Jabber Complete How-To Guide for Certificate Validation

Contents

Introduction

This document combines several Cisco resources into a complete, unified how-to guide that is used in order to implement all of the requirements for certificate validation in Cisco Jabber. This is necessary because Cisco Jabber now requires the use of certificate validation in order to establish secure connections with servers. This requirement entails many changes that might be required for user environments.

> **Note**: This guide is for on-premise deployments only. There is currently no change required for cloud service deployments, because they are validated against the Public Certificate Authority (CA).

Which Jabber Clients are affected by this change?

Here is a table that lists all of the clients that implement certificate validation:

Table 1

Desktop Clients	Mobile and Tablet Clients

Jabber for Macintosh Version 9.2 (September 2013) Jabber for Microsoft (MS) Windows Version 9.2.5 (September 2013)	Jabber for iPhone Version 9.5 (October 2013 Jabber for iPhone and iPad Version 9.6 (November 2013) Jabber for Android Version 9.6 (December 2

What does this mean for the Jabber environment?

When you install or upgrade to any client listed in **Table 1**, mandatory certificate validation with servers is used for secure connections. Essentially, when Jabber Clients attempt to make a secure connection now, servers present Cisco Jabber with certificates. Cisco Jabber then attempts to validate those certificates against the certificate store of the device. If the client cannot validate the certificate, it prompts you to confirm that you want to accept the certificate, and place it in its Enterprise Trust store.

Which certificates are required?

Here is a list of on-premise servers and the certificates that they present to Cisco Jabber in order to establish a secure connection:

Table 2

Server	Certificate
Cisco Unified Presence	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager IM and Presence	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)
Cisco WebEx Meetings Server	HTTP (Tomcat)

Here are some important points to note:

- Apply the most recent Service Update (SU) for Cisco Unified Presence (CUP) or Cisco Unified Communications Manager (CUCM) IM and Presence before you begin the certificate signing process.
- The required certificates apply to all server versions. For example, both CUP Version 8.x and CUCM IM and Presence Version 9.x and later present the client with Extensible Messaging and Presence Protocol (XMPP) and HTTP certificates.
- Each node in a cluster, subscribers and publishers, runs a Tomcat service and can present the client with an HTTP certificate. Plan to sign the certificates for each node in the cluster.
- In order to secure Session Initiation Protocol (SIP) signaling between the client and CUCM, use Certification Authority Proxy Function (CAPF) enrollment.

What methods are available for certificate validation?

There are currently several methods of certification validation that can be used.

Method 1: Users simply click **Accept** to all certificate popups. This might be the most ideal solution for smaller environments. If you click **Accept**, certificates are placed into the Enterprise Trust store on the device. After certificates are placed in the Enterprise Trust store, users are no longer prompted when they log into the Jabber Client on that local device.

Method 2: The required certificates (**Table 2**) are downloaded from the individual servers (by default, these are self-signed certificates) and installed into the Enterprise Trust store of the user device. This might be the ideal solution if your environment does not have access to a Private or Public CA for certificate signing.

Several methods can be used in order to push these certificates to users, but one quick method is to employ the use of the Microsoft Windows Registry:

1. From one of the machines, accept all of the certificates that are presented to Jabber into the Enterprise Trust Store.
2. In order to verify that the certificates are present, enter the **Certmgr.msc** command and navigate to **Enterprise Trust > Certificates**.
3. Open **Regedit** with a **run** command and navigate to **HKCU > Software > Microsoft > SystemCertificates > trust > Certificates**.
4. Right-click and export the Certifates folder in the registry as a **.reg** file.
5. Push out this file via Group Policy Object (GPO) to all users (or other preferred method).

This completes the install of Enterprise Trust Certificates for Jabber, and users are no longer prompted.

Method 3: A Public or Private CA (**Table 2**) signs all of the required certificates. This is the Cisco recommended method. This method requires that a Certificate Signing Request (CSR) is generated for each of the certificates, is signed, re-uploaded to the server, and then imported to the Trusted Root Certificate Authorities Store on user devices. See the **Generate a CSR** and the **How do I get certificates to user devices certificate stores?** sections of this document for more information.

> **Note**: In the case of a Public CA, the root certificate should already be in the client trust store.

It is important to remember that Public CAs typically require CSRs in order 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, Organizational Unit (OU), or other fields
- Use specific bit lengths in the public key for the server

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

In order to prevent issues with your CSRs, review the format requirements from the public CA to which you plan to submit the CSRs. Then ensure that the information you enter when you configure your server conforms to the format that the public CA requires.

