Mobile and Remote Access Through Cisco Expressway

Deployment Guide

First Published: April 2014

Last Updated: November 2017

Cisco Expressway X8.9.1

Cisco Unified Communications Manager 10 or later

Cisco Unified Communications Manager IM and Presence Service 10 or later

Cisco Unity Connection 10 or later

Contents

Preface

Change History

Table 1 Mobile and Remote Access Through Cisco Expressway Deployment Guide Change History

Date	Change	Reason
November 2017	Clarified which Cisco IP Phones in the 88xx series support MRA (*Configuration Overview* section).	Content defect
September 2017	Updated software version requirements for SIP path headers.	CDETS CSCvd84831
April 2017	Added details on partial support for Cisco Jabber SDK features.	Content defect
January 2017	Updated section on unsupported features when using MRA. Added description of Maintenance Mode. Clarified that Expressway-C and Expressway-E need separate IP addresses.	X8.9.1 release
December 2016	Updated.	X8.9 release
September 2016	Unsupported deployments section updated. Minimum versions note about TLS added.	Clarification to avoid misconfiguration
August 2016	Updated DNS prerequisite to create reverse lookup entries for Expressway-E	Customer found defect
June 2016	HTTP Allow list feature updates.	X8.8 release
February 2016	Troubleshooting topic updated with information about CSCux16696. Republished with X8.7.1.	Notable issue discovered post X8.7 but not yet fixed in X8.7.1.
November 2015	Updated.	X8.7 release
July 2015	Updated.	X8.6 release
June 2015	Updated. Note about internal DNS lookups for UC nodes.	X8.5.3 release
April 2015	Information about authorization rate control and document defects addressed.	X8.5.2 release
February 2015	SSO feature changes: SHA-256 signing of SAML requests by default, changed wording of IdP prerequisites.	X8.5.1 release
December 2014	Added new features and corrections from X8.2 version.	X8.5 release
August 2014	Re-issued X8.1.1 version of this document with shared line limitation, as per X8.2 version.	Content defect
July 2014	Re-issued with updated client support details and a media encryption limitation removed.	Content defect
July 2014	Re-issued with updated firewall advice and unsupported deployment.	Content defect

Table 1 Mobile and Remote Access Through Cisco Expressway Deployment Guide Change History (continued)

Date	Change	Reason
July 2014	Re-issued with updated domains screenshot.	Content defect
June 2014	Republished for X8.2.	X8.2 release
April 2014	Initial release of document.	Introduction of MRA

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*

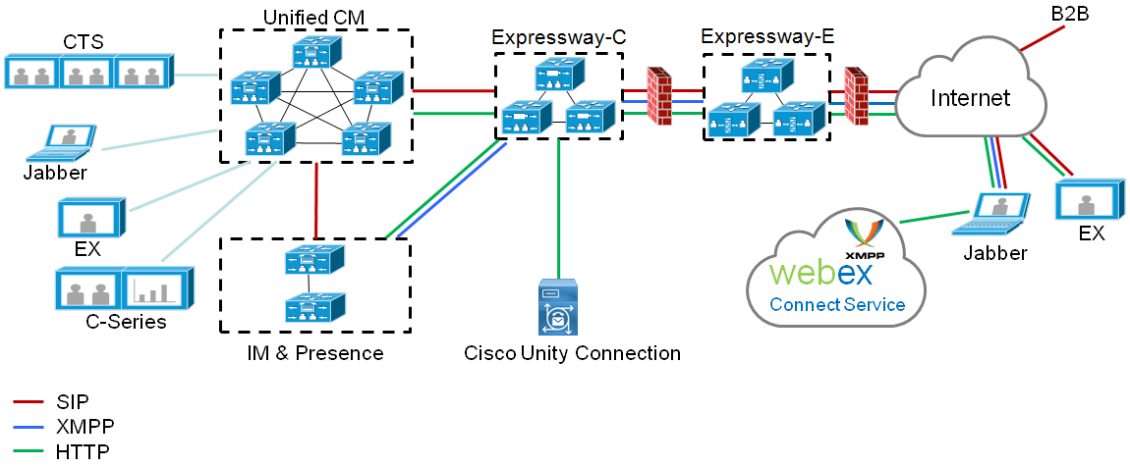
Mobile and Remote Access Overview

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:

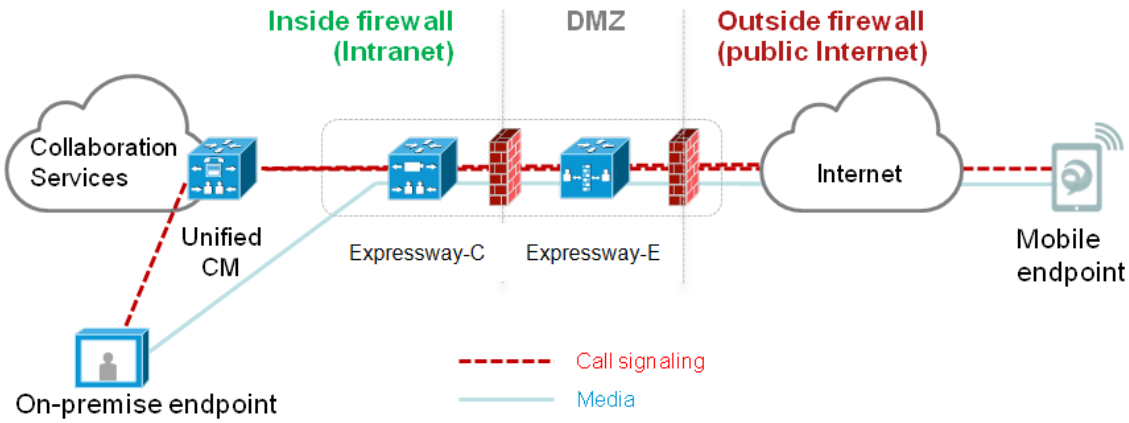
- **Off-premises access**: a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- **Security**: secure business-to-business communications
- **Cloud services**: enterprise grade flexibility and scalable solutions providing rich WebEx integration and Service Provider offerings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

Deployment Scope

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

- Mobile and Remote Access
- Microsoft Interoperability
- Jabber Guest services
- Hybrid Services (connector host)

Jabber Client Connectivity Without VPN

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

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

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

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

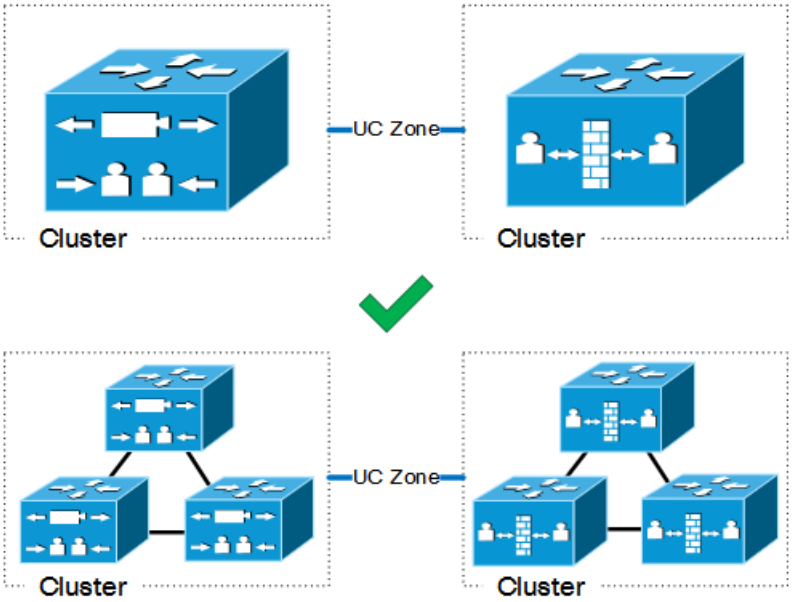
Deployment Scenarios

This section describes the supported deployment environments:

- Single network elements
- Single clustered network elements
- Multiple clustered network elements
- Hybrid deployment
- Unsupported deployments

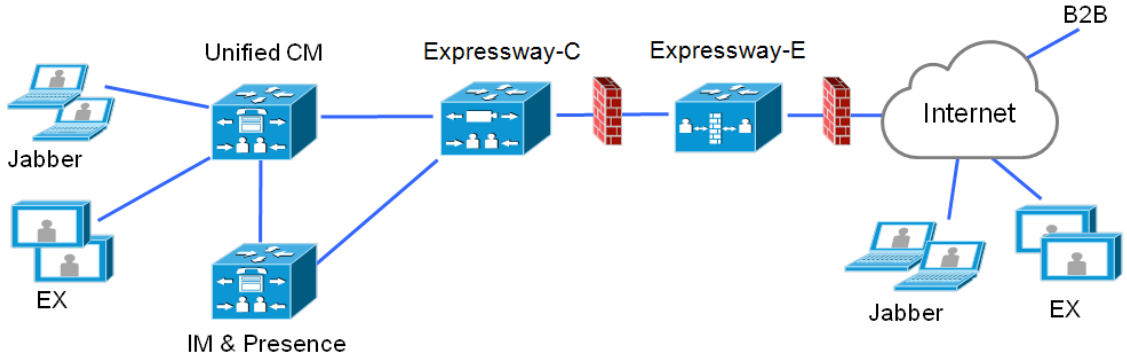
Note: The only supported Mobile and Remote Access deployments are based on one-to-one Unified Communications zones between Expressway-C clusters and Expressway-E clusters.

Figure 3 Supported MRA Traversal Connections



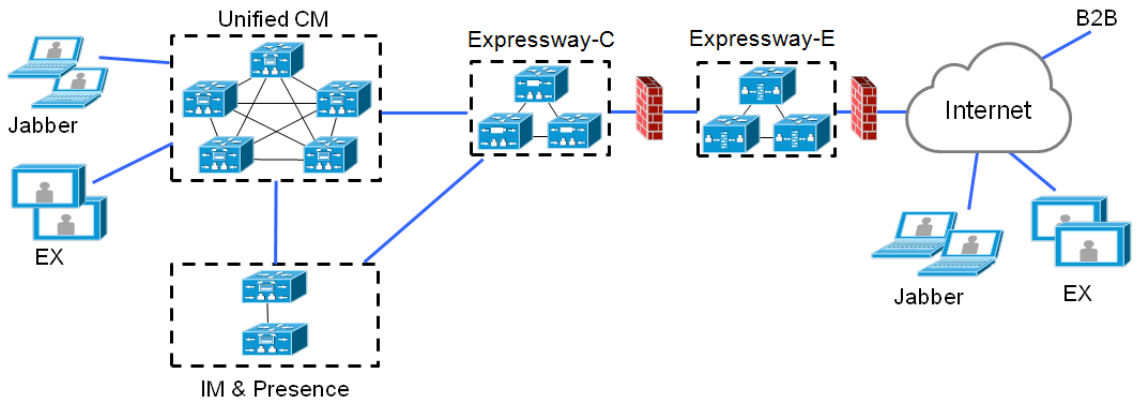
Single Network Elements

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



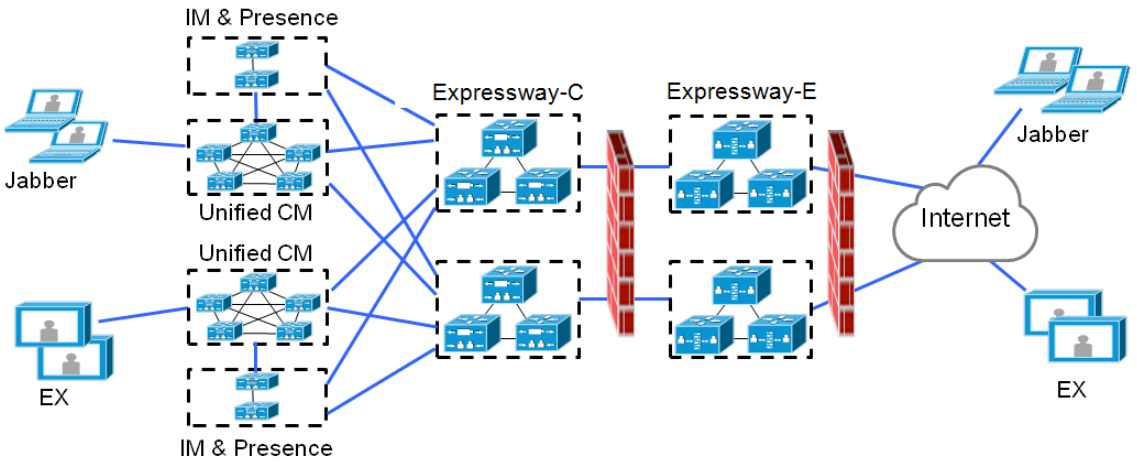
Single Clustered Network Elements

In this scenario each network element is clustered.



Multiple Clustered Network Elements

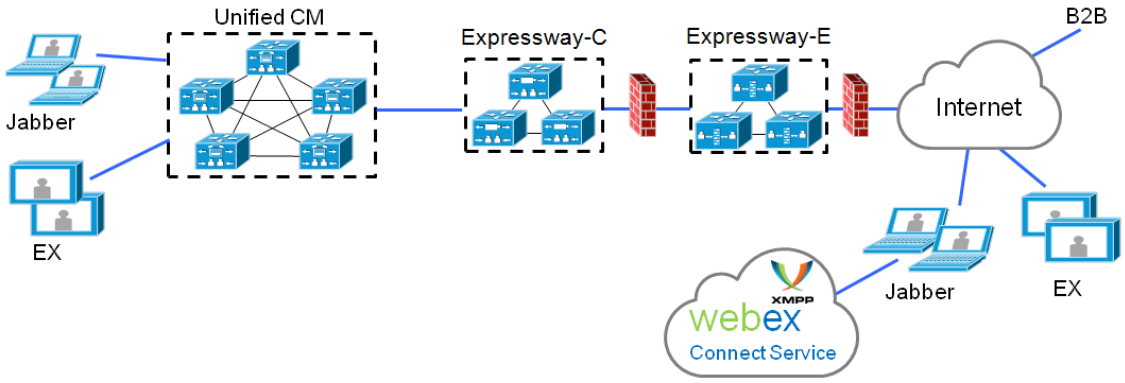
In this scenario there are multiple clusters of each network element.



- Jabber clients can access their own cluster through 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

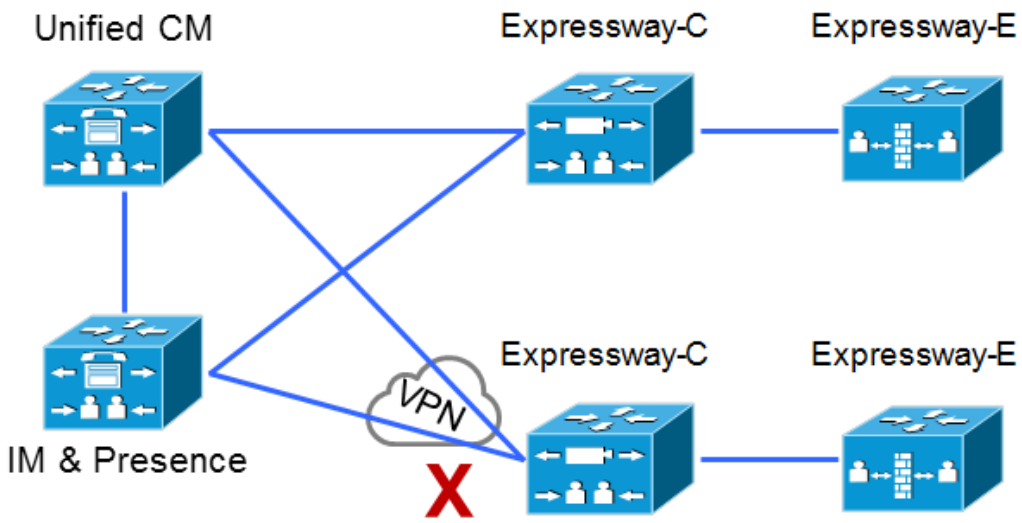
In this scenario, IM and Presence services for Jabber clients are provided via the WebEx cloud.



Unsupported Deployments

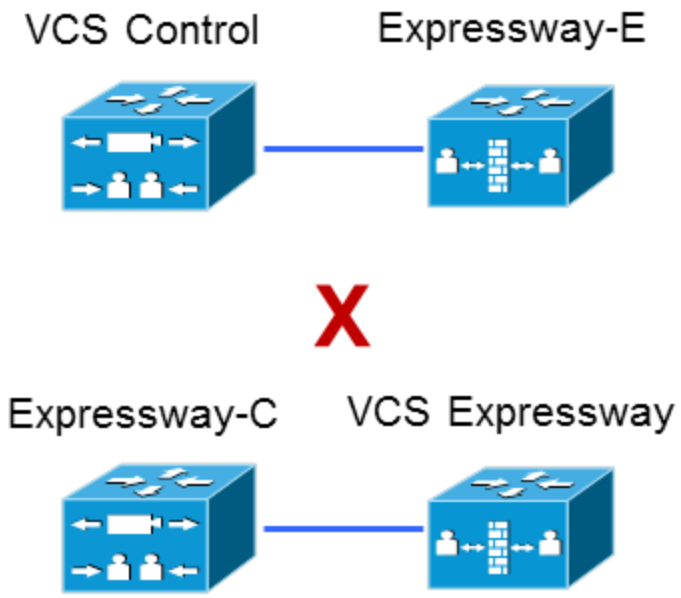
VPN Links

VPN links, between the Expressway-C and the Unified CM services / clusters, are not supported.



Traversal Zones Between VCS Series and Expressway Series

"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*.

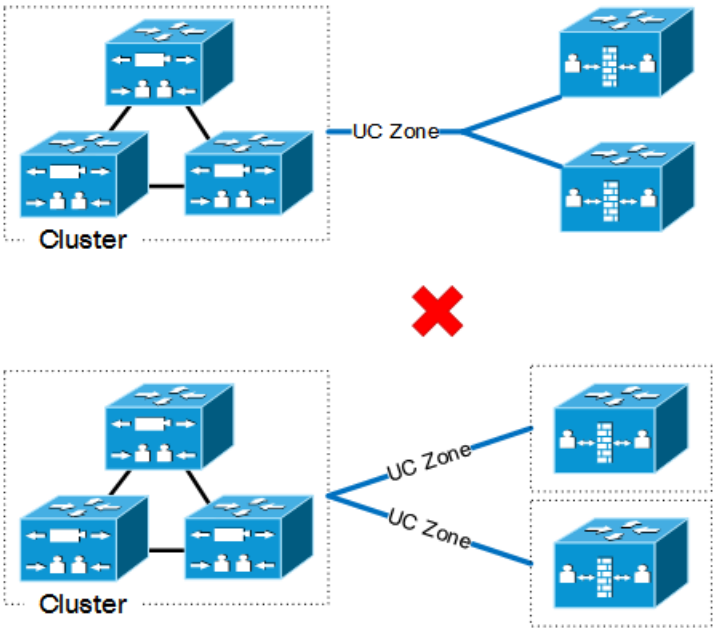


Explicitly, we do not support VCS Control traversal to Expressway-E, nor do we support Expressway-C traversal to VCS Expressway.

Unclustered or Many-to-One Traversal Connections

We do not support Unified Communications zones from one Expressway-C cluster to multiple unclustered Expressway-Es.

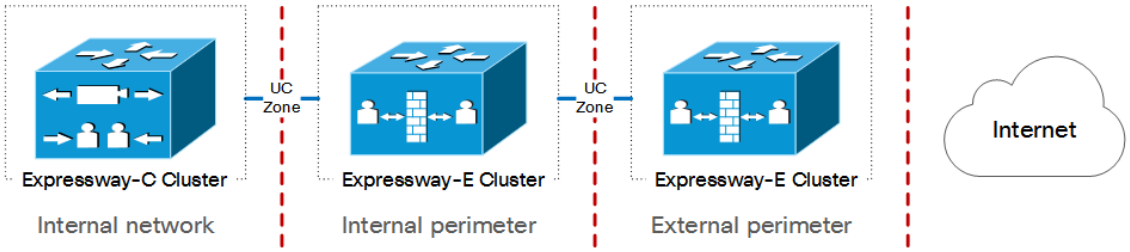
We also do not support multiple Unified Communications zones from one Expressway-C cluster to multiple Expressway-Es or Expressway-E clusters.



Nested Perimeter Networks

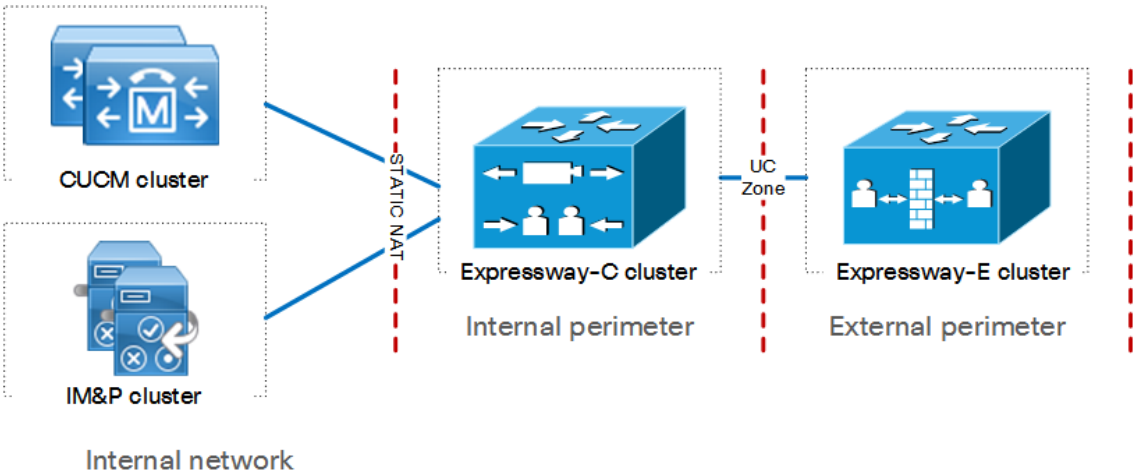
MRA is not currently supported over chained traversal connections (using multiple Expressway-Es to cross multiple firewalls).

This means that you cannot use Expressway-E to give Mobile and Remote Access to endpoints that must traverse a nested perimeter network to call internal endpoints.



Expressway-C in DMZ with Static NAT

We do not support Expressway-C in a DMZ that uses static NAT. This is because the Expressway-C does not perform the SDP rewriting that is required to traverse static NAT-enabled firewalls. You should use the Expressway-E for this purpose.



You could potentially place the Expressway-C in a DMZ that does not use static NAT, but we strongly discourage this deployment because it requires a lot of management on the inmost firewall. We always recommend placing the Expressway-C in the internal network.

Unsupported Features When Using Mobile and Remote Access

Not all features are supported in every deployment scenario when using Mobile and Remote Access. This section lists features which are known not to work in certain situations:

Unsupported Endpoint Features

- Call recording for Cisco Jabber endpoints connected over Mobile and Remote Access (MRA).
- The Cisco IP Phone 78xx series and the 8811, 8841, 8845, 8861 and 8865 models, support shared line or multiline features when connected through MRA (if Path Header support is enabled). We do not support shared line or multiline over MRA for other endpoints, phones, and soft clients.
- Custom embedded tabs for Cisco Jabber endpoints connected over MRA.
- Directory access mechanisms other than the Cisco User Data Service (UDS).
- Certificate provisioning to remote endpoints. For example, the Certificate Authority Proxy Function (CAPF). If you can do the first-time configuration on premises (inside the firewall) then you can support endpoints that use CAPF. After that you can use them over MRA - but you can't do the initial configuration over MRA.

- 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, Unified CM and endpoints use UPDATE to implement blind transfer, which does not work correctly over MRA.
- Peer-to-peer file transfer when using IM and Presence Service and Jabber is not supported over MRA. These features are supported over MRA:
  - Managed File Transfer (MFT) with IM and Presence Service 10.5.2 and later and Jabber 10.6 and later clients.
  - File transfer with WebEx Messenger Service and Cisco Jabber.
- Additional mobility features including GSM handoff and session persistency.
- Hunt group/hunt pilot/hunt list.
- Self-care portal.

Unsupported Expressway Features and Limitations

- The Expressway cannot be used for Jabber Guest when it is used for Mobile and Remote Access (MRA).
- The Expressway-C used for MRA cannot also be used for Microsoft gateway service. Microsoft gateway service requires a dedicated Expressway-C.
- MRA is not supported in IPv6 only mode.
- 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, and we currently recommend that you do not exceed 50 domains.
- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM (the same limit as Small / Medium VM servers).
- Not all contact center features are supported by Expressway when connected through MRA.

Unsupported Contact Center Features

This section applies if you use the Cisco Unified Contact Center Express (Unified CCX) solution through Mobile and Remote Access (MRA).

Expressway does not support some Unified CCX features for contact center agents or other users who connect over MRA. Unsupported features include:

- Deskphone control functions (due to no support for CTI-QBE protocol).
- Built in Bridge (BIB) functions, which means that silent monitoring and recording, and agent greeting are not available.
- Shared line and multiline support for the Cisco IP Phone 78xx series or the 8811, 8841, 8845, 8861 and 8865 models, is available from X8.9 but is not in earlier Expressway versions.

Notes:

- Jabber for Mac and Jabber for Windows are not capable of deskphone control when they are connected over MRA. This is because the Expressway pair does not traverse the CTI-QBE protocol.
- If these Jabber applications, or other CTI applications, can connect to CUCM CTIManager (directly or through the VPN) they *can* provide deskphone control of clients that are connected over MRA.

Configuration Overview

This section summarizes the steps to configure your Unified Communications system for Mobile and Remote Access. It assumes that the following items are already 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 are 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

- Expressway X8.1.1 or later (this document describes X8.9.1)
- Unified CM 10.0 or later
- IM and Presence Service 10.0 or later
- Cisco Unity Connection 10.0 or later

IP Addresses

You must assign separate IP addresses to the Expressway-C and the Expressway-E. Do not use a shared address for both elements, as the firewall will not be able to distinguish between them.

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

Expressway X8.6 and later:

Mobile and Remote Access is supported with the following Cisco IP Phones, when the phones are running firmware version 11.0(1) or later. We recommend Expressway X8.7 or later for use with these phones.

- Cisco IP Phone 8811, 8841, 8845, 8861 and 8865
- Cisco IP Phone 7800 Series

MRA is supported with the Cisco DX Series endpoints running firmware version 10.2.4(99) or later. This support was announced with Expressway version X8.6.

- Cisco DX650
- Cisco DX80
- Cisco DX70

When deploying DX Series, IP Phone 7800, or IP Phone 8811, 8841, 8845, 8861 and 8865 endpoints to register with Cisco Unified Communications Manager via MRA, be aware of the following:

- **Phone security profile:** If the phone security profile for any of these endpoints has **TFTP Encrypted Config** checked, you will not be able to use the endpoint through MRA. This is because the MRA solution does not

support devices interacting with CAPF (Certificate Authority Proxy Function).

- **Trust list:** You cannot modify the root CA trust list on these endpoints. Make sure that the Expressway-E's server certificate is signed by one of the CAs that the endpoints trust, and that the CA is trusted by the Expressway-C and the Expressway-E.
- **Bandwidth restrictions:** The **Maximum Session Bit Rate for Video Calls** on the default region on Cisco Unified Communications Manager is 384 kbps by default. The **Default call bandwidth** on Expressway-C is also 384 kbps by default. These settings may be too low to deliver the expected video quality for the DX Series.
- **Off-hook dialling:** The way KPML dialing works between these endpoints and Unified CM means that you need CUCM 10.5(2)SU2 or later to be able to do off-hook dialing via MRA. You can work around this dependency by using on-hook dialing.

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 provided in the installation and configuration guide for the relevant 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 the *Cisco Jabber Planning Guide* (for your version) on the Jabber Install and Upgrade Guides page.

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>` SRV records. For example:

Domain	Service	Protocol	Priority	Weight	Port	Target host
example.com	cisco-uds	tcp	10	10	8443	cucmserver1.example.com
example.com	cisco-uds	tcp	10	10	8443	cucmserver2.example.com

Notes:

- **Important! From version X8.8 onward, you must create forward and reverse DNS entries for all Expressway-E systems, so that systems making TLS connections to them can resolve their FQDNs and validate their certificates.**
- Ensure that the `cisco-uds` 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.
- You must create internal DNS records, for both forward and reverse lookups, for all Unified Communications nodes used with Mobile and Remote Access. This allows Expressway-C to find the nodes when IP addresses or hostnames are used instead of FQDNs.

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, page 47 for more information.
- Do not use a shared address for the Expressway-E and the Expressway-C, as the firewall cannot distinguish between them. If you use static NAT for IP addressing on the Expressway-E, make sure that any NAT operation on the Expressway-C does not resolve to the same traffic IP address. We do not support shared NAT addresses between Expressway-E and Expressway-C.

- 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.

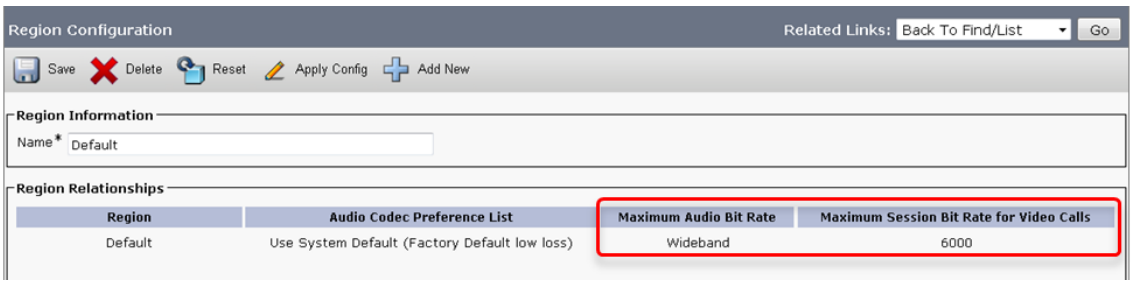
Unified CM

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.

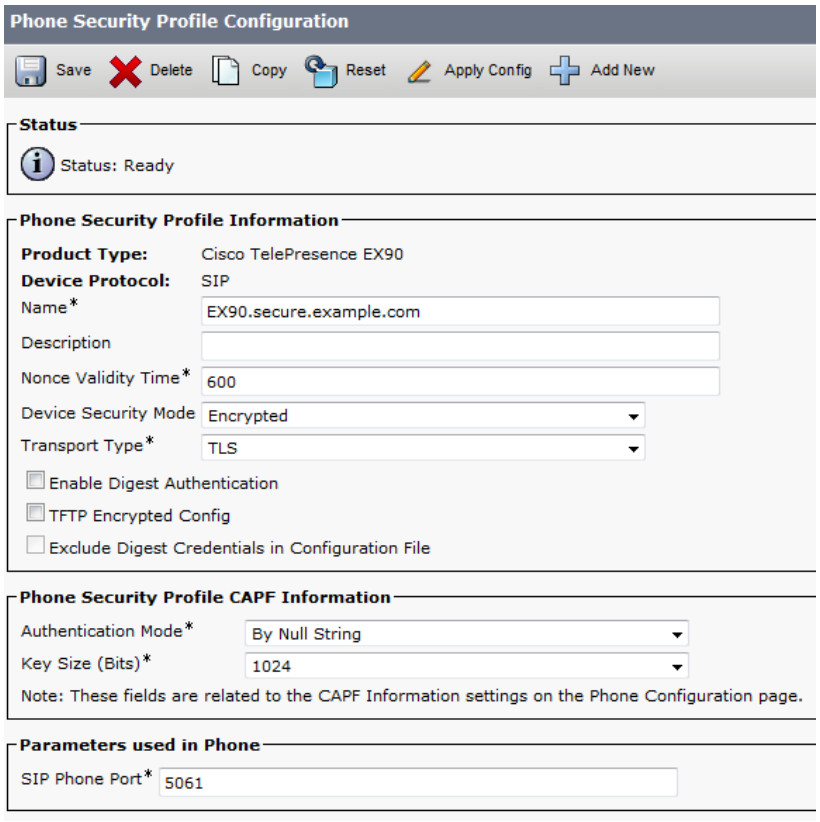
2. Ensure that the **Maximum Session Bit Rate for Video Calls** between and within regions (**System > Region Information > Region**) is set to a suitable upper limit for your system, for example 6000 kbps.



   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.)

   Note: Your secure profiles must set **Device Security Mode** to *Encrypted* because the Expressway does not allow unencrypted TLS connections. When **Device Security Mode** is set to *Authenticated*, Unified CM only offers the NULL-SHA cipher suite, which the Expressway rejects.



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, page 25

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. [Recommended] Disable automated intrusion protection on the Expressway-C and configure it on Expressway-E.

   From X8.9, this feature is enabled by default on new installations. See Expressway Automated Intrusion Protection, page 53.
3. Set **Unified Communications mode** to *Mobile and Remote Access*.
4. Configure the Unified CM, IM and Presence Service, and Cisco Unity Connection servers on the Expressway-C.
5. Configure the domains on the Expressway-C for which services are to be routed to Unified CM.
6. [Optional] Create additional deployments and associate domains and UC services with them.
7. Install appropriate server certificates and trusted CA certificates.
8. Configure a Unified Communications traversal zone connection between the Expressway-E and the Expressway-C.
9. If required, configure the HTTP server allow list for any web services inside the enterprise that need to be accessed from remote Jabber clients.
10. [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

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

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

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

Installing Expressway Security Certificates

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

1. Install a suitable server certificate on both the Expressway-C and the Expressway-E.
   - The certificate must include the **Client Authentication** extension. The system will not let you upload a server certificate without this extension when Unified Communications features are enabled.
   - The Expressway includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR:
     - Ensure that the CA that signs the request does not strip out the client authentication extension.
     - The generated CSR includes the client authentication request and any relevant subject alternate names for the Unified Communications features that have been enabled (see Server Certificate Requirements for Unified Communications, page 22).
   - 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 *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

Configuring Encrypted Expressway Traversal Zones

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

- 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 Expressway-C or a traversal server zone when selected on Expressway-E) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.
- Both Expressways must trust each other's server certificate. As each Expressway acts both as 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.
Authentication section		
Authentication policy	*Do not check credentials*	*Do not check credentials*
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

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 CA-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 X8.5.3 Release Notes* have the details of the workarounds.

Expressway Certificates

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

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

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

Note:

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

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

Expressway-C server certificate requirements

The Expressway-C server certificate 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.

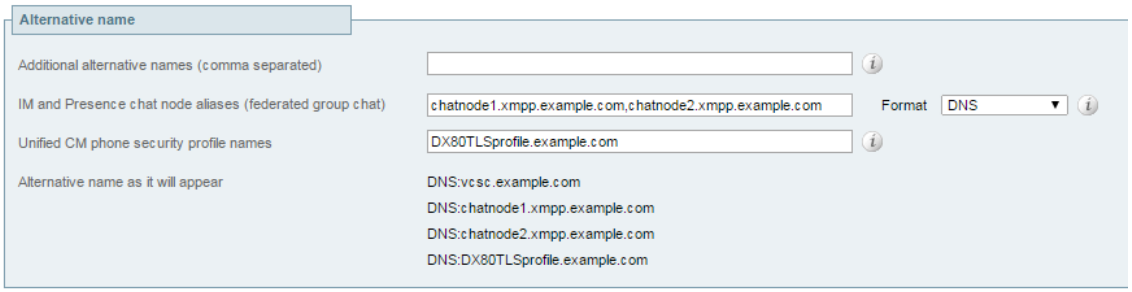
Having the secure phone profiles as alternative names means that Unified CM can communicate via TLS with the Expressway-C when it is forwarding messages from devices that use those profiles.

- **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 4 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 alternative names (SAN):

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

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

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

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

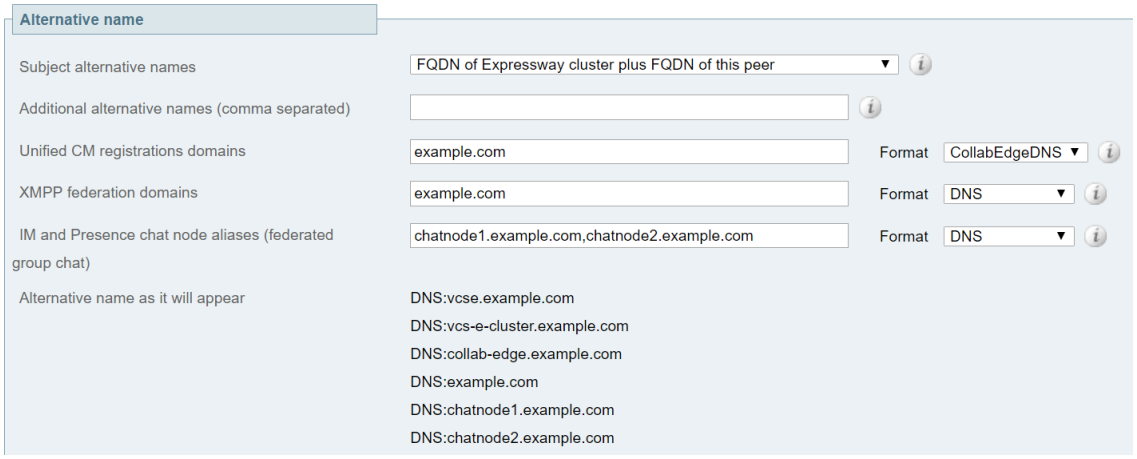
- **XMPP federation domains**: the domains used for point-to-point XMPP federation. These are configured on the IM&P servers and should also be configured on the Expressway-C as domains for XMPP federation.

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

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

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

Figure 5 Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator



See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

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

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

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

For information about how to do this, see:

- Configuring a Secure Traversal Zone Connection for Unified Communications, page 20 (if your system does not already have a secure traversal zone in place)
- Server Certificate Requirements for Unified Communications, page 22

If you want to use XMPP federation, the IM&P servers must be discovered on the Expressway-C. So that all relevant information is 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

Make sure that the following basic system settings are configured on Expressway:

1. **System host name** and **Domain name** are specified (**System > DNS**).
2. Local DNS servers are specified (**System > DNS**).
3. 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.

[Recommended] Disabling Automated Intrusion Protection on Expressway-C

If your Expressway-C is newly installed with X8.9, the automated intrusion protection service is running by default. This could prevent your deployment working properly, so we recommend you disable it on the Expressway-C as follows:

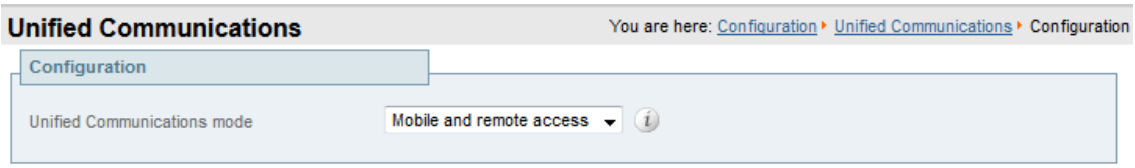
1. Go to **System > Administration**.
2. Switch **Automated protection service** to *Off*.
3. Click **Save**.

See Automated Intrusion Protection, page 1.

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**.



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

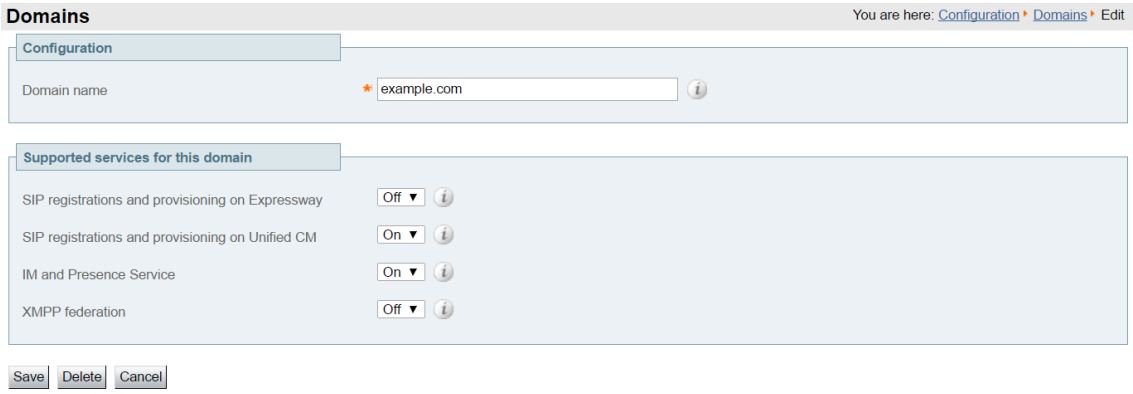
You must configure the domains for which registration, call control, provisioning, messaging and presence services are to be routed to Unified CM.

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 Expressway**: the Expressway is authoritative for this SIP domain. The Expressway acts as a SIP registrar for the domain, and accepts registration requests for any SIP endpoints attempting to register with an alias that includes this domain.
   - **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. For example, the same domain may be used by endpoints such as Jabber or EX Series devices that require line-side Unified Communications support, and by other endpoints such as third-party SIP or H.323 devices that require Expressway support. (In this scenario, the signaling messages sent from the endpoint indicate whether line-side unified communications or Expressway support is required.)

   Note that these settings are not entirely independent. You cannot disable **SIP registration and provisioning on Unified CM** 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 on Unified CM is ignored and the Expressway-C behaves as though it was *On*.



Enabling Shared Line / Multiple Lines for MRA Endpoints

Requires Unified CM 11.5(1)SU3 or later.

If you want MRA endpoints to be able to register multiple lines, or to share lines with other endpoints, then you must enable SIP Path headers on the Expressway-C. Due to a known issue in Unified CM 11.5(1)SU2, only enable SIP Path headers if you are running Unified CM version 11.5(1)SU3 or later (CDETS CSCvd84831 refers).

The default behavior is for the Expressway-C to rewrite the Contact header in REGISTER messages. When you turn SIP Path headers on, the Expressway-C does not rewrite the Contact header, but adds its address into the Path header instead.

1. On the Expressway-C, go to **Configuration > Unified Communications > Configuration**.
2. Change **SIP Path headers** to *On*.

3. Click **Save**.

   The Expressway-C puts its address in the Path headers of registrations from now on, and preserves the Contact header.
4. Refresh your Unified CM servers (**Configuration > Unified Communications > Unified CM servers**, click **Refresh servers**).

Note: This feature is disabled by default, because it impacts some features on earlier versions of Unified CM.

If you are using a Unified CM version before 11.5(1)SU3, and you enable SIP Path headers on Expressway-C, the following Unified CM features will *report the MRA devices' IP addresses instead of the Expressway's IP address*:

- Device Mobility
- Real-Time Monitoring Tool (RTMT)
- Cisco Emergency Responder (CER)

Other features may also be affected by this change. The devices' IP addresses are not useful for determining their location, as they are typically from reserved private ranges and could overlap with your organization's internal range.

Discover 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?, page 31

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

Trust 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**).

Discover 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 must enter an FQDN when **TLS verify mode** is *On*.
   c. Enter the **Username** and **Password** of an account that can access this server.

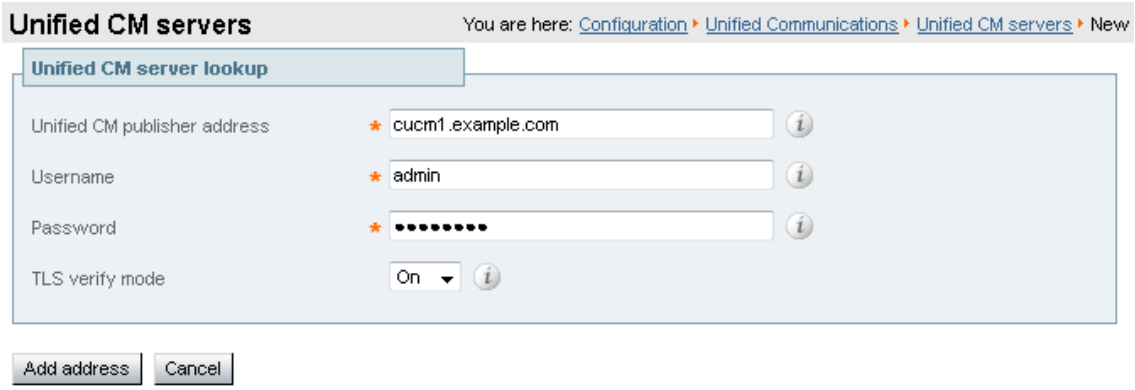
      Note: These credentials are stored permanently in the Expressway database. The corresponding Unified CM user must have the *Standard AXL API Access* role.
   d. [Recommended] Leave **TLS verify mode** switched *On* to ensure Expressway verifies the node's certificates.

      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.

Discover 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**.

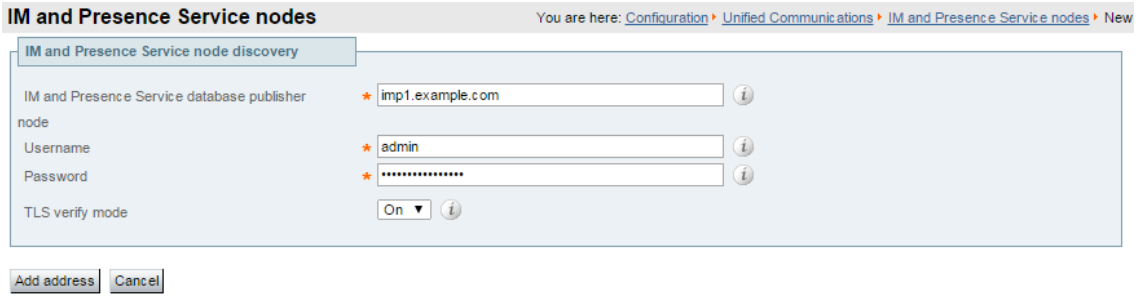
      You must enter an FQDN when **TLS verify mode** is *On*.
   c. Enter the **Username** and **Password** of an account that can access this server.

      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.

Discover 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 must enter an 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

About the HTTP Server Allow List on Expressway-C

Expressway-C automatically adds rules to allow external clients to access the Unified Communications nodes you discovered during MRA configuration. These include Unified CM nodes (that are running the CallManager and TFTP service), IM and Presence Service nodes, and Cisco Unity Connection nodes.

You can see the rules on **Configuration > Unified Communications > HTTP server allow list > Automatically added rules**.

Note: You cannot delete auto-added rules from the allow list.

You can manually add rules to the allow list if clients from outside need to access other web services inside the enterprise. For example, these services may require you to configure the allow list.

- Jabber Update Server
- Directory Photo Host
- Advanced File Transfer (AFT)
- Problem Report Tool server

AFT feature

For the AFT feature to work across Expressway, make sure that *all* Unified CM IM and Presence Service nodes are on the allow list, whether manually or automatically added.

Automatically Added Rules

Expressway automatically edits the HTTP allow list when you discover or refresh Unified Communications nodes. This page shows the discovered nodes, and the rules that apply to those nodes.

The first list is Discovered nodes, and contains all the nodes currently known to this Expressway-C. For each node, the list contains the node's address, its type, and the address of its publisher.

The second list is the rules that have been added for you, to control client access to the different types of Unified Communications nodes. For each type of node in your MRA configuration, you'll see one or more rules in this list. They are shown in the same format as the editable rules, but you cannot modify these rules.

Table 2 Properties of Automatically Added Allow List Rules

Column	Description
Type	This rule affects all nodes of the listed type: ■ Unified CM servers: Cisco Unified Communications Manager nodes ■ IM and Presence Service nodes: Cisco Unified Communications Manager IM and Presence Service nodes ■ Unity Connection servers: Cisco Unity Connection nodes ■ TFTP: TFTP nodes
Protocol	The protocol on which the rule allows clients to communicate with these types of nodes.

Table 2 Properties of Automatically Added Allow List Rules (continued)

Column	Description
Ports	The ports on which the rule allows clients to communicate with these types of nodes.
Match type	*Exact* or *Prefix*. Depends on the nature of the service the clients access with the help of this rule.
Path	The path to the resource that clients access with the help of this rule. This may not be present, or may only be a partial match of the actual resource, if the rule allows *Prefix* match.
Methods	The HTTP methods that will be allowed through by this rule, eg. `GET`.

Edit the HTTP Allow List

1. Go to **Configuration > Unified Communications > HTTP allow list > Editable rules** to view, create, modify, or delete HTTP allow list rules.

   The page has two areas; one for controlling the default HTTP methods, and the other showing the editable rules.

2. [Optional] Use the checkboxes to modify the set of default HTTP methods, then click **Save**.

   You can override the defaults while you're editing individual rules. If you want to be as secure as possible, clear all methods from the default set and specify methods on a per rule basis.

   Note: When you change the default methods, all rules that you previously created with the default methods will use the new defaults.

3. [Recommended] Delete any rules you don't need by checking the boxes in the left column, then clicking **Delete**.
4. Click **New** to create a rule.

5. Configure the rule to your requirements. Here is some advice for each of the fields:

Table 3 Properties of Manually Added Allow List Rules

Column	Description
Description	Enter a meaningful description for this rule, to help you recognize its purpose.
Url	Specify a URL that MRA clients are allowed to access. For example, to allow access to `https://www.example.com:8080/resource/path` just type it in exactly like that. a. The protocol the clients are using to access the host must be `http://` or `https://` b. Specify a port when using a non-default port eg. `:8080` (Default ports are 80 (http) and 443 (https)) c. Specify the path to limit the rule scope (more secure), eg. `/resource/path` If you select *Prefix match* for this rule, you can use a partial path or omit the path. Be aware that this could be a security risk if the target resources are not resilient to malformed URLs.
Allowed methods	Select *Use defaults* or *Choose methods*. If you choose specific HTTP methods for this rule, they will override the defaults you chose for all rules.
Match type	Select *Exact match* or *Prefix match*. Your decision here depends on your environment. It is more secure to use exact matches, but you may need more rules. It is more convenient to use prefix matches, but there is some risk of unintentionally exposing server resources.
Deployment	If you are using multiple deployments for your MRA environment, you also need to choose which deployment uses the new rule. You won't see this field unless you have more than one deployment.

6. Click **Create Entry** to save the rule and return to the editable allow list.
7. [Optional] Click **View/Edit** to change the rule.

Upload Rules to the HTTP Allow List

1. Go to **Configuration > Unified Communications > HTTP allow list > Upload rules**.
2. Browse to and select the CSV file containing your rule definitions.
   See Allow List Rules File Reference, page 60.
3. Click **Upload**.
   The Expressway responds with a success message and displays the **Editable rules** page.

Setting Up the Expressway-E

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

Configuring DNS and NTP Settings

Make sure that the following basic system settings are configured on Expressway:

1. **System host name** and **Domain name** are specified (**System > DNS**).
2. Public DNS servers are specified (**System > DNS**).
3. 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.

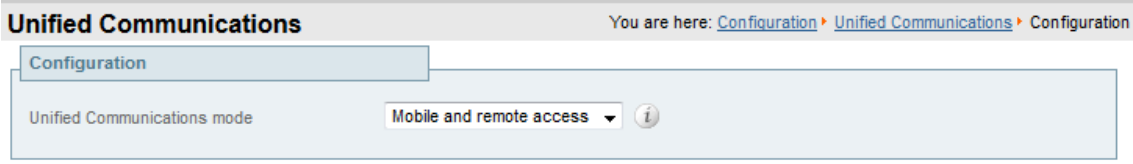
Note: The combination of <**System host name**>.<**Domain name**> is the FQDN of this Expressway-E. Ensure that this FQDN is resolvable in public DNS.

If you have a cluster of Expressway-Es, make sure 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**.



Using Deployments to Partition Unified Communications Services

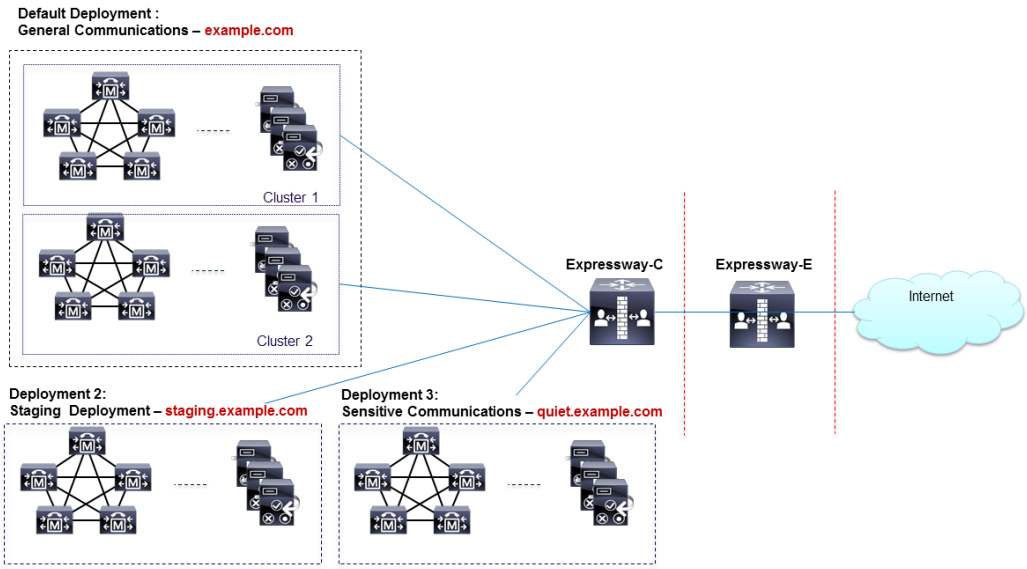
A deployment is an abstract boundary used to enclose a domain and one or more Unified Communications service providers (such as Unified CM, Cisco Unity Connection, and IM and Presence Service nodes). The purpose of multiple deployments is to partition the Unified Communications services available to Mobile and Remote Access (MRA) users. So different subsets of MRA users can access different sets of services over the same Expressway pair.

We recommend that you do not exceed ten deployments.

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, as a third set.

Figure 6 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 through Mobile and Remote Access, create as many deployments as you need. Associate a different domain with each one, 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 Discover Unified Communications Servers and Services, page 28.
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 that access 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

Note: Jabber clients are the *only* endpoints supported for SSO through Mobile and Remote Access (MRA).

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

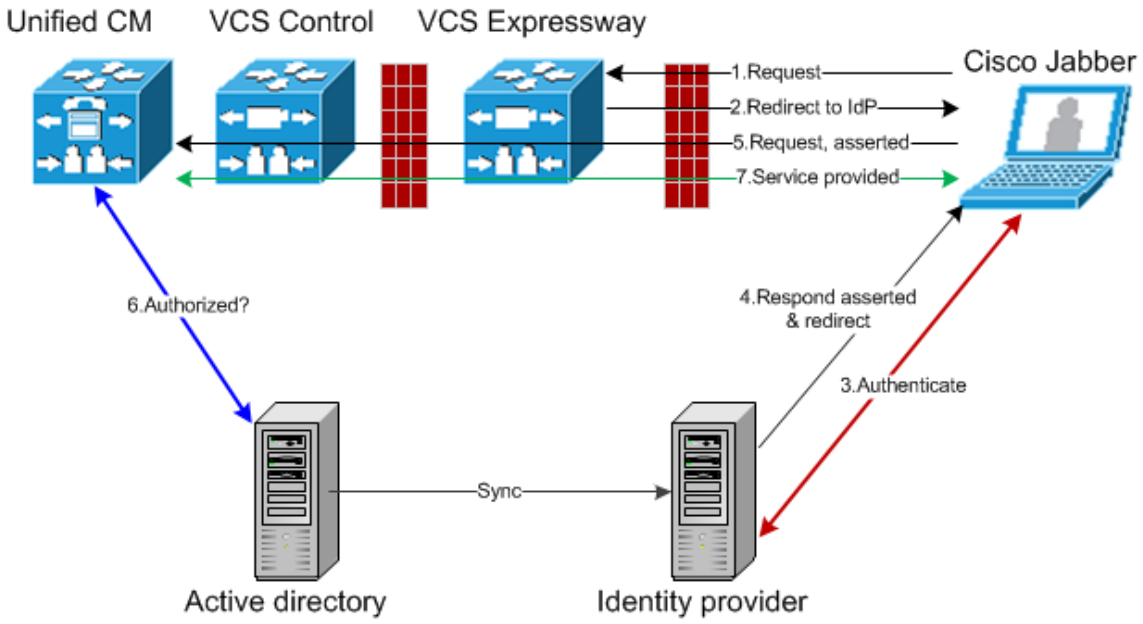
How it works

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 7 Remote single sign-on for on-premises UC services



Understanding the SSO options for MRA

The Expressway options for SSO over the edge (**Configuration > Unified Communications > Configuration** page) are:

- *Exclusive*: This is the most secure option. Requires authentication through the IdP, which is the only permitted authentication agent. Authentication can be certificate-based, two-factor, or username and password. This option only allows Jabber clients through MRA. The clients must be in SSO authentication mode.
- *On*: Allows authentication through the IdP or the Expressway pair. The Expressway supports username and password authentication only. If the IdP is the authentication agent, certificate-based or two-factor authentication is also available. This option allows Jabber clients in SSO authentication mode or basic authentication mode through MRA. And (non-SSO) endpoints, including IP phones and TelePresence devices.
  - Jabber clients in SSO authentication mode first try to authenticate at the IdP. If that fails, they attempt to authenticate through the Expressway.
  - Jabber clients in basic authentication mode use username and password authentication.
  - Other endpoints and IP phones also use username and password authentication.
- *Off*: Requires authentication through the Expressway, which is the only permitted authentication agent. Username and password is the only supported authentication method. Endpoints, IP phones, and Jabber clients in basic authentication mode are allowed through MRA.

Note: When the Expressway is used as the authentication agent, the authentication request is proxied through the Expressway pair, which returns the authorization token.

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 MRA mode and has discovered the required Unified CM resources.
- The required Unified CM resources are in the HTTP 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 Unified CM:

- Users who are associated with non-SSO MRA clients or endpoints, have their credentials stored in Unified CM. Or Unified CM is configured for LDAP authentication.

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 through 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 (primary) Expressway-C; ensure that it includes the externally resolvable address of the (primary) 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 primary 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.

You also need to add a claim rule, for each relying party trust, that sets the uid attribute of the SAML response to the AD attribute value that users are authenticating with.

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)
- Add a claim rule to send identity as `uid` attribute

To sign the whole response:

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

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

To add a claim rule for each Relying Party Trust:

1. Open the Edit Claims Rule dialog, and create a new claim rule that sends AD attributes as claims
2. Select the AD attribute to match the one that identify the SSO users to the internal systems, typically email or SAMAccountName
3. Enter `uid` as the Outgoing Claim Type

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* or *Exclusive*.

   Select the same value on the Expressway-C and Expressway-E.

   - *Exclusive*: This is the most secure option. Requires authentication through the IdP, which is the only permitted authentication agent. Authentication can be certificate-based, two-factor, or username and password. This option only allows Jabber clients through MRA. The clients must be in SSO authentication mode.
   - *On*: Allows authentication through the IdP or the Expressway pair. The Expressway supports username and password authentication only. If the IdP is the authentication agent, certificate-based or two-factor authentication is also available. This option allows Jabber clients in SSO authentication mode or basic authentication mode through MRA. And (non-SSO) endpoints, including IP phones and TelePresence devices.
     - Jabber clients in SSO authentication mode first try to authenticate at the IdP. If that fails, they attempt to authenticate through the Expressway.
     - Jabber clients in basic authentication mode use username and password authentication.
     - Other endpoints and IP phones also use username and password authentication.
   - *Off*: Requires authentication through the Expressway, which is the only permitted authentication agent. Username and password is the only supported authentication method. Endpoints, IP phones, and Jabber clients in basic authentication mode are allowed through MRA.
3. Click **Save**.

Extend SIP Authorization Token Lifetime

[Optional, when **Single Sign-on Support** is *On*]

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* or *Exclusive*.

   Select the same value on the Expressway-C and Expressway-E.

   - *Exclusive*: This is the most secure option. Requires authentication through the IdP, which is the only permitted authentication agent. Authentication can be certificate-based, two-factor, or username and password. This option only allows Jabber clients through MRA. The clients must be in SSO authentication mode.
   - *On*: Allows authentication through the IdP or the Expressway pair. The Expressway supports username and password authentication only. If the IdP is the authentication agent, certificate-based or two-factor authentication is also available. This option allows Jabber clients in SSO authentication mode or basic authentication mode through MRA. And (non-SSO) endpoints, including IP phones and TelePresence devices.
     - Jabber clients in SSO authentication mode first try to authenticate at the IdP. If that fails, they attempt to authenticate through the Expressway.
     - Jabber clients in basic authentication mode use username and password authentication.
     - Other endpoints and IP phones also use username and password authentication.
   - *Off*: Requires authentication through the Expressway, which is the only permitted authentication agent. Username and password is the only supported authentication method. Endpoints, IP phones, and Jabber clients in basic authentication mode are allowed through MRA.
3. Click **Save**.

Check for Internal SSO Availability

[Optional, when **Single Sign-on Support** is *On*]

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*.

Allow Jabber iOS clients to use embedded Safari browser

[Optional, when **Single Sign-on Support** is *On*]

Choose whether to allow SSO authentication for Jabber iOS clients through the Apple Safari browser, rather than through the Jabber default browser. The default for this setting is *No*.

This option applies if you use single sign-on (SSO) and have Cisco Jabber iOS endpoints that access Unified Communications services from outside the network. In this case, by default the identity provider's authentication page is displayed in an embedded web browser (not the Safari browser) on the iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices. From X8.9, you can optionally configure Expressway-E to allow Jabber on iOS devices to use the native Safari browser. Because the Safari browser *is* able to access the device trust store, you can now enable password-less authentication or two-factor authentication in your SSO deployment.

Caveat

A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the identity provider authentication completes, uses a custom URL scheme that invokes a custom protocol handler. It's possible that another application other than Jabber could intercept the scheme and gain control from iOS. In that case, the application would have access to the OAuth token in the URL.

If you are confident that your iOS devices will not have other applications that register the Jabber custom URL scheme, for example because all mobile devices are managed, then it's safe to enable the option. If you are concerned about the possibility of another app intercepting the custom Jabber URL, then do **not** enable the embedded Safari browser.

Note: To ensure a consistent user experience for on premise and over the edge access, if you enable this option then also enable the corresponding option in Unified CM. The relevant Unified CM setting is **Use Native Browser** in **System > Enterprise Parameters > SSO Configuration**.

Dial via Office-Reverse through MRA

Your mobile workers need the same high quality, security and reliability that they experience when placing calls in the office. You can assure them of just that when you enable the Dial via Office-Reverse (DVO-R) feature and they are using Cisco Jabber on a dual-mode mobile device. DVO-R routes Cisco Jabber calls through the enterprise automatically.

DVO-R handles call signaling and voice media separately. All call signaling, including the signaling for Mobile and Remote Access on Expressway, traverses the IP connection between the client and Cisco Unified Communications Manager. Voice media traverses the cellular interface and hairpins at the enterprise Public Switched Telephone Network (PSTN) gateway.

Moving audio to the cellular interface ensures high-quality calls and securely maintained audio even when the IP connection is lost.

You can configure DVO-R so that, when a user makes a call, the return call from Cisco Unified Communications Manager goes to either:

- The user’s Mobile Identity (mobile number).
- An Alternate Number for the user (such as a hotel room).

This feature is dependent on the following versions of related systems:

- Cisco Unified Communications Manager 11.0(1) or later
- Cisco Jabber 11.1 or later

Dial via Office-Reverse through MRA

Figure 8 DVO-R calling

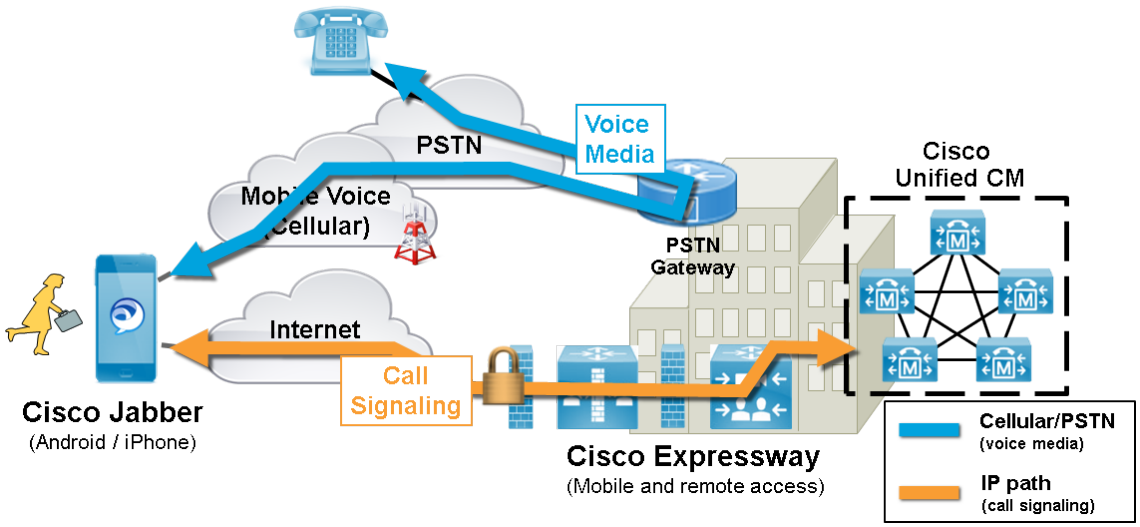


Figure 9 DVO-R using Mobility Identity

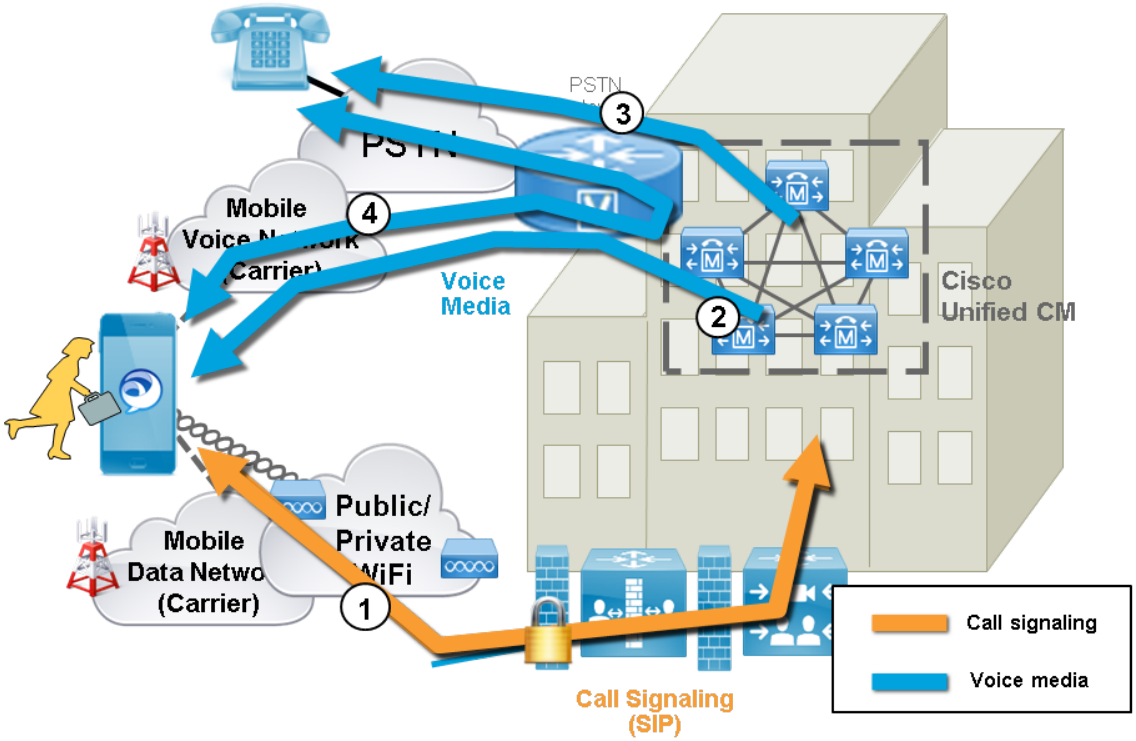
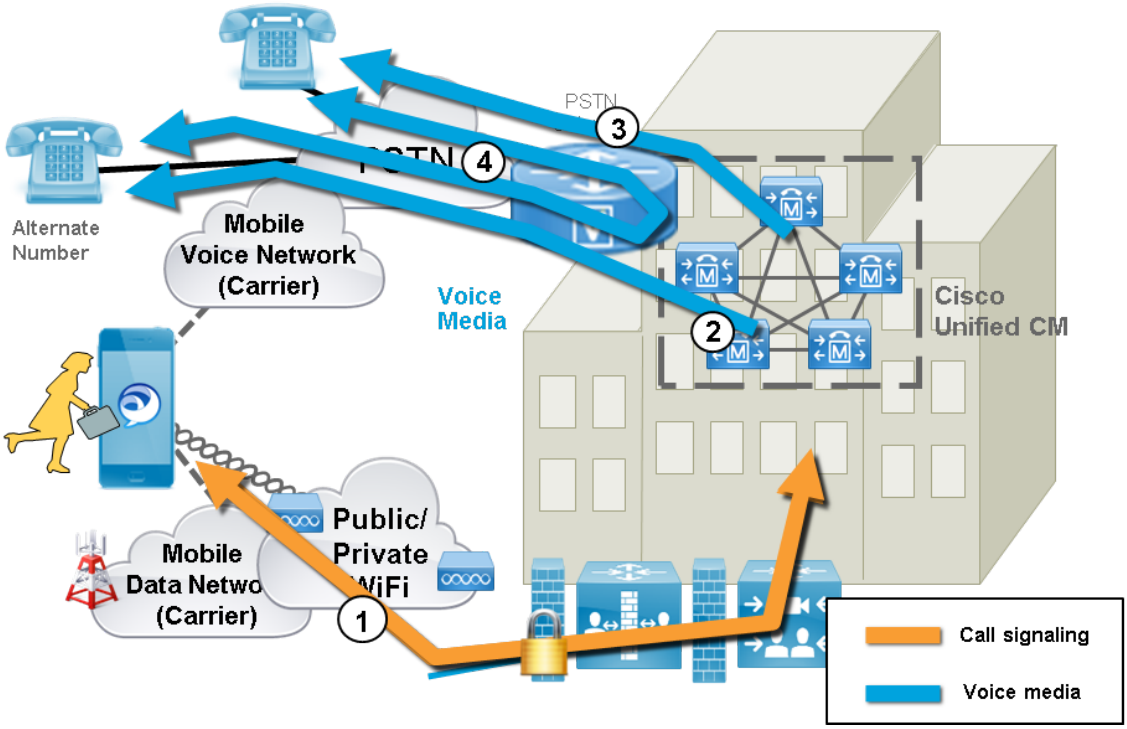


Figure 10 DVO-R using Alternate Number



How DVO-R works with Expressway Mobile and Remote Access

1. When you dial a number, a signal is sent to Cisco Unified Communications Manager over the IP path (WLAN or mobile network). See stage 1 of Figure 2 or Figure 3.
2. Cisco Unified Communications Manager calls your mobile number or the Alternate Number you set (see stage 2 of Figure 2 or Figure 3.)
3. When you answer, Cisco Unified Communications Manager extends the call to the number you dialed and you hear ring back (see stage 3 of Figure 2 or Figure 3).
4. When the person answers, the ongoing call is hairpinned at the enterprise PSTN gateway.

- If you made the call using a Mobile Identity, your call is anchored at the enterprise gateway. The call is active on your mobile and desk phone, so you can switch between the two (see stage 4 of Figure 2).
- If you specified an Alternate Number, your ongoing call is not anchored and you cannot pick up on your desk phone (see stage 4 of Figure 3).

Note the following:

- You can use Dual Tone Multi Frequency-based (DTMF) mid-call features (for example *81 for hold) on anchored calls if there is out-of-band DTMF relay between the PSTN gateway and Cisco Unified Communications Manager. You cannot utilize mid-call features when using an Alternate Number.
- To prevent the callback leg from Cisco Unified Communications Manager routing to your voicemail – thus stopping the voicemail call going through to the person you are dialing – Cisco recommends that you set your DVO-R voicemail policy to 'user controlled'. This ensures you must generate a DTMF tone by pressing any key on the keypad before your call can proceed.

Note: Although this feature now works for users calling over Mobile and Remote Access, there is no configuration on the Expressway. There is some configuration required on the Unified CM nodes and Cisco Jabber clients.

Configuration checklist for DVO-R

1. Set up Cisco Unified Communications Manager to support DVO-R.
2. Set up DVO-R for each device.
3. Set up user-controlled voicemail avoidance.
4. Add Remote Destination (optional).
5. Configure Cisco Jabber client settings.

See *Configuring Dial via Office-Reverse to Work with Mobile and Remote Access* at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-configuration-examples-list.html for more information.

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 Internal Infrastructure and Endpoints

Purpose	Protocol	Expressway-C (source)	Internal Device Port/Range
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/HTTPS (configuration file retrieval)	TCP	Ephemeral port	(Unified CM) HTTP 6970 **Or** HTTPS 6972 if you have Cisco Jabber 11.x or later with Unified CM 11.x or later
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 (Media recipient eg. endpoint)
SIP signaling	TCP	25000 to 29999	5060 (Unified CM)
Secure SIP signaling	TLS	25000 to 29999	5061 (Unified CM)

* 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

Maintenance Mode on the Expressway

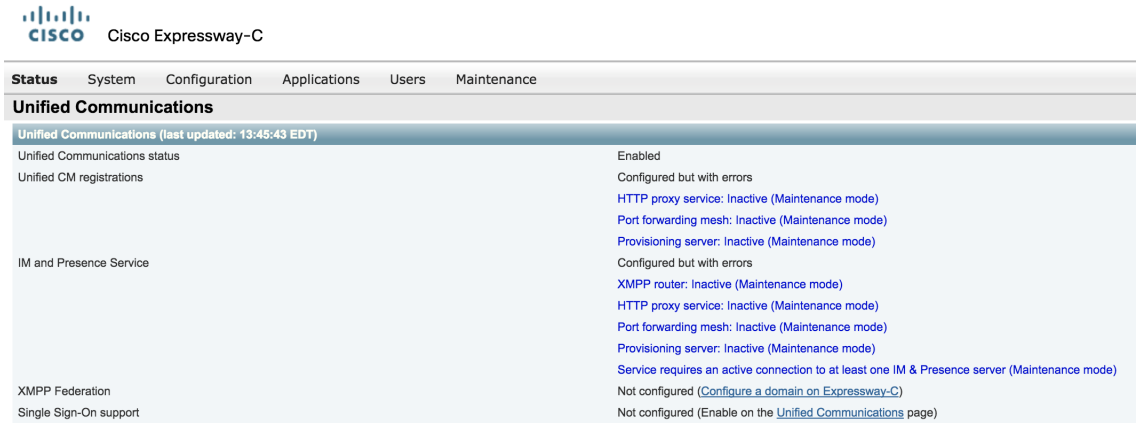
Maintenance mode on the Expressway has been enhanced so that you can bring an MRA system down in a managed way.

When you engage maintenance mode, the Expressway stops accepting new calls or proxy (MRA) traffic. Existing calls and chat sessions are not affected.

As users end their sessions normally, the system comes to a point when it is not processing any traffic of a certain type, and then it shuts that service down.

If users try to make new calls or start new chat sessions while the Expressway is in maintenance mode, the clients will receive a service unavailable response, and they might then choose to use another peer (if they are capable). This fail-over behavior depends on the client, but restarting the client should resolve any connection issues if there are active peers in the cluster.

The Unified Communications status pages also show (Maintenance Mode) in any places where MRA services are affected.



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.

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: 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

- 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 Endpoint Features when Using Mobile and Remote Access

See Unsupported Endpoint Features, page 13

Expressway Limitations and Unsupported Features when Using Mobile and Remote Access

- The Expressway cannot be used for Jabber Guest when it is used for Mobile and Remote Access (MRA).
- The Expressway-C used for MRA cannot also be used for Microsoft gateway service. Microsoft gateway service requires a dedicated Expressway-C.
- MRA is not supported in IPv6 only mode.
- 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, and we currently recommend that you do not exceed 50 domains.
- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM (the same limit as Small / Medium VM servers).
- Not all contact center features are supported by Expressway when connected through MRA.

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 primary 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

From X8.9 onwards, automated intrusion protection is enabled, by default, for the following categories:

- http-ce-auth
- http-ce-intrusion
- sshpfwd-auth
- sshpfwd-intrusion
- xmpp-intrusion

This change affects new systems. Upgraded systems keep their existing protection configuration.

On Expressway-C:

The Expressway-C receives a lot of inbound traffic from Unified CM and from the Expressway-E when it is used for Mobile and Remote Access.

If you want to use automated protection on the Expressway-C, you should add exemptions for all hosts that use the automatically created neighbor zones and the Unified Communications secure traversal zone. The Expressway does not automatically create exemptions for discovered Unified CM or related nodes.

On Expressway-E:

You should 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.

Partial Support for Cisco Jabber SDK

You can use the following supported Cisco Jabber SDK features over MRA:

- Sign in/ sign out
- Register phone services
- Make or receive audio/ video calls
- Hold and resume, mute/ unmute, and call transfer

For more information, see the Getting Started Guide for Cisco Jabber SDK.

Appendix 1: Troubleshooting

General 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.

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
- _cisco-uds._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 taking place to or from devices registered with the Expressway, or that are 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.

The same set of call status information is also shown on the **Calls by registration** page (accessed via the **Registration details** page).

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 the Expressway-C, a Unified CM remote session has three components (as it uses the B2BUA to enforce media encryption). One of the Expressway components routes 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 the Expressway-E, there is one component and that routes the call through the **CollaborationEdgeZone**.

If both endpoints are outside of the enterprise (that is, off premises), you will see this treated as two separate calls.

Rich media sessions

If your system has a rich media session key installed and thus supports 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 following items:

- Number of nodes within a Unified CM cluster
- 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

Modifications to the Expressway's server certificate or trusted CA certificates need a Expressway restart for the changes to 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).

CiscoSSL 5.4.3 Rejects Diffie-Hellman Keys with Fewer than 1024 Bits

If you are running version 9.x, or earlier, of Unified CM or Unified CM IM&P, with Expressway version X8.7.2 or later, then the SSL handshake between the two systems will fail by default.

The symptom of this is that all MRA endpoints fail to register or make calls after you upgrade to Expressway X8.7.2 or later.

The cause of this issue is an upgrade of the CiscoSSL component to 5.4.3 or later. This version rejects the default (768 bit) key provided by Unified CM when using D-H key exchange.

We recommend that you patch the Unified CM and IM and Presence Service nodes with the latest Service Update to avoid this issue.

Cisco Jabber Sign In Issues

Jabber popup warns about invalid certificate when connecting from outside the network

This is a symptom of an incorrectly configured server certificate on the Expressway-E. The certificate could be self-signed, or it may not have the external DNS domain of your organization listed as a subject alternative name (SAN).

This is expected behavior from Jabber. We recommend that you install a certificate issued by a CA that Jabber trusts, and that the certificate has the domains Jabber is using included in its list of SANs. See Server Certificate Requirements for Unified Communications, page 22.

Jabber Does Not Register for Phone Services

There is a case handling mismatch between the Expressway and the UDS (User Data Service) that prevents Jabber from registering for phone services if the supplied user ID does not match the case of the stored ID. Jabber still signs in but cannot use phone services.

Users can avoid this issue by signing in with the user ID exactly as it is stored in UDS.

Users can recover from this issue by signing out and resetting Jabber. See CSCux16696.

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.

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, page 50 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.

Invalid SAML Assertions

If clients fail to authenticate via SSO, one potential reason is that invalid assertions from the IDP are being rejected by the Expressway-C.

Check the logs for "Invalid SAML Response".

One example is when ADFS does not have a claim rule to send the users' IDs to the Expressway-C. In this case you will see "No uid Attribute in Assertion from IdP" in the log.

The Expressway is expecting the user ID to be asserted by a claim from ADFS that has the identity in an attribute called `uid`. You need to go into ADFS and set up a claim rule, on each relying party trust, to send the users' AD email addresses (or sAMAccountNames, depending on your deployment) as "uid" to each relying party.

"502 Next Hop Connection Failed" Messages

A 502 message on the Expressway-E indicates that the next hop failed (typically to the Expressway-C). Try the following steps:

1. Go to the **Status > Unified Communications** page on the Expressway-E. Did the Expressway-E report any issues?
2. If the status looks normal, click the **SSH tunnel status** link at the foot of the status page. If one or more tunnels to the Expressway-C node is down, that is probably causing the 502 error.

Allow List Rules File Reference

You can define rules using a CSV file. This topic provides a reference to acceptable data for each rule argument, and demonstrates the format of the CSV rules.

Table 4 Allow List Rule Arguments

Argument index	Parameter name	Required/Optional	Sample value
0	Url	Required	`protocol://host[:port][/path]` Where: ▪ protocol is `http` or `https` ▪ host may be a DNS name or IP address ▪ :port is optional, and may only be : followed by one number in the range 0-65535, eg. `:8443` If the port is not specified, then the Expressway uses the default port for the supplied protocol (80 or 443) ▪ /path is optional and must conform to HTTP specification
1	Deployment	Optional	Name of the deployment that uses this rule. Required when you have more than one deployment, otherwise supply an empty argument.
2	HttpMethods	Optional	Comma-delimited list of HTTP methods, optionally in double-quotes, eg. `"GET,PUT"`
3	MatchType	Optional	`exact` or `prefix`. Default is `prefix`
4	Description	Optional	Text description of the rule. Enclose with double quotes if there are spaces.

Example CSV file

```
Url,Deployment,HttpMethods,MatchType,Description
https://myServer1:8443/myPath1,myDomain1,GET,,"First Rule"
http://myServer2:8000/myPath2,myDomain200,"GET,PUT",exact,
https://myServer3:8080/myPath3,myDomain1,,prefix,"Third Rule"
https://myServer4/myPath4,myDomain1,,prefix,"Fourth Rule"
http://myServer5/myPath5,myDomain1,,prefix,"Fifth Rule"
```

- List the parameter names (as shown) in the first line of the file
- One rule per line, one line per rule
- Separate arguments with commas
- Correctly order the rule values as shown in the table above
- Enclose values that have spaces in them with double quotes

Allow List Tests File Reference

You can define tests using a CSV file. This topic provides a reference to acceptable data for each test argument, and demonstrates the format of the CSV tests.

Table 5 Allow List Test Arguments

Argument index	Parameter name	Required/Optional	Sample value
0	Url	Required	`protocol://host[:port][/path]` Where: ▪ protocol is `http` or `https` ▪ host may be a DNS name or IP address ▪ :port is optional, and may only be : followed by one number in the range 0-65535 ▪ /path is optional and must conform to HTTP specification
1	ExpectedResult	Required	`allow` or `block`. Specifies whether the test expects that the rules should allow or block the specified URL.
2	Deployment	Optional	Name of the deployment to test with this URL. If you omit this argument, the test will use the default deployment.
3	Description	Optional	Text description of the rule. Enclose with double quotes if there are spaces.
4	HttpMethod	Optional	Specify one HTTP method to test eg. `PUT`. Defaults to `GET` if not supplied.

Example CSV file

```
Url,ExpectedResult,Deployment,Description,HttpMethod
https://myServer1:8443/myPath1,block,"my deployment","a block test",GET
http://myServer2:8000/myPath2,allow,"my deployment","an allow test",PUT
https://myServer4/myPath4,allow,,,GET
http://myServer4/myPath4,block,,,POST
```

- List the parameter names (as shown) in the first line
- One test per line, one line per test
- Separate arguments with commas
- Correctly order the test values as shown in the table above
- Enclose values that have spaces in them with double quotes

Cisco Legal Information

Cisco Trademark