Unified CM Requirements

Unified CM Dial Plan

The Unified CM dial plan is not impacted by devices registering via Expressway. Remote and mobile devices still register directly to Unified CM and their dial plan will be the same as when it is registered locally.

Unified CM and Expressway in Different Domains Deployment

Unified CM nodes and Expressway peers can be located in different domains. For example, your Unified CM nodes may be in the `enterprise.com` domain and your Expressway system may be in the `edge.com` domain.

In this case, Unified CM nodes must use IP addresses or FQDNs for the **Server host name** / **IP address** to ensure that Expressway can route traffic to the relevant Unified CM nodes.

Unified CM servers and IM and Presence Service servers must share the same domain.

DNS Host Name / FQDN

The first character of the DNS host name defined for the Unified CM must be a letter (do not start with a digit or special character).

Server Certificate Requirements for Unified Communications Manager

Cisco Unified Communications Manager Certificates

Two Cisco Unified Communications Manager certificates are significant for Mobile and Remote Access:

- *CallManager* certificate
- *Tomcat* certificate

These certificates are automatically installed on the Cisco Unified Communications Manager and by default they are self-signed and have the same common name (CN).

We recommend using CA-signed certificates. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. So if the *CallManager* and *tomcat* self-signed certificates have the same CN in the Expressway's trusted CA list, the Expressway can only trust one of them. This means that either secure HTTP or secure SIP, between Expressway-C and Cisco Unified Communications Manager, will fail.

Also, when generating tomcat certificate signing requests for any products in the Cisco Collaboration Systems Release 10.5.2, you need to be aware of CSCus47235. You need to work around this issue to ensure that the FQDNs of the nodes are in the certificates as Subject Alternative Name (SAN) entries. The *Expressway X8.5.3 Release Note* on the Release Notes page has details of the workarounds.

IM and Presence Service Certificates

Two IM and Presence Service certificates are significant if you use XMPP:

- *cup-xmpp* certificate
- *tomcat* certificate

We recommend using CA-signed certificates. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. If the cup-xmpp and tomcat (self-signed) certificates have the same CN, Expressway only trusts one of them, and some TLS attempts between Cisco Expressway-E and IM and Presence Service servers will fail. For more details, see CSCve56019.

Expressway Certificates

The Expressway certificate signing request (CSR) tool prompts for and incorporates the relevant Subject Alternative Name (SAN) entries as appropriate for the Unified Communications features that are supported on that Expressway.

A table that lists which CSR alternative name elements apply to which Unified Communications features, is provided in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

Expressway-C Server Certificate Requirements

The Expressway-C server certificate must include the following elements in its list of subject alternate names:

- **Unified CM phone security profile names**
- **IM and Presence chat node aliases (federated group chat)**

  The Expressway-C automatically includes the chat node aliases in the certificate signing request (CSR), providing it has discovered a set of IM and Presence Service servers.

  We recommend that you use DNS format for the chat node aliases when generating the CSR. You must include the same chat node aliases in the Expressway-E server certificate's alternative names.

More details, including the process to generate the CSR, are provided in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

Expressway-E Server Certificate Requirements

The Expressway-E server certificate needs to include the following elements in its list of subject alternative names (SAN):

- **Unified CM registrations domains**
- **XMPP federation domains**
- **IM and Presence chat node aliases (federated group chat)**

More details, including the process to generate the CSR, are provided in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

Unified CM Denial of Service Threshold

High volumes of Mobile and Remote Access calls may trigger denial of service thresholds on Unified CM. This is because all the calls arriving at Unified CM are from the same Expressway-C (cluster).

If necessary, we recommend that you increase the level of the **SIP Station TCP Port Throttle Threshold** (**System** > **Service Parameters**, and select the **Cisco CallManager** service) to 750 KB/second.