



Unified Communications

- [Unified Communication Prerequisites, on page 1](#)
- [Mobile and Remote Access Overview, on page 13](#)
- [XMPP Federation Through Expressway, on page 15](#)
- [Delayed Cisco XCP Router Restart, on page 18](#)
- [Jabber Guest Services Overview, on page 19](#)
- [Meeting Server Web Proxy on Expressway, on page 20](#)

Unified Communication Prerequisites

Configuring a Secure Traversal Zone Connection for Unified Communications

Unified Communications features such as Mobile and Remote Access or Jabber Guest, require a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E. This involves:

- Installing suitable security certificates on the Expressway-C and the Expressway-E.
- Configuring a Unified Communications traversal zone between the Expressway-C and the Expressway-E.



Note Configure only one *Unified Communications traversal zone* per Expressway traversal pair. That is, one *Unified Communications traversal zone* on the Expressway-C cluster, and one corresponding *Unified Communications traversal zone* on the Expressway-E cluster.

Installing Expressway Security Certificates

You must set up trust between the Expressway-C and the Expressway-E:

1. Install a suitable server certificate on both the Expressway-C and the Expressway-E.
 - The certificate must include the **Client Authentication** extension. The system will not let you upload a server certificate without this extension when Unified Communications features are enabled.
 - The Expressway includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR:
 - Ensure that the CA that signs the request does not strip out the client authentication extension.

- The generated CSR includes the client authentication request and any relevant subject alternate names for the Unified Communications features that have been enabled (see [Server Certificate Requirements for Unified Communications](#)).
 - To generate a CSR and /or to upload a server certificate to the Expressway, go to **Maintenance > Security > Server certificate**. You must restart the Expressway for the new server certificate to take effect.
2. Install on both Expressways the trusted Certificate Authority (CA) certificates of the authority that signed the Expressway's server certificates.

There are additional trust requirements, depending on the Unified Communications features being deployed.

For Mobile and Remote Access deployments:

- The Expressway-C must trust the Unified CM and IM&P tomcat certificate.
- If appropriate, both the Expressway-C and the Expressway-E must trust the authority that signed the endpoints' certificates.

For Jabber Guest deployments:

- When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the Expressway-C either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server's certificate.

To upload trusted Certificate Authority (CA) certificates to the Expressway, go to **Maintenance > Security > Trusted CA certificate**. You must restart the Expressway for the new trusted CA certificate to take effect.

See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway Configuration Guides](#) page.

Configuring Encrypted Expressway Traversal Zones

To support Unified Communications features via a secure traversal zone connection between the Expressway-C and the Expressway-E:

- Configure the Expressway-C and Expressway-E with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on Expressway-C or a traversal server zone when selected on Expressway-E) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.
- Both Expressways must trust each other's server certificate. As each Expressway acts both as client and server, you must ensure that each Expressway's certificate is valid both as client and server.
- Be aware that Expressway uses the SAN attribute (Subject Alternative Name) to validate the received certificate, not the CN (Common Name).
- If you require a H.323 or a nonencrypted connection, configure a separate pair of traversal zones.



Note If ICMP is blocked between Expressway-C and Expressway-E then secure test fails with “<Exp-E FQDN> cannot be reached” error. (simulated in TAC lab by creating a firewall rule in Expressway-E to drop the ICMP queries from Expressway-C).

To set up a secure traversal zone

To set up a secure traversal zone, configure your Expressway-C and Expressway-E as follows:

- Step 1** Go to **Configuration > Zones > Zones**.
- Step 2** Click **New**.
- Step 3** Configure the fields as follows (leave all other fields with default values):

	Expressway-C	Expressway-E
Name	“Traversal zone” for example	“Traversal zone” for example
Type	<i>Unified Communications traversal</i>	<i>Unified Communications traversal</i>
Connection credentials section		
Username	“exampleauth” for example	“exampleauth” for example Note: When creating users for a local authentication database, do not include a space in this field.
Password	“ex4mpl3.c0m” for example	Click Add/Edit local authentication database , then in the popup dialog click New and enter the Name (“exampleauth”) and Password (“ex4mpl3.c0m”) and click Create credential .
SIP section		
Port	Must match the Expressway-E setting.	7001 (default. See the <i>Cisco Expressway IP Port Usage Configuration Guide</i> , for your version, on the Cisco Expressway Series Configuration Guides page.)
TLS verify subject name	Not applicable	Enter the name to look for in the traversal client's certificate (must be in the SAN - Subject Alternative Name - attribute). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate.
Authentication section		

	Expressway-C	Expressway-E
Authentication policy	<i>Do not check credentials</i>	<i>Do not check credentials</i>
Location section		
Peer 1 address	Enter the FQDN of the Expressway-E. Note If you use an IP address (not recommended), that address must be present in the Expressway-E server certificate.	Not applicable
Peer 2...6 address	Enter the FQDNs of additional peers if it is a cluster of Expressway-Es.	Not applicable

Step 4 Click **Create zone**.