Here is a possible requirement you might encounter:

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

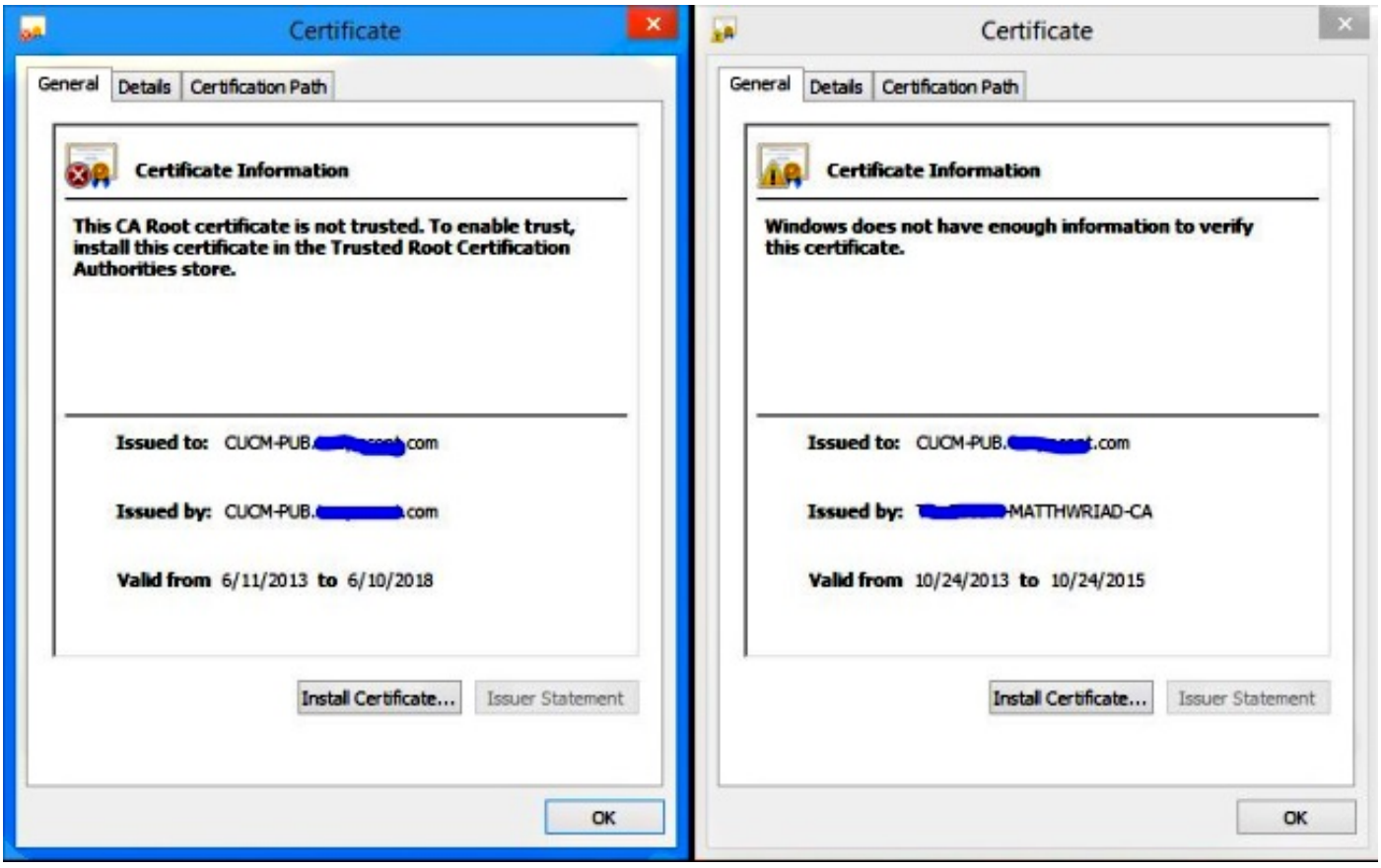
For example, in order to sign the HTTP and XMPP certificates for a single CUCM IM and Presence node, you might need to submit each CSR to different public CAs.

Verify if a Certificate is Self-Signed or CA-Signed

> **Note**: This example is for CUCM Version 8.x. The process might vary between servers.

1. Navigate to **Cisco Unified OS Administration**.
2. Choose **Security > Certificate Management**.
3. Find and click the **Tomcat-Trust Certificate .pem** file.
4. Click **Download**, and **Save**.
5. Navigate to the file, and rename it with the **.cer** extension.
6. Open and view this file (MS Windows users).
7. Verify the **Issued by** field. If it matches the **Issued to** field, then the certificate is Self-Signed (see the **Example**).

Example: Self-Signed vs Private CA-Signed Certificate



Self-Signed

Private CA-Signed

Generate a CSR

Note: This example is for CUCM Version 8.x. The process might vary between servers.

1. Navigate to **Cisco Unified OS Administration**.
2. Choose **Security > Certificate Management**.
3. Click **Generate CSR**, and choose **Tomcat** from the drop-down list.
4. Click **Generate CSR**, and click **Close**.
5. Click **Download CSR**, and choose **Tomcat** from the drop-down list.
6. Click **Download CSR**, and save the file.
7. Send the **.csr** file to be signed by your Private CA Server or a Public CA.
   Note: Once you have this CSR file, the process varies based on your environment.
8. Click **Upload Certificate/Certificate Chain** under **Security > Certificate Management** In order to re-upload the new signed certificates that were issued to your server.

