Unified Communications Mobile and Remote Access via Cisco Expressway

Deployment Guide

Cisco Expressway X8.5.2
Cisco Unified CM 9.1(2)SU1 or later

April 2015

Contents

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:

- **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 WebEx integration and Service Provider offerings
- **Gateway and interoperability services**: media and signaling normalization, and support for non-standard endpoints

Figure 1: Unified Communications: mobile and remote access
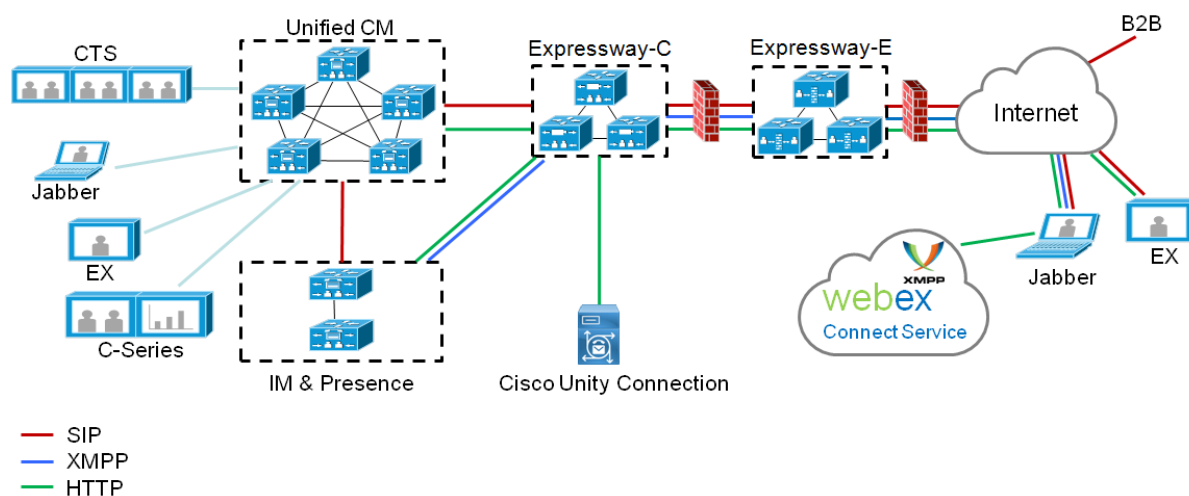
Note that third-party SIP or H.323 devices can register to a Cisco VCS connected via a neighbor zone to a Cisco Expressway and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.

Figure 2: Typical call flow: signaling and media paths
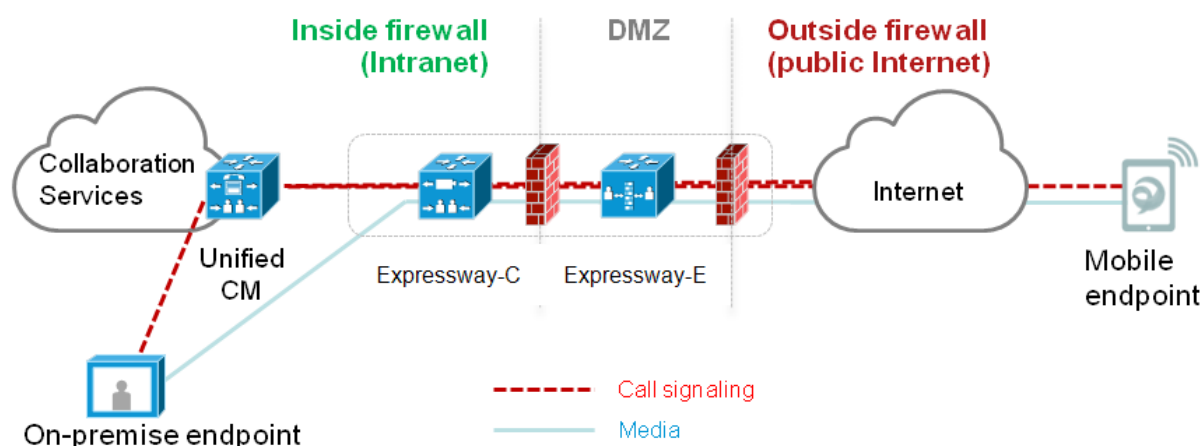
- Unified CM provides call control for both mobile and on-premises endpoints.
- Signaling traverses the Expressway solution between the mobile endpoint and Unified CM.
- Media traverses the Expressway solution and is relayed between endpoints directly; all media is encrypted between the Expressway-C and the mobile endpoint.

Jabber client connectivity without VPN

The mobile and remote access solution supports a hybrid on-premises and cloud-based service model, providing a consistent experience inside and outside the enterprise. It 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.

It allows Jabber clients that are outside the enterprise to:

- use instant messaging and presence services
- make voice and video calls
- search the corporate directory
- share content
- launch a web conference
- access visual voicemail

Note that Jabber Web and Cisco Jabber Video for TelePresence (Jabber Video) are not supported.

Related documentation

Information contained in the following documents and sites may be required to assist in setting up your Unified Communications environment:

- *Expressway Basic Configuration (Expressway-C with Expressway-E) Deployment Guide*
- *Expressway Cluster Creation and Maintenance Deployment Guide*
- *Certificate Creation and Use With Expressway Deployment Guide*
- *Expressway Administrator Guide*

- *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* (for your version), at Cisco Unified Communications Manager Configuration Guides
- *Directory Integration and Identity Management* in the Cisco Collaboration System 10.x Solution Reference Network Designs (SRND) document
- *SAML SSO Deployment Guide for Cisco Unified Communications Applications* (for your version), at Cisco Unified Communications Manager Maintain and Operate Guides
- Jabber client configuration details:
  - *Cisco Jabber for Windows*
  - *Cisco Jabber for iPad*
  - *Cisco Jabber for Android*
  - *Cisco Jabber for Mac*
  - *Cisco Jabber DNS Configuration Guide*

Deployment scenarios

This section describes the supported deployment environments:

- single network elements
- single clustered network elements
- multiple clustered network elements
- hybrid deployment
- unsupported deployments

Single network elements

In this scenario there are single (non-clustered) Unified CM, IM & Presence, Expressway-C and Expressway-E servers.
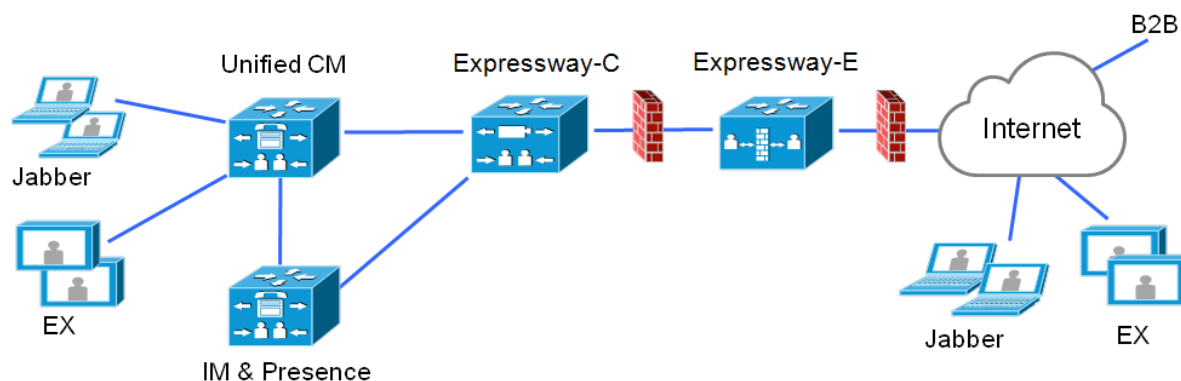
Single clustered network elements

In this scenario each network element is clustered.
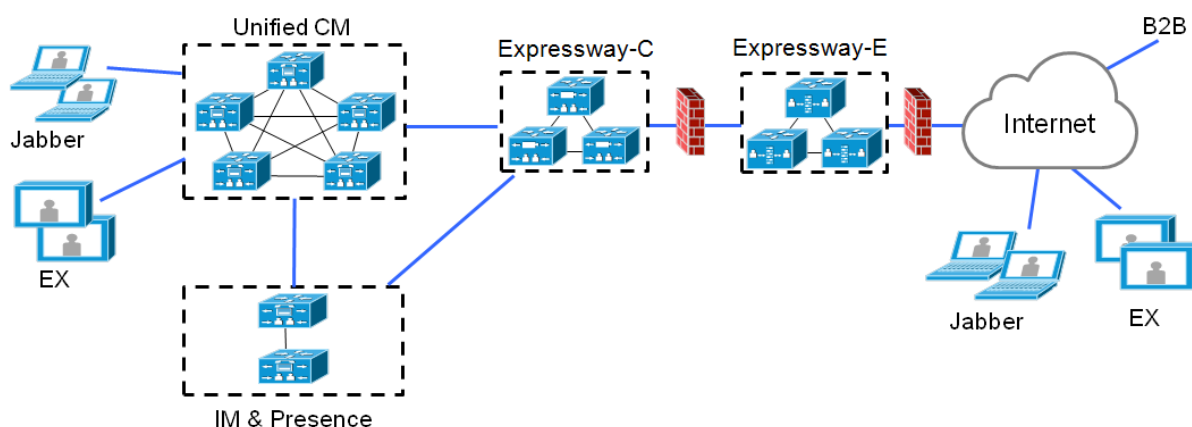
Multiple clustered network elements

In this scenario there are multiple clusters of each network element.
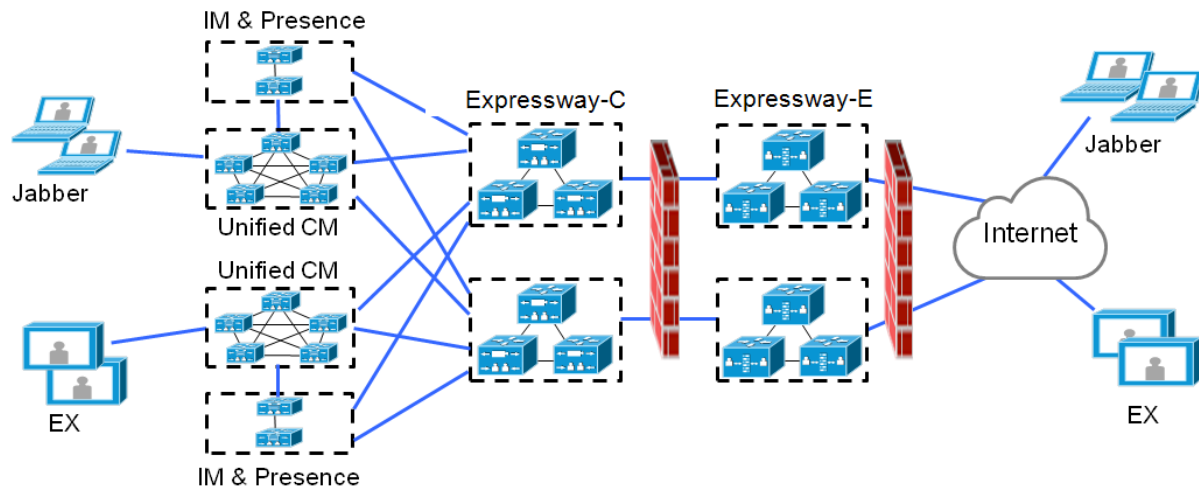
- Jabber clients can access their own cluster via any route
- Expressway-C uses round robin to select a node (publisher or subscriber) when routing home cluster discovery requests
- Each combination of Unified CM and IM and Presence Service clusters must use the same domain
- Intercluster Lookup Service (ILS) must be active on the Unified CM clusters
- Intercluster peer links must be configured between the IM and Presence Service clusters, and the Intercluster Sync Agent (ICSA) must be active

