Unified Communications Mobile and Remote Access via Cisco Expressway

Deployment Guide

Cisco Expressway X8.1.1 or later
Cisco Unified CM 9.1(2)SU1 or later

January 2015

Contents

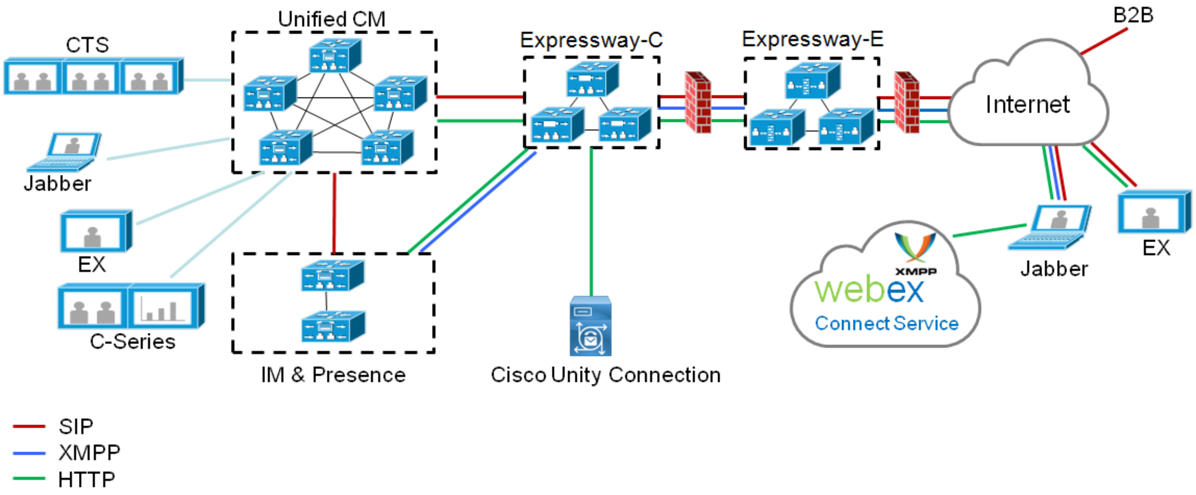
Mobile and remote access

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:

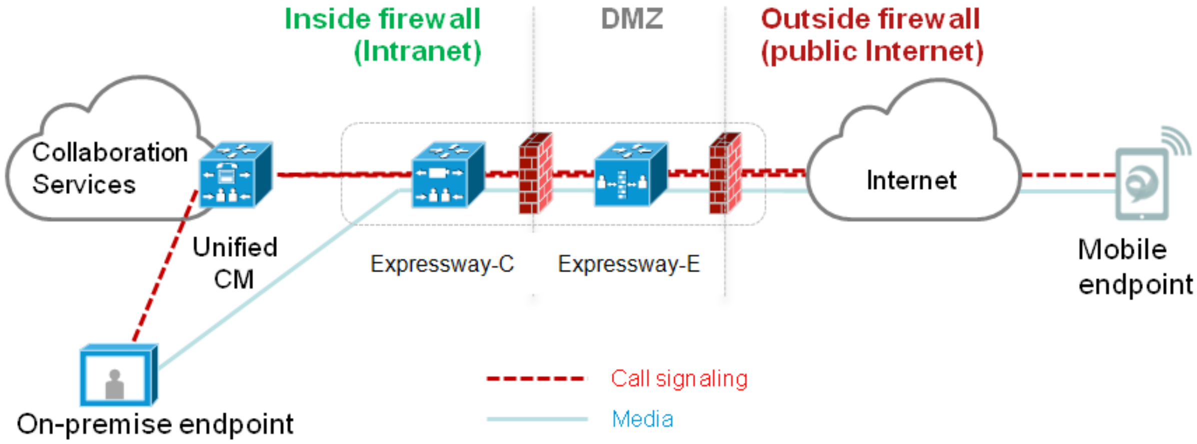
- **Off-premises access**: a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- **Security**: secure business-to-business communications
- **Cloud services**: enterprise grade flexibility and scalable solutions providing rich WebEx integration and Service Provider offerings
- **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 Unified Client Services Framework 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*

- *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager Communications Manager*
- Jabber client configuration details:
  - *Cisco Jabber for Windows*
  - *Cisco Jabber for iPad*
  - *Cisco Jabber for Android*
  - *Cisco Jabber DNS Configuration Guide*