How do I import certificates into user device certificate stores?

Every server certificate should have an associated root certificate present in the trust store on the user device. Cisco Jabber validates the certificates that servers present against the root certificates in the trust store.

Import root certificates into the MS 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. If so, you must import the private CA certificate to the Trusted Root Certification Authorities store.
- The certificates are self-signed. If so, you must import self-signed certificates to the Enterprise Trust store.

You can use any appropriate method in order to import certificates into the MS Windows certificate store, such as:

- Use the Certificate Import Wizard in order to import certificates individually.
- Deploy certificates to users with the CertMgr.exe command line tool on MS Windows Server. (This option requires you to use the Certificate Manager tool, CertMgr.exe, not the Certificates MS Management Console, CertMgr.msc.)
- Deploy certificates to users with a GPO on MS Windows Server.

Note: For detailed instructions on how to import certificates, refer to the appropriate MS documentation.

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 FQDN as the server identity, not an IP address.

Identifier Fields

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

XMPP Certificates

- SubjectAltName\OtherName\xmppAddr
- SubjectAltName\OtherName\srvName
- SubjectAltName\dnsNames
- Subject CN

HTTP Certificates

- SubjectAltName\dnsNames
- Subject CN

Note: The Subject CN field can contain a wildcard (*) as the leftmost character; for example, *.cisco.com. Your CUCM, CUP, and Cisco Unity Connection servers might not support wildcard certificates. (Refer to enhancement Cisco bug ID CSCta14114).

Prevent Identity Mismatch

When a Jabber Client attempts 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. So, if your server certificates identify the servers with FQDNs, you must specify the server name as FQDN in many places on your servers.

Table 3 lists all of the places that need to specify the server name as it appears in the certificate, whether it is an IP address or a FQDN.

Table 3

Server	**Location (Setting must Match Certificate)**
Cisco Jabber Clients	Login Server Address (Differs for clients, normally under **Connection Setti** ** All Node Names (**System > Cluster Topology)** ****Caution**: Make sure that if you change this to FQDN, you can resolve thi DNS or the servers remain in the starting state! TFTP Servers (**Application > Cisco Jabber > Settings)**
CUP (Version 8.x and earlier)	Primary and Secondary Cisco Call Manager Cisco IP Phone (CCMCIP) (**Application > Cisco Jabber > CCMCIP Profile)** Voicemail Host Name (**Application > Cisco Jabber > Voicemail Server)** Mailstore Name **(Application > Cisco Jabber > Mailstore)** Conferencing Host Name (**Application > Cisco Jabber > Conferencing Server)** (Meeting Place Only) XMPP Domain (See the **Provide XMPP Domain to Clients** section)

CUCM IM and Presence (Version 9.x and later)	**All Node Names **(System > Cluster Topology**) ****Caution**: Make sure that if you change this to FQDN, you can resolve thi DNS or the servers remain in the starting state! TFTP Servers (**Application > Legacy Clients > Settings)** Primary and Secondary CCMCIP **(Application > Legacy Clients > CCMC Profile)** XMPP Domain (See the **Provide XMPP Domain to Clients** section)
CUCM (Version 8.x and earlier)	Server Name (**System > Server)**
CUCM (Version 9.x and later)	Server Name **(System > Server)** IM and Presence Server (**User Management > User Settings > UC Servi IM and Presence)** Voicemail Host Name **(User Management > User Settings > UC Service Voicemail)** Mailstore Name **(User Management > User Settings > UC Service > Mailstore)** Conferencing Host Name (**(User Management > User Settings > UC Ser > Conferencing)** (Meeting Place Only)
Cisco Unity Connection (All versions)	**No Change needed**

Provide XMPP Domain to Clients

The client identifies XMPP certificates with the XMPP domain, rather than with 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 these steps in order to ensure that the presence server provides the XMPP domain to the client:

1. Open the administration interface for your presence server, either the **Cisco Unified CM IM and Presence Administration** interface or the **Cisco Unified Presence Administration** interface.
2. Navigate to **System > Security > Settings**.
3. Locate the **XMPP Certificate Settings** section.
4. Specify the presence server domain in the **Domain name for XMPP Server-to-Server Certificate Subject Alternative Name** field.
5. Check the **Use Domain Name for XMPP Certificate Subject Alternative Name** check box.
6. Click **Save**.
7. After you save this change, you must regenerate the **cup-xmpp** certificate on the server.
8. Restart **XCP Router** in order for the change to take effect.

   Caution: A restart of the XCP Router impacts service.

Certificate Validation is now complete!

Related Information

- **Cisco Jabber 9.2.5 Release Notes**
- **Cisco Jabber: Mandatory Server Certificate Validation TechNote**
- **Technical Support & Documentation - Cisco Systems**