *Security Configuration on IM and Presence Service* chapter in Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.
Step 2	Download the HTTPS (tomcat) certificate for Cisco Unified Communications Manager and Cisco Unity Connection.	For more information, see the *Cisco Unified Communications Manager Security Guide* and the *Cisco Unified Communications Operating System Administration Guide* found here.
Step 3	Download the HTTP (tomcat) for Cisco WebEx Meetings Server.	For more information, see the *Cisco WebEx Meetings Server Administration Guide* found here.
Step 4	If you plan to configure remote access, download the Cisco VCS Expressway and Cisco Expressway-E Server certificate. The Server certificate is used for both HTTP and XMPP.	For more information, see Configuring Certificates on Cisco VCS Expressway.
Step 5	Generate a Certificate Signing Request (CSR).	
Step 6	Upload the certificate to the service.	If you use a multiserver SAN, you only need to upload a certificate to the service once per cluster per tomcat certificate and once per cluster per XMPP certificate.

	Command or Action	Purpose
		If you do not use a multiserver SAN, then you must upload the certificate to the service for every Cisco Unified Communications Manager node.
Step 7	Deploy CA Certificates to Clients, on page 2	To ensure that certificate validation occurs without users receiving a prompt to accept or decline certificates, deploy certificates to the local certificate store of the clients.

Deploy CA Certificates to Clients

To ensure that certificate validation occurs without users receiving a prompt to accept or decline certificates, deploy certificates to the local certificate store of the endpoint clients.

If you use a well-known public CA, then the CA certificate may already exist on the client certificate store or keychain. If so, you need not deploy CA certificates to the clients.

If the CA certificate is not already on the client certificate store or keychain, then deploy the CA certificate to the clients.

If your deployment size is	Then we recommend
To a large number of local machines	That you use a certificate deployment tool, such as Group Policy or a certificate deployment management application.
To a smaller number of local machines	That you manually deploy the CA certificates.

Manually Deploy CA Certificates to Cisco Jabber for Windows Clients

Procedure

Step 1 Make the CA certificate available to the Cisco Jabber for Windows client machine.

Step 2 From the Windows machine, open the certificate file.

Step 3 Install the certificate and then select **Next**.

Step 4 Select **Place all certificates in the following store**, then select **Browse**.

Step 5 Select the Trusted Root Certification Authorities store.
When you finish the wizard, a message is displayed to verify successful certificate import.

What to Do Next

Verify that the certificate is installed in the correct certificate store by opening the Windows Certificate Manager tool. Browse to **Trusted Root Certification Authorites** > **Certificates**. The CA root certificate is listed in the certificate store.

Manually Deploy CA Certificates to Cisco Jabber for Mac Clients

Procedure

Step 1 Make the CA certificate available to the Cisco Jabber for Mac client machine.

Step 2 From the Mac machine, open the certificate file.

Step 3 Add to the login keychain for the current user only, then select **Add**.

What to Do Next

Verify that the certificate is installed in the correct keychain by opening the Keychain Access Tool and selecting Certificates. The CA root certificate is listed in the keychain.

Manually Deploy CA Certificates to Mobile Clients

To deploy the CA certificates to an iOS client, you need a certificate deployment management application. You can email the CA certificate to users, or make the certificates available on a web server for users to access. Users can download and install the certificate using the certificate deployment management tool.

However, Jabber for Android does not have a certificate management tool, you must use the following procedure.

Procedure

Step 1 Download the CA certificate to the device.

Step 2 Tap the device **Settings** > **Security** > **Install from device storage** and follow the instructions.

Certificate Validation for Cloud Deployments

Cisco WebEx Messenger and Cisco WebEx Meeting 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 —T his 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 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.