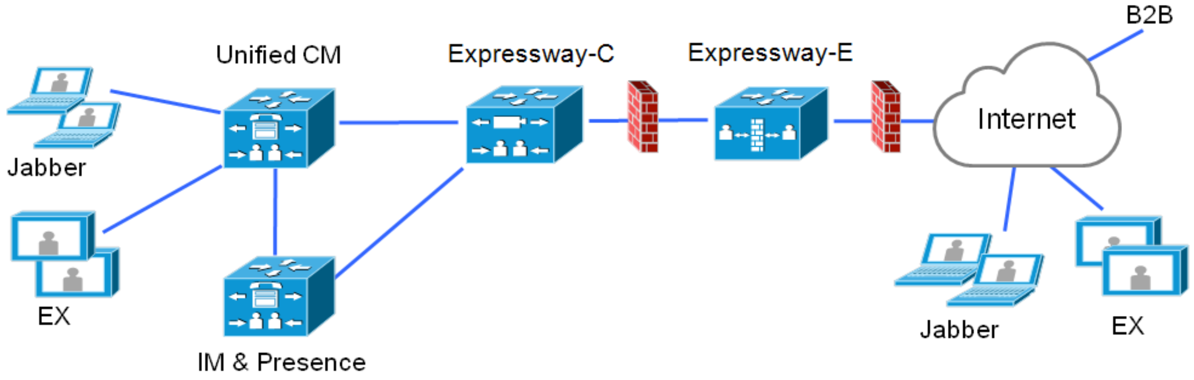
Deployment scenarios

This section describes the supported deployment environments:

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

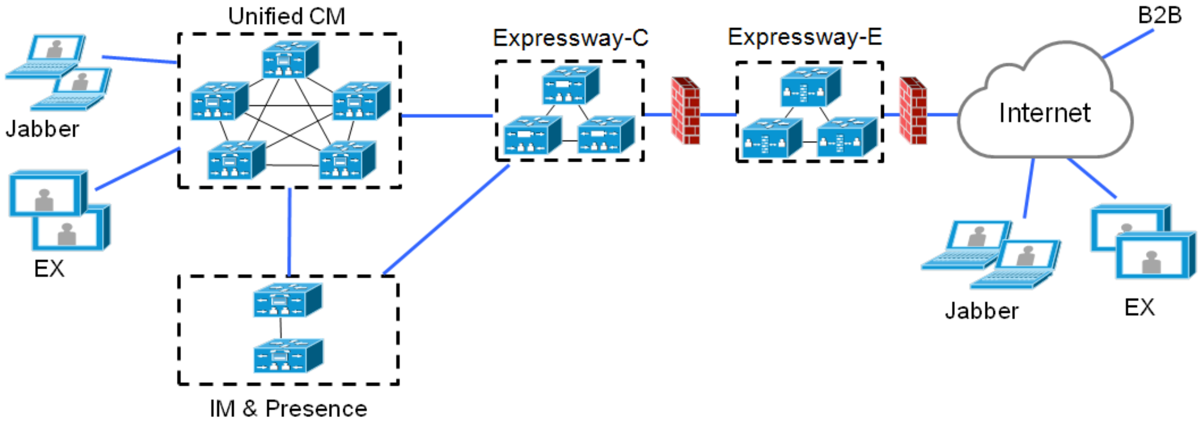
Single network elements

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



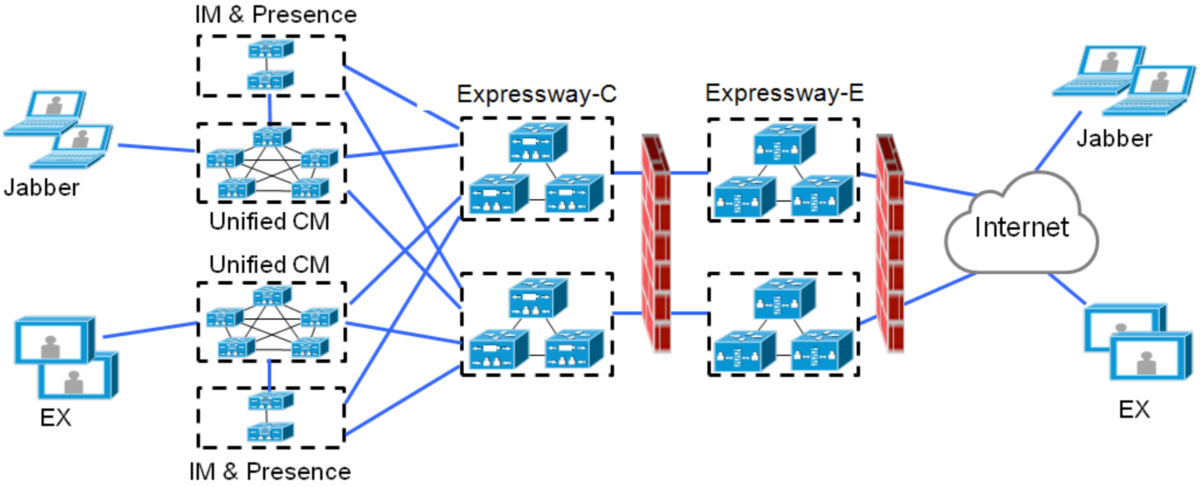
Single clustered network elements

In this scenario each network element is clustered.



Multiple clustered network elements

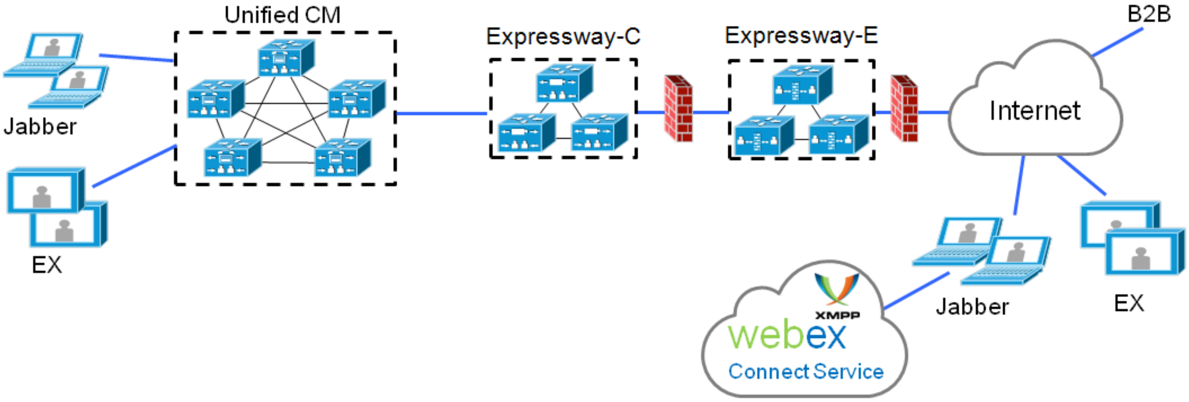
In this scenario there are multiple clusters of each network element.



Jabber clients can access their own cluster via any route. Each Unified CM and IM & Presence cluster combination must use the same domain.

Hybrid deployment

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



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 have been configured as specified in *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager Communications Manager*

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 & Presence 9.1(1) or later

Supported clients when using mobile and remote access

- Cisco Jabber for Windows 9.7 or later
- Cisco Jabber for iOS (iPhone and iPad) 9.6.1 or later
- Cisco Jabber for Android 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*.

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.

Client certificates are optional. If used, they should be installed by provisioning while the endpoint is inside the enterprise network, before taking it outside.

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
- 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*

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.

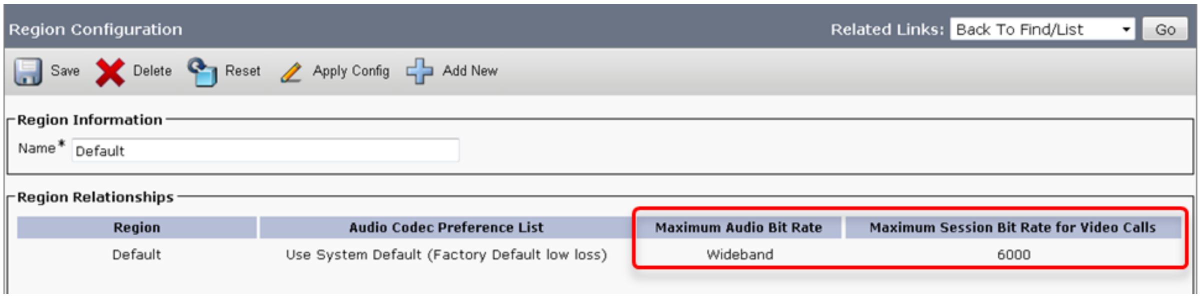
Firewall

- 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 Unified Communications port reference [p.23] 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, ILS (Intercluster Lookup Service) must be set up on all of the clusters. This is because the Expressway has to authenticate a client against its 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. See *Intercluster Lookup Service* for more information.
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.



Region Information

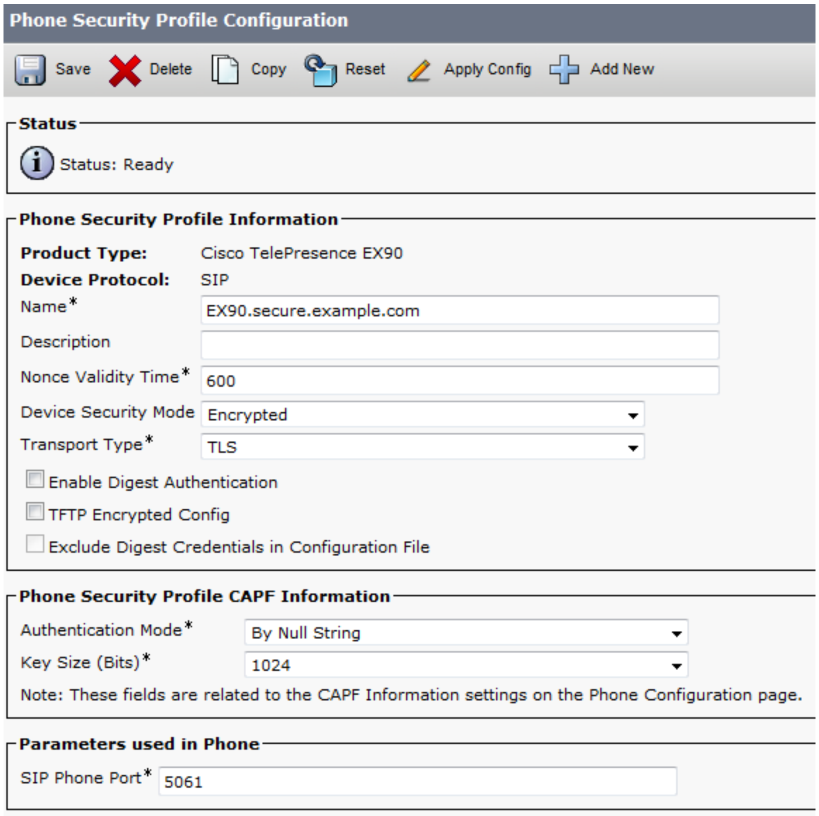
Name* Default

Region Relationships

Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
Default	Use System Default (Factory Default low loss)	Wideband	6000

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.) Also ensure that the **SIP phone port** is set to 5061.



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. Note that server names configured as fully qualified host names (FDQNs) are not supported.
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

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

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.14]

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 and IM&P servers on the Expressway-C.
4. Configure the domains on the Expressway-C for which services are to be routed to Unified CM.
5. Install appropriate server certificates and trusted CA certificates.
6. Configure a secure traversal zone connection between the Expressway-E and the Expressway-C.
7. If required, configure the HTTP server allow list for any web services inside the enterprise that need to be accessed from remote Jabber clients.

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.

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.

Note that this deployment requires valid certificates on both Expressway-C and Expressway-E. 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.

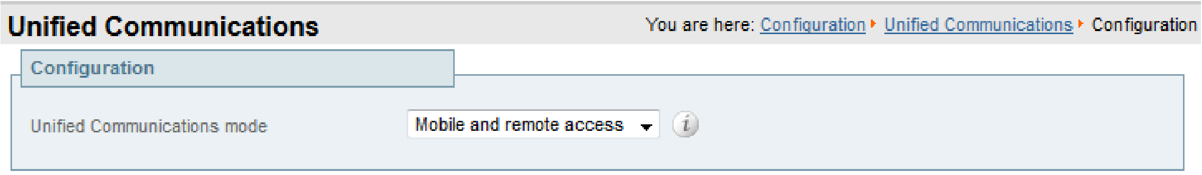
If you have a cluster of Expressways you must do this for every peer.

Configuring the Expressway-C for Unified Communications

Enabling 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**.


Unified Communications
You are here: Configuration ▸ Unified Communications ▸ Configuration
Configuration

Unified Communications mode: Mobile and remote access

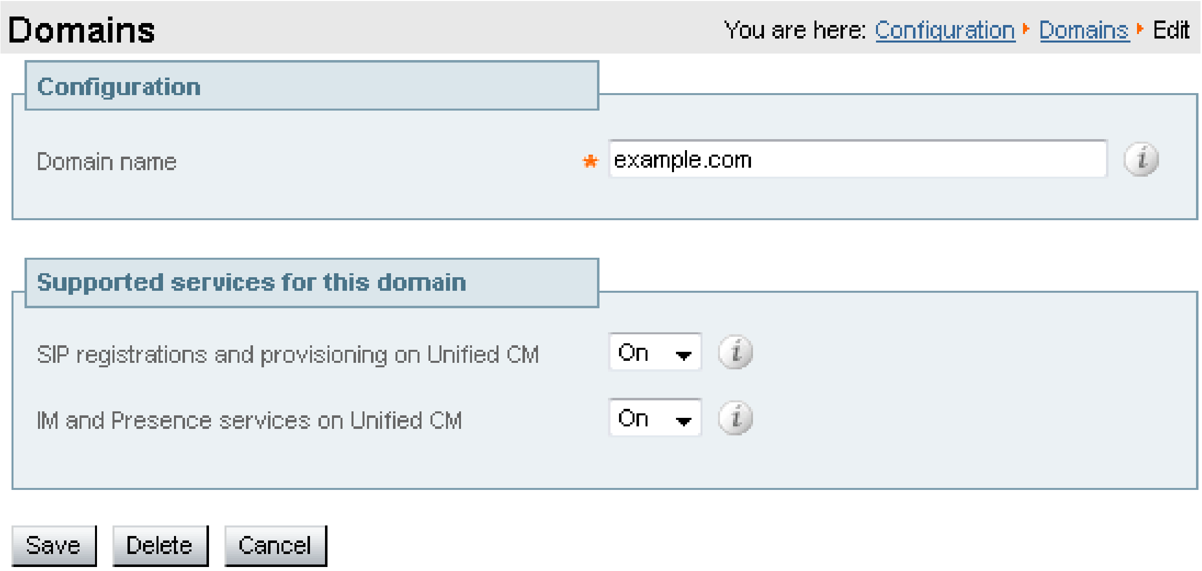
Note that you must select *Mobile and remote access* before you can configure the relevant domains and traversal zones.

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 services on Unified CM**: instant messaging and presence services for this SIP domain are provided by the Unified CM IM and Presence service.

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



Domains

You are here: Configuration ▸ Domains ▸ Edit

Configuration

Domain name * example.com

Supported services for this domain

SIP registrations and provisioning on Unified CM: On

IM and Presence services on Unified CM: On

Discovering IM&P and Unified CM servers

The Expressway-C must be configured with the address details of the IM&P servers and Unified CM servers that are to provide registration, call control, provisioning, messaging and presence services.

Note that IM&P server configuration is not required in the hybrid deployment model.

Uploading the IM&P / Unified CM tomcat certificate to the Expressway-C trusted CA list

If you intend to have **TLS verify mode** set to *On* (the default and recommended setting) when discovering the IM&P and Unified CM servers, the Expressway-C must be configured to trust the tomcat certificate presented by those IM&P and Unified CM servers.

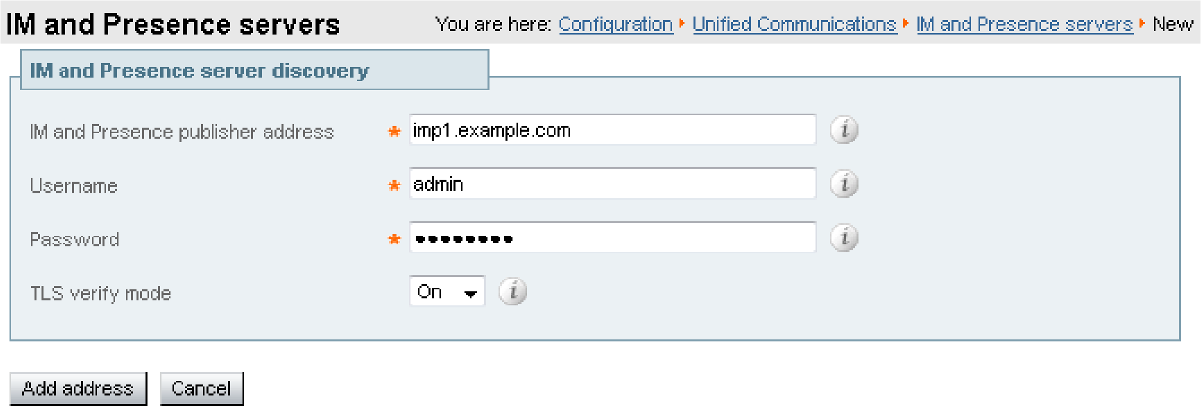
1. Determine the relevant CA certificates to upload:
   - If the servers are using self-signed certificates, the Expressway-C's trusted CA list must include a copy of the tomcat certificate from every IM&P / Unified CM server.
   - If the servers are using CA-signed certificates, the Expressway-C's trusted CA list must include the root CA of the issuer of the tomcat certificates.
2. Upload the trusted Certificate Authority (CA) certificates to the Expressway-C (**Maintenance > Security certificates > Trusted CA certificate**).

3. Restart the Expressway-C for the new trusted CA certificates to take effect (**Maintenance > Restart options**).

Configuring IM&P servers

To configure the IM&P servers used for remote access:

1. On Expressway-C, go to **Configuration > Unified Communications > IM and Presence servers**.
   The resulting page displays any existing servers that have been configured.
2. Add the details of an IM&P publisher:
   a. Click **New**.
   b. Enter the **IM and Presence publisher address** and the **Username** and **Password** credentials required to access the server. The address can be specified as an FQDN or as an IP address; we recommend using FQDNs when **TLS verify mode** is *On*.
      Note that these credentials are stored permanently in the Expressway database. The IM&P user must have the *Standard AXL API Access* role.
   c. We recommend leaving **TLS verify mode** set to *On* to ensure Expressway verifies the tomcat certificate presented by the IM&P server for XMPP-related communications.
      - If the IM&P server is using self-signed certificates, the Expressway-C's trusted CA list must include a copy of the tomcat certificate from every IM&P server.
      - If the IM&P server is using CA-signed certificates, the Expressway-C's trusted CA list must include the root CA of the issuer of the tomcat certificate.
   d. Click **Add address**.
      The system then attempts to contact the publisher and retrieve details of its associated nodes.



IM and Presence servers

You are here: Configuration ▸ Unified Communications ▸ IM and Presence servers ▸ New

IM and Presence server discovery

IM and Presence publisher address *	imp1.example.com
Username *	admin
Password *	•••••••••
TLS verify mode	On

   Note that the status of the IM&P server will show as **Inactive** until a valid traversal zone connection between the Expressway-C and the Expressway-E has been established (this is configured later in this process).
3. Repeat for every IM&P cluster.

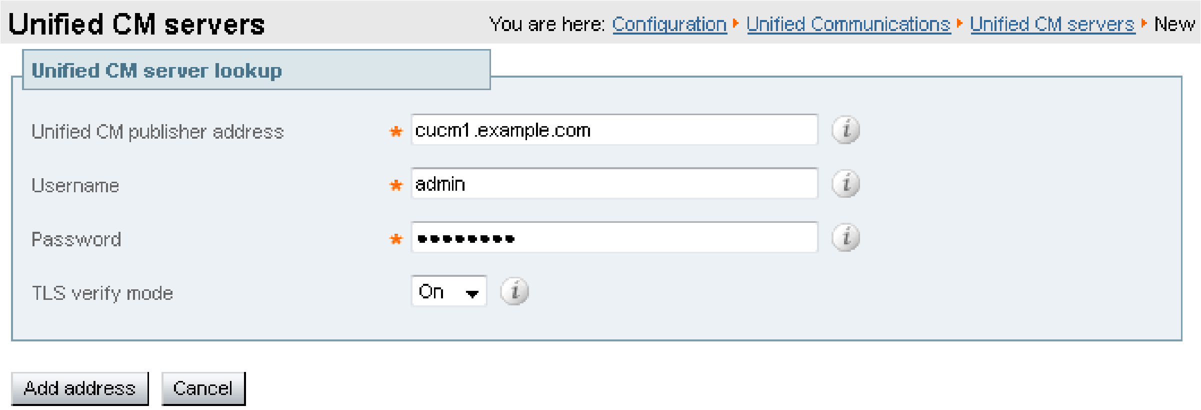
After configuring multiple publisher addresses, you can click **Refresh servers** to refresh the details of the nodes associated with selected addresses.

Configuring Unified CM servers

To configure the Unified CM servers used for remote access:

1. On Expressway-C, go to **Configuration > Unified Communications > Unified CM servers**.
   The resulting page displays any existing servers that have been configured.

2. Add the details of a Unified CM publisher:
   a. Click **New**.
   b. Enter the **Unified CM publisher address** and the **Username** and **Password** credentials of an application user account that can access the server. The address can be specified as an FQDN or as an IP address; we recommend using FQDNs when **TLS verify mode** is *On*.
   Note that these credentials are stored permanently in the Expressway database. The Unified CM user must have the *Standard AXL API Access* role.
   c. We recommend leaving **TLS verify mode** set to *On* to ensure Expressway verifies the certificates presented by the Unified CM server (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.
      - If the Unified CM server is using CA-signed certificates, the Expressway-C's trusted CA list must include the root CA of the issuer of the tomcat certificate and the CallManager certificate.
   d. Click **Add address**.
   The system then attempts to contact the publisher and retrieve details of its associated nodes.


You are here: Configuration ▸ Unified Communications ▸ Unified CM servers ▸ New
Add address
Cancel

Unified CM servers

Unified CM server lookup

Unified CM publisher address * cucm1.example.com

Username * admin

Password * •••••••••

TLS verify mode On

3. Repeat for every Unified CM cluster.

After configuring multiple publisher addresses, you can click **Refresh servers** to refresh the details of the nodes associated with selected 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.

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:

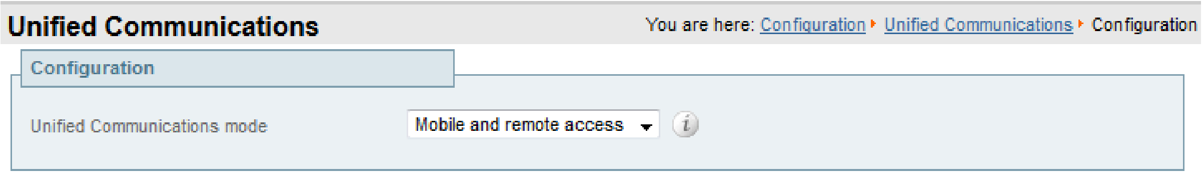
1. Ensure that **System host name** and **Domain name** are specified (**System > DNS**).
2. Ensure that public DNS servers are specified (**System > DNS**).
3. Ensure that all Expressway systems are synchronized to a reliable NTP service (**System > Time**). Use an **Authentication** method in accordance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

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

Configuring the Expressway-E for Unified Communications

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**.



Unified Communications

You are here: Configuration ▸ Unified Communications ▸ Configuration

Configuration

Unified Communications mode: Mobile and remote access

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*.

Setting up Expressway security certificates

This deployment requires secure communications between the Expressway-C and the Expressway-E, and between the Expressway-E and endpoints located outside the enterprise. Therefore, you must:

1. Install a suitable server certificate on both the Expressway-C and the Expressway-E. The certificate on each Expressway has different requirements for what needs to be included as subject alternate names as described in **Expressway-C / Expressway-E server certificate requirements** below.
   - The certificate must include the **Client Authentication** extension. (The system will not allow you to upload a server certificate without this extension when mobile and remote access is enabled.)
   - The Expressway includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR. This CSR includes the client authentication request and can be used to help ensure each Expressway certificate includes the correct subject alternate

names for Unified Communications and to establish a secure traversal zone. Ensure that the CA that signs the request does not strip out the client authentication extension.

- 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, and, if appropriate, the authority that signed the endpoints' certificates. The Expressway-C must also trust the Unified CM and IM&P tomcat 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.

Expressway-C server certificate requirements

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

- The **Chat Node Aliases** that are configured on the IM and Presence servers. These are required only for Unified Communications XMPP federation deployments that intend to use both TLS and group chat. (Note that Unified Communications XMPP federation will be supported in a future Expressway release).
  The Expressway-C automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM&P servers.
- The names, in FQDN format, of all of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. This ensures that Unified CM can communicate with Expressway-C via a TLS connection when it is forwarding messages from devices that are configured with those security profiles.

A new certificate may need to be produced 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. You must restart the Expressway-C for any new uploaded server certificate to take effect.

Expressway-E server certificate requirements

The Expressway-E server certificate needs to include the following elements in its list of subject alternate names:

- All of the domains which have been configured for Unified Communications. They are required for secure communications between endpoint devices and Expressway-E.
  This should include the email address domain entered by users of the client application (e.g. Jabber) and any presence domains (as configured on the Expressway-C) if they are different. There is no need to include the domains in DNS-SEC deployments.
- The same set of **Chat Node Aliases** as entered on the Expressway-C's certificate, if you are deploying federated XMPP.
  Note that the list of required aliases can be viewed (and copy-pasted) from the equivalent **Generate CSR** page on the Expressway-C.

A new certificate must be produced if new presence domains or chat node aliases are added to the system. You must restart the Expressway-E for any new uploaded server 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.

Setting up secure Expressway traversal zones

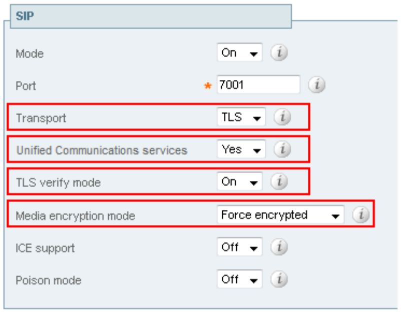
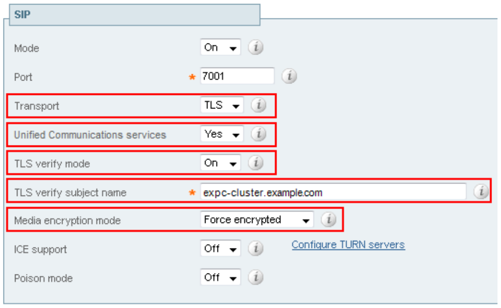
To support Unified Communications features such as mobile and remote access, there must be a secure traversal zone connection between the Expressway-C and the Expressway-E:

- The traversal client zone and the traversal server zone must be configured to use SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** must be *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 a H.323 or a non-encrypted connection is 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	*Traversal client*	*Traversal server*
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**.
H.323 Mode	*Off*	*Off*
SIP section		
Mode	*On*	*On*
Port	`7001`	`7001`
Transport	*TLS*	*TLS*
Unified Communications services	*Yes*	*Yes*
TLS verify mode	*On*	*On*
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.
Media encryption mode	*Force encrypted*	*Force encrypted*

	Expressway-C	Expressway-E
Location section		
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
	 SIP Mode: On Port: 7001 Transport: TLS Unified Communications services: Yes TLS verify mode: On Media encryption mode: Force encrypted ICE support: Off Poison mode: Off	 SIP Mode: On Port: 7001 Transport: TLS Unified Communications services: Yes TLS verify mode: On TLS verify subject name: expc-cluster.example.com Media encryption mode: Force encrypted ICE support: Off Configure TURN servers Poison mode: Off

Note that you should enable **Unified Communications services** on one traversal zone only per Expressway.

4. Click **Create zone**.

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.

Additional configuration

Configuring the HTTP server allow list 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 allowlisting, include:

- Visual Voicemail
- Jabber Update Server

- Custom HTML tabs / icons
- Directory Photo Host

The IP addresses of all discovered Unified CM nodes (that are running the CallManager or TFTP service) and IM&P nodes are added automatically to the allow list and cannot be deleted . Note, however, that they are not displayed on the **HTTP server allow list** page.

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 an HTTP server that a Jabber client located outside of the enterprise is 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.

Unified Communications port reference

This section summarizes the ports that need to be opened on the 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.

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	UDP	36002 to 59999 *	36000 to 36001 *

Outbound from Expressway-E (DMZ) to public internet

Purpose	Protocol	Expressway-E (source)	Internet endpoint (listening)
SIP media	UDP	36002 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 *
SIP signaling	TLS	>= 1024	5061
HTTPS (administrative access)	TCP	>= 1024	443

From Expressway-C to Unified CM / CUC

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 (configuration file retrieval)	TCP	Ephemeral port	6970
CUC (voicemail)	TCP	Ephemeral port	443 (CUC)
Media	UDP	36002 to 59999 *	>= 1024
SIP signaling	TCP/TLS	25000 to 29999	5060/5061

* The default media port range is 36000 to 59999. The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

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 consume any rich media session licenses.
- **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 consume system resources and each Expressway has a maximum limit of 150 concurrent calls (500 calls on Large VM servers).

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 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).

Expressway automated intrusion protection

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**).

You can enable the **HTTP proxy authorization failure** and **HTTP proxy protocol violation** categories.

Note:

- Do not enable the **HTTP proxy resource access failure** category.
- You may first have to enable the **Automated protection service** (**System > System administration**).

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.

Limitations

- The IPV4 protocol only is supported for mobile and remote access users
- SIP Early Media is not supported
- 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

- Directory access mechanisms other than UDS
- Certificate provisioning to remote endpoints e.g. CAPF
- File transfer (except when operating in hybrid Webex mode)

- Deskphone control (QBE/CTI)
- Additional mobility features including DVO-R, GSM handoff and session persistency
- 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

- 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)
- Calls involving secure endpoints remotely registered to Unified CM via Expressway may end up with a portion of the call using non-secure media; these portions will only ever be on sections of the call that are on premises (between the Expressway-C and endpoints registered locally to Unified CM), never on the public Internet
- Endpoint management capability (SNMP, SSH/HTTP access)
- Multi-domain and multi-customer support; each Expressway deployment supports only one IM&P domain (even though IM & Presence 10.0 or later supports multiple IM&P 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
- XMPP federation managed directly by Expressway-E (note that remote client access via Expressway for XMPP inter domain federation managed by CUP is supported)
- 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
- The Expressway-E DNS hostname must not contain underscore characters (it can only contain letters, digits and hyphens)
- 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

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 primary peer.

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. Call legs between Expressway-C and endpoints within the enterprise will not be encrypted.

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

Advanced Expressway-C configuration

This section covers the advanced Unified Communications settings that can be configured on Expressway-C.

Credential caching intervals

The Expressway caches endpoint credentials which have been authenticated by Unified CM. The caching of credentials reduces the frequency with which the Expressway has to submit endpoint credentials to Unified CM for authentication, and thus improves system performance.

To configure the caching settings, go to **Configuration > Unified Communications** and then click **Show advanced settings**.

The **Credentials refresh interval** specifies the number of minutes for which endpoint credentials are cached in the Expressway database. The default is 480 minutes.

The **Credentials cleanup interval** specifies the frequency with which the Expressway database runs a cleanup process to remove expired credentials. In large deployments, a regular cleanup process helps to maintain the system's performance. The default is 720 minutes.

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. Click **Start new log**.

3. (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.
4. Reproduce the system issue you want to trace in the diagnostic log.
5. Click **Stop logging**.
6. Click **Download log** to save the diagnostic log to your local file system. You are prompted to save the file (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
- _collab-edge._tcp
- _cuplogin._tcp
- _cisco-uds._tcp

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 Encryption 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 & Presence nodes (on Expressway go to **Configuration > Unified Communications**).

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).

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.26] 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.

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'><bind
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.

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.

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. You must ensure the hostname only contain letters, digits and hyphens.

Document revision history

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

Date	Description
January 2015	Re-issued X8.1.1 version of this document with single NIC and static NAT advice, as per X8.2 version.
August 2014	Re-issued X8.1.1 version of this document with shared line limitation, as per X8.2 version.
April 2014	Initial release.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.