Jabber Certificates Quick Start Guide

Current versions of Jabber require the tomcat.pem and cup-xmpp.pem certificates to be valid when connecting to Cisco Unified Communications Manager (CUCM), Cisco UnifiedPresence Server (CUPS)/Instant Messaging and Presence (IMP), Cisco Unity Connection (CUC), and WebEx Meeting Server (WMS). Only CUPS/IMP has the cup-xmpp.pem certificate.

Valid certificates will meet the following requirements.

The certificate subject cn or Subject Alternate Name must contain the FQDN, resolve by DNS, and match the UC service configuration.

Use nslookup to confirm both the host name and fully qualified domain name (FQDN), resolve to the correct IP address for all servers. While you are at it, confirm the IP address resolves to the correct hostname.

Confirm the UC service configuration contains the FQDN for all servers (CUCM, CUPS/IMP, CUC, WMS).

CUCM & IMP 9.0+
1. On CUCM, via User Management > User Settings > UC Service
2. On IMP, via System > Cluster Topology via Application > Legacy Clients > CCMCIP Profile

CUCM & CUPS 8.0, 8.5, 8.6
1. If you have CUCM and CUPS 8, the UC service profile is only on CUPS, via Application > Cisco Unified Personal Communicator

The Jabber client's OS must trust the certificate.

For client trust, you simply need to have the root certificate which signed the tomcat.pem and cup-xmpp.pem loaded in to the computer's Enterprise Trust certificate store.

By default CUCM, CUPS, CUC, and WMS servers will generate a self-signed, AKA root certificates for tomcat.pem and cup-xmpp.pem. You can get the client to trust the self-signed root certificates by doing one of the following.

1. Accepting the certificates when prompted, will automatically add them to Enterprise Trust certificate store.
2. Pre-load the certificates in to the Enterprise Trust certificate store. This can be done on each computer, or pushed out using AD.
Optionally, you can have the tomcat.pem and cup-xmpp.pem certificates signed by a 3rd party Certificate Authority (also known as CA). The advantage here is, most operating systems come pre-loaded with the root certificates for most 3rd party CA's, avoiding all client side certificate management. CUCM, CUPS/IMP, CUC, and WMS servers do not come pre-loaded with 3rd party CA root certificates. So, when using 3rd party signed certificates, you will need to load the certificate chain on to the servers as either tomcat-trust or cup-xmpp-trust. A certificate chain is the root certificate and any intermediate certificates used by the CA to sign the server’s tomcat.pem or cup-xmpp.pem certificate.

**Common Problems**

OS X will always prompt to trust a self-signed certificate even after it has been loaded in to the certificate store, so for OS X you will need 3rd party signed certificates to avoid the prompt.

If you have accepted a certificate at logon, then get prompted to accept them again at the next logon, you have a mis-match between your certificate subject cn or subject alternate name and the UC profile configuration.

If you pre-load certificates to the Enterprise Trust certificate store and still get prompted at logon, you probably have the wrong certificates. Look very closely at the subject and serial number of the certificate prompt and compare it with the one in the certificate store.

**References**

**JABBER WINDOWS 9.2.5 RELEASE NOTES, SET UP CERTIFICATE VALIDATION**


Important topics, search for:

- Required Certificates
- Get Certificates Signed by Certificate Authority
- Certificate Signing Request Formats and Requirements
- Server Identity in Certificates
- Import Root Certificates on Client Computers

**JABBER COMPLETE HOW-TO GUIDE FOR CERTIFICATE VALIDATION**