Hybrid deployment

In this scenario, IM and Presence services for Jabber clients are provided via the WebEx cloud.
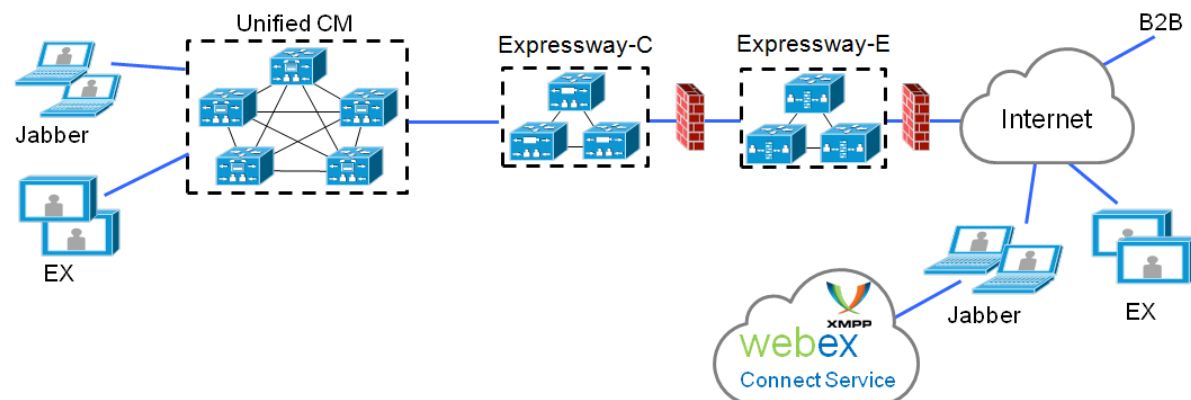
Unsupported deployments

VPN links, between the Expressway-C and the Unified CM services / clusters, are not supported.
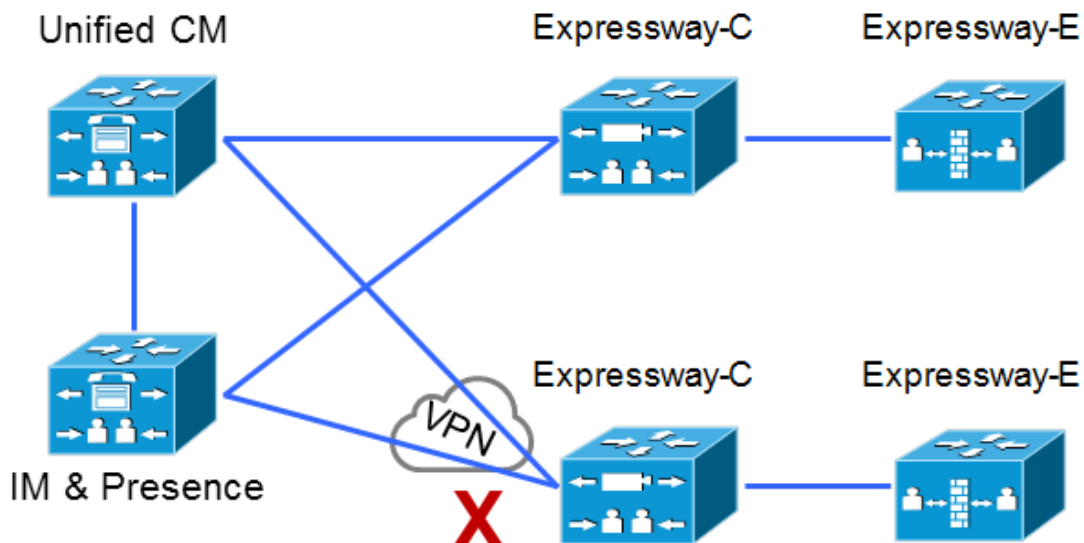
"Mixed" traversal connections are not supported. That is, we do not support traversal zones, or Unified Communications traversal zones, between Cisco VCS and Cisco Expressway *even though it is possible to configure these zones*.
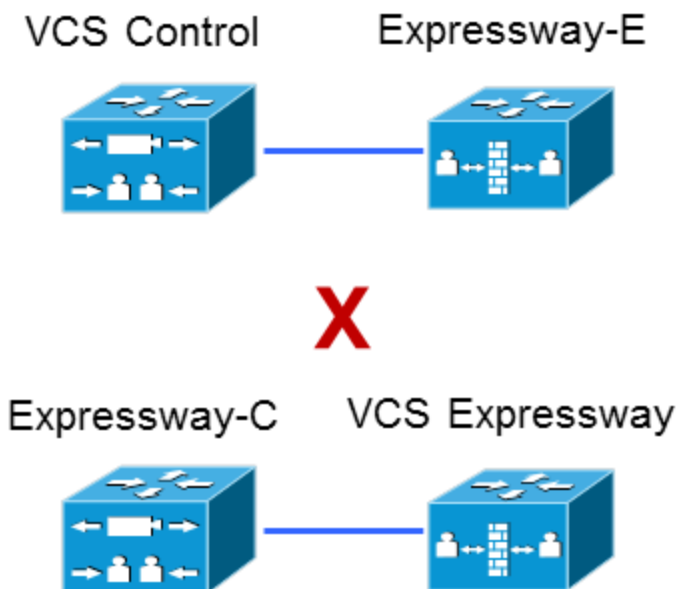
Explicitly, we do not support VCS Control traversal to Expressway-E, nor do we support Expressway-C traversal to VCS Expressway.

Configuration overview

This section summarizes the steps involved in configuring your Unified Communications system for mobile and remote access. It assumes that you already have set up:

- a basic Expressway-C and Expressway-E configuration as specified in *Expressway Basic Configuration Deployment Guide* (this document contains information about the different networking options for deploying the Expressway-E in the DMZ)
- Unified CM and IM and Presence Service have been configured as specified in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* (for your version), at Cisco Unified Communications Manager Configuration Guides

Prerequisites

Ensure that you are running the following software versions:

- Expressway X8.1.1 or later
- Unified CM 9.1(2)SU1 or later and IM and Presence Service 9.1(1) or later

Supported clients when using mobile and remote access

Expressway X8.1.1 and later:

- Cisco Jabber for Windows 9.7 or later
- Cisco Jabber for iPhone and iPad 9.6.1 or later
- Cisco Jabber for Android 9.6 or later
- Cisco Jabber for Mac 9.6 or later
- Cisco TelePresence endpoints/codecs running TC7.0.1 or later firmware

Configuration summary

EX/MX/SX Series endpoints (running TC software)

Ensure that the provisioning mode is set to *Cisco UCM via Expressway*.

On Unified CM, you need to ensure that the **IP Addressing Mode** for these endpoints is set to *IPV4_ONLY*.

These endpoints must verify the identity of the Expressway-E they are connecting to by validating its server certificate. To do this, they must have the certificate authority that was used to sign the Expressway-E's server certificate in their list of trusted CAs.

These endpoints ship with a list of default CAs which cover the most common providers (Verisign, Thawte, etc). If the relevant CA is not included, it must be added. See 'Managing the list of trusted certificate authorities' in the endpoint's administrator guide.

Mutual authentication is optional; these endpoints are not required to provide client certificates. If you do want to configure mutual TLS, you cannot use CAPF enrolment to provision the client certificates; you must manually apply the certificates to the endpoints. The client certificates must be signed by an authority that is trusted by the Expressway-E.

Jabber clients

Jabber clients must verify the identity of the Expressway-E they are connecting to by validating its server certificate. To do this, they must have the certificate authority that was used to sign the Expressway-E's server certificate in their list of trusted CAs.

Jabber uses the underlying operating system's certificate mechanism:

- Windows: Certificate Manager
- MAC OS X: Key chain access
- IOS: Trust store
- Android: Location & Security settings

Jabber client configuration details for mobile and remote access is contained within the relevant installation and configuration for that Jabber client:

- *Cisco Jabber for Windows*
- *Cisco Jabber for iPad*
- *Cisco Jabber for Android*
- *Cisco Jabber for Mac* (requires X8.2 or later)

DNS records

This section summarizes the public (external) and local (internal) DNS requirements. For more information, see *Cisco Jabber DNS Configuration Guide*.

Public DNS

The public (external) DNS must be configured with `_collab-edge._tls.<domain>` SRV records so that endpoints can discover the Expressway-Es to use for mobile and remote access. SIP service records are also required (for general deployment, not specifically for mobile and remote access). For example, for a cluster of 2 Expressway-E systems:

Domain	Service	Protocol	Priority	Weight	Port	Target host
example.com	collab-edge	tls	10	10	8443	expe1.example.com
example.com	collab-edge	tls	10	10	8443	expe2.example.com
example.com	sips	tcp	10	10	5061	expe1.example.com
example.com	sips	tcp	10	10	5061	expe2.example.com

Local DNS

The local (internal) DNS requires `_cisco-uds._tcp.<domain>` and `_cuplogin._tcp.<domain>` SRV records. For example:

Domain	Service	Protocol	Priority	Weight	Port	Target host
example.com	cisco-uds	tcp	10	10	8443	cucmserver.example.com
example.com	cuplogin	tcp	10	10	8443	cupserver.example.com

Ensure that the `cisco-uds` and `_cuplogin` SRV records are NOT resolvable outside of the internal network, otherwise the Jabber client will not start mobile and remote access negotiation via the Expressway-E.

Firewall

- Ensure that the relevant ports have been configured on your firewalls between your 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. See Mobile and remote access port reference [p.38] for more information.

