Server Certificate Requirements for Unified Communications

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.

The following table shows which CSR alternative name elements apply to which Unified Communications features:

Add these items as subject alternative names	**When generating a CSR for these purposes**			
	Mobile and Remote Access	Jabber Guest	XMPP Federation	Business to Business Calls
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM SIP registration domains)	Required on Expressway-E only	—	—	—
XMPP federation domains	—	—	Required on Expressway-E only	—
IM and Presence chat node aliases (federated group chat)	—	—	Required	—
Unified CM phone security profile names	Required on Expressway-C only	—	—	—
(Clustered systems only) Expressway Cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C only	—

Note

- You may need to produce a new server certificate for the Expressway-C if chat node aliases are added or renamed. Or when IM and Presence nodes are added or renamed, or new TLS phone security profiles are added.
- You must produce a new Expressway-E certificate if new chat node aliases are added to the system, or if the Unified CM or XMPP federation domains are modified.
- You must restart the Expressway for any new uploaded server certificate to take effect.

More details about the individual feature requirements per Expressway-C / Expressway-E are described below.

Expressway-C server certificate requirements

The Expressway-C server certificate must include the elements listed below in its list of Subject Alternative Names (SAN).

- **Unified CM phone security profile names**: The names of the **Phone Security Profiles** in Unified CM are configured for encrypted Transport Line Signaling (TLS) and are used for devices requiring remote access. Use the Fully Qualified Domain Name (FQDN) format and separate multiple entries with commas.

  It is essential to generate Certificate Signing Request (CSR) for the new node while adding a new Expressway-C node to an existing cluster of Expressway-C. It is mandated to put secure profile names as they are on CUCM, if secure registration of Mobile and Remote Access (MRA) client is needed over MRA. CSR creation on the new node will fail if "Unified CM phone security profile names" are just names or hostnames on CUCM device security profiles. This will force Administrators to change the value of "Unified CM phone security profile names" on CUCM under the **Secure Phone Profile** page.

  From X12.6, it is mandated that the Unified CM phone security profile name must be a Fully Qualified Domain Name (FQDN). It cannot be just any name or hostname or a value.

  For example, `jabbersecureprofile.domain.com`, `DX80SecureProfile.domain.com`

  Note The FQDN can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter.

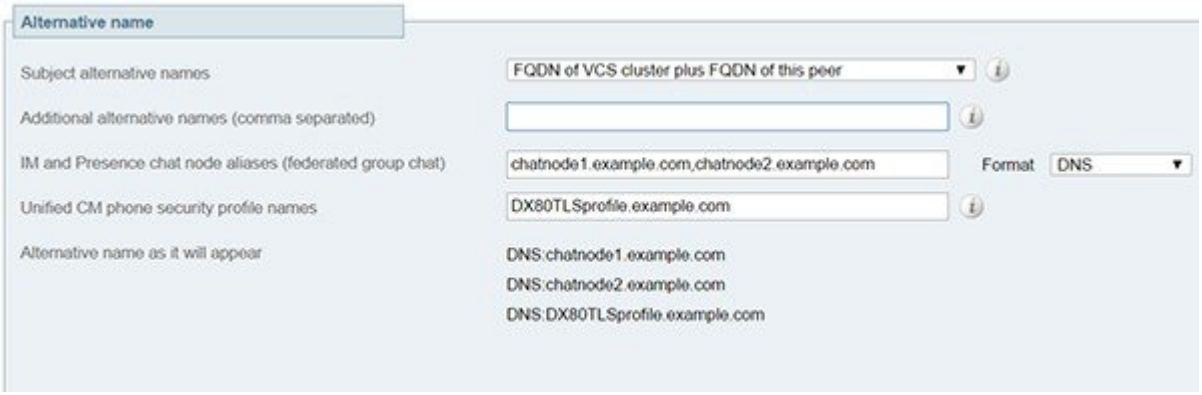
  Having the secure phone profiles as alternative names means that Unified CM can communicate via Transport Line Signaling (TLS) with the Expressway-C when it is forwarding messages from devices that use those profiles.

- **IM and Presence chat node aliases (federated group chat):** the **Chat Node Aliases** (e.g. chatroom1.example.com) that are configured on the IM and Presence servers. These are required only for Unified Communications XMPP federation deployments that intend to support group chat over TLS with federated contacts.

  The Expressway-C automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM&P 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.

Figure 1: Enter subject alternative names for security profiles and chat node aliases on the Expressway-C's CSR generator



Expressway-E server certificate requirements

The Expressway-E server certificate must include the elements listed below in its list of subject alternative names (SAN). If the Expressway-E is also known by other FQDNs, all of the aliases must be included in the server certificate SAN.

- **Unified CM registrations domains:** all of the domains which are configured on the Expressway-C for Unified CM registrations. Required for secure communications between endpoint devices and Expressway-E.

  The Unified CM registration domains used in the Expressway configuration and Expressway-E certificate, are used by Mobile and Remote Access clients to lookup the *_collab-edge* DNS SRV record during service discovery. They enable MRA registrations on Unified CM, and are primarily for service discovery.

  These service discovery domains may or may not match the SIP registration domains. It depends on the deployment, and they do not have to match. One example is a deployment that uses a .local or similar private domain with Unified CM on the internal network, and public domain names for the Expressway-E FQDN and service discovery. In this case, you need to include the public domain names in the Expressway-E certificate as SANs. There is no need to include the private domain names used on Unified CM. You only need to list the edge domain as a SAN.

  Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. You may select *CollabEdgeDNS* format instead, which simply adds the prefix collab-edge. to the domain that you enter. This format is recommended if you do not want to include your top level domain as a SAN (see example in following screenshot).

- **XMPP federation domains:** the domains used for point-to-point XMPP federation. These are configured on the IM&P servers and should also be configured on the Expressway-C as domains for XMPP federation.

  Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the Expressway software.

- **IM and Presence chat node aliases (federated group chat):** the same set of **Chat Node Aliases** as entered on the Expressway-C's certificate. They are only required for voice and presence deployments which will support group chat over TLS with federated contacts.

You can copy the list of chat node aliases from the equivalent **Generate CSR** page on the Expressway-C.

Figure 2: Enter subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator