Mobile and Remote Access Through Cisco Expressway Deployment Guide (X14.2)

First Published: 2022-08-10

CONTENTS

CHAPTER 1

MRA Overview

About Mobile and Remote Access

Cisco Unified Communications Mobile and Remote Access (MRA) is part of the Cisco Collaboration Edge Architecture. MRA 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 outside the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The MRA solution provides the following functions:

- **Off-premises access**: a consistent experience outside the network for Jabber and EX/MX/SX Series clients

- **Security**: secure business-to-business communications

- **Cloud services**: enterprise grade flexibility and scalable solutions providing rich Cisco Webex integration and service provider offerings

- **Gateway and interoperability services**: media and signaling normalization, and support for nonstandard endpoints

Figure 1: Unified Communications: Mobile and Remote Access

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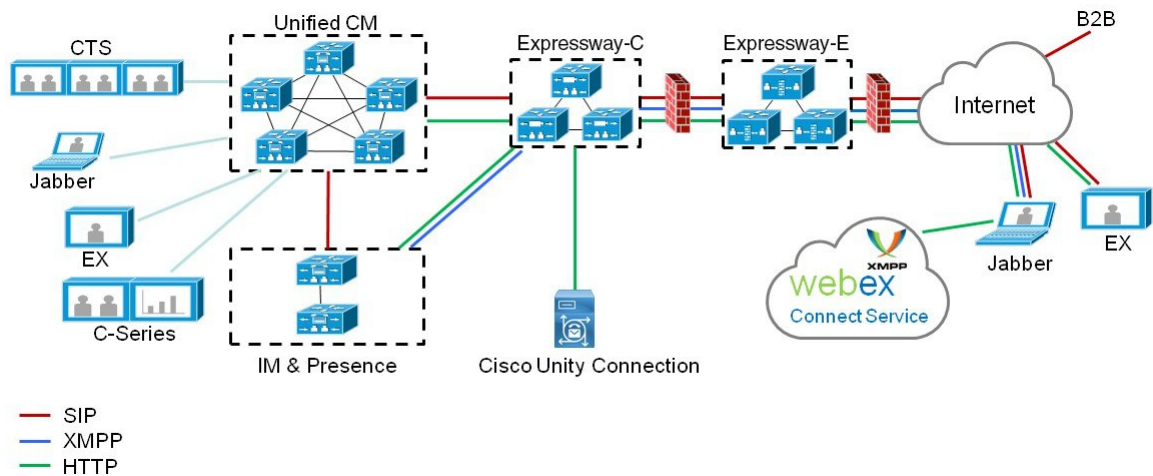
Note   Third-party SIP or H.323 devices can register to the Expressway-C and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.

Figure 2: Typical Call Flow - Signaling and Media Paths
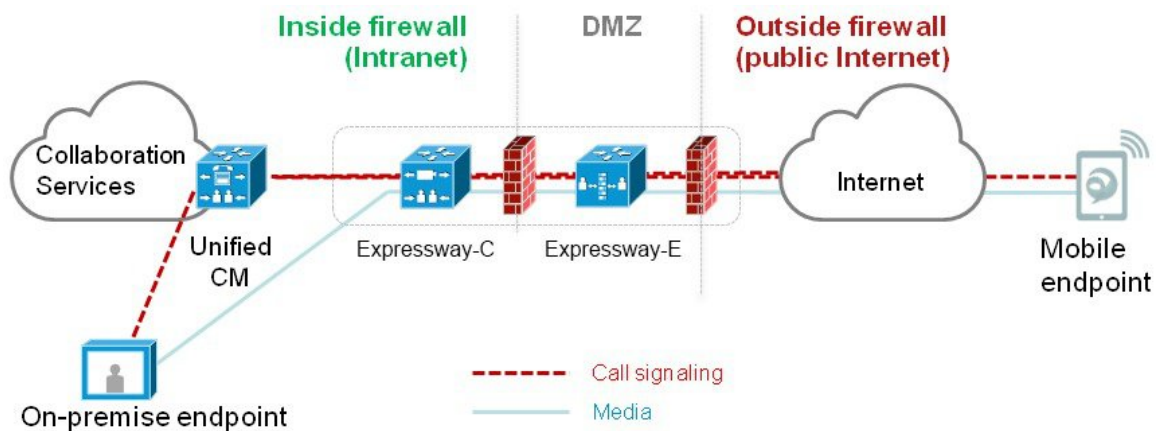
Unified CM provides call control for both mobile and on-premise endpoints. Signaling traverses, the Expressway solution between the mobile endpoint and Unified CM. Media traverses the Expressway solution, which relays the media between the endpoints directly. All media is encrypted between the Expressway-C and the mobile endpoint.

Core Components

Any MRA solution requires Expressway and Unified CM, with MRA-compatible soft clients and/or fixed endpoints. The solution can optionally include the IM and Presence Service and Unity Connection. This guide assumes that you have already set up the following:

- A basic Expressway-C and Expressway-E configuration, as specified in the Expressway Basic Configuration Deployment Guide (The document describes the networking options for deploying Expressway-E in the DMZ.)

- Unified CM and IM and Presence Service are configured as specified in the configuration and management guides for your version, at Cisco Unified Communications Manager Configuration Guides.

- If used, IM and Presence Service and/or Unity Connection are similarly configured as specified in the relevant Cisco Unified Communications Manager Configuration Guides.

Protocol Summary

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

Table 1: Protocols and Associated Services

Protocol	Security	Services
SIP	TLS	Session establishment – Register, Invite etc.
HTTPS	TLS	Logon, provisioning, configuration, directory, Visual Voicemail
Media	SRTP	Media - audio, video, content sharing
XMPP	TLS	Instant Messaging, Presence, Federation

Figure 3: Protocol Workload Summary
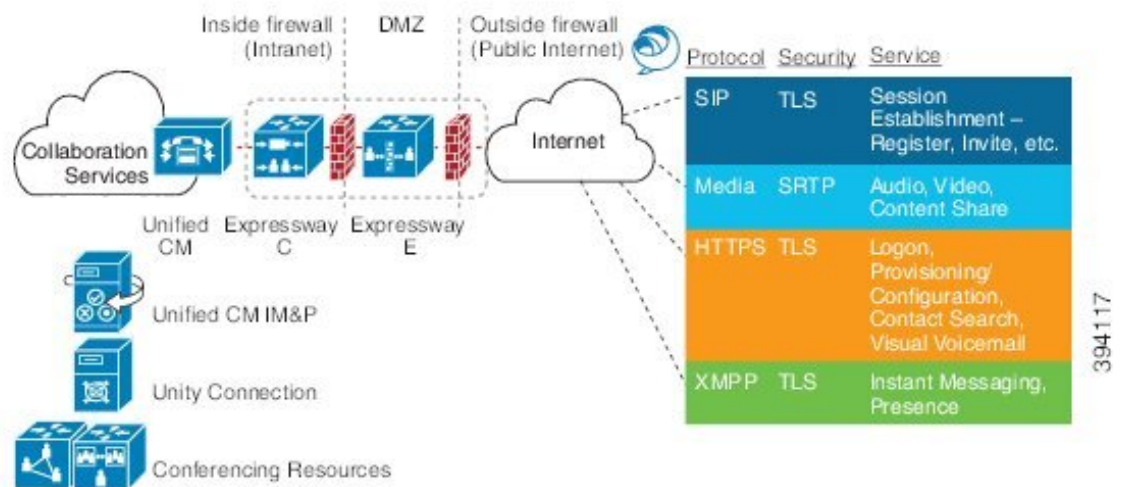
Jabber Client Connectivity Without VPN

The MRA solution supports a hybrid on-premises and cloud-based service model, providing a consistent experience inside and outside the enterprise. MRA provides a secure connection for Jabber application traffic and other devices with the required capabilities to communicate 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 Cisco Jabber Video for TelePresence (Jabber Video) does not work with MRA.

Deployment Scenarios

This section describes the supported deployment environments:

- Single network elements

- Single clustered network elements

- Multiple clustered network elements

- Hybrid deployment

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 4: Supported MRA Traversal Connections
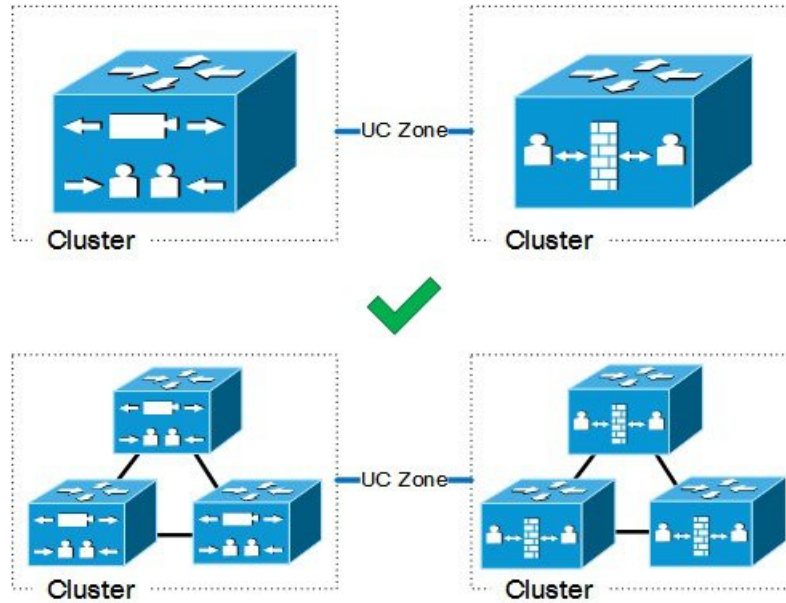
MRA with Standalone Network Elements

This scenario includes standalone (non-clustered) Unified CM, IM and Presence Service, Expressway-C, and Expressway-E servers.

Figure 5: Standalone Network Elements
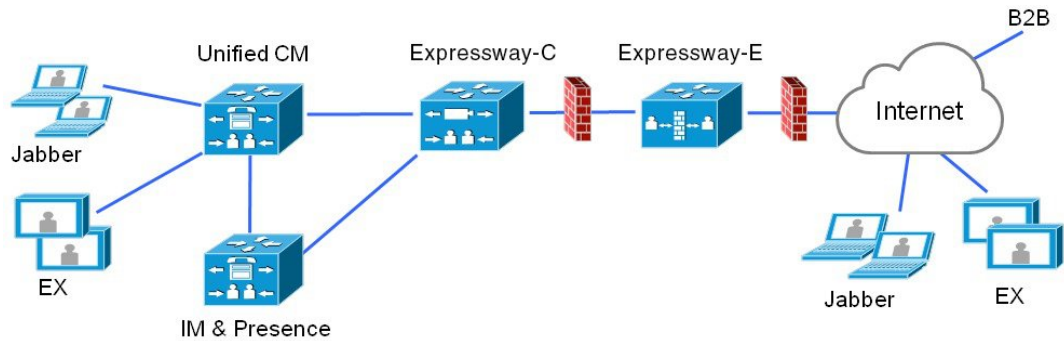
MRA with Clustered Network

In this scenario, each network element is clustered.

Figure 6: Single Clustered Network Elements
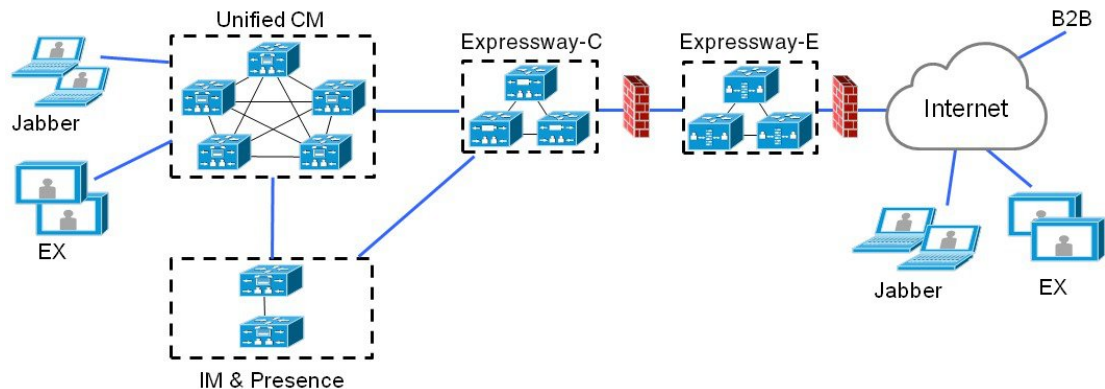
MRA with Multiple Clustered Networks

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

Figure 7: Multiple Clustered Network Elements
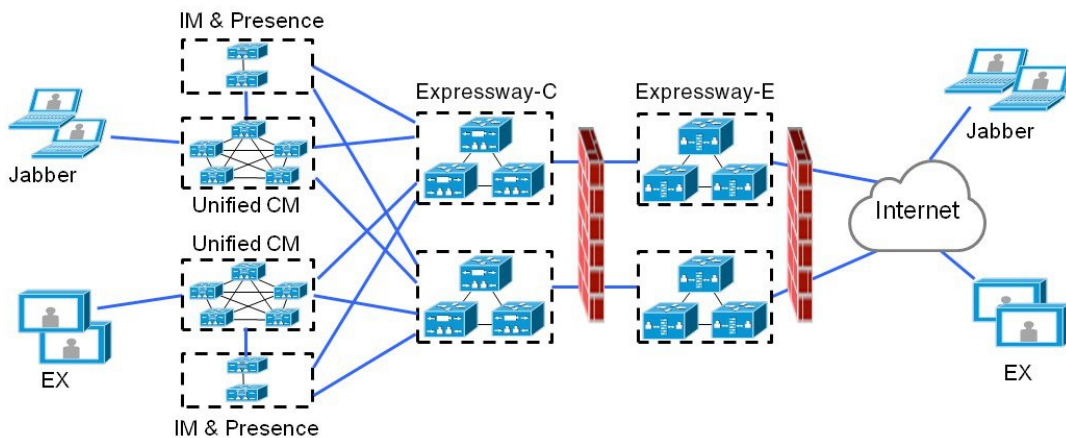
- Jabber clients can access their own cluster through any route.

- 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 peering must be set up between the IM and Presence Service clusters, and the Intercluster Sync Agent (ICSA) must be active.

Multiple Unified CM Clusters

If your MRA deployment includes multiple Unified CM clusters, configure Home Cluster Discovery for Unified CM. Expressway-C requires this configuration to direct MRA users to the correct home Unified CM cluster. Use either of the following configuration methods:

- Configure an Intercluster Lookup Service (ILS) network between your remote Unified CM clusters. ILS cluster discovery finds and connects your remote Unified CM clusters into an intercluster network, populating the Cluster View on each cluster. ILS is the preferred option for larger intercluster networks, and also if you also want to replicate your enterprise dial plan across all Unified CM clusters. However, note that MRA doesn't require dial plan replication to work.

- Configure each Unified CM cluster with a list of all the remote clusters under the Unified CM **Advanced Features** > **Cluster View** menu. This option does not allow for dial plan replication.

Unsupported Deployments

This topic highlights some deployments that are not supported over MRA.

VPN Links

MRA doesn't support VPN links between the Expressway-C and the Unified CM services / clusters.

Figure 8: VPN Links Unsupported
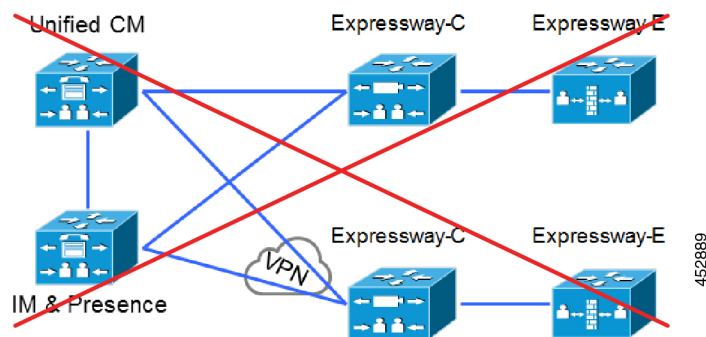
Traversal Zones Between VCS Series and Expressway Series

MRA doesn't support "Mixed" traversal connections. Even though it's possible to configure traversal zones between Cisco VCS and Cisco Expressway, MRA doesn't support them.

Explicitly, we don't support VCS Control traversal to Expressway-E, nor do we support Expressway-C traversal to VCS Expressway.

Figure 9: Mixed Traversal Zones
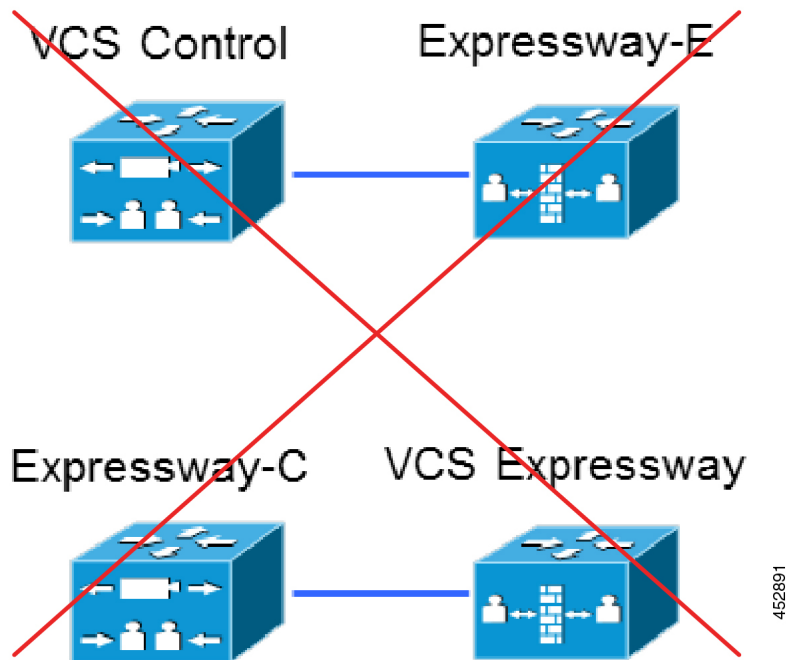
Unclustered or Many-to-One Traversal Connections

We don't support Unified Communications zones from one Expressway-C cluster to multiple unclustered Expressway-Es.

We also don't support multiple Unified Communications zones from one Expressway-C cluster to multiple Expressway-Es or Expressway-E clusters.

Figure 10: Unclustered or Many-to-One Traversal Connections
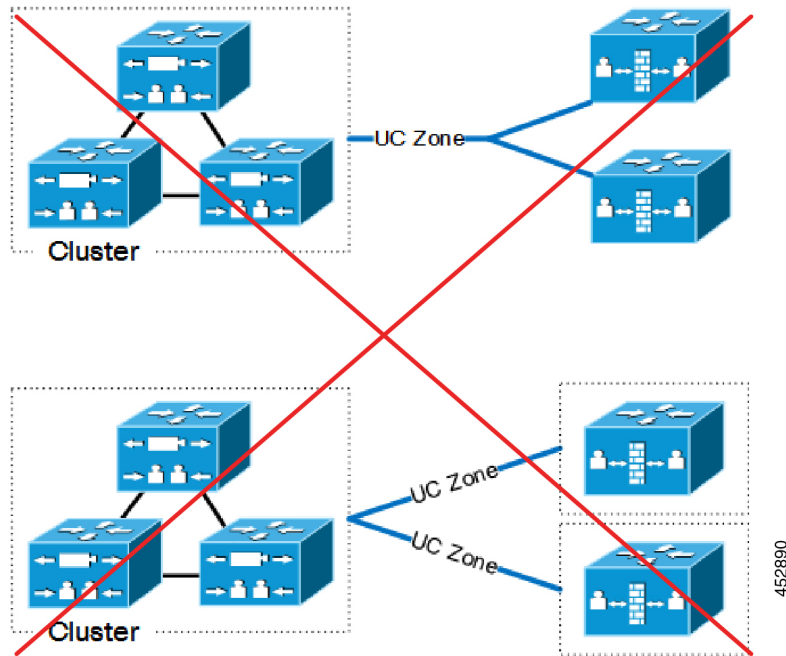
Nested Perimeter Networks

MRA doesn't support chained traversal connections (using multiple Expressway-Es to cross multiple firewalls). You can't use Expressway-E to give Mobile and Remote Access to endpoints that must traverse a nested perimeter network to call internal endpoints.

Figure 11: Nested Perimeter Networks
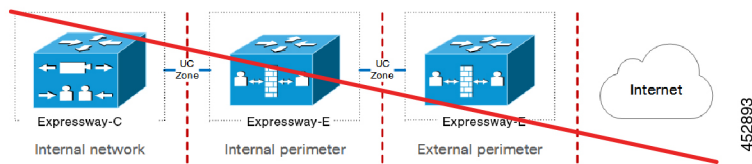
Expressway-C in DMZ with Static NAT

We don't support Expressway-C in a DMZ that uses static NAT. Static NAT firewall traversal requires SDP rewriting, which Expressway-C doesn't support—use the Expressway-E instead.

Figure 12: Expressway-C in DMZ with Static NAT
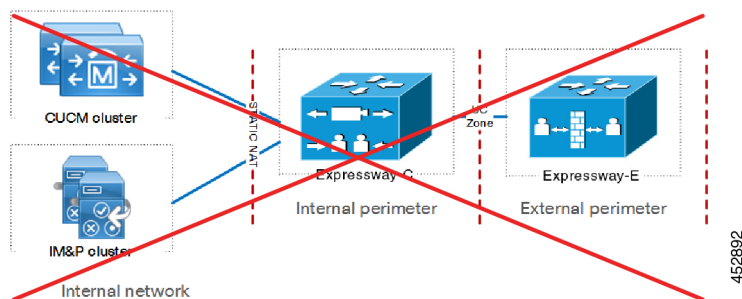
Unsupported Expressway Combinations

The following major Expressway-based deployments don't work together. You can't implement them together on the same Expressway (or traversal pair):

- Mobile and Remote Access

- Microsoft interoperability, using the Expressway-C-based B2BUA

- Jabber Guest services

Capacity Information

For details on MRA registration limits and other capacity information, refer to "Cluster License Usage and Capacity Guidelines" section in *Cisco Expressway Administrator Guide* at Expressway configuration guides page.

MRA Requirements and Prerequisites

This chapter contains information on the requirements and prerequisites that your deployment must meet in order to configure and deploy Mobile and Remote Access.

Mobile and Remote Access Ports

For MRA port information, go to the *Cisco Expressway IP Port Usage Configuration Guide* at Cisco Expressway Series Configuration Guides. The guide describes the ports that you can use between Expressway-C in the internal network, Expressway-E in the DMZ, and the public internet.

Network Infrastructure Requirements

IP Addresses

Assign separate IP addresses to the Expressway-C and the Expressway-E. Do not use a shared address for both elements, as the firewall cannot distinguish between them.

Network Domain

The ideal scenario for MRA is to have a single domain with a split DNS configuration, and this is the recommended approach. This is not always possible, so there are some other approaches to deal with various alternative scenarios.

Note The domain to which the calls are routed must match with the MRA domain to which the endpoints were registered. For example, if endpoints are registered with the domain `exp.example.com`, the calls must be routed to this domain, and it must not be routed to the domain `cluster1.exp.example.com`.

DNS

Single Domain with Split DNS - Recommended

A single domain means that you have a common domain (`example.com`) with separate internal and external DNS servers. This allows DNS names to be resolved differently by clients on different networks depending on DNS configuration, and aligns with basic Jabber service discovery requirements.

Dual Domain without Split DNS

From X12.5, the Cisco Expressway Series supports the case where MRA clients use an external domain to lookup the *_collab-edge* SRV record, and the *_cisco-uds* SRV record for that same external domain cannot be resolved by the Expressway-C. This is typically the case when split DNS is not available for the external domain. And prior to X12.5 this required a pinpoint subdomain or some other DNS workaround on the Expressway-C, to satisfy the client requirements for resolving the *_cisco-uds* record.

Limitation: This case is not supported for Unified CM nodes identified by IP addresses, only for FQDNs.

This feature also supports a secondary case, for MRA deployments that only allow Jabber access over MRA even if users are working on-premises. In this case only one domain is required and typically the DNS records are publicly resolvable (although this is not required if MRA access is disallowed for users when off premises). The change in X12.5 means that there is no need to have a *_cisco-uds._tcp.<external-domain>* DNS SRV record available to Cisco Expressway-C or to the Jabber clients.

Single Domain without Split DNS

Deployments that require Jabber clients to always connect over MRA also benefit from the X12.5 update that no longer requires the Expressway-C to resolve the *_cisco-uds* DNS SRV record. So administrators only need to configure the *_collab-edge* DNS SRV record, and Jabber clients using service discovery will only have the option of connecting over MRA.

URL for Cisco Meeting Server Web Proxy and MRA domain cannot be the same

If you use both the CMS Web Proxy service and MRA on the same Expressway, the following configuration items must be assigned different values per service. If you try to use the same value, the service that was configured first will work, but the other one will fail:

- MRA domain(s). The domain(s) configured on Expressway and enabled for Unified CM registration

- CMS Web Proxy URL link. Defined in the Expressway "Guest account client URI" setting on the **Expressway > Configuration > Unified Communications > Cisco Meeting Server** page.

Multiple External Domains for Mobile and Remote Access

Cisco Expressway supports Mobile and Remote Access with multiple external domains. With this deployment, you will have more than one external domain where your MRA clients may reside. MRA must be able to connect to all of them. To configure this deployment, do the following:

For Expressway-E:

- On public DNS, configure `_collab-edge._tls.<domain>` DNS SRV records for each Edge domain.

- Configure A records that point the Expressway-E hostname to the public IP address of Expressway-E.

For Expressway-C:

- For internal DNS, add A and PTR records that point to Expressway-E FQDN. Add these records to all Expressway-C nodes.

- Configure the `_cisco_uds` SRV record for every domain to point to your Unified Communications Manager clusters.

- On the **Domains** page of Expressway-C, add each of the internal domains that point to the Unified Communications Manager cluster.

For more detail, including a configuration checklist that summarizes the domain-specific configuration tasks for multiple domains, see Multidomain Configuration Summary.

SRV Records

This section summarizes the public (external) and local (internal) DNS requirements for MRA. For more information, see the *Cisco Jabber Planning Guide* for your version on the Jabber Install and Upgrade Guides page.

Public DNS (External Domains)

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.

Table 2: Example: 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

Local DNS (Internal Domains)

Although we recommend that the local, internal DNS is configured with _cisco-uds._tcp.<domain> SRV records, from X12.5 this is no longer a *requirement*.

👉

Important From version X8.8, if you use the IM and Presence Service over MRA (or any XMPP federation that uses XCP TLS connections between Expressway-C and Expressway-E), **you must create forward and reverse DNS entries for each Expressway-E system**. This is so that Expressway-C systems making TLS connections to them can resolve the Expressway-E FQDNs and validate the Expressway-E certificates. This requirement affects only the internal, LAN-side interface and does not apply to the external IP-side.

Table 3: Example: Local DNS

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

Create internal DNS records, for both forward and reverse lookups, for all Unified Communications nodes used with MRA. This allows Expressway-C to find the nodes when IP addresses or hostnames are used instead of FQDNs.

Ensure that the cisco-uds SRV records are NOT resolvable outside of the internal network, otherwise the Jabber client will not start MRA negotiation via the Expressway-E.

Firewall Configuration

- Ensure that the relevant ports are 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.

  No inbound ports are required to be opened on the internal firewall. The internal firewall must allow the following outbound connections from Expressway-C to Expressway-E: SIP: TCP 7001; Traversal Media: UDP 2776 to 2777 (or 36000 to 36011 for large VM/appliance); XMPP: TCP 7400; HTTPS (tunneled over SSH between C and E): TCP 2222.

  The external firewall must allow the following inbound connections to Expressway: SIP: TCP 5061; HTTPS: TCP 8443; XMPP: TCP 5222; Media: UDP 36002 to 59999.

  For more information, see *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

- 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.

- The traversal zone on the Expressway-C points to the Expressway-E through the **Peer address** field on the traversal zone, which specifies the address of the Expressway-E server.

  - For dual NIC deployments, you can specify the Expressway-E address using a FQDN that resolves to the IP address of the internal interface. With split DNS you can optionally use the same FQDN as is available on the public DNS. If you don't use split DNS you must use a different FQDN.

  - For single NIC with static NAT (this deployment is NOT recommended), you must specify the Expressway-E address using a FQDN that resolves to the public IP address. This also means that

the external firewall must allow traffic from the Expressway-C to the external FQDN of the Expressway-E. This is known as NAT reflection, and may not be supported by all types of firewalls.

For more information, see the "Advanced networking deployments" appendix in the Expressway Basic Configuration (Expressway-C with Expressway-E) Deployment Guide

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 MRA-connected devices.

Unified Communications Requirements

Product Versions

The following table provides minimum releases of Cisco UC products in order for MRA to be supported with various features.

Table 4: Product Versions

Product	MRA Support	Legacy Authentication (LDAP)	Legacy Authentication with SSO	OAuth with Refresh	OAuth Refresh with SSO	Push Notifications
Expressway	X8.1.1	X8.1.1	X8.5.1	X8.10.1	X8.10.1	X8.10.1
Unified CM	10.0	-	SAML SSO: 10.5(1)	11.5(1) SU3	10.5(2)	11.5(1) SU3
IM and Presence Service (optional)	10.0	-	SAML SSO: 10.5(1)	11.5(1) SU3	10.5(2)	11.5(1) SU3
Cisco Unity Connection (optional)	10.0	-	Clusterwide SAML SSO: 11.5(1) Per node SSO: OpenAM: 8.6(2) SAML SSO: 10.0(1)	-	-	NA

Unified CM Requirements

The following Cisco Unified Communications Manager configuration requirements exist for deploying Mobile and Remote Access:

Basic MRA Requirements for Unified CM

- **IP addressing**—Unified CM must be using IPv4 addressing as Expressway does not support IPv6.

- **Cisco AXL Web Service**—This service must be running on the publisher node.

- **Multiple Unified CM clusters**—If you have multiple Unified CM clusters, configure **Home Cluster Discovery**. End users must have the **Home Cluster** field assigned in **End User Configuration** so that Expressway-C can direct MRA users to the correct Unified CM cluster. Use either of the following configuration methods:

  - Option 1: ILS Network—Configure an Intercluster Lookup Service (ILS) network between your remote Unified CM clusters. ILS completes cluster discovery automatically, populating the **Cluster View** for each cluster, connecting your clusters into an intercluster network. ILS can also replicate your enterprise dial plan across all Unified CM clusters, although this functionality is not required by MRA. ILS is the recommended approach, particularly for large intercluster networks.

  - Option 2: Manual Connections—Configure each Unified CM cluster manually with connections to the other remote clusters. From Cisco Unified CM Administration, choose **Advanced Features** > **Cluster View** and add the remote clusters. Note that this option does not allow for dial plan replication.

- **MRA Access Policy**—If you have Cisco Jabber clients using OAuth authentication over MRA, make sure that your Jabber users' User Profiles allow Mobile and Remote Access. Check that the following settings exist within the **User Profile Configuration** of Unified CM:

  - The **Enable Mobile and Remote Access** check box must be checked (the default setting is checked).

  - The **Jabber Desktop Client Policy** and **Jabber Mobile Client Policy** fields must be set to allow the appropriate Jabber services for your deployment (the default setting is **IM & Presence, Voice and Video calls**).

- **Push Notifications**—If you are deploying Cisco Jabber or Webex on iOS or Android clients over MRA, you must configure Push Notifications and Cisco Cloud Onboarding in Unified Communications Manager. For configuration details, see the *Push Notifications Deployment Guide*.

- **OAuth**—If you are using OAuth on Expressway, you must also enable OAuth Refresh Logins on Cisco Unified Communications Manager as well. This can be turned on in Cisco Unified CM Administration by setting the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled**.

- If you want to deploy SAML SSO for MRA users and clients, you must configure it on Cisco Unified Communications Manager before you configure it on Expressway.

- For video calling over MRA, it's recommended that you reconfigure the **Maximum Session Bit Rate for Video Calls** setting within the **Region Configuration** as the default value of 384 kbps is not enough for video.

- If Unified Communications Manager and Expressway are in different domains, you must use either IP addresses or FQDNs for the Cisco Unified Communications Manager server address.

- Denial of Service Thresholds—High volumes of Mobile and Remote Access calls may trigger denial of service thresholds on Unified CM when all calls arrive at Unified CM from the same Expressway-C (cluster). If necessary, we recommend that you increase the level of the **SIP Station TCP Port Throttle Threshold** service parameter to **750 KB/second**. You can access the parameter from **System** > **Service Parameters** menu, selecting the **Cisco CallManager** service.

- For information on certificate requirements, see .

Additional Requirements for ICE Media Path Optimization

Additional requirements exist if you are deploying ICE Media Path Optimization. For details, see .

IM and Presence Service Requirements

To deploy IM clients over MRA, the following configuration requirements exist for the IM and Presence Service:

- The **Cisco AXL Web Service** must be running on the IM and Presence Service database publisher node.

- If you have multiple IM and Presence Service clusters within the same domain, you must configure intercluster peering between the clusters.

- IPv4 addressing must be used as Expressway does not support IPv6 addressing.

- For information on certificate requirements, see .

Certificate Requirements

This topic covers the following certificate requirements for Mobile and Remote Access (MRA):

- Certificate exchange requirements for your UC servers

- Certificate signing request (CSR) requirements for Expressway servers that deploy MRA

- Managing mTLS Client Certificate for MRA Onboarding

Certificate Exchange Requirements

We recommend that you use CA-signed certificates for Mobile and Remote Access.

The following table shows the certificates that each application uses for Mobile and Remote Access along with the certificate upload requirements for those applications.

This table assumes that you're using CA-signed certificates for all certificates that MRA uses.

Table 5: Certificate Exchange Requirements (CA-Signed Certificates)

UC application	Presents these certificates for MRA	Exchange Requirements

Unified CM	CallManager, Tomcat	Each Unified CM cluster must trust the Expressway-C certificate. For each cluster, make sure of the following:
		
		• **If Mixed mode is enabled**—The Expressway-C certificate must be installed to the **CallManager-trust** and **Tomcat-trust** store on Unified CM.
		
		• **If Mixed mode is disabled**—The root CA certificate that signs the Expressway-C certificate must be installed to the **CallManager-trust** and **Tomcat-trust** store on Unified CM. And, restart the following:
		
		    • Tomcat Service
		
		    • CallManager Service
		
		    • HA Proxy Service (if using TLS on Tomcat)

IM and Presence Service	cup-xmpp, Tomcat	Each IM and Presence Service cluster must trust the Expressway-C certificate. For each cluster, make sure of the following: • The root CA certificate that signs the Expressway-C certificate is installed to the **cup-xmpp-trust** and **Tomcat-trust** store of the IM and Presence Service.

UC application	Presents these certificates for MRA	Exchange Requirements
Expressway-C	Expressway-C certificate (CA-signed)	Expressway-C must trust the certificates presented by each Unified CM and IM and Presence Service cluster. In addition, Expressway-C must trust the Expressway-E certificates. Make sure of the following: • Expressway-C's trusted CA list must include the root CA certificate that signs the Unified CM and IM and Presence Service certificates for all UC clusters. • Expressway-C's trusted CA list must include the CA certificate chain (<u>root</u> and <u>intermediate</u>certificates) that signs the Expressway-E certificate. • If appropriate, Expressway-C's trusted CA list must include any endpoint certificates. • **Note:** Make sure that you add all <u>root</u> and <u>intermediate</u> Certificate Authority (CA) certificates or full Certificate Authority (CA) chain used to sign the Expressway-C certificate to the *tomcat*-trust and *CallManager*-trust list of Cisco Unified Communications Manager (UCM), even though the UCM is operating in the *non-secure* mode. **Reason** - The traffic server service in Expressway sends its certificate whenever a server (UCM) requests it. These requests are for services running on ports other than 8443 (for example, ports 6971, 6972,...). This enforces certificate verification even if UCM is in *non-secure* mode.
Expressway-E	Expressway-E certificate (CA-signed)	Expressway-E must trust the Expressway-C certificate. Make sure of the following: • Expressway-E's trusted CA list must include the CA certificate chain (root and intermediate certificates) that signs the Expressway-C certificate. • If appropriate, Expressway-E's trusted CA list must include any endpoint certificates.

Certificate management is simplified if you use the same CA to sign certificates for all applications as it is already installed on each application. However, you may want to limit certificate costs by using a public CA for Expressway-E and an enterprise CA for internal applications.

Note You can also use self-signed certificates for Cisco Unified Communications Manager and the IM and Presence Service. Then, the certificate requirements will be same as in the above table with one exception. On Expressway-C, rather than installing the root CA certificate(s) that signs the Unified CM and IM and Presence Service certificates, install the actual certificates that Unified CM (CallManager, Tomcat) and IM and Presence Service (cup-xmpp, Tomcat) use for Mobile and Remote Access.

> **Note** For the UC traversal zone between Expressway-C and Expressway-E, it's not sufficient to install the root CA certificate that the other Expressway application uses. You must install the CA certificate chain (root plus intermediate certificates) that the other Expressway application uses.

CSR Requirements for Expressway Servers

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 highlights CSR requirements when generating the Expressway-C and Expressway-E certificates for Mobile and Remote Access.

Table 6: CSR Requirements for Expressway Servers with Mobile and Remote Access

CSR Extension	Expressway-C Requirement	Expressway-E Requirement
Subject Alternative Names	The Expressway-C list of Subject Alternative Names must include: • Phone Security Profiles used by MRA endpoints • Expressway cluster name (for clustered Expressways only) • IM and Presence chat node aliases (for Federated group chat)	The Expressway-E list of Subject Alternative Names must include: • Unified CM Registration Domains • XMPP Federation Domains • IM and Presence chat node aliases (for Federated group chat)
Client Authentication	The certificate must include the Client Authentication extension. The system won't let you upload a certificate without this extension. **Note** Make sure that the CA that signs the request doesn't strip out the client authentication extension.	The certificate must include the Client Authentication extension. The system won't let you upload a certificate without this extension. **Note** Make sure that the CA that signs the request doesn't strip out the client authentication extension.

> **Note** We recommend that you use DNS format for the chat node aliases when generating the CSRs for both Expressways.

> **Note** Expressway-C automatically includes the chat node aliases in the certificate signing request (CSR), providing it has discovered a set of IM and Presence Service servers.

Generating CSRs and Uploading Certificates on Expressway

The following steps describe how to generate CSRs and upload certificates onto Expressway.

1. Go to **Maintenance** > **Security** > **Server** to generate a CSR and upload a server certificate to Expressway.

2. Go to **Maintenance** > **Security** > **Trusted CA** and upload trusted Certificate Authority (CA) certificates to Expressway.

3. Restart the Expressway for the new trusted CA certificate to take effect.

> **Note**   For detailed procedures and information on how to use the Certificate Signing Request tool to generate CSRs for Cisco Expressway certificates, and how to upload and download certificates on Expressway refer to the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page.

Managing mTLS Client Certificate for MRA Onboarding

If your MRA client presents a client certificate, please ensure to add the CA certificate that signed the client certificate to the mTLS CA trust list.

The CA certificate page for mTLS is accessed from the Trusted CA certificate page (**Maintenance** > **Security** > **Trusted CA certificate**).

This page only applies if you use Expressway for Mobile and Remote Access (MRA) with Cisco Unified Communications products, and onboarding with activation codes is enabled for MRA.

The following steps describe how to upload mTLS certificates onto Expressway

1. Go to **Maintenance** > **Security** > **CA Certificate**.

2. Click **Activation Code onboarding trusted CA certificate** link under Related tasks to upload CA certificate for mTLS connection.

3. Upload CA certificate and click **Append CA certificate for mTLS**.

Endpoint Requirements

MRA-Compatible Clients

Table 7: MRA-Compatible Client Versions

Jabber	MRA Support	Legacy Authentication (LDAP)	Legacy Authentication with SSO	OAuth with Refresh	OAuth Refresh with SSO	APNS
Cisco Jabber for Windows	9.7	-	10.6	11.9	11.9	NA
Cisco Jabber for iPhone and iPad	9.6.1	-	10.6	11.9	11.9	11.9

Jabber	MRA Support	Legacy Authentication (LDAP)	Legacy Authentication with SSO	OAuth with Refresh	OAuth Refresh with SSO	APNS
Cisco Jabber for Android (includes Chromebook)	9.6	-	10.6	11.9	11.9	NA
Cisco Jabber for Mac	9.6	-	10.6	11.9	11.9	NA

Jabber clients 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 MRA are provided in the installation and configuration guide for the relevant client:

- Cisco Jabber for Windows

- Cisco Jabber for iPhone and iPad

- Cisco Jabber for Android

- Cisco Jabber for Mac (requires X8.2 or later)

Cisco Webex Clients

Expressway supports calling for MRA-connected Webex clients that are running a compatible software version:

- Cisco Webex for Windows

- Cisco Webex for Mac

- Cisco Webex for iPhone and iPad

- Cisco Webex for Android

MRA-Compatible Endpoints

Table 8: MRA-Compatible Endpoints

Endpoints	MRA Support
Cisco IP Phone 7800 Series	11.0(1)

Endpoints	MRA Support
Cisco IP Phone 8800 Series **except** Cisco Wireless IP Phone 8821 and 8821-EX and Cisco Unified IP Conference Phone 8831	11.0(1)
Cisco IP Conference Phone 7832	12.1(1)
Cisco IP Conference Phone 8832	12.1(1)
Android-based Cisco DX650, DX70, and DX80 devices	10.2.4(99)

Cisco Webex Desk Series endpoints, such as:
  • Cisco Webex DX80
  • Cisco Webex Desk Pro
	All CE releases supported by the hardware

Cisco Webex Board Series endpoints, such as:
  • Cisco Webex Board 55
  • Cisco Webex Board 70
  • Cisco Webex Board 85s
	All CE releases supported by the hardware

Cisco Webex Room Series endpoints, such as:
  • Cisco Webex Room 55
  • Cisco Webex Room 70 G2
  • Cisco Webex Room 55 Dual
  • Cisco Webex Room 70 Dual G2
  • Cisco Webex Room Panorama
  • Cisco Webex Room 70 Panorama
  • Cisco Webex Room 70D Panorama Upgrade
  • Cisco Webex Room Kit
  • Cisco Webex Room Kit Pro
  • Cisco Webex Room Kit Plus
  • Cisco Webex Room Kit Mini
  • Cisco WebEx Codec Plus
	All CE releases supported by the hardware

Cisco TelePresence endpoints: SX Series, EX Series, MX Series, Profile Series, C Series	TC7.1

Endpoints	MRA Support
Cisco TelePresence and Webex endpoints: • DX70 • DX80 • MX700 • MX800 • MX800 Dual • SX10 • SX20 • SX80 • MX200 G2 • MX300 G2	CE 8.2

EX, MX, and SX Series Endpoints (Running TC Software)

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

These devices 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.

The devices ship with a list of default CAs which cover the most common providers (including Verisign and Thawte). If the relevant CA is not included, it must be added (for instructions, see the endpoint administrator guide).

Mutual authentication is optional, and these devices 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. Instead, manually apply the certificates to the devices. The client certificates must be signed by an authority that is trusted by the Expressway-E.

Considerations for Android-based DX650, DX80, and DX70 Devices and Supported IP Phone 7800 and 8800 models

If you deploy these devices to register with Cisco Unified Communications Manager through MRA, be aware of the following points. For DX endpoints, these considerations only apply to Android-based devices and do not apply to DX70 or DX80 devices running CE software:

- **Trust list**: You cannot modify the root CA trust list on Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series devices. Make sure that the Expressway-E's server certificate is signed by one of the CAs that the devices trust, and that the CA is trusted by the Expressway-C and the Expressway-E.

- **Off-hook dialing**: The way KPML dialing works between these devices and Unified CM means that you need Cisco Unified Communications Manager 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.

Which MRA Features are Supported

For information about which features are supported over MRA for specific clients and endpoints, refer to the relevant product documentation:

Endpoint	Refer to...
Cisco Jabber	See "Supported Services" in the "Remote Access" chapter of the *Planning Guide for Cisco Jabber* (for your version).
Cisco IP Phone 7800 Series	See "Phone Features Available for Mobile and Remote Access Through Expressway" in the "Phone Features and Setup" chapter, *Cisco IP Phone 7800 Series Administration Guide for Cisco Unified Communications Manager*.
Cisco IP Conference Phone 7832	See "Phone Features Available for Mobile and Remote Access Through Expressway" in the "Phone Features and Setup" chapter, *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager*.
Cisco IP Phone 8800 Series	See "Phone Features Available for Mobile and Remote Access Through Expressway" in the "Phone Features and Setup" chapter, *Cisco IP Phone 8800 Series Administration Guide for Cisco Unified Communications Manager*.
Cisco IP Conference Phone 8832	See "Phone Features Available for Mobile and Remote Access Through Expressway" in the "Phone Features and Setup" chapter, *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager*.

Limitations and Feature Support

MRA supports different features in different deployment scenarios, and when different clients and endpoints are used. This section provides information about:

- Key unsupported features for clients and endpoints

- Unsupported Expressway features that don't work in certain MRA situations

UC Feature Support and Limitations

This section lists some key client and endpoint features that we know don't work with MRA-connected devices.

Note Refer to your endpoint or client documentation for more information. The following list isn't exhaustive.

- **Multiple IM and Presence clusters with different releases**—If you have multiple IM and Presence Service clusters configured on Cisco Expressway-C, and some of them run pre-11.5 software, MRA endpoints may not be able to use features that require 11.5. The reason is that, using a round robin approach, Cisco Expressway-C may select a cluster on an older software version.

- **Expressway-E with dual network interface**—In Expressway-E systems that use dual network interfaces, XCP connections (for IM and Presence Service XMPP traffic) always use the internal interface. XCP connections may fail if the Expressway-E internal interface is on a separate network segment and is used

for system management only, and where the Expressway-C traversal zone connects to the Expressway-E external interface.

- **Cisco Jabber with E911**—If you deploy Cisco Jabber clients over MRA with the E911NotificationURL feature, configure a static HTML page for the notification. MRA does not support scripts and link tags for the web page.

- **Cisco Jabber Directory access**—MRA supports Cisco Jabber directory access using the Cisco User Data Services (UDS). MRA doesn't support other directory access methods for Jabber.

- **Unified Contact Center Express feature support**—MRA doesn't support some Cisco Unified Contact Center Express features. For details, refer to the Unified Contact Center Express documentation.

- **Endpoint failover behavior**:

  - 78XX / 88XX series phones registered over MRA and using OAuth token may get de-registered when a CUCM node goes down but, will continue to communicate with another active node. And the phones will re-register after some time.

    Jabber registered over MRA and using OAuth token may get de-registered when a CUCM node goes down and displays a message "Your session is expired. Sign in again to keep using Cisco Jabber". You can sign in to your Jabber to continue using the service.

  - Cisco Jabber clients support IM and Presence Service and SIP Registration Failover over MRA. For more information, see SIP Registration Failover for Cisco Jabber. However, they don't support any other type of MRA - related redundancy or failover - including Voicemail and User Data Services (UDS). Clients use a single UDS server only.

    If an Expressway-C or Expressway-E node fails, active MRA calls through the failed Expressway node also fail. This behavior applies to all device types, including Jabber clients.

    For Unified CM failover over MRA, Cisco IP Phones need clustered Expressway-C and Expressway-E servers. IP Phones need at least the same number of Expressway-C and Expressway-E servers in the cluster as the number of Unified CMs in the Call Manager group configured on the IP phone. Note that devices running TC or CE software don't need clustered Expressway servers for Unified CM failover.

- **Chat over MRA with OAuth Refresh Logins**—Cisco Jabber 12.5 or later is needed if you want chat/messaging services over MRA with OAuth Refresh Authentication (self-describing tokens) and with IM and Presence Service presence redundancy groups. With pre-12.5 Jabber, user login fails in this scenario.

- **Call Recording over MRA**—Includes the following limitations:

  - MRA supports recording tones for Cisco Jabber clients and Webex Unified CM registered applications. Also note that CTI monitoring of Jabber mobile devices requires Unified CM 12.5(1)SU1 or later.

- **Silent Monitoring over MRA**—The following monitoring features are supported for compatible MRA-connected endpoints, provided that the deployed UC products are running compatible versions, the Silent Monitoring feature is configured on Cisco Unified Communications Manager, and SIP Path Headers are enabled on Expressway (as described in Enable SIP Path Headers, on page 74):

  - Silent Monitoring is supported from X12.6.1.

  - Whisper Coaching and Whisper Announcements are supported from X12.6.2.

- **Encrypted iX Channel**—The Expressway doesn't encrypt the iX protocol on behalf of other entities. As a result, iX must be encrypted end to end, or unencrypted end to end. When iX is encrypted, the endpoints and conferencing server must handle encryption.

Note For iX to work over MRA, configure the conferencing server with an encrypted trunk to Unified CM and make sure that the endpoints/Jabber are running a suitable, iX-capable software version.

- **Certificate Authority Proxy Function (CAPF) over MRA**—MRA doesn't support certificate provisioning for remote endpoints. This limitation includes the Certificate Authority Proxy Function (CAPF). To use CAPF, complete the first-time configuration, including CAPF enrollment, on premises (inside the firewall). To complete subsequent certificate operations, you must bring the endpoints back on-premises.

- **Encrypted TFTP**—MRA supports encrypted TFTP configuration files over MRA when the CAPF enrollment has already been completed on-premises.

- **Session Refresh features**—The following session refresh features that rely on the SIP UPDATE method (RFC 3311) fail over MRA:

  - Request to display the security icon on MRA endpoints for end-to-end secure calls

  - Request to change the caller ID to display name or number on MRA endpoints

- **P2P File Transfer**—MRA doesn't support peer-to-peer file transfer when using IM and Presence Service and Jabber.

- **Managed File Transfer over MRA**—MRA supports Managed File Transfer (MFT) over MRA when using IM and Presence Service 10.5.2 and later (restricted version) and Jabber 10.6 and later clients. MRA doesn't support MFT with an unrestricted version of IM and Presence Service.

- **File Transfer for Webex Messenger Service and Cisco Jabber** — MRA supports file transfer with Webex Messenger Service and Cisco Jabber.

- **Mobility Feature Support**—MRA doesn't support additional Mobility features, including Session Handoff.

- **Hunt Group Support**—MRA supports hunt groups (including hunt pilots and hunt lists) when using Unified CM version 11.5(1)SU5, or any later version that has the relevant change.

- **Self-Care Portal Access**—MRA doesn't support the Cisco Unified Communications Self Care Portal.

- **Key Expansion Module (KEM) is supported for Compatible Phones**

Note **Note:** To deploy the feature, SIP path headers must be enabled on Expressway, and you need a Unified CM software version that supports path headers (Release 11.5(1)SU4 or later is recommended)

- **MRA Single Sign On** — MRA only supports single IdP certificate for signing SAML assertions. It doesn't support multiple IdP Signing certificates at this point.

- **Load Balancing over MRA** — When Expressway identifies a load (number of registrations) is skewed across nodes, load re-balancing triggers. During rebalancing, endpoints registered via loaded path are redirected to CUCM via a least loaded path. This process continues till the load is balanced across cluster. This Load balancing feature is supported only with newer versions of Jabber client. Refer to Jabber guide to know the supported version for this feature.

Unsupported Expressway Features and Limitations

- Currently, if one Expressway node in a clustered deployment fails or loses network connectivity for any reason (including if the Unified CM restarts or fails), all active calls going through the affected node will fail. The calls are not handed over to another cluster peer. Bug ID CSCtr39974 refers. This is not an MRA-specific issue and applies to all call types.

- We do not support third-party network load balancers between MRA clients and Expressway-E.

- Custom embedded tabs for Cisco Jabber endpoints connected over MRA works only for very basic HTML content (no JavaScript(s) or Dynamic HTML).

- The Expressway cannot be used for Jabber Guest when it's 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.

- Maintenance mode is not supported over MRA for endpoints running CE software. The Expressway drops MRA calls from these endpoints when you enable maintenance mode.

- As Expressway only supports IPv4 mode for MRA connections, the IP configuration settings "IPv6 only" or "Both" are not supported. In the case of "Both", as Expressway does not proxy IPv6 MRA traffic from clients, intermittent issues may arise if clients send IPv6 instead of IPv4.

- Endpoint management capability (SNMP, SSH/HTTP access) is not supported.

- **Multiple Presence Domains over MRA**—This feature is supported from Expressway X12.6.3 with IM and Presence Service 10.0(x) or later. Compatible clients can be deployed into an infrastructure that has users in more than one domain or in domains with subdomains. We recommend no more than 75 domains in a Unified Communications default deployment.

  For XMPP/chat & presence federation through Expressway, the existing requirement that XMPP federation is supported on a single Expressway cluster only still applies.

  Note that for Expressway releases prior to X12.6.3, support for multiple presence domains was a preview feature with the following limitations:

  - Before X8.5, each Expressway deployment supported only one Presence domain. (Even though IM and Presence Service 10.0 and 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. However, this feature is in preview status only, and we recommend that you do not exceed 50 domains.

- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM.

- The Expressway does not support some Cisco Unified Contact Center Express features for contact center agents or other users who connect over MRA. Jabber for Mac and Jabber for Windows cannot provide deskphone control over MRA, because the Expressway pair does not traverse the CTI-QBE protocol.

  However, if these Jabber applications, or other CTI applications, can connect to Unified CM CTIManager (directly or through the VPN), they can provide deskphone control of MRA-connected clients.

- For ICE passthrough calls, if Host and Server-reflexive addresses cannot negotiate successfully, endpoints can utilize relay address of the TURN server to establish optimized media path. However, when Expressway is used as a TURN server and if static NAT is configured on the Expressway-E, the media cannot be passed using the relay address (CDETS CSCvf85709 refers). In this case, default traversal path is used to traverse the media. That is, the media passes through Expressway-C and Expressway-E.

- The Expressway-E does not support TURN relay over TCP for ICE passthrough calls.

- From X12.5.5, support for static NAT functionality on TURN is extended to clustered systems (support for standalone systems was introduced in X12.5.3). However, peers which are configured as TURN servers must be reachable using the private addresses for their corresponding public interfaces.

- **Redirect URI support** — This feature will not work in a cluster deployment, when Expressway-E observes two different source IP addresses. For example, Jabber orWebex client on mobile has an IP address different than that of the external browser on the mobile. This may be due to:

  - There is change in IP address during mobile roaming

  - If user is behind firewall configured for NAT with multiple public IP address

  - Split VPN configuration

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.

MRA OAuth Token Authorization with Endpoints / Clients

In standard MRA mode (no ICE) regardless of any MRA access policy settings configured on Unified CM, Cisco Jabber users will be able to authenticate by username and password or by traditional single sign-on in the following case:

- You have Jabber users running versions before 11.9 (no refresh token support) and is configured to allow non-token authentication.

In ICE passthrough mode, the ICE MRA call path must be encrypted end-to-end (see *Signaling Path Encryption Between Expressway-C and Unified CM* in the Expressway MRA Deployment Guide). Typically for end-to-end

encryption, Unified CM must be in mixed mode for physical endpoints. For Jabber clients however, you can achieve the end-to-end encryption requirement by leveraging SIP OAuth with Unified CM clusters that are not in mixed mode.

Note   You must enable SIP OAuth if the Unified CM is not in mixed mode, but SIP OAuth is not required for Jabber if you're able to register using standard secure profiles.

More information is in the *Configure MRA Access Control* section of the *Expressway MRA Deployment Guide* and in the *Deploying OAuth with Cisco Collaboration Solution Release 12.0* White Paper.

HSM Support

As well as being one of the features that we currently provided in Preview status only, the following additional points apply to HSM support in Expressway:

- Like other features that are enabled by option keys (see previous section) you can't use HSM with Expressways that use Smart Licensing.

- Although the "SafeNet Luna" network device appears in the Expressway user interface, this device is not currently supported by Expressway at all and SafeNet Luna settings must not be configured.

CHAPTER 3

MRA Configuration

MRA Configuration Overview

This chapter contains configuration tasks that describe how to complete the base configuration that provides Mobile and Remote Access for compatible endpoints. These procedures can be used for single cluster, multi-cluster, single domain and multi-domain scenarios.

MRA Configuration Task Flow

Complete the following tasks to complete the basic configuration for Mobile and Remote Access.

Before you begin

• Review the MRA Requirements chapter before you configure MRA.

• Make sure that your system has the required certificates to deploy MRA. For details, refer to Certificate Requirements, on page 17

Procedure

	Command or Action	Purpose
Step 1	Set Expressway Server Address, on page 32	Set the System host name, domain name, and NTP source for each Expressway-C and E server.
Step 2	Enable SIP, on page 33	Make sure that SIP is enabled on both Expressway-E and Expressway-C.
Step 3	Configure Automated Intrusion Protection, on page 33	Recommended. Disable Automated Intrusion Prevention on Expressway-C and enable it on Expressway-E.
Step 4	Enable Mobile and Remote Access, on page 34	Set the Unified Communications mode to Mobile and Remote Access.

	Command or Action	Purpose
Step 5	Add Domains, on page 34	On Expressway-C, add internal UC domains and any other relevant domains, such as edge domains, and Presence domains.
Step 6	Add Internal UC Clusters: • Add Unified CM Cluster • Add IM and Presence Service Clusters • Add Cisco Unity Connection Clusters	From each Expressway-C cluster, create connections to your internal UC clusters.
Step 7	Configure MRA Access Control, on page 38	Configure settings for MRA Access Control, including OAuth authentication and SAML SSO settings.
Step 8	Configure OAuth on UC Applications, on page 45	Recommended. If your system supports it, configure OAuth authentication.
Step 9	SAML SSO Configuration, on page 47	Optional. Configure SAML SSO, allowing for common identity between external Jabber clients and users' Unified CM profiles.
Step 10	Configure Secure Traversal Zone, on page 50	Configure an encrypted UC traversal zone between Expressway-C and Expressway-E.

What to do next

After you complete your basic MRA setup, refer to the following chapters:

- ICE Media Path Optimization, on page 55—ICE is an optional feature that optimizes the media path for MRA calls. ICE lets MRA-registered endpoints send media to each other directly, such that the media bypasses the WAN and Expressway servers.

- Features and Additional Configurations, on page 69—Refer to this chapter for information on MRA features and optional configurations.

- Onboarding MRA Devices, on page 91—After you have configured your system, device activation codes provide a secure method to onboard remote MRA devices.

Set Expressway Server Address

Use this procedure to set FQDNs and NTP servers for each of your Cisco Expressway-C and Expressway-E servers.

✎

Note A single Expressway server can have a single host name and domain name, even if you have multiple Edge domains.

Step 1 On Cisco Expressway-C, configure server address information:

a) Go to **System** > **DNS**.

    b) Assign the **System host name** and **Domain name** for this server.

    c) Enter the IP addresses of up to five DNS servers that the Expressway will query when attempting to locate a domain. These fields must use an IP address, not a FQDN.

> **Note** If you are deploying split DNS, Expressway-C points to an internal DNS server while Expressway-E points to a public DNS server.

Step 2 Configure NTP settings:

    a) Go to the **System** > **Time** menu and point to a reliable NTP server.

    b) Enter the NTP authentication method:

- Disabled—No authentication is used

- Symmetric key—When using this method, you must specify a Key ID, Hash method and Pass phrase.

- Private key—Uses an automatically generated private key.

Step 3 Repeat this procedure on each server in the Expressway-C cluster.

Step 4 After configuring Expressway-C, repeat this procedure for each server in the Expressway-E cluster.

Enable SIP

Enable SIP on the Expressway-C and Expressway-E clusters.

> **Note** SIP and H.323 protocols are disabled by default on new installs of X8.9.2 and later versions.

Step 1 On the Expressway-C primary peer, go to **Configuration** > **Protocols** > **SIP**.

Step 2 Set **SIP mode** to **On**.

Step 3 Click **Save**.

Step 4 Repeat the procedure on Expressway-E primary peer.

Configure Automated Intrusion Protection

We recommend that you disable Automated Intrusion Protection on Expressway-C and enable the service on Expressway-E.

> **Note** If your Expressway-C is newly installed from X8.9 onwards, the automated intrusion protection service is running by default on both Expressway-C and Expressway-E (check this).

Step 1 On Expressway-C, disable Automated Intrusion Protection:

a) Go to **System** > **Administration**
b) Set **Automated protection service** to **Off**.
c) Click **Save**.

Step 2 On Expressway-E, enable Automated Intrusion Protection (the service is On by default):

a) Go to **System** > **Administration**.
b) Set **Automated protection service** to **On**.
c) Click **Save**.

Note If you have multiple MRA users using the same IP address (for example, if you have multiple MRA users behind a NAT with the same public IP address), automated intrusion protection may trigger due to all of the traffic from the same IP address. In this case, configure an exemption on the IP address. For details, see Configure Exemptions, on page 105.

Enable Mobile and Remote Access

You must enable Mobile and Remote Access mode on Expressway before you can configure domains and traversal zones.

Step 1 On the Expressway-C, go to **Configuration** > **Unified Communications** > **Configuration**.
Step 2 Set **Unified Communications mode** to **Mobile and Remote Access**.
Step 3 Click **Save**.
Step 4 Repeat this procedure on Expressway-E.

Add Domains

On Expressway-C add the domains that your MRA deployment uses. Depending on the complexity of your system, this may be a single enterprise-wide domain or multiple domains, including:

- Enterprise domain

- Internal UC domains (if they are different from the enterprise domain)

- Edge domains (if they are different from the other domains)

- Presence domains (if they are different from the other domains)

Step 1 On Expressway-C, go to **Configuration** > **Domains**.
Step 2 Enter the **Domain name**.
Step 3 For each of the following services, set the corresponding drop-down to **On** or **Off** depending on whether you want to apply that service to this domain.

- **SIP registrations and provisioning on Expressway**—Expressway acts as a SIP registrar and accepts registration requests for any SIP domain.

- **SIP registrations and provisioning on Unified CM**—End registration and call control is handled by Unified CM. Expressway acts as a gateway for UC services.

- **IM and Presence Service**—The client obtains services from the IM and Presence Service.

- **XMPP federation**—Enables XMPP federation between this domain and a partner domain.

Step 4 If you have multiple **Deployments** configured, assign the deployment to which this domain applies. Note that this field appears only if you have configured multiple Deployments.

Step 5 Click **Save**.

Step 6 Repeat this procedure if you need to add additional domains.

Figure 13: Domains

Add Unified CM Cluster

Use this procedure to create connections from Expressway-C to each Cisco Unified Communications Manager cluster. Each Expressway-C cluster must be able to reach each Unified CM cluster node.

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

- The load is distributed across the nodes based on resource usage. Endpoints receives the least loaded node to reach CUCM. There is no load balancing of calls, only the initial registrations are load balanced. As the registrations are load balanced, probability of calls overloading on a single node is reduced.

Step 1 On the Expressway-C primary peer, go to **Configuration** > **Unified Communications** > **Unified CM servers**.

Step 2 Click **New** and add the following details for the publisher node:

- **Unified CM publisher address**—The server address of the publisher node

- **Username** and **Password** —User ID and Password of an account that can access the server.

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

- **TLS verify mode**

- **AEM GCM media encryption**—Set to On to enable AEM GCM support.

- **Deployment**—If you have configured multiple Deployments, select the appropriate deployment. This field doesn't appear unless you have configured deployments.

Step 3   Click **Add Address** to test the connection.

Step 4   If you have multiple Unified CM clusters, repeat steps 2 and 3 to add publisher nodes for additional Unified CM clusters to this Expressway-C cluster.

Step 5   After you added all Unified CM publisher nodes, click **Refresh Servers**.
Expressway-C discovers and adds the subscriber nodes for each cluster.

Step 6   If you have multiple Expressway-C clusters, repeat this procedure on other Expressway-C clusters until all Expressway-C clusters have connections to all Unified CM clusters and nodes.

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>'.

From version X12.5, Expressway automatically generates a neighbor zone named "CEOAuth <Unified CM name>" between itself and each discovered Unified CM node when SIP OAuth Mode is enabled on Unified CM. For details, see Configure SIP OAuth Mode, on page 46.

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.

Add IM and Presence Service Clusters

Use this procedure to create connections from Expressway-C to each IM and Presence Service cluster. Each Expressway-C cluster must be able to reach each IM and Presence Service cluster node.

Step 1 On Expressway-C, go to **Configuration** > **Unified Communications** > **IM and Presence Service nodes**.

Step 2 Click **New** and add the following details for database publisher node:

- **IM and Presence database publisher name**—Server address of the database publisher node

- **Username** and **Password**—User ID and Password of an account that can access the 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.

- **TLS verify mode**

- **Deployment**—If you configured multiple Deployments, select the appropriate deployment.

   Note This field doesn't appear unless you have configured deployments.

Step 3 Click **Add Address** to test the connection.

Step 4 If you have multiple IM and Presence clusters, repeat steps 2 and 3 to add database publisher nodes for those additional clusters to this Expressway-C cluster.

Step 5 After you have added all IM and Presence database publisher nodes, click **Refresh Servers**.
Expressway-C discovers and adds subscriber nodes for each IM and Presence cluster.

Step 6 If you have multiple Expressway-C clusters, repeat this procedure on other Expressway-C clusters until each Expressway-C cluster has a connection to each IM and Presence cluster node.

Add Cisco Unity Connection Clusters

Use this procedure to create connections from Expressway-C to each Cisco Unity Connection cluster. Each Expressway-C cluster must be able to reach each Cisco Unity Connection cluster node.

Step 1 On Expressway-C, go to **Configuration** > **Unified Communications** > **Unity Connection servers**.

Step 2 Click **New** and add the following details for publisher node:

- **Unity Connection publisher name**—Server address of the publisher node

- **Username** and **Password**—User ID and Password of an account that can access the server.

   Note These credentials are stored permanently in the Expressway database. The corresponding Cisco Unity Connection user must have the System Administrator role.

- **TLS verify mode**

- **Deployment**—If you configured multiple Deployments, select the appropriate deployment.

   Note This field doesn't appear unless you have configured deployments.

Step 3   Click **Add Address** to test the connection.

Step 4   If you have multiple Unity Connection clusters, repeat steps 2 and 3 to add publisher nodes for those additional clusters to this Expressway-C cluster.

Step 5   After you have added all Unity Connection clusters to this Expressway-C, click **Refresh Servers**.
Expressway-C discovers and adds the subscriber nodes for each cluster.

Step 6   If you have multiple Expressway-C clusters, repeat this procedure on other Expressway-C clusters until each Expressway-C cluster has a connection to each Unity Connection cluster node.

Configure MRA Access Control

Define how clients must authenticate for Mobile and Remote Access (MRA) requests.

⚠️

Caution   If you are upgrading from X8.9 or earlier, the settings applied after the upgrade are not the same as listed here. R refer instead to the upgrade instructions in the Expressway Release Notes.

Step 1   On the Expressway-C, go to **Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**.

Step 2   Configure authentication settings:

- From the **Authentication Path** field, select if you want to use SAML SSO, LDAP or Local Database authentication to authenticate user credentials.
- Select **Authorize by OAuth token** to enable OAuth authentication on Expressway. This option is supported with SAML SSO only.

Step 3   Configure the additional fields. For additional information about the field settings, see Expressway (Expressway-C) Settings for Access Control, on page 38

Expressway (Expressway-C) Settings for Access Control

The following table provides descriptions that appear under MRA Access Control (**Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**). You can use this configuration page to configure OAuth authentication settings and SAML SSO settings for Mobile and Remote Access.

Table 9: Settings for MRA Access Control

Field	Description
Authentication path	Hidden field until MRA is enabled. Defines how MRA authentication is controlled. • **SAML SSO authentication**—Clients are authenticated by an external IdP. • **UCM/LDAP basic authentication**—Clients are authenticated locally by the Unified CM against their LDAP credentials. • **SAML SSO and UCM/LDAP**—Allows either method. • **None**—No authentication is applied. The default until MRA is first enabled. The "None" option is required (rather than just leaving MRA turned off) because some deployments must turn on MRA to allow functions which are not actually MRA. (Such as the Web Proxy for Meeting Server, or XMPP Federation.) Only these customers should use "None". **It is not recommended in other cases.** Default Setting: **None** before MRA is turned on. After MRA is turned on, the default is **UCM/LDAP**.
Authorize by OAuth token with refresh	This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them. OAuth is supported by Cisco Jabber and Cisco Webex clients as well as by Cisco IP Phones that onboard using device activation codes in MRA mode. **Important:** From X8.10.1, the Expressway fully supports the benefits of self-describing tokens (including token refresh, fast authorization, and access policy support). However, not all of the benefits are actually available throughout the wider solution. Depending on what other products you use (Unified CM, IM and Presence Service, Cisco Unity Connection) and what versions they are on, not all products fully support all benefits of self-describing tokens. If you use this option on Expressway, **you must also enable OAuth with refresh on the Unified CMs, and on Cisco Unity Connection if used**. The process is summarized below. Default Setting: On
Authorize by OAuth token (previously SSO Mode)	Available if **Authentication path** is SAML SSO or SAML SSO and UCM/LDAP. This option requires authentication through the IdP. Currently, only Cisco Jabber and Cisco Webex clients can use this authorization method, which is not supported by other MRA endpoints. Default Setting: Off
Authorize by user credential	Available if **Authentication path** is UCM/LDAP or SAML SSO and UCM/LDAP. Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices. Default Setting: Off

Field	Description
Identity providers: Create or modify IdPs	Available if **Authentication path** is SAML SSO or SAML SSO and UCM/LDAP. For more information, see Identity Provider Selection, on page 45.
SAML Metadata	Available if **Authentication path** is SAML SSO or SAML SSO and UCM/LDAP. Determines how to generate the metadata file for the SAML agreement. The possible modes are: • **Cluster**: Generates a single clusterwide SAML metadata file. You must import only this file to IdP for the SAML agreement. • **Peer**: Generates the metadata files for each peer in a cluster. You must import each metadata file into IdP for the SAML agreement.
Identity providers: Export SAML data	Available if **Authentication path** is SAML SSO or SAML SSO and UCM/LDAP. For details about working with SAML data, see SAML SSO Authentication Over the Edge, on page 42.
Allow Jabber iOS clients to use embedded Safari	The IdP or Unified CM authentication page is displayed in an embedded web browser (not the Safari browser) on iOS devices by default. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices. This setting optionally allows 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 OAuth deployment. A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the 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. Default Setting: No

Field	Description

Check for internal authentication availability	Available if **Authorize by OAuth token with refresh** or **Authorize by OAuth token** is enabled.
	
	The default is No, for optimal security and to reduce network traffic.
	
	Controls how the Expressway-E reacts to remote client authentication requests by selecting whether the Expressway-C should check the home nodes.
	
	The request asks whether the client may try to authenticate the user by OAuth token, and includes a user identity with which the Expressway-C can find the user's home cluster:
	
	  • *Yes*: The *get_edge_sso* request will ask the user's home Unified CM if OAuth tokens are supported. The home Unified CM is determined from the identity sent by the Jabber client's *get_edge_sso* request.
	
	  • *No*: If the Expressway is configured not to look internally, the same response will be sent to all clients, depending on the Edge authentication settings.
	
	The option to choose depends on your implementation and security policy. If all Unified CM nodes support OAuth tokens, you can reduce response time and overall network traffic by selecting *No*. Or select *Yes* if you want clients to use either mode of getting the edge configuration—during rollout or because you can't guarantee OAuth on all nodes.
	
	Caution: **Setting this to Yes has the potential to allow rogue inbound requests from unauthenticated remote clients.** If you specify No for this setting, the Expressway prevents rogue requests.
	
	Default Setting: No

Allow activation code onboarding	Only available if **Authorize by OAuth token with refresh** or **Authorize by OAuth token** is enabled. This setting enables onboarding by activation code in the Expressway. The default value is **No**. Set the value to **Yes** to enable this option. Default Setting: No
SIP token extra time to live	Available if **Authorize by OAuth token** is *On*. Optionally extends the time-to-live for simple OAuth tokens (in seconds). Gives users a short window to accept calls after their credentials expire. However, it increases the potential security exposure. Default Setting: 0 seconds
WebEx Client Embedded Browser Support	Applies to Jabber and WebEx clients that send a SSO redirect URI. Default value: *No*. Set the value to Yes to enable this option. This feature enhances the security of Jabber and Webex Client Embedded Browser support. It allows the client to use the Embedded browser for Unified Communications Manager (and MRA) OAuth flow and improves the user experience.

✎

Note   On Expressway, you can check what authorization methods your Unified CM servers support. This displays the version numbers in use.

On Expressway, go to **Configuration** > **Unified Communications** > **Unified CM servers**.

SAML SSO Authentication Over the Edge

SAML-based SSO is an option for authenticating Unified Communications service requests. The requests can originate inside the enterprise network, or as described here, from clients requesting Unified Communications services from outside through MRA.

SAML SSO authentication over the edge requires an **external** identity provider (IdP). It relies on the secure traversal capabilities of the Expressway pair at the edge, and on trust relationships between the internal service providers and an externally resolvable 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.

The Expressway supports two types of OAuth token authorization with SAML SSO:

- Simple (standard) tokens. These always require SAML SSO authentication.

- Self-describing tokens with refresh. These can also work with Unified CM-based authentication

✎

Note   - When the Jabber endpoint uses SSO with no refresh and originally authenticates remotely to Unified CM through Expressway/MRA and then moves back to the local network, no reauthentication is required for the endpoint (edge to on premises).

- When the Jabber endpoint originally authenticates in the local network directly to Unified CM and then uses Expressway/MRA to access Unified CM remotely, reauthentication is required for the endpoint (On premises to edge).

About Simple OAuth Token Authorization

Prerequisites

- Cisco Jabber 10.6 or later. Jabber clients are the only endpoints supported for OAuth token authorization through Mobile and Remote Access (MRA).

- 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

How it works

Cisco Jabber determines whether it is inside the organization's network before requesting a Unified Communications service. If Jabber is outside the network, it requests the service from the Expressway-E on the edge of the network. If SAML SSO authentication 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 Unified Communications service trusts the IdP and the Expressway-E, so it provides the service to the Jabber client.

Figure 14: Simple OAuth token-based authorization for on-premises UC services
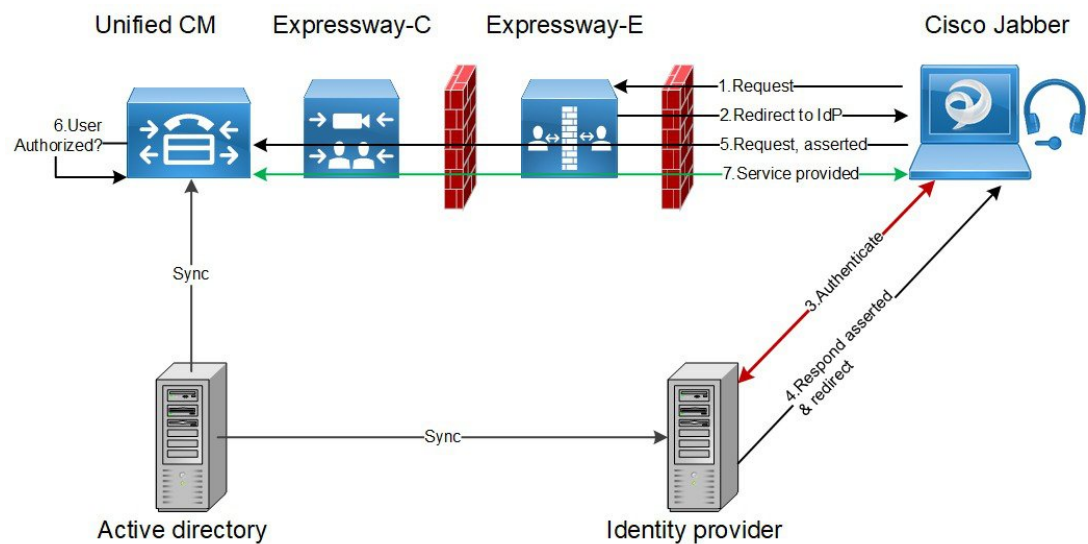
About Self-Describing OAuth Token Authorization with Refresh

Expressway supports using self-describing tokens as an MRA authorization option from X8.10.1. (Set **Authorize by OAuth token with refresh** to **Yes**.) Self-describing tokens offer significant benefits:

- Token refresh capability, so users do not have to repeatedly re-authenticate.

- Fast authorization.

- Access policy support. The Expressway can enforce MRA access policy settings applied to users on the Unified CM.

- Roaming support. Tokens are valid on-premises and remotely, so roaming users do not need to re-authenticate if they move between on-premises and off-premises.

Expressway uses self-describing tokens in particular to facilitate Cisco Jabber users. Jabber users who are mobile or work remotely, can authenticate while away from the local network (off-premises). If they originally authenticate on the premises, they do not have to re-authenticate if they later move off-premises. Similarly, users do not have to re-authenticate if they move on-premises after authenticating off-premises. Either case is subject to any configured access token or refresh token limits, which may force re-authentication.

For users with Jabber iOS devices, the high speeds supported by self-describing tokens optimize Expressway support for Apple Push Notifications (APNs).

We recommend self-describing token authorization for all deployments, assuming the necessary infrastructure exists to support it. Subject to proper Expressway configuration, if the Jabber client presents a self-describing token then the Expressway simply checks the token. No password or certificate-based authentication is needed. The token is issued by Unified CM (regardless of whether the configured authentication path is by external IdP or by the Unified CM). Self-describing token authorization is used automatically if all devices in the call flow are configured for it.

The Expressway-C performs token authorization. This avoids authentication and authorization settings being exposed on Expressway-E.

Prerequisites

- Expressway is already providing Mobile and Remote Access for Cisco Jabber.

- All other devices in the call flow are similarly enabled.

- You have the following minimum product versions installed, or later:

    - Expressway X8.10.1

    - Cisco Jabber iOS 11.9

        If you have a mix of Jabber devices, with some on an older software version, the older ones will use simple OAuth token authorization (assuming SSO and an IdP are in place).

    - Cisco Unified Communications Manager 11.5(SU3)

    - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)

    - Cisco Unity Connection 11.5(SU3)

- Make sure that self-describing authentication is enabled on the Cisco Expressway-C (**Authorize by OAuth token with refresh** setting) and on Unified CM and/or IM and Presence Service (**OAuth with Refresh Login Flow** enterprise parameter).

- You must refresh the Unified CM nodes defined on the Expressway. This fetches keys from the Unified CM that the Expressway needs to decrypt the tokens.

OAuth Token Prerequisites

This topic provides information on the prerequisites that your deployment must meet for OAuth tokens.

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 OAuth is configured on the Expressway-C.

- The Expressway-C has MRA enabled 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 to be accessed by OAuth are in the same deployment as the domain to be called from Jabber clients.

On 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-OAuth 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.

Identity Provider Selection

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

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. 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

Configure OAuth on UC Applications

To use OAuth authentication on Expressway with MRA, you must also have it enabled on your internal UC applications, such as Cisco Unified Communications Manager and Cisco Unity Connection (if it is deployed).

Step 1   On Expressway-C, verify that your MRA Access Control settings have OAuth token refresh enabled.

   a)   On Expressway-C, go to **Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**.
   b)   Check the **Authorize by OAuth token with refresh** check box.

c) Click **Save**.

Step 2 On the Cisco Unified Communications Manager publisher node, enable the **OAuth Refresh Login Flow** enterprise parameter:

a) From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

b) Set the **OAuth with Refresh Login Flow** parameter to **Enabled**.

c) Click **Save**.

Note When Expressway is configured with a different domain from CUCM, the CUCM admin needs to update Exp-C Hostname entry manually to FQDN, by appending the relevant system domain of Exp-C.

Step 3 On Cisco Unity Connection, enable OAuth Refresh Logins and then configure the Authz Server.

a) From Cisco Unity Connection Administration, choose **System Settings** > **Enterprise Parameters**.

b) Configure the settings under **SSO and OAuth Configuration**.

c) Set the **OAuth with Refresh Login** enterprise parameter to **Enabled**.

d) Click **Save**.

e) Choose **System Setting** > **Authz Server**.

f) Edit the existing configuration or add a new Authz server.

g) Add `CUCM Publisher` to the Authz server settings.

h) Click **Save**.

What to do next

If your system meets the necessary requirements, enable SIP OAuth Mode on Cisco Unified Communications Manager.

Configure SIP OAuth Mode

Use this procedure to enable SIP OAuth Mode on Cisco Unified Communications Manager. SIP OAuth Mode is recommended if you want secure SIP line signaling and your system supports it.

Note From X14.0 release, SIP OAuth Mode is supported for 7800 and 8800 series Cisco IP Phones. For more detailed information on SIP OAuth Mode, refer to the "Configure SIP OAuth Mode" chapter of *Feature Configuration Guide for Cisco Unified Communications Manager*.

Before you begin

OAuth Refresh Logins must be enabled on Cisco Unified Communications Manager. This is set with the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled**.

Step 1 For each server that uses SIP OAuth, set the SIP OAuth ports.

a) From Cisco Unified CM Administration, choose **System** > **Cisco Unified CM**.

b) Set the **TCP Port Settings**.

c) Click **Save**.

Step 2 Configure an OAuth Connection to Expressway-C:

a) From Cisco Unified CM Administration, choose **Device** > **Expressway-C**.

b) Click **Add New**.

c) Add the Expressway-C address

d) Click **Save**.

Step 3 Enable SIP OAuth Mode:

a) On the Unified CM publisher node, log in to the Command Line Interface.

b) Run the `utils sipOAuth-mode enable` CLI command.

Step 4 Restart the **Cisco CallManager** service:

a) From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**

b) From the **Server** drop-down list, select the server.

c) Check the **Cisco CallManager** service and click **Restart**.

d) Restart each node where endpoints register with SIP OAuth Mode.

Step 5 Enable OAuth Authentication within the Phone Security Profile.

a) From Cisco Unified CM Administration, choose **System** > **Security Profile** > **Phone Security Profile**.

b) Click **Find** and select the profile that is associated to your MRA endpoints.

c) Check the **Enable OAuth Authentication** check box.

d) If you are using ICE Media Path Optimization, set the **Device Security Mode** to **Encrypted** and **Transport Type** to **TLS**.

e) Click **Save**.

SAML SSO Configuration

Complete the following tasks if you want to configure SAML SSO in Cisco Expressway for Mobile and Remote Access.

Before you begin

• Configure SAML SSO for your internal UC applications. For details, see *SAML SSO Deployment Guide for Cisco Unified Communications Solutions*.

• Within the MRA Access Control settings on Expressway-C, the **Authentication path** field must be set to either **SAML SSO authentication** or **SAML SSO and UCM/LDAP**.

⚠️

Caution The following changes require the SAML metadata to be updated:

• Expressway change: Expressway-C certificate, FQDN, adding a cluster (send the metadata to be imported again)

• IDP change: FQDN, certificates, or anything that affect the trust relationship with the clients (reimport the latest metadata)

Procedure

	Command or Action	Purpose
Step 1	Export the SAML Metadata from the Expressway-C, on page 48	Export a metadata file from Expressway-C.
Step 2	Configure the Identity Provider	Import the Expressway metadata to the Identity Provider (IdP), configure the IdP and then export a metadata file from the IdP.
Step 3	Import the SAML Metadata from the IdP, on page 49	Import the Idp metadata to Expressway-C and complete the configuration.
Step 4	Associate Domains with an IdP, on page 49	In Expressway-C, associate the domain to the Identity Provider.
Step 5	Configure ADFS for SAML SSO, on page 50	ADFS only. If you're using is Active Directory Federation Services, complete these additional tasks on the IdP to complete the configuration.

Export the SAML Metadata from the Expressway-C

From X12.5, Cisco Expressway supports using a single, cluster-wide metadata file for SAML agreement with an IdP. Previously, you had to generate metadata files per peer in an Expressway-C cluster (for example, six metadata files for a cluster with six peers). For the cluster-wide option, run this procedure on the Expressway-C primary peer.

Note If you change any of the following Expressway settings in a SAML SSO deployment, you must re-export metadata from the primary peer and reimport metadata to the IdP:

- The primary peer

- The server certificates

- Any SSO-enabled domains

- The IP address or hostname of the Expressway-E peers

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

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

Step 2 In **MRA Access Control** section, choose a mode from the SAML Metadata list:

- **Cluster**: Generates a single cluster-wide SAML metadata file. You must import only this file to an IdP for the SAML agreement.

> • **Peer**: Generates the metadata files for each peer in a cluster. You must import each metadata file to IdP for the SAML agreement. The Peer option is selected by default when Expressway is upgraded from an earlier SAML SSO enabled release to 12.5.

For new deployments, the SAML Metadata mode always defaults to **Cluster**.

For existing deployments, the mode defaults to **Cluster** if SAML SSO was disabled in your previous Expressway release, or to **Peer** if SAML SSO was previously enabled.

Step 3 Click **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.

Step 4 If you choose **Cluster** for SAML Metadata, click **Generate Certificate**.

Step 5 Do the following:

> • On cluster-wide mode, to download the single cluster-wide metadata file, click **Download**.
> • On per-peer mode, to download the metadata file for an individual peer, click **Download** next to the peer. To export all in a .zip file, click **Download All**.

Step 6 Copy the resulting file(s) to a secure location that you can access when you need to import SAML metadata to the IdP.

Import the SAML Metadata from the IdP

Step 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.

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

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

Step 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.

Step 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**).

Associate Domains with an IdP

You need to associate a domain with an IdP if you want the MRA users of that domain to authenticate through 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.

Step 1   On the Expressway-C, 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.

Step 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.

Step 3   Check the boxes next to the domains you want to associate with this IdP.

If you see *(Transfer)* next to the check box, checking it breaks the domain's existing association and associates the domain with this IdP.

Step 4   Click **Save**.

The selected domains are associated with this IdP.

Configure ADFS for SAML SSO

If you are using Active Directory Federation Services (ADFS) for the Identity Provider, complete these additional configurations on ADFS.

After creating Relying Party Trusts for the Expressway-Es, you must set some properties of each entity, to ensure that Active Directory Federation Services (ADFS) formulates the SAML responses as Expressway-E expects them. In addition, you also need to add a claim rule, for each relying party trust,

Step 1   Configure ADFS to sign the whole response. In Windows PowerShell®, run the following command for each Expressway-E's <Name> once per Relying Party Trust created on ADFS:

`Set-ADFSRelyingPartyTrust -TargetName "<Name>" -SAMLResponseSignature MessageAndAssertion`where <Name> must be a display name for the Relying Party Trust of Expressway-E as set in ADFS.

Step 2   Add a Claim Rule for each relying party trust:
   a)   Open the **Edit Claims Rule** dialog and create a new claim rule that sends AD attributes as claims.
   b)   Select the AD attribute to match the one that identify the OAuth users to the internal systems, typically email or SAMAccountName.
   c)   Enter **`uid`** as the **Outgoing Claim Type**.

Configure Secure Traversal Zone

Configure an encrypted zone of type "Unified Communications traversal" on both Expressway-C and Expressway-E. Complete the procedure on both Expressway-C and Expressway-E.

✎

Note This configuration automatically sets up 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.

Before you begin

- Make sure that Expressway-C and Expressway-E trust each other's certificates. 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. For detailed information on certificate exchange requirements, see Certificate Requirements, on page 17.

- Be aware that Expressway uses the SAN attribute to validate received certificates, not the CN.

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

Step 1 On the Expressway-C primary peer, go to **Configuration** > **Zones** > **Zones**.

Step 2 Click **New**.

Step 3 Configure the fields in the below table. Apply the settings for the appropriate Expressway server (C or E).

Table 10: UC Traversal Zone Settings

Field	Expressway-C Settings	Expressway-E Settings
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**. In the popup dialog click **New** and enter the **Name** ("exampleauth") and **Password** ("ex4mpl3.c0m") and click **Create credential**.
SIP section		
Port	Must match the Expressway-E setting.	**7001** (default. See the *Cisco Expressway IP Port Usage Configuration Guide* , for your version, on the Cisco Expressway Series configuration guides page.)

Field	Expressway-C Settings	Expressway-E Settings
TLS verify subject name	Not applicable	Enter the name to look for in the traversal client's certificate (must be in the Subject Alternative Name attribute). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate.
Authentication section		
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. If you have configured Expressway-E with a dual NIC interface for MRA, enter the FQDN of Expressway-E's internal interface (not the IP address). Expressway-C requires a local DNS record that points to the FQDN of the Expressway-E's internal LAN.	Not applicable
Peer 2...6 address	Enter the FQDNs of additional peers if it is a cluster of Expressway-Es.	Not applicable

Step 4 Click **Create zone**.

Step 5 Repeat these steps on the Expressway-E primary peer, applying the settings in the Expressway-E column.

Secure Communications Configuration

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 hostname 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.

Media Encryption

ICE Media Path Optimization

ICE Media Path Optimization

From X12.5, we support Interactive Connectivity Establishment (ICE) Media Path Optimization. This feature optimizes the media path for MRA endpoints, letting MRA-registered endpoints pass media directly between the endpoints, thereby bypassing the WAN and the Expressway servers.

This feature uses the ICE protocol (RFC 5245). Background information about ICE is provided in the *About ICE and TURN Services* section of the *Cisco Expressway Administrator Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html.

How ICE Works

Before Cisco Expressway X12.5, ICE is supported only with the Cisco Expressway-C B2BUA as one of the ICE endpoints. When B2BUA acts as an endpoint, ICE candidates are negotiated between the endpoints and B2BUA. Therefore, the media always traverses through Cisco Expressway-E and Cisco Expressway-C.

The following figure shows an MRA call that does not use ICE to optimize the media path. The media traverses through both the Cisco Expressway-E and the Cisco Expressway-C.

Figure 15: MRA Call Flow without ICE Media Path Optimization
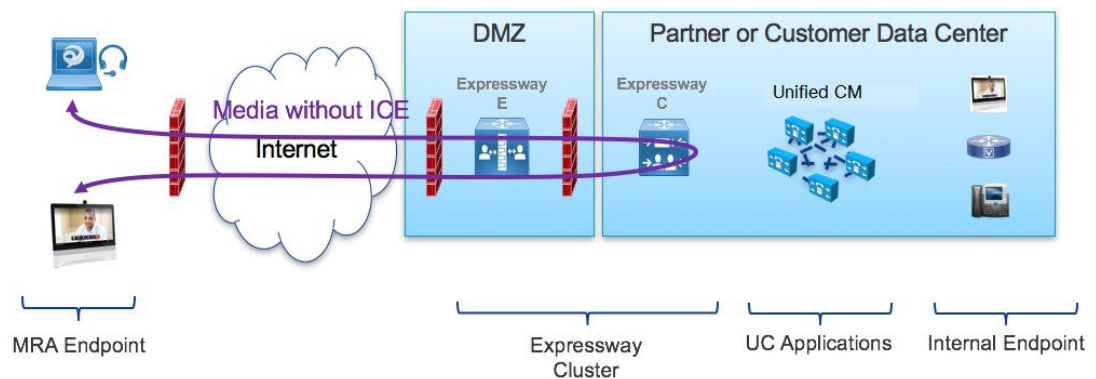
With ICE Media Path Optimization, introduced in Cisco Expressway X12.5, each endpoint can pass the ICE candidates to the other endpoint through zones that traverse the SIP signaling. As a result, endpoints use the ICE protocol to negotiate the most optimal path for media. The most optimal path may be one of the following:

- **Host address**—Represents the host IP address of the endpoint which is behind the NAT device.

- **Server-reflexive address**—Represents the publicly accessible address of the endpoint on the NAT device.

- **Relay address**—Represents the relay address of the endpoint configured on the TURN server.

In all ICE calls, initially media traverses through the Cisco Expressway-E and Cisco Expressway-C and then switches the media path depending on the negotiated ICE candidate type. This ensures that if endpoints are not ICE-capable, Cisco Expressway can use the legacy traversal path to pass media without disruption.

The following sections illustrate the MRA media path for each of the three ICE candidates.

MRA Call Flow with ICE using Host Address

The following figure shows an MRA call with ICE where the Host address is used to establish the media path. The media directly passes between the endpoints using the Host address, because the endpoints reside in the same network with no firewall between them.

Figure 16: MRA Call Flow with ICE using Host Address
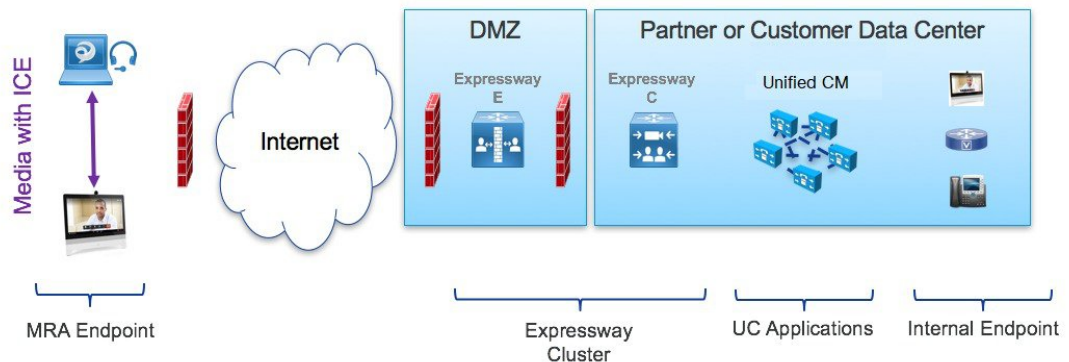
MRA Call Flow with ICE using Server Reflexive Addressing

The following figure shows an MRA call with ICE where both endpoints are behind different firewalls, thereby preventing the Host address from being used. Instead, the media passes between the endpoints using Server-reflexive addressing because the endpoints are behind different firewalls.

Figure 17: MRA Call Flow with ICE using Server Reflexive Addressing
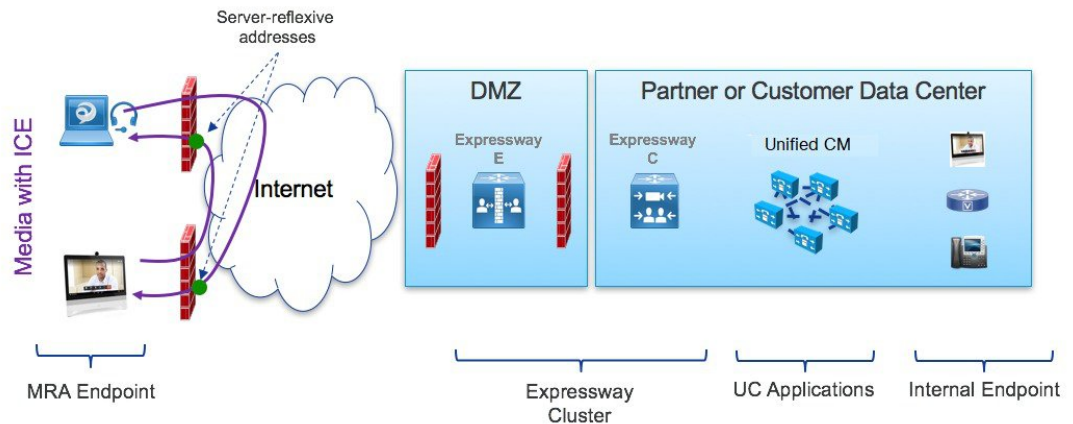
MRA Call Flow with ICE using Relay Address

In cases where the Host and Server-reflexive addresses cannot negotiate successfully, like deployments with a symmetric NAT, endpoints can utilize TURN Relay as the ICE optimized media path. The following figure shows an MRA call with ICE where endpoints use the Relay address of the Cisco Expressway TURN server to send media between endpoints.

Figure 18: MRA Call Flow with ICE using Relay Address
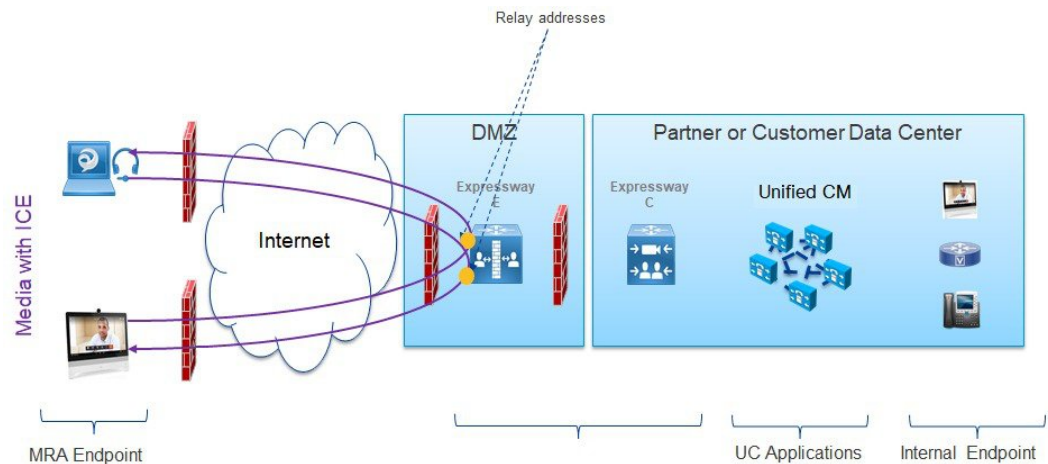
Signaling Path Encryption Between Expressway-C and Unified CM

Security and encryption are important factors when considering direct endpoint-to-endpoint messaging. Because MRA endpoints are sending signaling and media over the internet, they are forced to operate in encrypted mode. In normal MRA mode (without ICE), encryption is always required between the endpoint and the Expressway-C but optional between the Expressway-C and Unified CM. This is possible because the Expressway-C can terminate the media stream and decrypt the packets if the internal leg is unencrypted.

The following figure shows the encryption without ICE Passthrough where encryption is forced between MRA endpoints and Expressway-C, and optional in the internal network. On an MRA call, a different encryption

key is exchanged on each leg (Key 1 and Key 2), and the Expressway-C decrypts and re-encrypts the media between the 2 legs. The invite to Unified CM does not need a key if the internal leg is not encrypted.

Figure 19: Encryption without ICE Passthrough
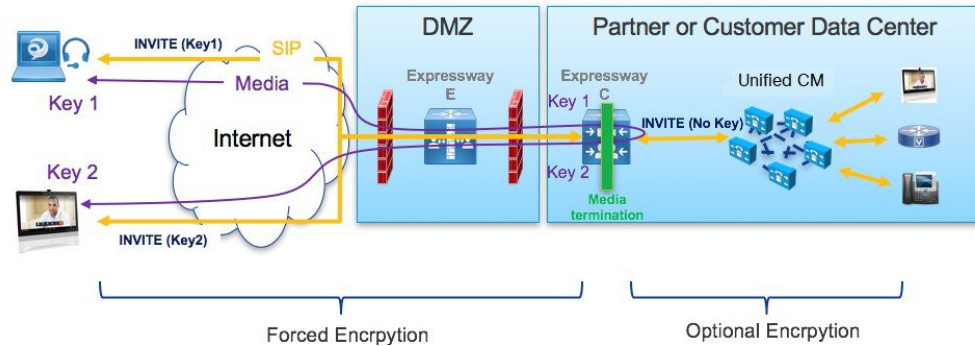
However, with ICE passthrough mode, the endpoints must be able to exchange their crypto keys end-to-end because the media packets are sent to each other directly and not through the Expressway-C. Whenever crypto keys are included in a SIP message, the message must be sent over TLS to protect the key. Because the SIP signaling path must be encrypted end-to-end to send the crypto keys end-to-end, the internal leg between the Expressway-C and Unified CM must be encrypted. If the signaling path is unencrypted, the crypto keys are dropped during call setup.

The following figure shows the encryption required with ICE Passthrough where the signaling leg between the Expressway-C and Unified CM is also encrypted.

Figure 20: Encryption with ICS Passthrough
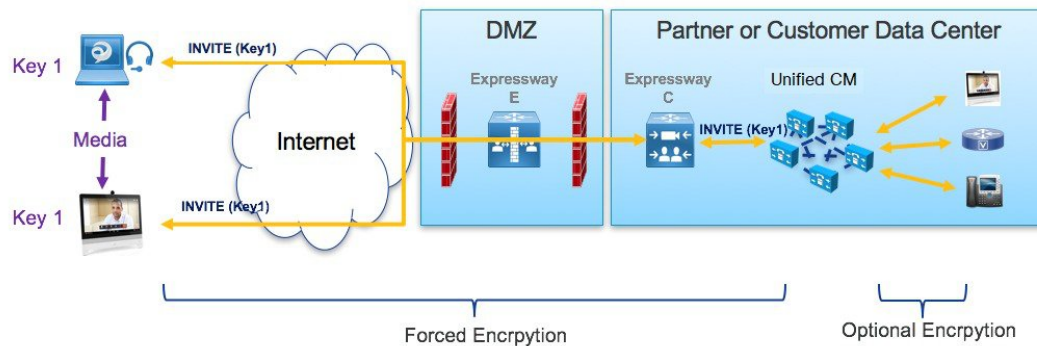
Supported Components

Cisco Expressway-based Deployments

Currently, ICE Media Path Optimization support exists only on MRA deployments. It is not tested and supported on the following service deployments:

- Cisco Webex Hybrid Services
- Jabber Guest
- Collaboration Meeting Room (CMR) Cloud

• Business to Business Calling

HCS Deployments

ICE passthrough can be used to optimize the media path of the MRA calls in the following HCS deployment types:

• HCS Shared Architecture

• HCS Dedicated Server and HCS Dedicated Instance

• Customer-owned Collaboration Architecture

Note HCS Contact Center does not support ICE passthrough.

Supported Components

ICE Media Path Optimization is supported with the following components:

• HCS 11.5 or later (for HCS deployments)

• Cisco Unified Communications Manager (Unified CM) 11.5 or later

• Cisco Expressway-C and Cisco Expressway-E X12.5 or later

Supported Endpoints

The following ICE-capable endpoints can send media directly to each other when they are MRA-registered and ICE Media Path Optimization is enabled:

• Cisco Jabber clients, version 12.5 or later subject to using Unified Communications Manager 12.5 or later

• Cisco IP Conference Phone 7832, version 12.5(1) or later

• Cisco IP Phone 7800 Series (MRA-compatible models only), version 12.5(1) or later

• Cisco IP Phone 8800 Series (MRA-compatible models only), version 12.5(1) or later

• Cisco TelePresence DX, MX, SX Series, CE version 9.6.1 or later

Prerequisites for ICE Media Path Optimization

The following Cisco Unified Communications Manager prerequisites exist when deploying MRA endpoints with ICE Media Path Optimization:

Secure Mode Must be Running on Unified CM

It's mandatory that one of the following secure modes be running on Cisco Unified Communications Manager:

- **SIP OAuth Mode** is recommended for those endpoints that support it. SIP OAuth Mode is supported for:

  - Cisco Jabber or Webex clients on Unified CM Release 12.5(x) or later

  - Cisco IP Phone 7800 or 8800 series on Unified CM Release 14 or later

- **Mixed mode** must be enabled if you are deploying SIP OAuth Mode over MRA with ICE and your endpoints do not support SIP OAuth Mode. This includes non-supported Cisco IP Phone or TelePresence devices. Mixed mode is also required for Cisco Jabber clients if you are not enabling SIP OAuth Mode, or if you are running a Unified CM release that is prior to 12.5(x).

  Mixed mode can be enabled by running the `utils ctl set-cluster mixed-mode` CLI command on the publisher node.

Phone Security Profile Must Include TLS Encryption

It's mandatory that all MRA endpoints that use ICE Media Path Optimization be associated to a TLS-encrypted Phone Security Profile. Within the Phone Security Profile, the following settings must exist:

- **Device Security Mode** is set to **Encrypted**

- **Transport Type** is set to **TLS**

- **Enable OAuth Authentication** is checked (if you are using SIP OAuth Mode) - CONFIRM

In addition, if mixed mode is enabled on Unified CM, the phone security profile name must be in the form of an FQDN.

Configuration

For details on how to configure SIP OAuth Mode, refer to the "SIP OAuth Mode" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

For details on how to configure mixed mode and a TLS-encrypted phone security profile, see the *Security Guide for Cisco Unified Communications Manager*.

ICE Media Path Optimization Task Flow

Complete the following tasks to configure ICE Media Path Optimization for your MRA deployment.

Procedure

	Command or Action	Purpose
Step 1	Configure ICE Settings, on page 61	On Unified CM, configure ICE settings that you can apply to MRA endpoints.
Step 2	Install Server Certificates, on page 62	On Expressway-C, install appropriate server certificates and trusted CA certificates.
Step 3	Change CEtcp Neighbor Zones to CEtls Neighbor Zones, on page 62	On Expressway-C, change the existing CEtcp neighbor zone to a CEtls neighbor zone.

	Command or Action	Purpose
Step 4	Set Up the UC Traversal Zone for ICE Passthrough Support, on page 63	On Expressway-C, set up the UC traversal zone for MRA.
Step 5	Set Up the UC Neighbor Zone for ICE Passthrough Support, on page 63	On Expressway-C, set up the UC neighbor zone for MRA.
Step 6	Use CLI to Configure ICE Passthrough on Cisco Expressway Zones, on page 63	On Expressway-C, configure ICE Media Path Optimization for the UC and CEtls neighbor zones.
Step 7	Set Up Cisco Expressway-E as TURN Server, on page 64	On Expressway-E, configure TURN relay services.

Configure ICE Settings

On Cisco Unified Communications Manager, configure ICE settings within a Common Phone Profile, which you can apply to a group of MRA phones that use the profile.

Note As an alternative to using a Common Phone Profile, ICE settings can be applied in any of the below Unified CM configuration windows as a part of the Product-Specific Configuration Layout. If conflicting configurations exist, the prioritized order below determines which configuration gets applied to the phone:

1. Phone Configuration—Configure ICE settings on a phone-by-phone basis

2. Common Phone Profile Configuration—Configure ICE settings to be applied to a group of phones that use the profile.

3. Enterprise Phone Configuration—Configure ICE settings that are applied cluster-wide to phones that use those settings.

Regardless of which configuration window you use, by default ICE is **Enabled** with **Host** as the default candidate, and Server Reflexive addressing also being **Enabled**. However, to use Expressway-E relayed TURN services you must specify the Expressway-E server in the ICE settings of one of these windows.

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Do either of the following:

- Click **Add New** to create a new profile.
- Click **Find** and select an existing profile. For example, the default Standard Common Phone Profile, which is assigned to new phones by default.

Step 3 Under **Interactive Connectivity Establishment (ICE)**, configure the following ICE settings:

- **ICE**—Make sure this is set to Enabled.
- **Default Candidate Type**—**Host** is recommended.
- **Server Reflexive Address**—Make sure this is set to **Enabled**
- **Primary TURN Server Host Name or IP Address**—Enter the FQDN of an Expressway-E node to act as the primary TURN server.
- **Secondary TURN Server Host Name or IP Address**—Enter the FQDN of an Expressway-E node to act as the secondary TURN server.

> • **TURN Server Transport Type**—**Auto** is recommended.
> • **TURN Server Username**—Enter a username that can access the Expressway-E server.
> • **TURN Server Password**—Enter the password for the user whom can access Expressway-E.

Step 4 Click **Save**.

Step 5 To apply the profile to a phone, do the following:

a) Choose **Device** > **Phone**.
b) Click **Find** and select the phone to which you want to apply the profile.
c) Select the **Common Phone Profile** that you created.
d) Click **Save**.

Install Server Certificates

This procedure describes how to install server certificates.

Step 1 Generate a new CSR for the server certificate (**Maintenance** > **Security** > **Server Certificate**).

For more information, see the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

Step 2 While generating the CSR, include the name of the phone security profile that you have associated with the endpoints in the Subject Alternate Names (SAN).

For more information, see CSR Requirements for Expressway Servers, on page 20.

Step 3 Install the server certificate that is signed from the trusted certificate authority on Cisco Expressway-C.

This certificate allows the endpoints using the phone security profile to register over the TLS connection between Cisco Expressway-C and Unified CM.

Change CEtcp Neighbor Zones to CEtls Neighbor Zones

On Cisco Expressway-C, change the existing CEtcp neighbor zones that are already configured for MRA to CEtls neighbor zones.

Before you begin

Make sure that Unified CM is in a secure mode with one of the following modes being enabled:

> • Mixed Mode
>
> • SIP OAuth Mode

Step 1 Go to **Configuration** > **Unified Communications** > **Unified CM servers**.

Step 2 Select the Unified CM Servers that you already discovered and click **Refresh Servers** to update the configuration.

Step 3 Verify that the Unified CM status shows *TLS: Active*.

If there is not already a CEtcp neighbor zone created, you may need to add your Unified CM servers and then refresh servers. Go to Add Unified CM Cluster, on page 35.

Cisco Expressway-C automatically generates non-configurable CEtls neighbor zones between itself and each discovered Unified CM node if Unified CM cluster is in Secure mode. For more information, see Automatically Generated Zones and Search Rules, on page 36.

Set Up the UC Traversal Zone for ICE Passthrough Support

This procedure describes how to set up the UC Traversal Zone for ICE passthrough support.

Step 1 In Cisco Expressway-C, go to **Configuration** > **Zones** > **Zones**.

Step 2 Choose the Unified Communications traversal zone to Cisco Expressway-E.

Step 3 In the SIP pane, set **ICE Passthrough support** to *On* and **ICE Support** to *Off*.

Note ICE Passthrough support takes precedence over ICE Support. Best practice is to turn on ICE Passthrough support and turn off ICE support.

Set Up the UC Neighbor Zone for ICE Passthrough Support

This procedure describes how to set up the UC Neighbor Zone for ICE passthrough support.

Step 1 In Cisco Expressway-C, go to **Configuration** > **Unified Communications** > **Unified CM Servers**.

Step 2 Choose a server.

Step 3 In the Unified CM server lookup pane, set **ICE Passthrough support** to *On*.

Use CLI to Configure ICE Passthrough on Cisco Expressway Zones

The ICE Passthrough option in Cisco Expressway is a per-zone setup. You must enable ICE Passthrough on each Unified CM traversal client zone and CEtls neighbor zone.

You can use the CLI, instead of the web interface, to configure zones for ICE Passthrough.

Step 1 Go to **Configuration** > **Zones** and click the Unified CM Traversal zone to Cisco Expressway-E.

Step 2 In the URL, note the ID of the zone. For example, in the following URL, 4 is the zone ID.

```
https://expressway.example.com/editzone?id=4
```

Step 3 Repeat steps 1 and 2 for the CEtls neighbor zone.

Step 4 Log in to the CLI of the Cisco Expressway-C as administrator.

Step 5 Run the following command to enable ICE Passthrough on Unified CM traversal client zone:

```
xConfiguration Zones Zone <Unified Communication Traversal client zone ID> TraversalClient SIP Media
 ICEPassThrough Support: On
```

Step 6 Run the following command to enable ICE Passthrough on the CEtls neighbor zone:

```
xConfiguration Zones Zone <CEtls Neighbor zone ID> Neighbor SIP Media ICEPassThrough Support: On
```

Set Up Cisco Expressway-E as TURN Server

You can use the Cisco Expressway-E server where the TURN server is running to allocate relay address and to retrieve the server reflexive address. This is typically a Cisco Expressway-E in the cluster used for MRA, but it is not required to be a Cisco Expressway-E server. You can use any compliant TURN server.

The following steps summarize the configuration required on the Cisco Expressway-E TURN server:

Step 1 Configure the TURN server (**Configuration** > **Traversal** > **TURN**) with the following settings:

- **TURN services**: Set to *On*.

- **TCP 443 TURN service**: Set to *Off*.

- **TURN port multiplexing**: Set to *Off*. This option is available only on Large system.

- **TURN requests port**: Retain the default values. On Small and Medium systems, the default port is 3478. On Large systems, the default port range is 3478 to 3483.

  Note   On a Large system, the **TURN request port** field is available only if **TURN port multiplexing** is set to *On*.

- **TURN requests port range start**: Retain the default values.

- **TURN requests port range end**: Retain the default values.

  Note   The **TURN requests port range start** and **TURN requests port range end** options are available only on Large systems and if **TURN port multiplexing** is set to *Off*.

- **Delegated credential checking**: Retain the default values.

- **Authentication realm**: Retain the default value. The default value is TANDBERG.

- **Media port range start**: Retain the default value. The default value is 24000.

- **Media port range end**: Retain the default value. The default value is 29999.

Step 2 Configure the credentials (**Configuration** > **Authentication** > **Devices** > **Local database**) for TURN clients to authenticate with the TURN server.

Step 3 Click **Save**.

Step 4 Verify if the TURN server status is changed to *Active* under **TURN server status**.

For more information on the steps to configure TURN services on Cisco Expressway-E, see *Configuring TURN Services* section in the *Cisco Expressway Administrator Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

ICE Passthrough Metrics Use

This section describes how to work with metrics for ICE passthrough in Cisco Expressway:

- View ICE Passthrough Metrics in Cisco Expressway-C
- Use the collectd Daemon to Gather Metrics
- View Call Types in the Call History
- Bandwidth Manipulation

View ICE Passthrough Metrics in Expressway-C

In Expressway-C, you can view metrics data for completed ICE passthrough calls. Various metrics are available for each server that is configured to route ICE passthrough calls. Values are updated once every 24 hours.

Figure 21: Metrics Example

- The **Peer** field shows the IP address or hostname of each node.

- The most recent 24-hour interval of data is shown.

- Each peer address is a link that takes you to the history for that node.

- The interval start time reflects the time of day of the most recent server restart.

- Each column shows information for a separate cluster.

Step 1 In Expressway-C, go to **Status** > **ICE Passthrough metrics**.

The page is organized into these sections:

- **Metrics**: For each peer, the time interval for which metrics are shown. For this interval, the number of B2BUA connected calls, the number of ICE calls, and the percentage of ICE vs total B2BUA calls. N/A values result when no ICE calls were processed during this 24-hour interval.

- **Call types**: For each call type, the percentage of placed ICE calls with each call type.

- **Advanced**: Other metrics that can help with troubleshooting.

Step 2 For a detailed description of any field, click the **i** icon next to the field name.

Step 3 To sort, click a column name and then the **Up** or **Down** arrow, to sort the data by that column.

Step 4 Click **Export to CSV** to create a spreadsheet of the values on the page you are displaying.

Step 5 Click the IP address or hostname for a cluster to display the **ICE Call Metrics History** page, which shows a history of values for that cluster.

- Each column shows a separate parameter.

- Each row shows the values for a different interval, with the most recent shown first.

- Each value is a raw value, not a percentage.

- The page can display up to 60 records (that is, the 60 most recent 24-hour intervals).

Metric Collection with the collectd Daemon

As an alternative to viewing metrics for ICE passthrough calls, you can use the *collectd* daemon to gather the metrics. Details about setting up the server for collection are in the *Cisco Expressway Serviceability Guide* on the Expressway Maintain and Operate Guides page, in the "Introducing System Metrics Collection" section.

View Call Types in the Call History

For ICE passthrough calls, the call type is shown in the call history.

Step 1 In Cisco Expressway-C, navigate to **Status** > **Calls** > **History**.

Step 2 Choose one of the following actions.

- Click the value in the **Start time** column to view the call detail record (CDR).

- Choose View in the **Actions** column.

Step 3 Examine the value in the **ICE Passthrough call type** field.

Possible values are:

- *none*: Indicates optimized media path was not used for the call. The call is processed and connected using Cisco Expressway B2BUA.

- *host_to_host*: Indicates optimized media path for the call was established using the host addresses of the endpoints.

- *host_to_srvrflx*: Indicates optimized media path for the call was established between the host address of one of the endpoints and the server-reflexive address of the other endpoint.

- *host_to_relay*: Indicates optimized media path for the call was established between the host address of one of the endpoints and the TURN relay address of the other endpoint.

- *srvrflx_to_srvrflx*: Indicates optimized media path for the call was established using the server-reflexive addresses of the endpoints.

- *srvrflx_to_relay*: Indicates optimized media path for the call was established between the server-reflexive address of one of the endpoints and the TURN relay address of the other endpoint.

- *relay_to_relay*: Indicates optimized media path for the call was established using the relay addresses of the endpoints.

Step 4 (Optional) To view the details of the B2BUA call leg, choose the call leg that shows the B2BUA type in the **Call components** section.

Bandwidth Manipulation

When ICE is negotiated, media moves off the Cisco Expressway, which results in a reduction in media bandwidth. When the **Status** > **Bandwidth** > **Links** page displays current bandwidth, the total current usage reflects less utilization when ICE is in use.

Note Bandwidth usage does not include the bandwidth that the TURN server uses.

Features and Additional Configurations

After you have completed the basic setup for Mobile and Remote Access, use this chapter to configure features and optional configurations for MRA.

Deployment Partitions

A deployment is an abstract boundary that is 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.

Deployments and their associated domains and services are configured on the Expressway-C.

One primary deployment (called "Default deployment" unless you rename it) 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.

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 22: Multiple Deployments to Partition Unified Communications Services Accessed from Outside the Network
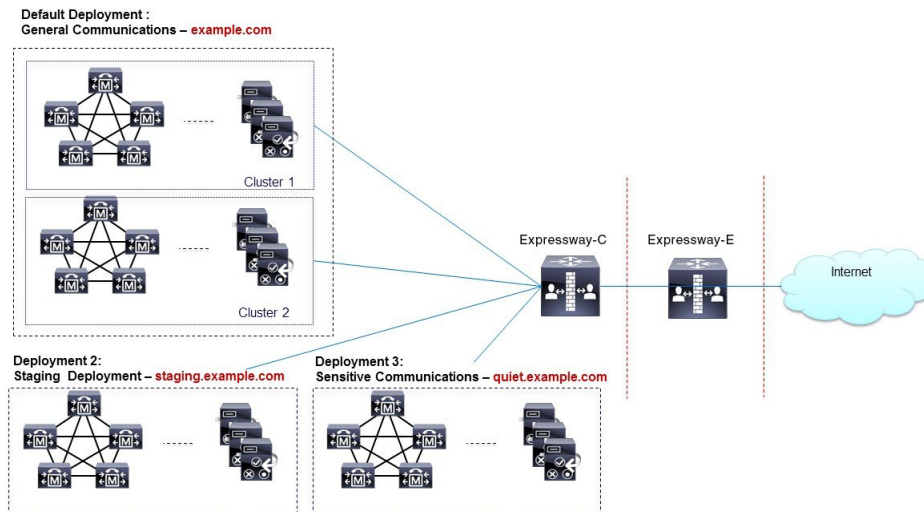
Assign Deployment Partitions for UC Services

Use this optional procedure if you have multiple internal UC clusters and you want to partition internal UC services by creating a boundary. One example where this might be useful is if you have a cluster for enterprise UC services and a second staging cluster.

> **Note** If you don't create any new deployments, then all internal UC applications belong to a single enterprise-wide Default Deployment.

Step 1 On Expressway-C, create your deployments:

a) Go to **Configuration** > **Unified Communications** > **Deployments** and click **New**.

b) Create the new deployment.

c) Repeat for each deployment that want to add.

Step 2 Assign UC domains to your deployments:

a) Go to **Configuration** > **Domains**.

b) Select the domain that you want to assign.

c) Select the **Deployment** that you want to assign to this domain.

d) Click **Save.**

e) Repeat this step to assign deployments to additional domains.

Step 3   Assign UC Services to your Deployments:

a)   Go to **Configuration** > **Unified Communications** and select the relevant UC application.

b)   Select the server that you want to assign.

c)   In the **Deployment** field, select the deployment you want to assign.

d)   Click **Save**.

e)   Repeat for each node on each UC cluster.

Push Notifications over MRA

If your MRA deployment includes Cisco Jabber or Webex clients that run on iOS or Android devices, you must deploy Push Notifications. Without Push Notifications, your system may not be able to send calls or messages to clients that have entered into background mode.

How Push Notifications Work

When your cluster is enabled for Push Notifications, Cisco Unified Communications Manager and the IM and Presence Service use either the Apple or Google cloud's Push Notification service to send push notifications for calls and messages to Cisco Jabber or Webex clients that run on iOS or Android devices. Push Notifications let your system communicate with the client, even after it has entered into background mode (also known as suspended mode). Without Push Notifications, the system may not be able to send calls or messages to clients that have entered into background mode.

At startup, mobile and remote Cisco Jabber or Cisco Webex clients that are installed on Android and iOS platform devices register to Cisco Unified Communications Manager and the IM and Presence Service via Expressway-E. So long as the client remains in foreground mode, new calls or messages can be sent to the client via Expressway-E. However, once the client moves to background mode, standard communication channels are unavailable. Push Notifications provides an alternative channel to reach the client via the appropriate partner cloud (Apple or Google).
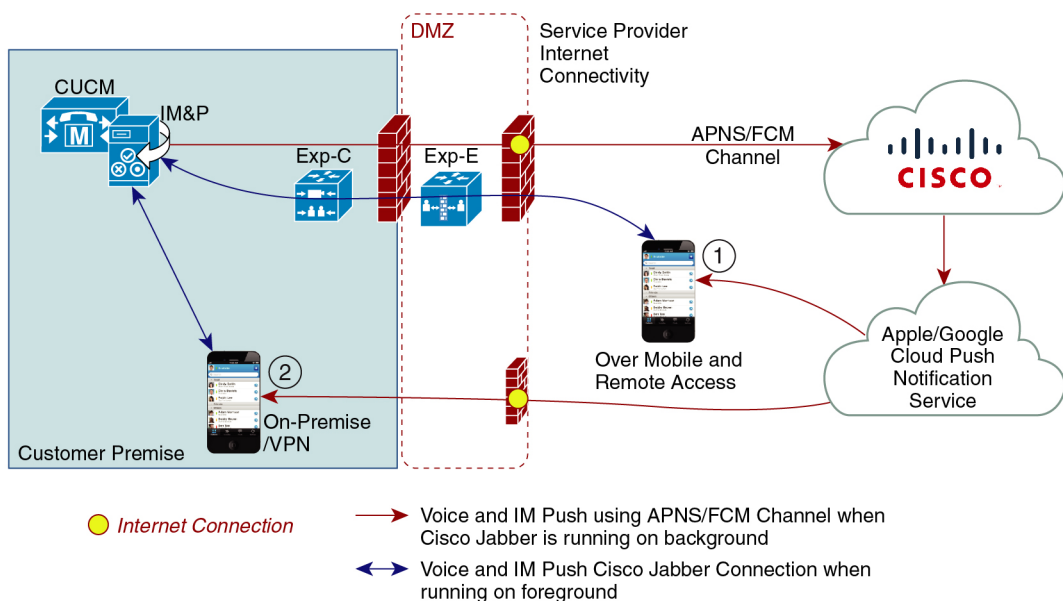
Push Notifications Requirements

No specific configuration is needed on the Expressway for Push Notifications, assuming Expressway-E is already providing Mobile and Remote Access (MRA) for Jabber iOS devices. However, these prerequisites and recommendations apply:

- Push Notifications in the Expressway require a network connection between Cisco Jabber and the Push Notification servers in the Apple cloud.

  They cannot work in a private network, with no internet connection.

- Expressway is already providing Mobile and Remote Access for Jabber for iPhone and iPad. MRA must be fully configured (domain, zone, server settings).

- Depending on your Unified CM configuration, you may need a forward proxy to send Push Notifications to the Cisco Collaboration Cloud.

- We recommend using self-describing token authorization.

- Expressway-E restart required for Push Notifications with instant messages. After you enable Push Notifications on the IM and Presence Service you need to restart the Expressway-E. Until the restart, Expressway-E cannot recognize the push capability on IM and Presence Service and does not send PUSH messages to the Jabber clients.

Configure Push Notifications for MRA

The following requirements exist when deploying Push Notifications over MRA:

- OAuth token validation must be configured on Expressway.

- Unified CM must be configured to use a forward proxy server for HTTPS connections to Cisco cloud services.

Note The former built-in forward proxy in Expressway is removed from the product in X12.6.2 and later versions. For earlier Expressway versions, the built-in forward proxy is not supported and should not be used.

For detailed procedures, see Push Notifications Deployment Guide.

Enable Push Notifications for Android Devices

This feature is enabled through the Expressway command line interface.

The CLI command to enable PUSH for Android over MRA: **xConfiguration XCP Config FcmService: On**

Note
- Perform this **only** if all IM and Presence Service nodes that service Android users are also running a supported release.

- This feature must be turned on Expressway-E only.

- IM and Presence services for users who are currently signed in over MRA will be disrupted when this command is used, so those users will need to sign in again.

The table gives a perspective of Expressway CLI enable/disable command for Android Push Notification. Administrators can decide whether they should turn the CLI command *On* or *Off*.

Table 11: Solution Matrix

Mixed version IM&P clusters	Expected status of FCM flag on Expressway X12.7	Comment
Any 11.5(1) SU with 12.5(1) SU2 (and lower)	OFF	Android push (FCM) NOT supported
11.5(1) SU8 (and lower) OR 12.5(1) SU2 (and lower) with 12.5(1) SU3	OFF	Android push (FCM) NOT supported
11.5(1) SU8 (and lower) OR 12.5(1) SU2 (and lower) with 12.5(1) SU4 (and higher)	OFF	Android push (FCM) supported on 12.5(1) SU4 (and higher) version
11.5(1) SU9 (and higher) OR 12.5(1) SU4 (and higher) with 12.5(1) SU3	ON	Android push (FCM) supported on all 12.5(1) versions
11.5(1) SU9 (and higher) with 12.5(1) SU4 (and higher)	Flag not required (Expressway X12.7 relies fully on new discovery mechanism)	Android push (FCM) supported on 12.5(1) SU4 (and higher) version

Fast Path Registration

Configure Fast Path Registration

When Fast Path Registration is enabled, Expressway caches the initial routing calculation and then uses a Pre-Routed Route Header to route subsequent packets using the cached routing result. This feature reduces the server workload, leading to increased capacities.

On Expressway-E, set both the Digest Cache Interval and Digest Cache Lifetime to 7200 with the following commands:

- `xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: "7200"`
- `xConfiguration Authentication Remote Digest Cache Lifetime: "7200"`

Enable SIP Path Headers

The default setting for Expressway-C is to rewrite the Contact header in SIP REGISTER messages. When you enable SIP Path Headers, Expressway-C adds its address into the Path header but does not rewrite the Contact header. This setting is required for some features to work over MRA, including:

- Shared Lines and Multiple Lines
- BiB Call Recording
- Silent Monitoring
- Key Expansion Modules

Note It's recommended that you deploy a minimum Unified CM release of 11.5(1)SU4. For details, see CSCvd84831.

Step 1 On Expressway-C turn on SIP Path headers:

a) On Expressway-C go to **Configuration** > **Unified Communications** > **Configuration**.
b) Set **SIP Path headers** to **On**.
c) Click **Save**.

Step 2 After saving your settings, refresh Unified CM Servers:

a) Go to **Configuration** > **Unified Communications** > **Unified CM Servers**.
b) Click **Refresh Servers**.

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 callers or endpoints registered to Expressway to call 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.

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

See Cisco Expressway SIP Trunk to Unified CM Deployment Guide for more information about configuring a SIP trunk.

See Configure OAuth on UC Applications, on page 45 for information on how to configure OAuth-based authorization for SIP trunks.

Configure SIP Ports for Trunk Connections

If you have configured a SIP trunk between Expressway and Cisco Unified Communications Manager, use this procedure to configure the port settings that the trunk uses.

Step 1   Configure SIP line registration listening ports on Unified CM:

a)   From Cisco Unified CM Administration, choose **System** > **Cisco Unified CM**.
b)   Set the **SIP Phone Port** to **5060**.
c)   Set the **SIP Phone Secure Port** to **5061**.
d)   Click **Save**.

Step 2   Configure SIP trunk listening ports on Unified CM:

a)   From Cisco Unified CM Administration, choose **System** > **Security** > **SIP trunk Security Profile**.
b)   Click **Find** and select the profile that you are using for the SIP trunk.
c)   Configure the **Incoming Port** to be different from the Line ports.
d)   Click **Save** and then click **Apply Config**.

Step 3   Configure SIP trunk listening ports on Expressway:

a)   On Expressway-C, go to **Configuration** > **Zones** > **Zones**
b)   Select the Unified CM neighbor zone that is used for the SIP trunk.
c)   Set the **SIP Port** to the same value as the **Incoming Port** that was configured in the SIP Trunk Security Profile.
d)   Click **Save**.

BiB Recording over MRA

The Expressway supports Built-in-Bridge (BiB) recording over MRA. This feature can help organizations to comply with the phone recording requirements of the European Union's Markets in Financial Instruments Directive (MiFID II).

How it Works

- BiB can be used to record the audio portion of calls that are made or received by users working off-premises.

- BiB is always enabled on the Expressway.

- BiB is configurable on Cisco Unified Communications Manager. When BiB is enabled, Unified CM forks the call to and from the endpoint to a media recording server.

Bandwidth and Capacity Requirements

If you plan to use this feature, be aware that it has significant impact on bandwidth and call capacity:

- It requires additional network bandwidth to be provisioned. Details are provided in the "Capacity Planning for Monitoring and Recording" section of the Cisco Collaboration System 12.x Solution Reference Network Designs (SRND). Enabling BiB for MRA endpoints typically needs double bandwidth as, assuming both sides of the call are recorded, each BiB-enabled call consumes double the usual bandwidth.

- Enabling BiB on MRA endpoints reduces the overall call capacity of Expressway nodes down to approximately one-third of their original capacity. This is because each call that is being recorded has two additional SIP dialogs associated with it (so essentially equivalent to three calls).

Configuration Requirements

To deploy BiB Recording over MRA, configure the following:

- BiB Recording must be configured on Cisco Unified Communications Manager. For detailed procedures, see the "Call Recording" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

- SIP Path Headers must be enabled on Expressway. For details, see Enable SIP Path Headers, on page 74.

In addition, the following requirements must be met:

- Compatible clients are required:

    - Cisco Jabber for Windows 11.9

    - Cisco Jabber for Mac 11.9

    - Cisco Jabber for iPhone and iPad 11.9

    - Cisco Jabber for Android 11.9

    - Cisco IP Phone 7800 Series, Cisco IP Conference Phone 7832, or Cisco IP Phone 8800 Series devices which support MRA (not all these phones are MRA-compatible)

- The phones which currently support MRA are listed in the MRA Infrastructure Requirements section of this guide or ask your Cisco representative for details.

- Registrar/call control agent: Cisco Unified Communications Manager 11.5(1)SU3 BiB is not supported on Expressway-registered endpoints.

- Edge traversal: Expressway X8.11.1 or later

- Recording server: Out of scope for this document. (Information about configuring recording for Cisco Unified Communications Manager is available in the *Feature Configuration Guide for Cisco Unified Communications Manager*.)

HTTP Allow List

The HTTP Allow list is a type of access list for HTTP services. Expressway-C adds both inbound and outbound rules automatically. For example, Expressway adds inbound rules automatically that allow external clients to access the Unified Communications nodes that were discovered during MRA configuration. These include Unified CM nodes (running CallManager and TFTP service), IM and Presence Service nodes, and Cisco Unity Connection nodes.

However, in some cases, you may need to edit the inbound rules to allow certain types of access. You cannot edit outbound rules.

- To view Inbound rules, go to **Configuration** > **Unified Communications** > **HTTP allow list** > **Automatic inbound rules**.

- To view Outbound rules, go to **Configuration** > **Unified Communications** > **HTTP allow list** > **Automatic outbound rules**.

Editing the HTTP Allow List

You can add your own inbound rules to the HTTP Allow List if remote clients need to access other web services inside the enterprise. For example, these services may require you to configure the allow list:

- Jabber Update Server

- Cisco Extension Mobility

- Directory Photo Host

- Managed File Transfer

- Problem Report Tool server

- Visual Voicemail

<link to Appendix and other places for more info>

You can't add outbound rules to the HTTP Allow List. In addition, you can't edit or delete auto-added rules in the list.