- If your Expressway-E has one NIC enabled and is using static NAT mode, note that:
  You must enter the FQDN of the Expressway-E, as it is seen from outside the network, as the peer address on the Expressway-C's secure traversal zone. The reason for this is that in static NAT mode, the Expressway-E requests that incoming signaling and media traffic should be sent to its external FQDN, rather than its private name.
  This also means that the external firewall must allow traffic from the Expressway-C to the Expressway-E's external FQDN. This is known as NAT reflection, and may not be supported by all types of firewalls.
  See the *Advanced network deployments* appendix, in the *Expressway Basic Configuration (Expressway-C with Expressway-E) Deployment Guide*, for more information.
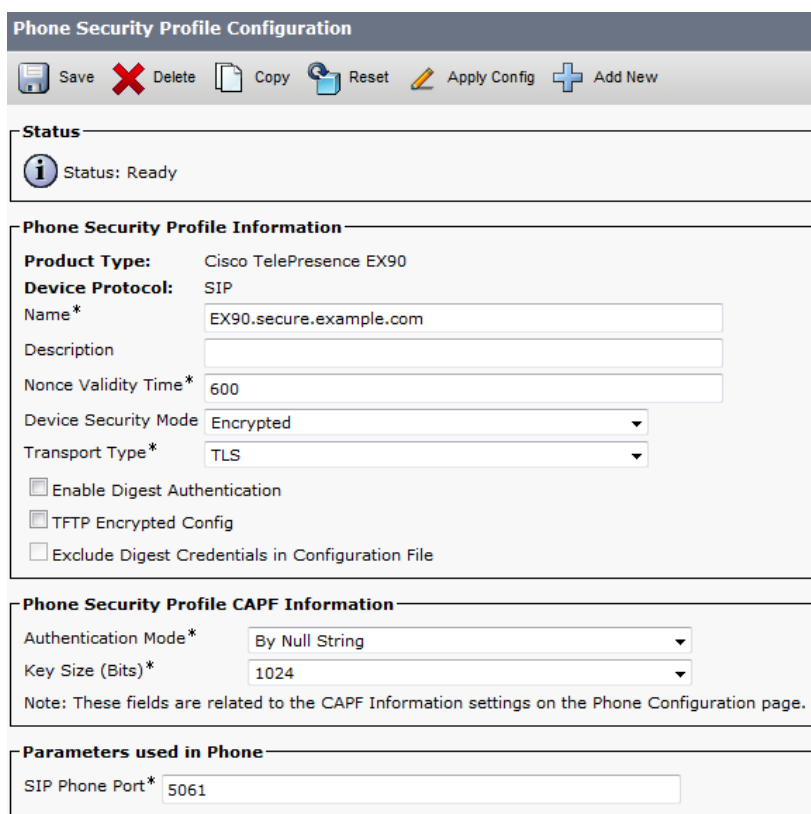
Unified CM

1. If you have multiple Unified CM clusters, you must confgure ILS (Intercluster Lookup Service) on all of the clusters.
   This is because the Expressway needs to communicate with each user's home Unified CM cluster, and to discover the home cluster it sends a UDS (User Data Service) query to any one of the Unified CM nodes.
   Search for "Intercluster Lookup Service" in the Unified CM documentation for your version.

2. Ensure that the **Maximum Session Bit Rate for Video Calls** between and within regions (**System > Region Information > Region**) is set to a suitable upper limit for your system, for example 6000 kbps.

See *Region setup* for more information.

3. The **Phone Security Profiles** in Unified CM (**System > Security > Phone Security Profile**) that are configured for TLS and are used for devices requiring remote access must have a **Name** in the form of an FQDN that includes the enterprise domain, for example jabber.secure.example.com. (This is because those names must be present in the list of Subject Alternate Names in the Expressway-C's server certificate.)

Phone Security Profile Configuration

Save | Delete | Copy | Reset | Apply Config | Add New

Status
Status: Ready

Phone Security Profile Information

Product Type:	Cisco TelePresence EX90
Device Protocol:	SIP
Name*	EX90.secure.example.com
Description	
Nonce Validity Time*	600
Device Security Mode	Encrypted
Transport Type*	TLS

☐ Enable Digest Authentication
☐ TFTP Encrypted Config
☐ Exclude Digest Credentials in Configuration File

Phone Security Profile CAPF Information

Authentication Mode*	By Null String
Key Size (Bits)*	1024

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port*	5061

4. If Unified CM servers (**System > Server**) are configured by **Host Name** (rather than IP address), then ensure that those host names are resolvable by the Expressway-C.

5. If you are using secure profiles, ensure that the root CA of the authority that signed the Expressway-C certificate is installed as a *CallManager-trust* certificate (**Security > Certificate Management** in the **Cisco Unified OS Administration** application).

6. Ensure that the **Cisco AXL Web Service** is active on the Unified CM publishers you will be using to discover the Unified CM servers that are to be used for remote access. To check this, select the **Cisco Unified Serviceability** application and go to **Tools > Service Activation**.

7. We recommend that remote and mobile devices are configured (either directly or by Device Mobility) to use publicly accessible NTP servers.
   a. Configure a public NTP server **System > Phone NTP Reference**.
   b. Add the Phone NTP Reference to a Date/Time Group (**System > Date/Time Group**).
   c. Assign the Date/Time Group to the Device Pool of the endpoint (**System > Device Pool**).

IM and Presence Service

Ensure that the **Cisco AXL Web Service** is active on the IM and Presence Service publishers that will discover other IM and Presence Service nodes for remote access. To check this, select the **Cisco Unified Serviceability** application and go to **Tools > Service Activation**.

If you are deploying Mobile and Remote Access with multiple IM and Presence Service clusters, you must configure Intercluster peer links between the clusters, and the Intercluster Sync Agent (ICSA) must be active on all clusters. This ensures that the user database is replicated between clusters, allowing Expressway-C to correctly route XMPP traffic.

For details of the correct configuration, refer to the chapter "Intercluster Peer Configuration" in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*. You can find the

correct document for your version at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Expressway

The following steps summarize the configuration required on the Expressway-E and the Expressway-C. Full details are described in section Configuring mobile and remote access on Expressway [p.21]

1. Ensure that **System host name** and **Domain name** are specified for every Expressway, and that all Expressway systems are synchronized to a reliable NTP service.

2. Set **Unified Communications mode** to *Mobile and remote access*.

3. Configure the Unified CM, IM and Presence Service, and Cisco Unity Connection servers on the Expressway-C.

4. Configure the domains on the Expressway-C for which services are to be routed to Unified CM.

5. [Optional] Create additional deployments and associate domains and UC services with them.

6. Install appropriate server certificates and trusted CA certificates.

7. Configure a Unified Communications traversal zone connection between the Expressway-E and the Expressway-C.

8. If required, configure the HTTP server allow list (whitelist) for any web services inside the enterprise that need to be accessed from remote Jabber clients.

9. [Optional] Configure SSO over collaboration edge, to allow for common identity between external Jabber clients and the users' Unified CM profiles

Note that configuration changes on the Expressway generally take immediate effect. If a system restart or other action is required you will be notified of this either through a banner message or via an alarm.

Unified Communications prerequisites

Configuring a secure traversal zone connection for Unified Communications

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be 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: You should configure only one *Unified Communications traversal* zone per Expressway.

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 allow you to upload a server certificate without this extension when Unified Communications features have been 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 [p.18] if appropriate).
   - To generate a CSR and /or to upload a server certificate to the Expressway, go to **Maintenance > Security certificates > 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 certificates > Trusted CA certificate**. You must restart the Expressway for the new trusted CA certificate to take effect.

See *Certificate Creation and Use With Expressway Deployment Guide* for full information about how to create and upload the Expressway's server certificate and how to upload a list of trusted certificate authorities.

Configuring encrypted Expressway traversal zones

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

- The Expressway-C and Expressway-E must be configured with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on a Expressway-C, or a traversal server zone when selected on an 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 a client and as a server you must ensure that each Expressway's certificate is valid both as a client and as a server.

- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

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

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
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	*Unified Communications traversal*	*Unified Communications traversal*
Connection credentials section		
Username	"exampleauth" for example	"exampleauth" for example
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	7001	7001
TLS verify subject name	Not applicable	Enter the name to look for in the traversal client's certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate.
Location section		

	Expressway-C	Expressway-E
Peer 1 address	Enter the FQDN of the Expressway-E. Note that 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

4. Click **Create zone**.

Server certificate requirements for Unified Communications

Cisco Unified Communications Manager certificates

The two Cisco Unified Communications Manager certificates that are significant for Mobile and Remote Access are the *CallManager* certificate and the *tomcat* certificate. These 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 externally-signed certificates for best end-to-end security between external endpoints and internal endpoints. However, if you do use self-signed certificates, the two certificates must have different common names. This is because the Expressway does not allow two self-signed certificates with the same CN. If the *CallManager* and *tomcat* self-signed certs have the same CN in the Expressway's trusted CA list, then it 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 within 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 Names. The *Expressway X8.5.2 Release Notes* have the details of the workarounds.

Expressway certificates

The Expressway certificate signing request (CSR) tool prompts for and incorporates the relevant subject alternate 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:

CSR SAN element	Mobile and remote access	Jabber Guest	XMPP federation
Unified CM registrations domains	✓ (Expressway-E only)	X	X
XMPP federation domains	X	X	✓ (Expressway-E only)

CSR SAN element	Mobile and remote access	Jabber Guest	XMPP federation
IM and Presence chat node aliases (federated group chat)	X	X	✓
Unified CM phone security profile names	✓ (Expressway-C only)	X	X

Note:

- A new Expressway-C certificate may need to be produced for the Expressway-C if chat node aliases are added or renamed, such as when an IM and Presence node is added or renamed, or if new TLS phone security profiles are added.

- A new Expressway-E certificate must be produced 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 needs to include the following elements in its list of subject alternate names:

- **Unified CM phone security profile names**: the names of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.
  Having the secure phone profiles as alternative names means that Unified CM can communicate via 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 3: Entering 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 needs to include the following elements in its list of subject alternate names:

- **Unified CM registrations domains**: all of the domains which are configured on the Expressway-C for Unified CM registrations. They are required for secure communications between endpoint devices and Expressway-E.
  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.
  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.
  Note that you can copy the list of chat node aliases from the equivalent **Generate CSR** page on the Expressway-C.

Figure 4: Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator

Configuring mobile and remote access on Expressway

This section describes the steps required to enable and configure mobile and remote access features on Expressway-C and Expressway-E, and how to discover the Unified CM servers and IM&P servers used by the service.

Installing Expressway security certificates and setting up a secure traversal zone

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be 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

For information about how to do this, see:

- Configuring a secure traversal zone connection for Unified Communications [p.16] (if your system does not already have a secure traversal zone in place)
- Server certificate requirements for Unified Communications [p.18]

Note that if XMPP federation is to be used, the IM&P servers need to be discovered on the Expressway-C for all the relevant information to be available when generating certificate signing requests.

Setting up the Expressway-C

This section describes the configuration steps required on the Expressway-C.

Configuring DNS and NTP settings

Check and configure the basic system settings on Expressway:

1. Ensure that **System host name** and **Domain name** are specified (**System > DNS**).
2. Ensure that local DNS servers are specified (**System > DNS**).
3. Ensure that all Expressway systems are synchronized to a reliable NTP service (**System > Time**). Use an **Authentication** method in accordance with your local policy.

If you have a cluster of Expressways you must do this for every peer.

Enabling the Expressway-C for mobile and remote access

To enable mobile and remote access functionality:

1. Go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Mobile and remote access*.
3. Click **Save**.

Note that you must select *Mobile and remote access* before you can configure the relevant domains and traversal zones.

Configuring the domains to route to Unified CM

You must configure the domains for which registration, call control, provisioning, messaging and presence services are to be routed to Unified CM.