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.



Note The parameter used to define the Unified CM node within the Host Name/IP Address of Unified CM (FQDN preferred) must be present within the *Unified CM tomcat* certificate as Subject Alternative Name (SAN).

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.

The Endpoint supports OAuth Authentication functionality. The Phone Security Profile configuration is detailed as follows:

1. The Endpoint is linked to Phone Security Profile with Device Security Mode set as *Encrypted* and **with** OAuth Authentication enabled, then the Phone does not require its Security Profile Name to be part of the Subject Alternate Name (SAN) list of Expressway-C certificate.
2. The Endpoint is linked to Phone Security Profile with Device Security Mode set as *Encrypted* but **without** OAuth Authentication enabled, then the Phone requires its Security Profile Name to be part of the Subject Alternate Name (SAN) list of Expressway-C certificate.

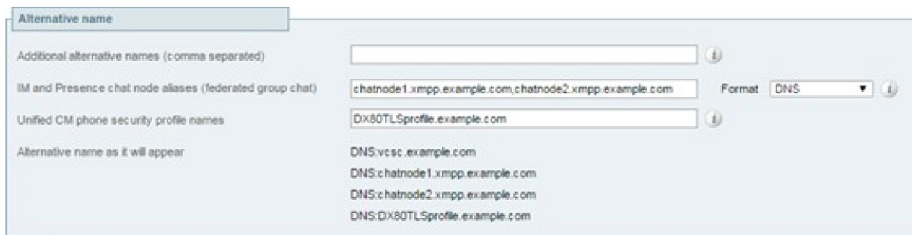
Having the secure phone profiles as alternative names means that Unified CM can communicate via Transport Line Signaling (TLS) with the Expressway-C when it is forwarding messages from devices that use those profiles.

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



454313

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 don't 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.



Note 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.



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

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

The screenshot shows a form titled "Alternative name" with the following fields and values:

Field	Value	Format
Subject alternative names	FQDN of Expressway cluster plus FQDN of this peer	(Dropdown)
Additional alternative names (comma separated)	(Empty)	(Dropdown)
Unified CM registrations domains	example.com	CollabEdgeDNS
XMPP federation domains	example.com	DNS
IM and Presence chat node aliases (federated group chat)	chatnode1.example.com,chatnode2.example.com	DNS
Alternative name as it will appear	DNS:vcse.example.com DNS:vcs-e-cluster.example.com DNS:collab-edge.example.com DNS:example.com DNS:chatnode1.example.com DNS:chatnode2.example.com	

454312

For detailed information, see *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway Configuration Guides](#) page.

Certificates for mTLS if you use MRA onboarding

If you enable activation code onboarding over MRA, the necessary CA certificates for mutual TLS are automatically generated (mutual TLS is a requirement for activation code onboarding). The certificates are available on the CA certificate page for mTLS, which you access from the Trusted CA certificate page (**Maintenance > Security > Trusted CA certificate**).

Managing Domain Certificates and Server Name Indication

Multitenancy is part of Cisco Hosted Collaboration Solution (HCS), and allows a service provider to share a Expressway-E cluster among multiple tenants.

Using the Server Name Indication (SNI) protocol extension within TLS, the Expressway can now store and use domain-specific certificates that can be offered to a client during the TLS handshake. This capability

allows seamless integration of endpoints registering through MRA in a multitenant environment, and ensures the certificate domain name matches the client's domain. During a TLS handshake, the client includes an SNI field in the *ClientHello* request. The Expressway looks up its certificate store and tries to find a match for the SNI hostname. If a match is found the domain-specific certificate is returned to the client.



Note In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

See *Multitenancy with Cisco Expressway* on the [Cisco Hosted Collaboration Solution](#) page.

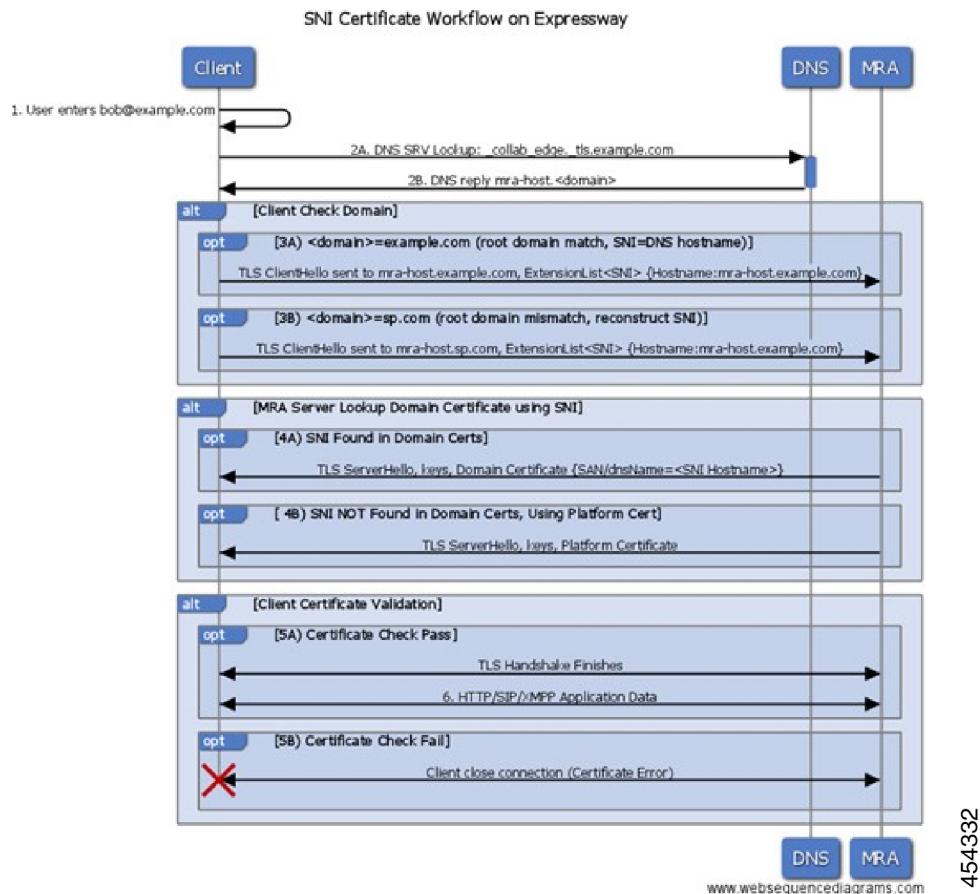
SNI Call Flow

1. On the MRA client being registered, the user enters **bob@example.com** where **example.com** is the user's service domain (customer domain).
2. The client does a DNS resolution.
 - a. It sends a DNS SRV request for **_collab-edge._tls.example.com**.
 - b. The DNS replies to the request:
 - In a single tenant setup: the DNS reply usually includes the hostname within the service domain (for example, **mra-host.example.com**).
 - In a multitenant setup: DNS may instead return the service provider's MRA hostname in the service provider's domain, which is different from the user's service domain (for example, **mra-host.sp.com**).
3. The client sets up SSL connection.
 - a. The client sends SSL ClientHello request with an SNI extension:
 - If the DNS-returned hostname has the same domain as the user's service domain, the DNS hostname is used in SNI server_name (unchanged).
 - Otherwise, in the case of a domain mismatch, the client sets the SNI server_name to the DNS hostname plus the service domain (for example instead of the DNS-returned **mra host.sp.com** it changes to **mra-host.example.com**).
 - b. The Expressway-E searches its certificate store to find a certificate matching the SNI hostname.
 - If a match is found, the Expressway-E will send back the certificate (SAN/dnsName=SNI hostname)
 - Otherwise, MRA will return its platform certificate.
 - c. The client validates the server certificate.
 - If the certificate is verified, SSL setup continues and SSL setup finishes successfully.
 - Otherwise, a certificate error occurs.

4. Application data starts.



Note For SIP and HTTPS, the application starts SSL negotiation immediately. For XMPP, the SSL connection starts once the client receives XMPP StartTLS.



Managing the Expressway's Domain Certificates

You manage the Expressway's domain certificates through the **Domain certificates** page (**Maintenance > Security > Domain certificates**). These certificates are used to identify domains when multiple customers - in a multitenant environment - are sharing an Expressway-E cluster to communicate with client systems using TLS encryption and with web browsers over HTTPS. You can use the domain certificate page to:

- View details about the currently loaded certificate.
- Generate a Certificate Signing Request (CSR).
- Upload a new domain certificate.

- Configure the Automated Certificate Management Environment (ACME) service to automatically submit a CSR to an ACME provider, and automatically deploy the resulting server certificate.



Note We highly recommend using certificates based on RSA keys. Other types of certificate, such as those based on DSA keys, are not tested and may not work with the Expressway in all scenarios. Use the **Trusted CA certificate** page to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway.

Viewing a Currently Uploaded Domain Certificate

When you click on a domain, the domain certificate data section shows information about the specific domain certificate currently loaded on the Expressway.

To view the currently uploaded domain certificate file, click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format.

To delete the currently uploaded domain, click **Delete**.



Note Do not allow your domain certificate to expire as this may cause other external systems to reject your certificate and prevent the Expressway from being able to connect to those systems.

Adding a New Domain

Step 1 Go to **Maintenance > Security > Domain certificates**.

Step 2 Click **New**.

Step 3 Under **New local domain**, enter the name of the domain you wish to add.

Example:

An example valid domain name is `100.example-name.com`.

Step 4 Click **Create domain**.

Step 5 The new domain will be added on the **Domain certificates** page and you can proceed to upload a certificate for the domain.

Generating a Certificate Signing Request

The Expressway can generate domain CSRs, which removes the need to use an external mechanism to generate and obtain certificate requests.

Note

- Only one signing request can be in progress at any one time. This is because the Expressway must keep track of the private key file associated with the current request. To discard the current request and start a new request, click **Discard CSR**.
- The user interface provides an option to set the Digest Algorithm. The default is set to SHA-256, with options to change it to SHA-384 or SHA-512.
- The user interface provides an option to set the key length. Expressway supports a key length of 1024, 2048 and 4096.

Step 1 Go to **Maintenance > Security > Domain certificates**.

Step 2 Click on the domain for which you wish to generate a CSR.

Step 3 Click **Generate CSR** to go to the **Generate CSR** page.

Step 4 Enter the required properties for the certificate.

See [Domain Certificates and Clustered Systems](#), page 145 if your Expressway is part of a cluster.

Step 5 Click **Generate CSR**. The system will produce a signing request and an associated private key. The private key is stored securely on the Expressway and cannot be viewed or downloaded.

Note Never disclose your private key, not even to the certificate authority.

Step 6 You are returned to the **Domain certificate** page. From here you can:

- Download the request to your local file system so that it can be sent to a certificate authority. You are prompted to save the file (the exact wording depends on your browser).
- View the current request (click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format).

Uploading a New Domain Certificate

When the signed domain certificate is received back from the certificate authority, it must be uploaded to the Expressway. Use the **Upload new certificate** section to replace the current domain certificate with a new certificate.

Step 1 Go to **Maintenance > Security > Domain certificates**.

Step 2 Use the **Browse** button in the **Upload new certificate** section to select and upload the domain certificate PEM file.

Step 3 If you used an external system to generate the CSR you must also upload the server private key PEM file that was used to encrypt the domain certificate. (The private key file will have been automatically generated and stored earlier if the Expressway was used to produce the CSR for this domain certificate.)

- The server private key PEM file must not be password protected.
- You cannot upload a server private key if a certificate signing request is in progress.

Step 4 Click **Upload domain certificate data**.

Automated Certificate Management Environment Service

The Automated Certificate Management Environment (ACME) service on the Expressway-E, from version X12.5, can request and deploy domain certificates (used with SNI).

When you go to **Maintenance > Security > Domain certificates**, the list of domains has an ACME column that shows the status of the **ACME** service for each domain.

Click **View/Edit** next to the domain name to enable the ACME service.

The process of configuring ACME service for domain certificates is the same as it is for the server certificate, only from a different place in the Expressway-E interface.

See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway Configuration Guides](#) page.

Domain Certificates and Clustered Systems

When a CSR is generated, a single request and private key combination is generated for that peer only.

If you have a cluster of Expressways, you must generate a separate signing request on each peer. Those requests must then be sent to the certificate authority and the returned domain certificates uploaded to each relevant peer.



Note Make sure that the correct domain certificate is uploaded to the appropriate peer, otherwise the stored private key on each peer will not correspond to the uploaded certificate.

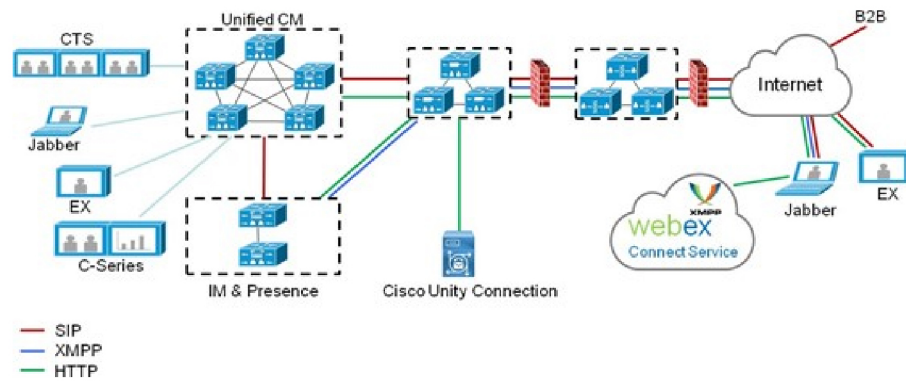
Mobile and Remote Access Overview

Cisco Unified Communications Mobile and Remote Access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides the following functions:

- **Off-premises access:** A consistent experience outside the network for Jabber and EX/MX/SX Series clients.
- **Security:** Secure business-to-business communications.
- **Cloud services:** Enterprise grade flexibility and scalable solutions providing rich Cisco Webex integration and service provider offerings.
- **Gateway and interoperability services:** Media and signaling normalization, and support for non-standard endpoints.

Figure 3: Unified Communications: Mobile and Remote Access

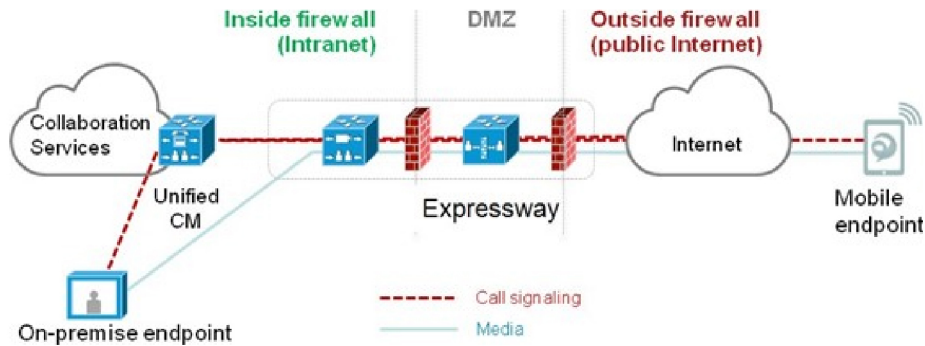


454334



Note Third-party SIP or H.323 devices can register to the Expressway-C and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.

Figure 4: Typical call flow - signaling and media paths



454333

Unified CM provides call control for both mobile and on-premises endpoints.

Signaling traverses the Expressway solution between the mobile endpoint and Unified CM. Media traverses the Expressway solution and is relayed between endpoints directly.

All media is encrypted between the Expressway-C and the mobile endpoint.

Deployment Scope

The following major Expressway-based deployments do not work together. They cannot be implemented together on the same Expressway (or traversal pair):

- Mobile and Remote Access
- Microsoft interoperability, using the Expressway-C-based B2BUA

- Jabber Guest services

Mobile and Remote Access Ports

Information about MRA ports is available in the *Cisco Expressway IP Port Usage Configuration Guide* at the [Cisco Expressway Series Configuration Guides](#) page. This includes ports that can potentially be used between the internal network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located), and between the DMZ and the public internet.

Jabber Client Connectivity Without VPN

The MRA solution supports a hybrid on-premises and cloud-based service model. This provides a consistent experience inside and outside the enterprise. MRA provides a secure connection for Jabber application traffic without having to connect to the corporate network over a VPN. It is a device and operating system agnostic solution for Cisco Jabber clients on Windows, Mac, iOS and Android platforms.

MRA allows Jabber clients that are outside the enterprise to do the following:

- Use instant messaging and presence services
- Make voice and video calls
- Search the corporate directory
- Share content
- Launch a web conference
- Access visual voicemail

Where to Get Detailed Configuration Information

For details about using Expressway for MRA, see the *Mobile and Remote Access Deployment Guide* on the [Expressway Configuration Guides](#) page. The guide describes:

- How to enable and configure MRA features on Expressway-C and Expressway-E?
- How to discover the Unified CM servers and IM&P servers used by the MRA service?
- MRA access control, including authentication settings, SAML SSO, and allow lists.
- How to enable support for push notifications?

XMPP Federation Through Expressway

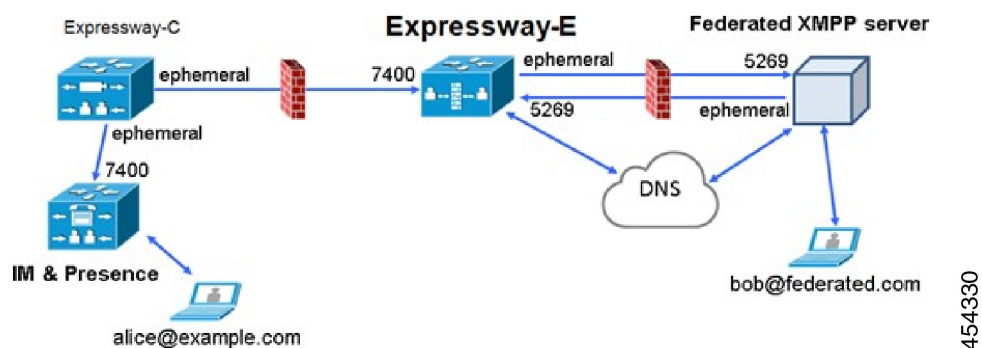
External XMPP federation enables users registered to Cisco Unified Communications Manager IM and Presence Service, to communicate via the Expressway-E with users from a different XMPP deployment.



Note This section describes XMPP federation as managed through Expressway, but it can also be managed through the IM and Presence Service, as described later in this guide.

The diagram shows XMPP message routing from the on-premises IM & Presence server, through the Expressway-C and Expressway-E Collaboration Edge solution, to the federated XMPP server. It also shows the ports and connections as the messages traverse DMZ firewalls. The “example.com” organization is using an Expressway federation model (left of picture), while the “federated.com” organization (right of picture) is using an IM and Presence Service in DMZ federation model.

Figure 5: Message routing for XMPP federation



Supported Systems

Expressway-E supports XMPP federation with the following products:

- Expressway X8.2 or later
- Cisco Unified Communications Manager IM and Presence Service 9.1.1 or later
- Cisco Webex Connect Release 6.x
- Cisco Jabber 9.7 or later
- Other XMPP standards-compliant servers

Limitations

- When using Expressway for XMPP federation, the Expressway-E handles the connection to the remote federation server and can only use Jabber IDs to manage XMPP messages. Expressway-E does not support XMPP address translation (of email addresses, for example).

If you, as an external user, try to chat with a user in an enterprise through federation, you must use the enterprise user’s Jabber ID to contact them through XMPP. If their Jabber ID does not match their email address (especially if their Jabber ID uses an internal user ID or domain) you are unable to have federation, as you won’t know the enterprise user’s email address. We therefore recommend that enterprises configure their Unified CM nodes to use the same address for a user’s Jabber ID and email when using Expressway

for XMPP federation. This limitation does *not* apply to users contacting each other within the enterprise (not using federation) even when federation is handled by Expressway-E. You can configure IM and Presence Service to use either the Jabber ID or the Directory URI (typically email) for non-federated use cases.

To make a user's Jabber ID resemble a user's email address, so that the federated partner can approximate email addresses for federation, set the following:

- a. Unified CM Lightweight Directory Access Protocol (LDAP) attribute for User ID to be the user's sAMAccountName
 - b. IM and Presence Service presence domain to be the same as the email domain.
 - c. Your email address to be the same as samaccountname@presencedomain.
- Simultaneous internal federation managed by IM and Presence Service and external federation managed by Expressway is not supported. If only internal federation is required then you must use interdomain federation on IM and Presence Service. The available federation deployment configuration options are:
 - External federation only (managed by Expressway).
 - Internal federation only (managed by IM and Presence Service).
 - Internal and external federation managed by IM and Presence Service, but requires you to configure your firewall to allow inbound connections.

Prerequisites

- Interdomain XMPP Federation must be **disabled** on the IM and Presence Service before you enable XMPP federation on Expressway:

Go to **Cisco Unified CM IM and Presence Administration > Presence > Inter Domain Federation > XMPP Federation > Settings** and ensure that **XMPP Federation Node Status** is set to *Off*.
- XMPP federation is only supported on a single Expressway cluster.
- An Expressway-C (cluster) and Expressway-E (cluster) must be configured for Mobile and Remote Access (MRA) to Unified Communications services, as described in the *Mobile and Remote Access via Cisco Expressway Deployment Guide*. If only XMPP federation is required (video calls and remote registration to Unified CM are not required), these items do not have to be configured:
 - Domains that support *SIP registrations and provisioning on Unified CM* or that support *IM and Presence services on Unified CM*.
 - Unified CM servers (you must still configure the IM&P servers).
 - HTTP server allow list.



Note

The federated communications are available to both on-premises clients (connected directly to IM and Presence Service) and off-premises clients (connected to IM and Presence Service through MRA).

- SIP and XMPP federations are separate and do not impact on each other. For example, it's possible to deploy SIP federation on IM and Presence Service and external XMPP federation on Expressway.
- If you deploy external XMPP federation through Expressway, do not activate the Cisco XCP XMPP federation Connection Manager feature service on the IM and Presence Service.
- If you intend to use both Transport Layer Security (TLS) and group chat, the Expressway-C and Expressway-E server certificates must include in their list of subject alternate names the **Chat Node Aliases** that are configured on the IM and Presence Service servers. Use either the XMPPAddress or DNS formats.



Note The Expressway-C automatically includes the chat node aliases in its certificate signing requests (CSRs), providing it has discovered a set of IM and Presence Service servers. When generating CSRs for the Expressway-E we recommend that you copy-paste the chat node aliases from the equivalent **Generate CSR** page on the Expressway-C.

Detailed Configuration Information

For information about configuring XMPP federation managed by IM and Presence Service, see [Interdomain Federation on IM and Presence Service for Cisco Unified Communications Manager](#).

For information about configuring XMPP federation managed by Expressway, see *XMPP Federation using Expressway or IM and Presence Service* on the [Expressway Configuration Guides](#) page.

Delayed Cisco XCP Router Restart

The delayed Cisco XCP Router restart feature is part of Cisco Hosted Collaboration Solution (HCS), and is only available when the Expressway-E is in multitenant mode. The Expressway-E enters multitenant mode when you add a second Unified CM traversal zone with a new SIP domain.



Note In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

Multitenancy allows a service provider to share an Expressway-E cluster among multiple tenants. Each tenant has a dedicated Expressway-C cluster that connects to the shared Expressway-E cluster.

Certain configuration changes on the Expressway-E cluster, or a customer's Expressway-C cluster, require a restart of the Cisco XCP Router on each Expressway-E in the shared cluster. The restart is required for Cisco XCP Router configuration changes to take effect across all nodes in a multitenant Expressway-E cluster. The restart affects all users across all customers.

To reduce the frequency of this restart, and the impact on users, you can use the delayed Cisco XCP Router restart feature.



Note Without the delayed restart feature enabled, the restart happens automatically and occurs each time you save any configuration change that affects the Cisco XCP Router. If multiple configuration changes are required, resulting in several restarts of the Cisco XCP Router, it can adversely affect users. We strongly recommend that multitenant customers enable the delayed Cisco XCP Router restart feature.

For more information, please see *Cisco Unified Communications XMPP Federation using IM and Presence Service or Expressway* on the [Expressway Configuration Guides](#) page.

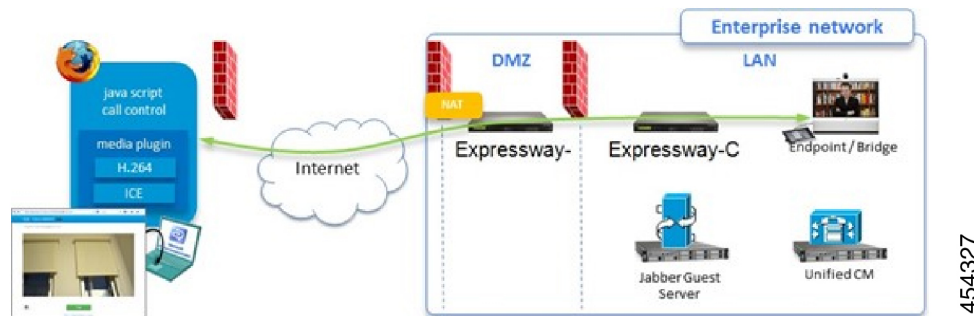
Jabber Guest Services Overview

Cisco Jabber Guest is a consumer to business (C2B) solution that extends the reach of Cisco's enterprise telephony to people outside of a corporate firewall who do not have phones registered with Cisco Unified Communications Manager.