1. On Expressway-C, go to **Configuration > Domains**.
2. Select the domains (or create a new domain, if not already configured) for which services are to be routed to Unified CM.
3. For each domain, turn *On* the services for that domain that Expressway is to support. The available services are:
   - **SIP registrations and provisioning on Unified CM**: Endpoint registration, call control and provisioning for this SIP domain is serviced by Unified CM. The Expressway acts as a Unified Communications gateway to provide secure firewall traversal and line-side support for Unified CM registrations.
   - **IM and Presence Service**: Instant messaging and presence services for this SIP domain are provided by the Unified CM IM and Presence service.
   - **XMPP federation**: Enables XMPP federation between this domain and partner domains.
   - **Deployment**: Associates the domain with the selected deployment, if there are multiple deployments. This setting is absent if there is only one deployment (there is always at least one).

   Turn *On* all of the applicable services for each domain.

   Note that these settings are not entirely independent. You cannot disable SIP registration and provisioning while using IM and Presence. You can disable IM and Presence while **SIP registrations and provisioning on Unified CM** is *On*, but the reverse is not true. So, if you switch **IM and Presence Service** *On*, then your setting for SIP registrations and provisioning is ignored and the Expressway-C behaves as though it was *On*.

Discovering Unified Communications servers and services

The Expressway-C must be configured with the address details of the Unified Communications services/nodes that are going to provide registration, call control, provisioning, voicemail, messaging, and presence services to MRA users.

IM and Presence Service configuration is not required if you're deploying the hybrid model, as these services are provided by the WebEx cloud.

Note: The connections configured in this procedure are static. You must refresh the configuration on the Expressway-C after you reconfigure or upgrade any of the discovered Unified Communications nodes. For more details, see Why should I refresh the discovered nodes? [p.26]

Go to **Configuration > Unified Communications > *<UC server type>*** and click **Refresh servers**.

Trusting the certificates presented to the Expressway-C

If **TLS verify mode** is *On* when discovering Unified Communications services, then you must configure the Expressway-C to trust the certificates presented by the IM and Presence Service nodes and Unified CM servers.

1. Determine the relevant CA certificates to upload:
   - If the servers' tomcat and CallManager certificates are CA-signed, the Expressway-C's trusted CA list must include the root CA of the certificate issuer.
   - If the servers are using self-signed certificates, the Expressway-C's trusted CA list must include the self-signed certificates from all discovered IM and Presence Service nodes, Cisco Unity Connection servers, and Unified CM servers.
2. Upload the required certificates to the Expressway-C (**Maintenance > Security certificates > Trusted CA certificate**).
3. Restart the Expressway-C (**Maintenance > Restart options**).

Discovering IM and Presence Service nodes

1. On Expressway-C, go to **Configuration > Unified Communications > IM and Presence Service nodes**.
   The page lists any IM and Presence Service nodes that have already been discovered.
2. Add the details of an IM and Presence Service database publisher node:
   a. Click **New**.
   b. Enter the address of the **IM and Presence Service database publisher node**.
      You can enter an FQDN or an IP address, but we recommend using the FQDN when **TLS verify mode** is *On*.
   c. Enter the **Username** and **Password** of an account that can access this server.

      Note: These credentials are stored permanently in the Expressway database. The corresponding IM and Presence Service user must have the *Standard AXL API Access* role.

   d. [Recommended] Leave **TLS verify mode** switched *On* to ensure Expressway verifies the node's tomcat certificate (for XMPP-related communications).
   e. [Optional] Select which deployment this node/cluster will belong to.

The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.

f.   Click **Add address**.

If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.

If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

Note: The status of the discovered node will be **Inactive** unless a valid traversal zone connection exists between the Expressway-C and the Expressway-E (may not yet be configured).

3.   Repeat the discovery procedure for other IM and Presence Service nodes/clusters, if required.

4.   Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

Discovering Unified CM servers

1.   On Expressway-C, go to **Configuration > Unified Communications > Unified CM servers**.
The page lists any Unified CM nodes that have already been discovered.

2.   Add the details of a Unified CM publisher node:

a.   Click **New**.

b.   Enter the **Unified CM publisher address**.
You can enter an FQDN or an IP address, but we recommend using the FQDN when **TLS verify mode** is *On*.

c.   Enter the **Username** and **Password** of an account that can access this server.

Note: These credentials are stored permanently in the Expressway database. The corresponding Unified CM user must have the *Standard AXL API Access* role.

d.   [Recommended] Leave **TLS verify mode** switched *On* to ensure Expressway verifies the node's certificates.
The Unified CM node presents its tomcat certificate for AXL and UDS queries, and its CallManager certificate for subsequent SIP traffic. If the Unified CM server is using self-signed certificates, the Expressway-C's trusted CA list must include a copy of the tomcat certificate and the CallManager certificate from every Unified CM server.

e.   [Optional] Select which deployment this node/cluster will belong to.
The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.

f.   Click **Add address**.

If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.

If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

3. Repeat the discovery procedure for other Unified CM nodes/clusters, if required.
4. Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

Discovering Cisco Unity Connection servers

1. On Expressway-C, go to **Configuration > Unified Communications > Unity Connection servers**. The page lists any Cisco Unity Connection nodes that have already been discovered.

2. Add the details of a Cisco Unity Connection publisher node:
   a. Click **New**.
   b. Enter the **Unity Connection address**.
      You can enter an FQDN or an IP address, but we recommend using the FQDN when **TLS verify mode** is *On*.
   c. Enter the **Username** and **Password** of an account that can access this server.

   Note: These credentials are stored permanently in the Expressway database.

   d. [Recommended] Leave **TLS verify mode** switched *On* to ensure Expressway verifies the node's tomcat certificate.
   e. [Optional] Select which deployment this node/cluster will belong to.
      The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.
   f. Click **Add address**.
      If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.
      If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

3. Repeat the discovery procedure for other Cisco Unity Connection nodes/clusters, if required.
4. Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

Automatically generated zones and search rules

Expressway-C automatically generates non-configurable neighbor zones between itself and each discovered Unified CM node. A TCP zone is always created, and a TLS zone is created also if the Unified CM node is configured with a **Cluster Security Mode** (**System > Enterprise Parameters > Security Parameters**) of *1 (Mixed)* (so that it can support devices provisioned with secure profiles). The TLS zone is configured with its **TLS verify mode** set to *On* if the Unified CM discovery had **TLS verify mode** enabled. This means that the Expressway-C will verify the CallManager certificate for subsequent SIP communications. Each zone is created with a name in the format 'CEtcp-<node name>' or 'CEtls-<node name>'.

A non-configurable search rule, following the same naming convention, is also created automatically for each zone. The rules are created with a priority of 45. If the Unified CM node that is targeted by the search rule has a long name, the search rule will use a regex for its address pattern match.

Note that load balancing is managed by Unified CM when it passes routing information back to the registering endpoints.

Why should I refresh the discovered nodes?

When the Expressway-C "discovers" a Unified Communications node, it establishes a connection to read the information required to create zones and search rules to proxy requests originating from outside of the network in towards that node.

This configuration information is static. That is, the Expressway only reads it when you manually initiate discovery of a new node, or when you refresh the configuration of previously discovered nodes. If any related configuration has changed on a node after you discover it, the mismatch between the new configuration and what the Expressway-C knows of that node will probably cause some kind of failure.

The information that the Expressway-C reads from the Unified Communications node is different for each node type and its role. The following list contains examples of UC configuration that you can expect to require a refresh from the Expressway. The list is not exhaustive; if you suspect that a configuration change on a node is affecting MRA services, you should refresh those nodes to eliminate one known source of potential problems.

- Changing cluster (e.g. adding or removing a node)
- Changing security parameters (e.g. Enabling Mixed Mode)
- Changing connection sockets (e.g. SIP port configuration)
- Changing TFTP server configuration
- Upgrading the software on the node

Configuring the HTTP server allow list (whitelist) on Expressway-C

Jabber client endpoints may need to access additional web services inside the enterprise. This requires an "allow list" of servers to be configured to which the Expressway will grant access for HTTP traffic originating from outside the enterprise.

The features and services that may be required, and would need whitelisting, include:

- Visual Voicemail
- Jabber Update Server

- Custom HTML tabs / icons
- Directory Photo Host
- Advanced File Transfer (AFT)
- Problem Report Tool server

Note: In order for the AFT feature to work across Expressway you must ensure that all Unified CM IM and Presence Service nodes, across all Unified CM IM and Presence Service clusters, have been added to the whitelist either manually or automatically.

To configure the set of addresses to which HTTP access will be allowed:

1. On Expressway-C, go to **Configuration > Unified Communications > Configuration**.
2. Click **HTTP server allow list**.
3. Configure the hostnames or IP addresses of any HTTP servers that external Jabber clients are allowed to access.
   Access is granted if the server portion of the client-supplied URI matches one of the names entered here, or if it resolves via DNS lookup to a specified IP address.

Expressway-C automatically whitelists the IP addresses of all discovered Unified CM nodes (that are running the CallManager and TFTP service), IM and Presence Service nodes, and Cisco Unity Connection nodes. These entries cannot be deleted. They are displayed in the **Auto-configured allow list** section of the **HTTP server allow list** page.

Setting up the Expressway-E

This section describes the configuration steps required on the Expressway-E.

Configuring DNS and NTP settings

Check and configure the basic system settings on Expressway:

1. Ensure that **System host name** and **Domain name** are specified (**System > DNS**).
2. Ensure that public DNS servers are specified (**System > DNS**).
3. Ensure that all Expressway systems are synchronized to a reliable NTP service (**System > Time**). Use an **Authentication** method in accordance with your local policy.

If you have a cluster of Expressways you must do this for every peer.

Note: The combination of <**System host name**>.<**Domain name**> is the FQDN of this Expressway-E. Ensure that this FQDN is resolvable in public DNS.

If you have a cluster of Expressway-Es, you must ensure that the **Domain name** is identical on each peer, and *it is case-sensitive*.

Enabling the Expressway-E for mobile and remote access

To enable mobile and remote access functionality:

1. Go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Mobile and remote access.*

3. Click **Save**.
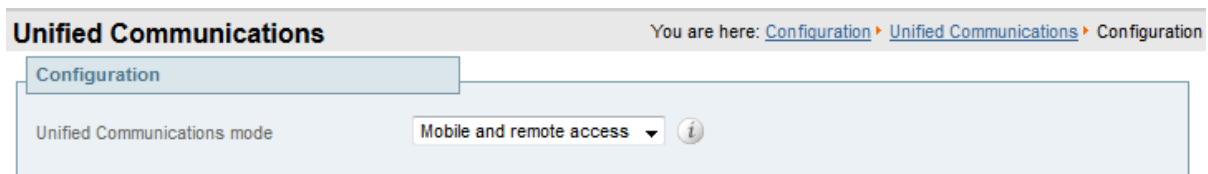
Ensuring that TURN services are disabled on Expressway-E

You must ensure that TURN services are disabled on the Expressway-E used for mobile and remote access.

1. Go to **Configuration > Traversal > TURN**.
2. Ensure that **TURN services** are *Off*.

Using deployments to partition Unified Communications services

A deployment is an abstract boundary used to enclose a domain and one or more Unified Communications service providers, such as Unified CM, Cisco Unity Connection, and IM and Presence Service nodes.

The purpose of multiple deployments is to partition the Unified Communications services available to mobile and remote access (MRA) users. This enables different subsets of MRA users to access different sets of services over the same Expressway pair. We recommend that you do not exceed 10 deployments.

For example, consider an implementation of two sets of Unified Communications infrastructure to provide a live MRA environment and a staging environment, respectively. This implementation might also require an isolated environment for sensitive communications.

Figure 5: Multiple deployments to partition Unified Communications services accessed from outside the network
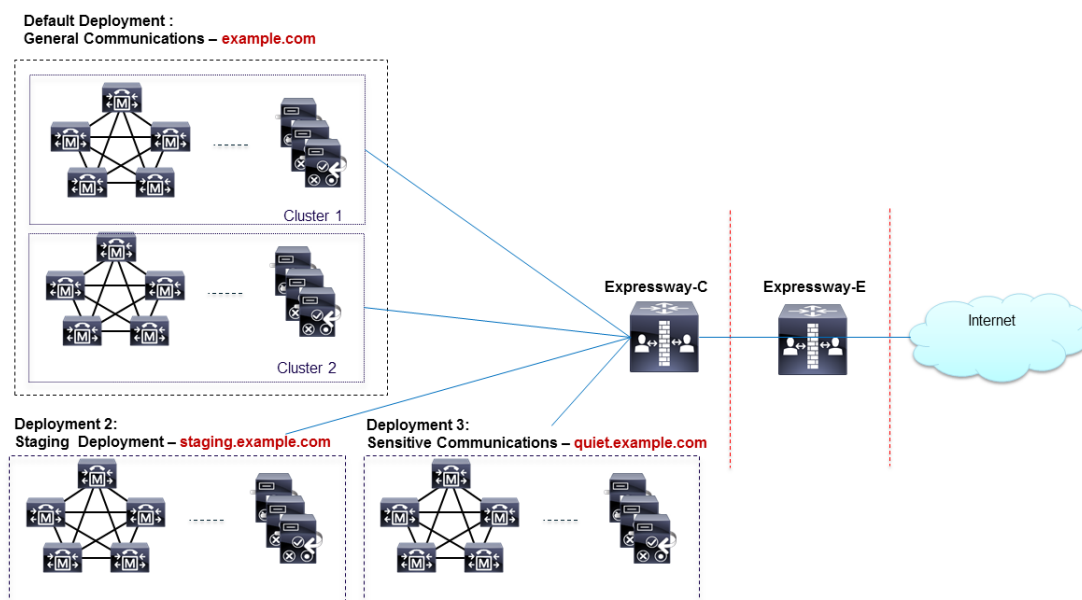
Deployments and their associated domains and services are configured on the Expressway-C.

There is one primary deployment, called "Default deployment" unless you rename it, that automatically encloses all domains and services until you create and populate additional deployments. This primary deployment cannot be deleted, even if it is renamed or has no members.

To partition the services that you provide via mobile and remote access, create as many deployments as you need, associate a different domain with each, and then associate the required Unified Communications resources with each deployment.

You cannot associate one domain with more than one deployment. Similarly, each Unified Communications node may only be associated with one deployment.

To create a new deployment:

1. Log in to the Expressway-C.
2. Go to **Configuration > Unified Communications > Deployments** and click **New**.
3. Give the deployment a name and click **Create deployment**.
   The new deployment is listed on the **Deployments** page and is available to select when editing domains or UC services.

To associate a domain with a deployment:

1. Go to **Configuration > Domains**.
   The domains and their associated services are listed here. The deployment column shows where the listed domains are associated.
2. Click the domain name, or create a new domain.
3. In the **Deployment** field, select the deployment which will enclose this domain.
4. Click **Save**.

To associate a Unified CM or other server/service with the deployment:

1. Go to **Configuration > Unified Communications >** and then **Unified CM servers**, or **IM and Presence Service nodes**, or **Unity Connection servers**.
   Any previously discovered service nodes of the selected type are listed here. The deployment column shows where the listed nodes are associated.
   If the list is not properly populated, see Discovering Unified Communications servers and services [p.23].
2. Click the server / service node name.
3. In the **Deployment** field, select which deployment will enclose this server / service node.
4. Click **Save**.

   Note: When you save this change, the Expressway-C refreshes the connection to the node, which may temporarily disrupt the service to the connected users.

5. Repeat for any other Unified Communications services that will belong to the deployment.

Single Sign-On (SSO) over the Collaboration Edge

Use this feature to enable single sign-on for endpoints accessing Unified Communications services from outside the network. Single sign-on over the edge relies on the secure traversal capabilities of the Expressway pair at the edge, and trust relationships between the internal service providers and the externally resolvable identity provider (IdP).

The endpoints do not need to connect via VPN; they use one identity and one authentication mechanism to access multiple Unified Communications services. Authentication is owned by the IdP, and there is no authentication at the Expressway, nor at the internal Unified CM services.

Supported endpoints

- Cisco Jabber 10.6 or later

Supported Unified Communications services

- Cisco Unified Communications Manager 10.5(2) or later
- Cisco Unity Connection 10.5(2) or later
- Cisco Unified Communications Manager IM and Presence Service 10.5(2) or later
- Other internal web servers, for example intranet

How it works

Cisco Jabber determines whether it is inside the organization's network before it requests a Unified Communications service. If it is outside the network, then it requests the service from the Expressway-E on the edge of the network. If single sign-on is enabled at the edge, the Expressway-E redirects Jabber to the IdP with a signed request to authenticate the user.

The IdP challenges the client to identify itself. When this identity is authenticated, the IdP redirects Jabber's service request back to the Expressway-E with a signed assertion that the identity is authentic.

The Expressway-E trusts the IdP, so it passes the request to the appropriate service inside the network. The Unified Communications service trusts the IdP and the Expressway-E, so it provides the service to the Jabber client.

Figure 6: Single sign-on for on-premises UC services
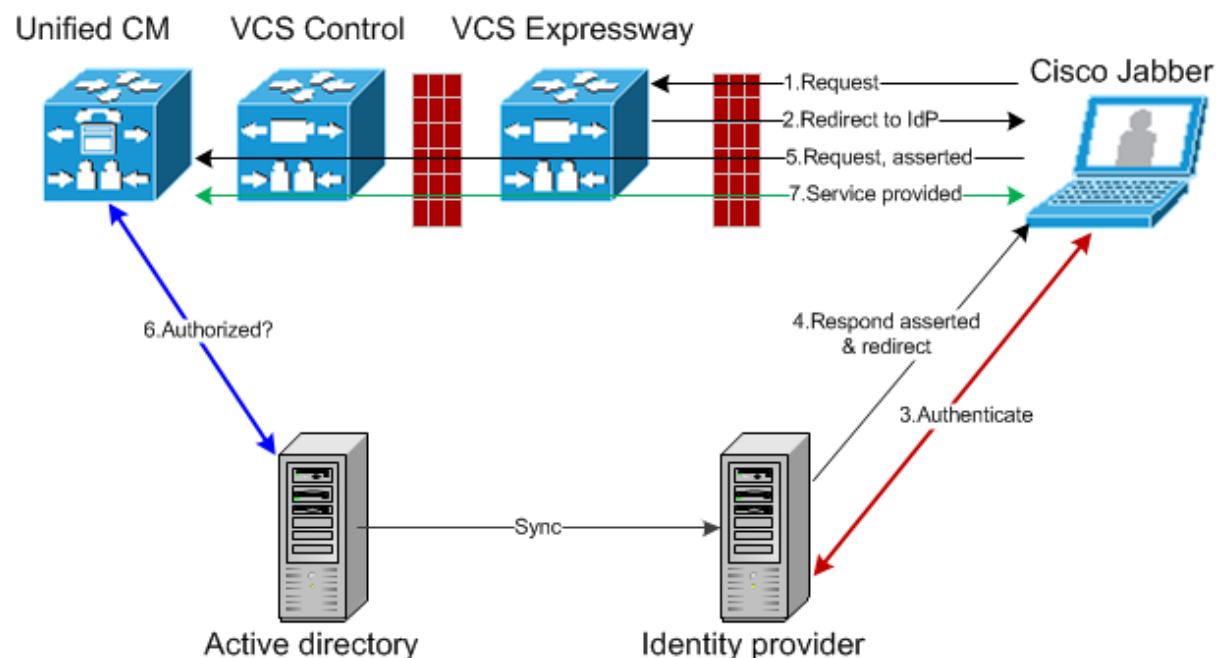
Single Sign-On prerequisites

On the Expressway pair:

- An Expressway-E and an Expressway-C are configured to work together at your network edge.
- A Unified Communications traversal zone is configured between the Expressway-C and the Expressway-E.
- The SIP domain that will be accessed via SSO is configured on the Expressway-C.
- The Expressway-C is in Mobile and remote access mode and has discovered the required Unified CM resources.
- The hostnames of the required Unified CM resources are added to the HTTP server allow list on the Expressway-C.
- If you are using multiple deployments, the Unified CM resources that will be accessed by SSO are in the same deployment as the domain that will be called from Jabber clients.

On the Cisco Jabber clients:

- Clients are configured to request the internal services using the correct domain names / SIP URIs / Chat aliases.
- The default browser can resolve the Expressway-E and the IdP.

On the Identity Provider:

The domain that is on the IdP certificate must be published in the DNS so that clients can resolve the IdP.

Selecting an Identity Provider (IdP)

Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services.

SAML-based SSO is an option for authenticating UC service requests originating from inside the enterprise network, and it is now extended to clients requesting UC services from outside via Mobile and Remote Access (MRA).

If you choose SAML-based SSO for your environment, note the following:

- SAML 2.0 is not compatible with SAML 1.1 and you must select an IdP that uses the SAML 2.0 standard.
- SAML-based identity management is implemented in different ways by vendors in the computing and networking industry, and there are no widely accepted regulations for compliance to the SAML standards.
- The configuration of and policies governing your selected IdP are outside the scope of Cisco TAC (Technical Assistance Center) support. Please use your relationship and support contract with your IdP Vendor to assist in configuring the IDP properly. Cisco cannot accept responsibility for any errors, limitations, or specific configuration of the IdP.

Although Cisco Collaboration infrastructure may prove to be compatible with other IdPs claiming SAML 2.0 compliance, only the following IdPs have been tested with Cisco Collaboration solutions:

- OpenAM 10.0.1
- Active Directory Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4

High level task list

1. Configure a synchronizable relationship between the identity provider and your on-premises directory such that authentication can securely be owned by the IdP. See *Directory Integration and Identity Management* in the Cisco Collaboration System 10.x Solution Reference Network Designs (SRND) document.
2. Export SAML metadata file from the IdP. Check the documentation on your identity provider for the procedure. For example, see *Enable SAML SSO through the OpenAM IdP* in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.
3. Import the SAML metadata file from the IdP to the Unified CM servers and Cisco Unity Connection servers that will be accessed by single sign-on. See the Unified Communications documentation or help for more details.
4. Export the SAML metadata files from the Unified CM servers and Cisco Unity Connection servers. For example, see *High-Level Circle of Trust Setup* in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.
5. Create the Identity Provider on the Expressway-C, by importing the SAML metadata file from the IdP.
6. Associate the IdP with SIP domain(s) on the Expressway-C.
7. Export the SAML metadata file(s) from the (master) Expressway-C; ensure that it includes the externally resolvable address of the (master) Expressway-E.
   The SAML metadata file from the Expressway-C contains the X.509 certificate for signing and encrypting SAML interchanges between the edge and the IdP, and the binding(s) that the IdP needs to redirect clients to the Expressway-E (peers).
8. Import the SAML metadata files from the Unified CM servers and Cisco Unity Connection servers to the IdP. An example using OpenAM is in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.
9. Similarly, import the SAML metadata file from the Expressway-C to the IdP. See your IdP documentation for details.
10. Turn on SSO at the edge (on the Expressway-C and the Expressway-E).

Importing the SAML metadata from the IdP

1. On the Expressway-C, go to **Configuration > Unified Communications > Identity providers (IdP)**. You only need to do this on the master peer of the cluster.

2. Click **Import new IdP from SAML**.

3. Use the **Import SAML file** control to locate the SAML metadata file from the IdP.

4. Set the **Digest** to the required SHA hash algorithm.
   The Expressway uses this digest for signing SAML authentication requests for clients to present to the IdP. The signing algorithm must match the one expected by the IdP for verifying SAML authentication request signatures.

5. Click **Upload**.
   The Expressway-C can now authenticate the IdP's communications and encrypt SAML communications to the IdP.

Note: You can change the signing algorithm after you have imported the metadata, by going to **Configuration > Unified Communications > Identity Providers (IdP)**, locating your IdP row then, in the **Actions** column, clicking **Configure Digest**).

Associating domains with an IdP

You need to associate a domain with an IdP if you want the MRA users of that domain to authenticate via the IdP. The IdP adds no value until you associate at least one domain with it.

There is a many-to-one relationship between domains and IdPs. A single IdP can be used for multiple domains, but you may associate just one IdP with each domain.

On the Expressway-C:

1. Open the IdP list (**Configuration > Unified Communications > Identity providers (IdP)**) and verify that your IdP is in the list.
   The IdPs are listed by their entity IDs. The associated domains for each are shown next to the ID.

2. Click **Associate domains** in the row for your IdP.
   This shows a list of all the domains on this Expressway-C. There are checkmarks next to domains that are already associated with this IdP. It also shows the IdP entity IDs if there are different IdPs associated with other domains in the list.

3. Check the boxes next to the domains you want to associate with this IdP.
   If you see *(Transfer)* next to the checkbox, checking it will break the domain's existing association and associate it with this IdP.

4. Click **Save**.
   The selected domains are associated with this IdP.

Exporting the SAML metadata from the Expressway-C

Note: The Expressway-C must have a valid connection to the Expressway-E before you can export the Expressway-C's SAML metadata.

---

1. Go to **Configuration > Unified Communications > Export SAML data**.
   This page lists the connected Expressway-E, or all the Expressway-E peers if it's a cluster. These are listed because data about them is included in the SAML metadata for the Expressway-C.

2. [Conditional] If you have configured multiple deployments, you must select a deployment before you can export the SAML metadata.

3. Click **Download** or **Download all**.
   The page also lists all the Expressway-C peers, and you can download SAML metadata for each one, or export them all in a .zip file.

4. Copy the resulting file(s) to a secure location that you can access when you need to import SAML metadata to the IdP.

Configuring IDPs

This topic covers any known additional configurations that are required when using a particular IDP for SSO over MRA.

These configuration procedures are required in addition to the prerequisites and high level tasks already mentioned, some of which are outside of the document's scope.

Active Directory Federation Services 2.0

After creating Relying Party Trusts for the Expressway-Es, you must set some properties of each entity, to ensure that AD FS formulates the SAML responses as Expressway-E expects them.

These procedures were verified on AD FS 2.0, although the same configuration is required if you are using AD FS 3.0.

You need to:

■ Sign the whole response (message and assertion)

To set these relying party trust properties for each entity:

In Windows PowerShell®, repeat the following command for each Expressway-E's *<EntityName>*:

```
Set-ADFSRelyingPartyTrust -TargetName "<EntityName>" -SAMLResponseSignature
MessageAndAssertion
```

Enabling Single Sign-On at the edge

On the Expressway-C:

1. Go to **Configuration > Unified Communications > Configuration**
2. Locate **Single Sign-on support** and select *On*
3. Click **Save**

[Optional] Extend the time-to-live of SIP authorization tokens, by entering a number of seconds for **SIP token extra time-to-live (in seconds)**. This setting gives users a short window in which they can still accept calls after their credentials expire, but you should balance this convenience against the increased security exposure.

On the Expressway-E:

1. Go to **Configuration > Unified Communications > Configuration**

2. Locate **Single Sign-on support** and select *On*

3. Click **Save**

[Optional] Choose how the Expressway-E reacts to **/get_edge_sso** requests by selecting whether or not the Expressway-C should check the home nodes.

The **/get_edge_sso** request from the client asks whether the client may try to authenticate the user by SSO. In this request, the client provides an identity of the user that the Expressway-C can use to find the user's home cluster:

- The default option is *Yes* to **Check for internal SSO availability**:
  The Expressway-E passes the request to the Expressway-C. The Expressway-C uses a round-robin algorithm to select a Unified CM node, and makes a UDS query for the supplied identity against that node. The Unified CM determines which node is the user's home node, and whether it is capable of doing SSO for the user, and then tells the Expressway-C the outcome. The Expressway-C then tells the Expressway-E which responds **true** or **false** to the client.

- If you select *No* to **Check for internal SSO availability**:
  The Expressway-E always responds **true** to **/get_edge_sso** requests. It does not make the inwards request to the user's home Unified CM, and thus cannot know whether SSO is really available there.

When the client receives a **true** response from Expressway-E, it will try to **/get_edge_config** via SSO. If it gets **false**, it will try **/get_edge_config** using whatever credentials it has - credentials which are independent from the identity managed by UDS inside the enterprise. If it gets **true** and SSO is not actually enabled on the user's home node, then **/get_edge_config** will fail and the client will not try the other authentication option.

The option you should choose depends entirely on your implementation. If you have a homogenous environment, in which all Unified CM nodes are capable of SSO, you can reduce response time and overall network traffic by selecting *No*. By contrast, if you want clients to use either mode of getting the edge configuration - during rollout or because you cannot guarantee that SSO is available on all nodes - you should select *Yes*.

Checking the status of Unified Communications services

You can check the status of the Unified Communications services on both Expressway-C and Expressway-E.

1. Go to **Status > Unified Communications**.
2. Review the list and status of domains, zones and (Expressway-C only) Unified CM and IM&P servers. Any configuration errors will be listed along with links to the relevant configuration page from where you can address the issue.

Mobile and remote access port reference

This section summarizes the ports that could potentially be used between your 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.

Outbound from Expressway-C (private) to Expressway-E (DMZ)

Purpose	Protocol	Expressway-C (source)	Expressway-E (listening)
XMPP (IM and Presence)	TCP	Ephemeral port	7400
SSH (HTTP/S tunnels)	TCP	Ephemeral port	2222
Traversal zone SIP signaling	TLS	25000 to 29999	7001
Traversal zone SIP media (for small/medium systems on X8.1 or later)	UDP	36000 to 59999*	36000 (RTP), 36001 (RTCP) (defaults)
Traversal zone SIP media (for large systems)	UDP	36000 to 59999*	36000 to 36011 (6 pairs of RTP and RTCP ports for multiplexed media traversal)

Outbound from Expressway-E (DMZ) to public internet

Purpose	Protocol	Expressway-E (source)	Internet endpoint (listening)
SIP media	UDP	36002 to 59999 or 36012 to 59999	>= 1024
SIP signaling	TLS	25000 to 29999	>= 1024

Inbound from public internet to Expressway-E (DMZ)

Purpose	Protocol	Internet endpoint (source)	Expressway-E (listening)
XMPP (IM and Presence)	TCP	>= 1024	5222
HTTP proxy (UDS)	TCP	>= 1024	8443
Media	UDP	>= 1024	36002 to 59999 or 36012 to 59999*
SIP signaling	TLS	>= 1024	5061
HTTPS (only required for external administrative access, which is strongly discouraged)	TCP	>= 1024	443

From Expressway-C to Unified CM / Cisco Unity Connection

Purpose	Protocol	Expressway-C (source)	Unified CM (listening)
XMPP (IM and Presence)	TCP	Ephemeral port	7400 (IM and Presence)
HTTP proxy (UDS)	TCP	Ephemeral port	8443 (Unified CM)
HTTP proxy (SOAP)	TCP	Ephemeral port	8443 (IM and Presence Service)
HTTP (configuration file retrieval)	TCP	Ephemeral port	6970
CUC (voicemail)	TCP	Ephemeral port	443 (Unity Connection)
Message Waiting Indicator (MWI) from Unity Connection	TCP	Ephemeral port	7080 (Unity Connection)
Media	UDP	36000 to 59999*	>= 1024
SIP signaling	TCP	25000 to 29999	5060
Secure SIP signaling	TLS	25000 to 29999	5061

* The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > Traversal Subzone**. In Large Expressway systems the first 12 ports in the range – 36000 to 36011 by default – are always reserved for multiplexed traffic. The Expressway-E listens on these ports. You cannot configure a distinct range of demultiplex listening ports on Large systems: they always use the first 6 pairs in the media port range. On Small/Medium systems you can explicitly specify which 2 ports listen for multiplexed RTP/RTCP traffic, on the Expressway-E (**Configuration > Traversal > Ports**). If you choose not to configure a particular pair of ports (**Use configured demultiplexing ports** = *No*), then the Expressway-E will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default).

Note that:

- Ports 8191/8192 TCP and 8883/8884 TCP are used internally within the Expressway-C and the Expressway-E applications. Therefore these ports must not be allocated for any other purpose. The Expressway-E listens externally on port 8883; therefore we recommend that you create custom firewall rules on the external LAN interface to drop TCP traffic on that port.
- The Expressway-E listens on port 2222 for SSH tunnel traffic. The only legitimate sender of such traffic is the Expressway-C (cluster). Therefore we recommend that you create the following firewall rules for the SSH tunnels service:
  - one or more rules to allow all of the Expressway-C peer addresses (via the internal LAN interface, if appropriate)
  - followed by a lower priority (higher number) rule that drops all traffic for the SSH tunnels service (on the internal LAN interface if appropriate, and if so, another rule to drop all traffic on the external interface)

Additional information

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.

Expressway call types and licensing

The Expressway distinguishes between the following 2 types of call:

- **Unified CM remote sessions**: these are "mobile and remote access" calls i.e.video or audio calls from devices located outside the enterprise that are routed via the Expressway firewall traversal solution to endpoints registered to Unified CM. These calls do not require rich media session licenses, although they do contribute to overall load.
- **Rich media sessions**: these calls consume rich media session licenses and consist of every other type of video or audio call that is routed through the Expressway. This includes business-to-business calls, B2BUA calls, and interworked or gatewayed calls to third-party solutions. The Expressway may take the media (traversal) or just the signaling (non-traversal).
  Audio-only SIP traversal calls are treated distinctly from video SIP traversal calls. Each rich media session license allows either 1 video call or 2 audio-only SIP traversal calls. Hence, a 100 rich media session license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other audio-only call (non-traversal, H.323 or interworked) will consume a rich media session license.

Both types of call contribute to the overall load on the system.

Note that:

- Expressway defines an "audio-only" SIP call as one that was negotiated with a single "m=" line in the SDP. Thus, for example, if a person makes a "telephone" call but the SIP UA includes an additional m= line in the SDP, the call will consume a video call license.
- While an "audio-only" SIP call is being established, it is treated (licensed) as a video call. It only becomes licensed as "audio-only" when the call setup has completed. This means that if your system approaches its maximum licensed limit, you may be unable to connect some "audio-only" calls if they are made simultaneously.

Deploying Unified CM and Expressway in different domains

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&P servers must share the same domain.

SIP trunks between Unified CM and Expressway-C

Expressway deployments for mobile and remote access do not require SIP trunk connections between Unified CM and Expressway-C. Note that the automatically generated neighbor zones between Expressway-C and each discovered Unified CM node are not SIP trunks.

However, you may still configure a SIP trunk if required (for example, to enable B2B calls to endpoints registered to Unified CM).

If a SIP trunk is configured, you must ensure that it uses a different listening port on Unified CM from that used for SIP line registrations to Unified CM. An alarm is raised on Expressway-C if a conflict is detected.

Configuring line registration listening ports on Unified CM

The listening ports used for line registrations to Unified CM are configured via **System > Cisco Unified CM**.

The **SIP Phone Port** and **SIP Phone Secure Port** fields define the ports used for TCP and TLS connections respectively and are typically set to 5060/5061.

Configuring SIP trunk listening ports

The ports used for SIP trunks are configured on both Unified CM and Expressway.

On Unified CM:

1. Go to **System > Security > SIP Trunk Security Profile** and select the profile used for the SIP trunk. If this profile is used for connections from other devices, you may want to create a separate security profile for the SIP trunk connection to Expressway.
2. Configure the **Incoming Port** to be different from that used for line registrations.
3. Click **Save** and then click **Apply Config**.

On Expressway:

1. Go to **Configuration > Zones > Zones** and select the Unified CM neighbor zone used for the SIP trunk. (Note that the automatically generated neighbor zones between Expressway-C and each discovered Unified CM node for line side communications are non-configurable.)
2. Configure the SIP **Port** to the same value as the **Incoming Port** configured on Unified CM.
3. Click **Save**.

See *Cisco TelePresence Cisco Unified Communications Manager with Expressway (SIP Trunk) Deployment Guide* for more information about configuring a SIP trunk.

Configuring secure communications

This deployment requires secure communications between the Expressway-C and the Expressway-E, and between the Expressway-E and endpoints located outside the enterprise. This involves the mandating of encrypted TLS communications for HTTP, SIP and XMPP, and, where applicable, the exchange and checking of certificates. Jabber endpoints must supply a valid username and password combination, which will be validated against credentials held in Unified CM. All media is secured over SRTP.

Expressway-C automatically generates non-configurable neighbor zones between itself and each discovered Unified CM node. A TCP zone is always created, and a TLS zone is created also if the Unified CM node is configured with a **Cluster Security Mode** (**System > Enterprise Parameters > Security Parameters**) of *1 (Mixed)* (so that it can support devices provisioned with secure profiles). The TLS zone is configured with its

TLS verify mode set to *On* if the Unified CM discovery had **TLS verify mode** enabled. This means that the Expressway-C will verify the CallManager certificate for subsequent SIP communications. Note that secure profiles are downgraded to use TCP if Unified CM is not in mixed mode.

The Expressway neighbor zones to Unified CM use the names of the Unified CM nodes that were returned by Unified CM when the Unified CM publishers were added (or refreshed) to the Expressway. The Expressway uses those returned names to connect to the Unified CM node. If that name is just the host name then:

- it needs to be routable using that name
- this is the name that the Expressway expects to see in the Unified CM's server certificate

If you are using secure profiles, ensure that the root CA of the authority that signed the Expressway-C certificate is installed as a *CallManager-trust* certificate (**Security > Certificate Management** in the **Cisco Unified OS Administration** application).

Media encryption

Media encryption is enforced on the call legs between the Expressway-C and the Expressway-E, and between the Expressway-E and endpoints located outside the enterprise.

The encryption is physically applied to the media as it passes through the B2BUA on the Expressway-C.

Limitations

- The IPV4 protocol only is supported for mobile and remote access users
- In Expressway-E systems that use dual network interfaces, XCP connections (for IM&P XMPP traffic) always use the non-external (i.e. internal) interface. This means that XCP connections may fail in deployments where the Expressway-E internal interface is on a separate network segment and is used for system management purposes only, and where the traversal zone on the Expressway-C connects to the Expressway-E's external interface.

Unsupported Jabber features when using mobile and remote access

- Calls to/from additional lines on IP phones and endpoints that support multiple lines; only the primary line is supported via Mobile and Remote Access
- Directory access mechanisms other than UDS
- Certificate provisioning to remote endpoints e.g. CAPF
- Features that rely on the SIP UPDATE method (RFC 3311) will not work as expected because the Expressway does not support this method. For example, CUCM and endpoints use UPDATE to implement blind transfer, which does not work correctly via MRA.
- Peer-to-peer file transfer when using IM and Presence Service and Jabber is unsupported via MRA
    - Managed File Transfer (MFT) with IM and Presence Service 10.5.2 (and later) and Jabber 10.6 (and later) clients is supported via MRA
    - File transfer with WebEx Messenger Service and Cisco Jabber is supported via MRA
- Deskphone control (QBE/CTI)
- Additional mobility features including DVO-R, GSM handoff and session persistency
- Hunt group/hunt pilot/hunt list
- Self-care portal

- Support for Jabber SDK

- Shared lines are supported in a limited way. Multiple endpoints can share a line but in-call features (like hold/resume) only work on the first endpoint that answers. Endpoints sharing the line may not correctly recognise the state of the call.

Unsupported features and limitations when using mobile and remote access

- The Expressway cannot be used for Jabber Guest when it is used for MRA.

- Secure XMPP traffic between Expressway-C and IM&P servers (XMPP traffic is secure between Expressway-C and Expressway-E, and between Expressway-E and remote endpoint).

- Endpoint management capability (SNMP, SSH/HTTP access).

- Multi-domain and multi-customer support is limited as follows:
  - Prior to X8.5, each Expressway deployment supported only one IM&P domain (even though IM and Presence Service 10.0 or later supports Multiple Presence Domains).
  - As of X8.5, you can create multiple deployments on the Expressway-C, but this feature is still limited to one domain per deployment.
  - As of X8.5.1, a deployment can have Multiple Presence Domains. This feature is in preview with X8.5.1, and we currently recommend that you do not exceed 10 domains.

- The Expressway-C used for Mobile and Remote Access cannot also be used as a Lync 2013 gateway (if required, this must be configured on a stand-alone Expressway-C.

- NTLM authentication via the HTTP proxy.

- Maintenance mode; if an Expressway-C or Expressway-E is placed into maintenance mode, any existing calls passing through that Expressway will be dropped.

- The Expressway-E must not have TURN services enabled.

- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM (the same limit as Small / Medium VM servers).

Protocol summary

The table below lists the protocols and associated services used in the Unified Communications solution.

Protocol	Security	Service
SIP	TLS	Session establishment – Register, Invite etc.
HTTPS	TLS	Logon, provisioning/configuration, directory, visual voicemail
RTP	SRTP	Media - audio, video, content sharing
XMPP	TLS	Instant Messaging, Presence, Federation

Clustered Expressway systems and failover considerations

You can configure a cluster of Expressway-Cs and a cluster of Expressway-Es to provide failover (redundancy) support as well as improved scalability.

Details about how to set up Expressway clusters are contained in *Expressway Cluster Creation and Maintenance Deployment Guide* and information about how to configure Jabber endpoints and DNS are contained in *Configure DNS for Cisco Jabber*.

Note that when discovering Unified CM and IM&P servers on Expressway-C, you must do this on the master peer.

Authorization rate control

The Expressway can limit the number of times that any user's credentials can be used, in a given configurable period, to authorize the user for collaboration services. This feature is designed to thwart inadvertent or real denial of service attacks, which can originate from multiple client devices authorizing the same user, or from clients that reauthorize more often than necessary.

Each time a client supplies credentials to authorize the user, the Expressway checks whether this attempt would exceed the **Maximum authorizations per period** within the previous number of seconds specified by the **Rate control period**.

If the attempt would exceed the chosen maximum, then the Expressway rejects the attempt and issues the HTTP error 429 "Too Many Requests".

The authorization rate control settings are configurable in the **Advanced** section of the **Configuration > Unified Communications > Configuration** page.

Credential caching

Note: These settings do not apply to clients that are using SSO (common identity) for authenticating via MRA.

The Expressway caches endpoint credentials which have been authenticated by Unified CM. This caching improves overall performance because the Expressway does not always have to submit endpoint credentials to Unified CM for authentication.

The caching settings are configurable in the **Advanced** section of the **Configuration > Unified Communications > Configuration** page.

Credentials refresh interval specifies the lifetime of the authentication token issued by the Expressway to a successfully authenticated client. A client that successfully authenticates should request a refresh before this token expires, or it will need to re-authenticate. The default is 480 minutes (8 hours).

Credentials cleanup interval specifies how long the Expressway waits between cache clearing operations. Only expired tokens are removed when the cache is cleared, so this setting is the longest possible time that an expired token can remain in the cache. The default is 720 minutes (12 hours).

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.

Expressway automated intrusion protection

You may need to enable the **Automated protection service** (**System > System administration**) if it is not yet running.

To protect against malicious attempts to access the HTTP proxy, you can configure automated intrusion protection on the Expressway-E (**System > Protection > Automated detection > Configuration**).

We recommend that you enable the following categories on the Expressway-E:

- **HTTP proxy authorization failure** and **HTTP proxy protocol violation**. Note: Do not enable the **HTTP proxy resource access failure** category.
- **XMPP protocol violation**

Note: The **Automated protection service** uses Fail2ban software. It protects against brute force attacks that originate from a single source IP address.

Appendix 1: Troubleshooting

General troubleshooting techniques

Checking alarms and status

When troubleshooting any issue, we recommend that you first check if any alarms have been raised (**Status > Alarms**). If alarms exist, follow the instructions provided in the **Action** column. You should check the alarms on both Expressway-C and Expressway-E.

Next, go to **Status > Unified Communications** to see a range of status summary and configuration information. You should check this status page on both Expressway-C and Expressway-E.

If any required configuration is missing or invalid an error message is shown and a link to the relevant configuration page is provided.

You may see invalid services or errors if you have changed any of the following items on Expressway:

- server or CA certificates
- DNS configuration
- domain configuration

In these cases, a system restart is required to ensure that those configuration changes take effect.

Checking and taking diagnostic logs

Jabber for Windows

The Jabber for Windows log file is saved as **csf-unified.log** under
C:\Users\<UserID>\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs.

The configuration files are located under **C:\Users\<UserID>\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Config**.

Performing Expressway diagnostic logging

The diagnostic logging tool in Expressway can be used to assist in troubleshooting system issues. It allows you to generate a diagnostic log of system activity over a period of time, and then to download the log.

Before taking a diagnostic log, you must configure the log level of the relevant logging modules:

1. Go to **Maintenance > Diagnostics > Advanced > Support Log configuration**.
2. Select the following logs:
   - developer.edgeconfigprovisioning
   - developer.trafficserver
   - developer.xcp
3. Click **Set to debug**.

You can now start the diagnostic log capture:

1. Go to **Maintenance > Diagnostics > Diagnostic logging**.
2. Optionally, select **Take tcpdump while logging**.
3. Click **Start new log**.
4. (Optional) Enter some **Marker** text and click **Add marker**.
   - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
   - You can add as many markers as required, at any time while the diagnostic logging is in progress.
   - Marker text is added to the log with a "`DEBUG_MARKER`" tag.
5. Reproduce the system issue you want to trace in the diagnostic log.
6. Click **Stop logging**.
7. Click **Download log** to save the diagnostic log archive to your local file system. You are prompted to save the archive (the exact wording depends on your browser).

After you have completed your diagnostic logging, return to the **Support Log configuration** page and reset the modified logging modules back to *INFO* level.

Checking DNS records

You can use the Expressway's DNS lookup tool (**Maintenance > Tools > Network utilities > DNS lookup**) to assist in troubleshooting system issues. The SRV record lookup includes those specific to H.323, SIP, Unified Communications and TURN services.

Note that performing the DNS lookup from the Expressway-C will return the view from within the enterprise, and that performing it on the Expressway-E will return what is visible from within the DMZ which is not necessarily the same set of records available to endpoints in the public internet.

The DNS lookup includes the following SRV services that are used for Unified Communications:

- _collab-edge._tls
- _cuplogin._tcp
- _cisco-uds._tcp

Note: the following SRV records may be queried by the lookup tool or the client, but they are not required. You can ignore name errors related to these:

- _cisco-phone-tftp._tcp
- _cisco-phone-http._tcp

Checking reachability of the Expressway-E

Ensure that the FQDN of the Expressway-E is resolvable in public DNS.

The FQDN is configured at **System > DNS** and is built as <**System host name**>.<**Domain name**>.

Checking call status

Call status information can be displayed for both current and completed calls:

- **Current calls**: the **Call status** page (**Status > Calls > Calls**) lists all the calls currently passing through the Expressway.
- **Completed calls**: the **Call history** page (**Status > Calls > History**) lists all the calls that are no longer active. The list is limited to the most recent 500 calls, and only includes calls that have taken place since the Expressway was last restarted.

If the Expressway is part of a cluster, all calls that apply to any peer in the cluster are shown, although the list is limited to the most recent 500 calls per peer.

Mobile and remote access calls have different component characteristics depending on whether the call is being viewed on the Expressway-C or Expressway-E:

- On an Expressway-C, a Unified CM remote session will have 3 components (as it uses the B2BUA to enforce media encryption). One of the Expressway components will route the call through one of the automatically generated neighbor zones (with a name prefixed by either **CEtcp** or **CEtls**) between Expressway and Unified CM.
- On an Expressway-E, there will be one component and that will route the call through the **CollaborationEdgeZone**.

Note that if both endpoints are outside of the enterprise (i.e. off premises), you will see this treated as 2 separate calls.

Rich media sessions

If your system has a rich media session key installed and thus has been extended to support business-to-business calls, and interworked or gatewayed calls to third-party solutions and so on, those calls are also listed on the call status and call history pages.

Checking devices registered to Unified CM via Expressway

Identifying devices in Unified CM

To identify devices registered to Unified CM via Expressway:

1. In Unified CM, go to **Device > Phone** and click **Find**.

2. Check the **IP Address** column. Devices that are registered via Expressway will display an **IP Address** of the Expressway-C it is registered through.

Identifying provisioned sessions in Expressway-C

To identify sessions that have been provisioned via Expressway-C:

1. In Expressway-C, go to **Status > Unified Communications**.

2. In the **Advanced status information** section, click **View provisioning sessions**.
   This shows a list of all current and recent (shown in red) provisioning sessions.

Ensuring that Expressway-C is synchronized to Unified CM

Changes to Unified CM cluster or node configuration can lead to communication problems between Unified CM and Expressway-C. This includes changes to:

- the number of nodes within a Unified CM cluster
- the host name or IP address of an existing node
- listening port numbers
- security parameters
- phone security profiles

You must ensure that any such changes are reflected in the Expressway-C. To do this you must rediscover all Unified CM and IM and Presence Service nodes (on Expressway go to **Configuration > Unified Communications**).

Checking SSO status and tokens

You can check and clear users' SSO tokens on **Users > SSO token holders**. This could help identify problems with a particular user's SSO access.

You can check SSO statistics on **Status > Unified Communications > View detailed SSO statistics**. Any unexpected requests or responses on this page could help identify configuration or authorization issues.

Expressway certificate / TLS connectivity issues

If the Expressway's server certificate or trusted CA certificates have been modified, you must restart the Expressway before those changes will take effect.

If you are using secure profiles, ensure that the root CA of the authority that signed the Expressway-C certificate is installed as a *CallManager-trust* certificate (**Security > Certificate Management** in the **Cisco Unified OS Administration** application).

Cisco Jabber sign in issues

Jabber cannot sign in due to XMPP bind failure

The Jabber client may be unable to sign in ("Cannot communicate with the server" error messages) due to XMPP bind failures.

This will be indicated by resource bind errors in the Jabber client logs, for example:

```
                          XmppSDK.dll #0, 201, Recv:<iq id='uid:527a7fe7:00000cfe:00000000' type='error'><
xmlns='urn:ietf:params:xml:ns:xmpp-bind'/><error code='409' type='cancel'><conflict
xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/></error></iq>
                          XmppSDK.dll #0, CXmppClient::onResourceBindError
                  XmppSDK.dll #0, 39, CTriClient::HandleDisconnect, reason:16
```

This typically occurs if the IM and Presence Intercluster Sync Agent is not working correctly. See IM and Presence intercluster deployment configuration for more information.

Jabber cannot sign in due to SSH tunnels failure

Jabber can fail to sign in due to the SSH tunnels failing to be established. The traversal zone between the Expressway-C and Expressway-E will work normally in all other respects. Expressway will report 'Application failed - An unexpected software error was detected in portforwarding.pyc'.

This can occur if the Expressway-E DNS hostname contains underscore characters. Go to **System > DNS** and ensure that the **System host name** only contains letters, digits and hyphens.

Jabber cannot sign in when connecting to different peers in a cluster of Expressway-Es

Jabber sign in failures have been seen when there is inconsistency of the DNS domain name between Expressway-E peers. The domain names must be identical, even with respect to case, on all peers in the cluster.

Go to **System > DNS** on each peer to make sure that **Domain name** is identical on all peers.

Expressway returns "401 unauthorized" failure messages

A "401 unauthorized" failure message can occur when the Expressway attempts to authenticate the credentials presented by the endpoint client.The reasons for this include:

■ The client is supplying an unknown username or the wrong password.
■ ILS (Intercluster Lookup Service) has not been set up on all of the Unified CM clusters. This may result in intermittent failures, depending upon which Unified CM node is being used by Expressway for its UDS query to discover the client's home cluster.

Call failures due to "407 proxy authentication required" or "500 Internal Server Error" errors

Call failures can occur if the traversal zones on Expressway are configured with an **Authentication policy** of *Check credentials*. Ensure that the **Authentication policy** on the traversal zones used for mobile and remote access is set to *Do not check credentials*.

Call bit rate is restricted to 384 kbps / video issues when using BFCP (presentation sharing)

This can be caused by video bit rate restrictions within the regions configured on Unified CM.

Ensure that the **Maximum Session Bit Rate for Video Calls** between and within regions (**System > Region Information > Region**) is set to a suitable upper limit for your system, for example 6000 kbps.

Endpoints cannot register to Unified CM

Endpoints may fail to register for various reasons:

- Endpoints may not be able to register to Unified CM if there is also a SIP trunk configured between Unified CM and Expressway-C. If a SIP trunk is configured, you must ensure that it uses a different listening port on Unified CM from that used for SIP line registrations to Unified CM. See SIP trunks between Unified CM and Expressway-C [p.41] for more information.
- Secure registrations may fail ('Failed to establish SSL connection' messages) if the server certificate on the Expressway-C does not contain in its Subject Alternate Name list, the names of all of the Phone Security Profiles in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Note that these names — in both Unified CM and in the Expressway's certificate — must be in FQDN format.

IM and Presence Service realm changes

Provisioning failures can occur when the IM and Presence Service realm has changed and the realm data on the Expressway-C has not been updated.

For example, this could happen if the address of an IM and Presence Service node has changed, or if a new peer has been added to an IM and Presence Service cluster.

The diagnostic log may contain an INFO message like "`Failed to query auth component for SASL mechanisms`" because the Expressway-C cannot find the realm.

Go to **Configuration > Unified Communications > IM and Presence Service nodes** and click **Refresh servers** and then save the updated configuration. If the provisioning failures persist, verify the IM and Presence Service nodes configuration and refresh again.

No voicemail service ("403 Forbidden" response)

Ensure that the Cisco Unity Connection (CUC) hostname is included on the HTTP server allow list on the Expressway-C.

"403 Forbidden" responses for any service requests

Services may fail ("403 Forbidden" responses) if the Expressway-C and Expressway-E are not synchronized to a reliable NTP server. Ensure that all Expressway systems are synchronized to a reliable NTP service.

Client HTTPS requests are dropped by Expressway

This can be caused by the automated intrusion protection feature on the Expressway-E if it detects repeated invalid attempts (404 errors) from a client IP address to access resources through the HTTP proxy.

To prevent the client address from being blocked, ensure that the **HTTP proxy resource access failure** category (**System > Protection > Automated detection > Configuration**) is disabled.

Unable to configure IM&P servers for remote access

'Failed: <address> is not a IM and Presence Server'

This error can occur when trying to configure the IM&P servers used for remote access (via **Configuration > Unified Communications > IM and Presence servers**).

It is due to missing CA certificates on the IM&P servers and applies to systems running 9.1.1. More information and the recommended solution is described in bug CSCul05131.

Document revision history

The following table summarizes the changes that have been applied to this document.

Date	Description
April 2015	Updated for X8.5.2, with information about authorization rate control and doc. defects addressed.
February 2015	Updated for X8.5.1 with SSO feature changes: SHA-256 signing of SAML requests by default, changed wording of IdP prerequisites.
December 2014	Updated with new features for X8.5 and corrections from X8.2 version.
August 2014	Re-issued X8.1.1 version of this document with shared line limitation, as per X8.2 version.
July 2014	Re-issued with updated client support details and a media encryption limitation removed.
July 2014	Re-issued with updated firewall advice and unsupported deployment.
July 2014	Re-issued with updated domains screenshot.
June 2014	Republished for X8.2.
April 2014	Initial release.