It allows an external user to click on a hyperlink (in an email or a web page) that will download and install (on first use) an H.264 plugin into the user's browser. It then uses http-based call control to “dial” a URL to place a call to a predefined destination inside the enterprise. The user is not required to open an account, create a password, or otherwise authenticate.

To enable the call to be placed, it uses the Expressway solution (a secure traversal zone between the Expressway-C and Expressway-E) as a Unified Communications gateway to traverse the firewall between the Jabber Guest client in the internet and the Jabber Guest servers inside the enterprise to reach the destination user agent (endpoint).

Figure 6: Jabber Guest Components



Information Scope

In versions X8.7 and earlier, all Expressway configuration required for deployment with Jabber Guest was contained in the Administrator Guide. From X8.8 onwards, that information is kept in a separate deployment guide. You can read more detailed information about Jabber Guest in the following documents:

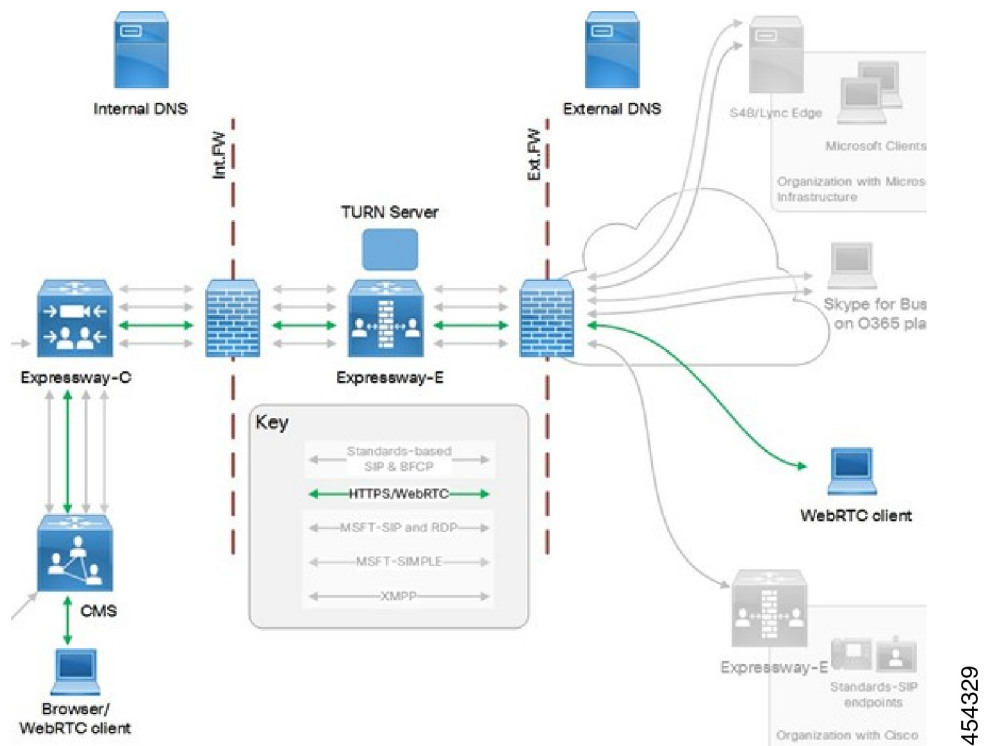
- *Cisco Expressway with Jabber Guest Deployment Guide*, at the [Expressway Configuration Guides](#) page.
- *Cisco Jabber Guest Server Installation and Configuration Guide*, for your version, at the [Jabber Guest Installation and Upgrade Guides](#) page.

- *Cisco Jabber Guest Administration Guide*, for your version, at the [Jabber Guest Maintain and Operate Guides](#) page.
- *Cisco Jabber Guest Release Notes*, for your version, at the [Jabber Guest Release Notes](#) page.

Meeting Server Web Proxy on Expressway

This option enables external users to join or administer Meeting Server spaces using their browser. All the external user needs is the URL to the space and their credentials for accessing the Meeting Server.

Figure 7: Meeting Server web proxy on Expressway



Cisco Meeting Server with Cisco Expressway Deployment Guide on the [Expressway Configuration Guides](#) page (previously called the *Cisco Expressway Traffic Classification Deployment Guide*).