Note For the Managed File Transfer feature to work across Expressway, make sure that all Unified CM IM and Presence Service nodes appear on the allow list, whether manually or automatically added.

Automatic Inbound 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 12: 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.
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 (such as **GET**).

Edit the HTTP Allow List

Step 1 Go to **Configuration** > **Unified Communications** > **HTTP allow list** > **Editable inbound 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.

Step 2 (Optional) Use the check boxes 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.

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

Step 3 [Recommended] Delete any rules you don't need by checking the boxes in the left column, then clicking **Delete**.

Step 4 Click **New** to create a rule.

Step 5 Configure the rule to your requirements.

Here is some advice for each of the fields.

Table 13: 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 can access. For example, to allow access to `http://www.example.com:8080/resource/path`, just type it in exactly like that. • The protocol the clients are using to access the host must be http:// or https:// • Specify a port when using a non-default port, for example, :8080 (Default ports are 80 (http) and 443 (https)) • Specify the path to limit the rule scope (more secure), for example, /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.

Step 6 Click **Create Entry** to save the rule and return to the editable allow list.

Step 7 (Optional) Click **View/Edit** to change the rule.

Upload Rules to the HTTP Allow List

✎

Note   You cannot upload outbound rules.

Step 1   Go to **Configuration** > **Unified Communications** > **HTTP allow list** > **Upload rules**.

Step 2   Browse to and select the CSV file containing your rule definitions.

See Allow List Rules File Reference, on page 123.

Step 3   Click **Upload**.

The Expressway responds with a success message and displays the **Editable inbound rules** page.

Dial via Office Reverse over MRA

Mobile workers need the same high quality, security, and reliability as when they place calls in the office. You can assure them of 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. 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).

Call Flow Examples for DVO-R over MRA

The following call flow describes a Dial via Office Reverse over MRA call when you are sending the return call to either a mobile identity or an alternate number. Refer to the subsequent images for illustrations of the call flow.

1. When you dial a number, a signal is sent to Cisco Unified Communications Manager over the IP path (WLAN or mobile network).

2. Cisco Unified Communications Manager calls your mobile number or the Alternate Number that you set.

3. When you answer, Cisco Unified Communications Manager extends the call to the number you dialed, and you hear ring back.

4. When the person answers, the ongoing call is hairpinned at the enterprise PSTN gateway and the following occurs:

   • With 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.

   • With an alternate number, your ongoing call is not anchored, and you cannot pick up on your desk phone.

Figure 23: DVO-R over MRA with Mobile Identity
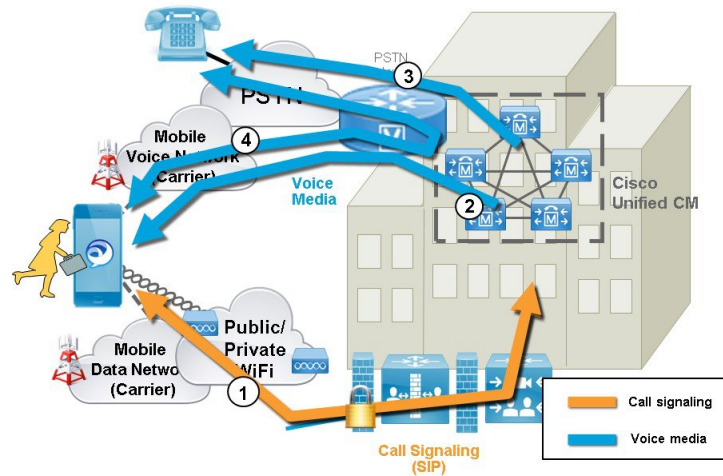

Figure 24: DVO-R over MRA with Alternate Number
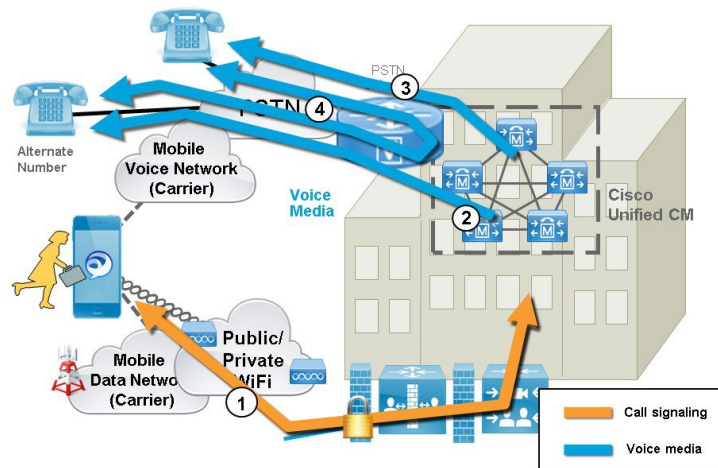
DVO Requirements

This feature requires the following versions of related systems:

   • Cisco Unified Communications Manager 11.0(1) or later

   • Cisco Jabber 11.1 or later

Additional Notes

- 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.

Configure Dial via Office-Reverse over MRA

There is no Expressway configuration requirement to make DVO-R work over MRA. However, there is configuration that is required on the Unified CM nodes and Cisco Jabber clients. The high-level configuration is as follows:

Step 1 Set up Cisco Unified Communications Manager to support DVO-R.

Step 2 Set up DVO-R for each device.

Step 3 Set up user-controlled voicemail avoidance.

Step 4 Add Remote Destination (optional).

Step 5 Configure Cisco Jabber client settings.

Note For a detailed configuration example that describes how to configure your UC applications and clients to make Dial via Office-Reverse to work over Mobile and Remote Access, see *Configuring Dial via Office-Reverse to Work with Mobile and Remote Access* at https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/200198-Configuring-Dial-via-Office-Reverse-to-W.html.

Multi-cluster Best Practices

This section outlines tips and best practices for configuring multi-cluster MRA Deployments. Following are some Best Practices to keep in mind when configuring multi-cluster MRA deployments:

- Every Expressway-C cluster must be able to connect to every UC cluster. Otherwise, Expressway-C can't proxy requests to all the UC clusters. On the primary peer of each Expressway-C cluster, add the publisher node for each UC cluster that Expressway-C must reach and then refresh servers. This will populate Expressway-C with the remaining subscriber nodes from the various UC clusters.

- If some clusters are sharing SIP domains: you must enable the **Home Cluster** setting for each user so that each user is assigned to a specific cluster. This setting appears in the **End User Configuration** window of Cisco Unified Communications Manager.

- If you have multiple Unified CM clusters within the same domain, the Intercluster Lookup Service (ILS) is recommended, particularly for large intercluster networks. After an initial setup, ILS provides automatic Cluster Discovery and dial plan replication across the ILS network. However, note that ILS is not

mandatory as you can configure cluster discovery manually. For details on how to configure an ILS network, see the *System Configuration Guide for Cisco Unified Communications Manager*.

- If you have multiple IM and Presence Service clusters within the same domain, you must configure intercluster peering with the Intercluster Sync Agent (ICSA) for the IM and Presence clusters that are in the same domain. For details on how to configure intercluster peering, see the *Configuration and Administration Guide for the IM and Presence Service*.

- If you have multiple edge clusters, configure load balancing between them:

  - If those edges are in same datacenter, you can use DNS SRVs for load balancing

  - If the edges are split across geographical boundaries (different cities or even continent), you can use GeoDNS, See below for an example of how to use GeoDNS SRV records to route requests to the appropriate Edge server:

GeoDNS Examples for Multi-cluster

GeoDNS over MRA is supported for the specific purpose of providing the nearest Expressway when the client is relatively distant from the Expressway that is used for MRA. This helps to minimize latency and network delays.

The following example illustrates a multi-cluster deployment with two Expressway-C clusters that connect to multiple Unified CM clusters. This example uses a single domain, but with two geographically displaced Expressway clusters, thereby providing two enterprise edges. Depending on the DNS provider, you can apply GeoDNS to SRV or CNAME record (SRV is preferred if available). Following are two examples of how to use GeoDNS where there are two Edge domains (one Edge in Europe and another in the US).
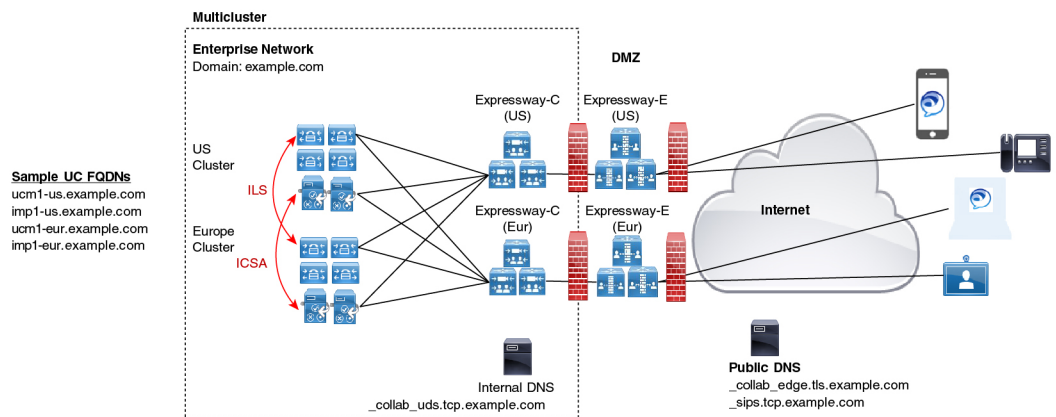
The preferred SRV approach, if the DNS provider supports it, is to create SRV records with priority settings that are based on the user's location (for example, the US or Europe). The SRV uses the user's location and the priority setting that is assigned to each Edge server to determine the server to which the request is sent. If that request fails, the other server provides a backup option.

Table 14: GeoDNS in SRV Records (Preferred approach)

SRV Records	User Location	Route to... (priority)

`_collab-edge.tls.example.com`
 	
`_sips_tcp.example.com`
	US	• `us-expc.example.com` (10)
		
		• `eur-expc.example.com` (20)

	Europe	• `eur-expc.example.com` (10) • `us-expc.example.com` (20)

Following is an example of a GeoDNS SRV configuration record that routes to two CNAME aliases (a main alias and a backup CNAME with a lower priority). Each CNAME record routes the call to different servers based on the user location. If the main CNAME fails, the backup CNAME sends the call to a server in a different region (a NA user is routed to a European-based Expressway).

Table 15: GeoDNS routing via CNAME

SRV Records	Route to CNAME (priority)	User Location	Route to...

`_collab-edge.tls.example.com`
 	
`_sips_tcp.example.com`
	`alias1.example.com` (10)	US	`us-expc.example.com`

		Europe	`eur-expc.example.com`
	`backup-alias1.example.com` (20)	US	`eur-expc.example.com`
		Europe	`us-expc.example.com`

Note For SRV approach, leave the weight setting in the SRV the same for all records.

Note You may also need to configure geographically based Calling Search Spaces and partitions on Unified CMso that you can route calls based on the caller's location. For example, you can create geographically based calling search spaces (a CSS for a specific city) and place all the phones that are in that city within that CSS (one CSS may be called "New_York_CSS" and a different CSS may be called "Chicago_CSS")

For a more detailed discussion, see "Scaling the Collaboration Edge Solution" in the *Preferred Architecture for Cisco Collaboration 12.x Enterprise On-Premises Deployments, CVD* at https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/12x/120/collbcvd/edge.html#pgfId-1081382.

Multidomain Best Practices

This section outlines domain-related information and configuration processes for customers whom want to deploy MRA with multiple domains. The ideal scenario for Mobile and Remote Access is a single domain for all Collaboration applications and endpoints, but this may not be possible in all cases. Depending on your

network, a multi-domain setup can have varying levels of complexity, so it's important to understand the different contexts within which the domain settings can be used.

Multiple Edge Domains

The following image illustrates a basic multi-domain scenario where the internal UC domain is different from the external domain.

Figure 25: Multiple Edge Domains
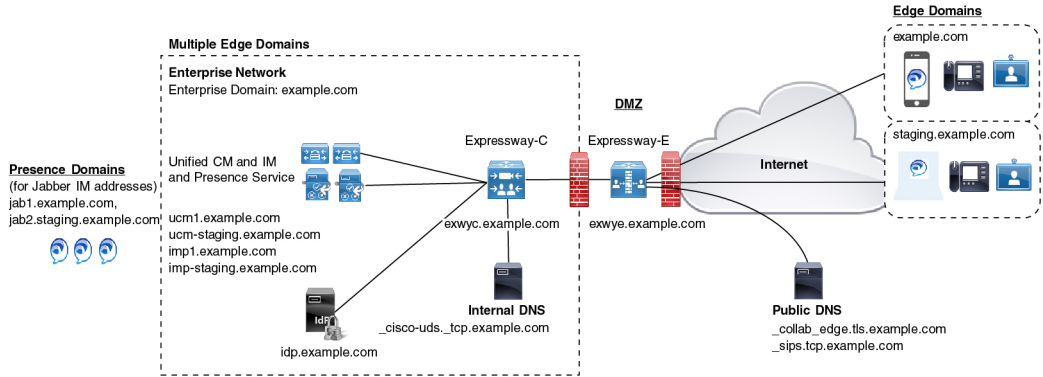
Note   MRA endpoints must have connectivity to the external public DNS server so that they can reach Expressway-E.

Multiple Domains with Separate Deployments

The following example illustrates a more complex multi-domain scenario where the internal UC environment is split into two Deployments: the Default UC Deployment, which encompasses the main UC applications, including both Expressways and a second Staging deployment. The two deployments are located in different domains. The Default Deployment has multiple UC clusters with ILS and ICSA being used to sync data between the internal clusters. This example also uses a cloud-based Identity Provider that is located in a separate external IdP domain.

Figure 26: Multiple Domains with Separate Deployments
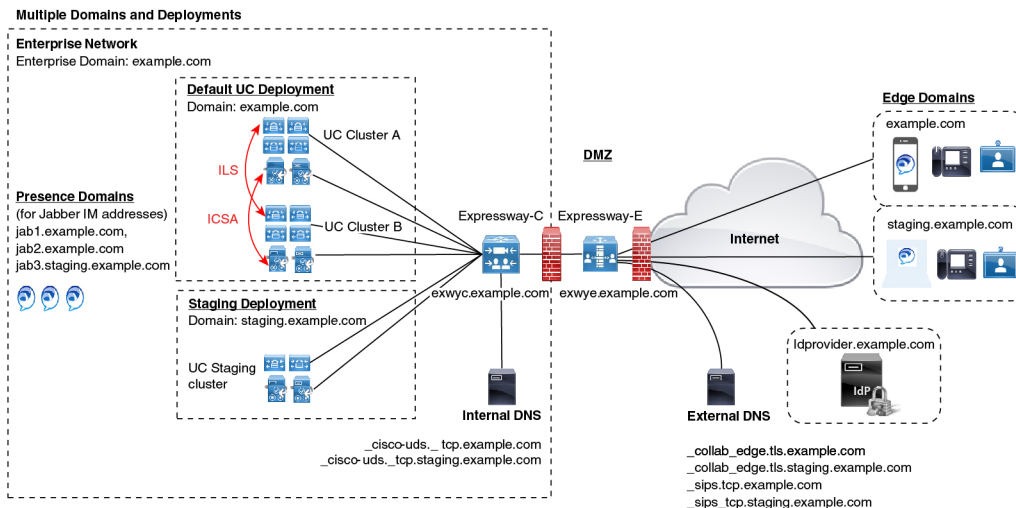
Domain Glossary

The following table outlines the different contexts in which the domain term may be used within an MRA Deployment and how to set them on Expressway. Depending on your deployment, the same domain may be applied for all these contexts.

Table 16: Domain Glossary

Term	Description
Edge domain	This term refers to the remote domain in which remote MRA endpoints connect to the on-premises UC network. This is configured on Expressway-C under the **Configuration** > **Domain** menu, and communicated to Expressway-E over the UC Traversal zone
Expressway Server Domain	For both Expressway-C and Expressway-E, the domain is a part of each server's FQDN address and is provisioned in the **System** > **DNS** window on each respective server. Each server supports a single domain only.
Internal UC Domain	This is the domain for internal UC applications such as Cisco Unified Communications Manager and the IM and Presence Service. These applications may be located in the same domain as Expressway or they may be in a different domain. **Note** If the internal UC applications are in a different domain than Expressway, then you must use FQDNs or IP addresses as server addresses for the UC server addresses. FQDNs are preferred.

Term	Description
Presence Domains	Presence domains are configured on the IM and Presence Service and may be used in the client's IM address (for example, user@domain). **Note** For MRA clients, if the Presence Domain is not the same as the Edge domain, add the Presence Domain to the Domain list on Expressway-C. **Note** Multiple Presence Domains over MRA is supported from Expressway X12.6.3 with IM and Presence Service, Release 10.0(1) or later. However, it's recommended that you do not exceed 75 domains within a single deployment.
MRA Activation Domain	If you are using activation code onboarding of MRA endpoints, the MRA Activation Domain is configured on Unified CM during the cloud onboarding process, representing the domain where MRA endpoints for that cluster must connect for the initial device activation. Each cluster can have a single MRA Activation Domain only.
MRA Service Domain	If you are using activation code onboarding of MRA endpoints, the MRA Service Domain is configured on Unified CM, representing the remote Edge domain where the endpoint connects for normal MRA use. If you have multiple Expressway clusters, the MRA Service Domain lets you specify which Expressway cluster is used for normal MRA operation. After an MRA device activates within the MRA Activation Domain, the device downloads its configuration file, which contains a redirect to the assigned MRA Service Domain. The device then looks up the `_collab_edge` SRV for that domain and attempts to register via the Expressway cluster that is assigned to the domain. MRA Service Domains can be applied to endpoints at the cluster, device pool, or individual device level. **Note** The MRA Activation domain gets added automatically to the list of available MRA Service Domains for a Unified CM cluster.

Multidomain Configuration Summary

The following table provides a configuration summary of domain-specific tasks for multidomain MRA scenarios.

✎

Note This summary does not replace the main configuration flow for setting up a basic MRA deployment—you can configure your system to support MRA over multiple domains by following the main configuration flow. However, for complex multidomain scenarios, this summary provides a helpful checklist of domain-specific tasks that you can use to verify that your domain setup is correct.

Table 17: MRA Multidomain Configuration Summary

Steps	Task
Step 1	Configure the Host Name and Domain Name for Expressway servers. See Set Expressway Server Address, on page 32.

Steps	Task

Step 2	On Expressway-C, add the domains for which MRA registration, call control, provisioning, messaging, and presence services are to be routed to Unified CM. This may include:
	
	    • Internal UC domains
	
	    • Edge domains (if they are different from the internal domains)
	
	    • Presence domains (if they are different from the other domains).
	
	See Add Domains, on page 34.

Step 3	(Optional). Assign Deployments to internal UC Applications. This optional configuration lets you partition internal UC services. For example, you could use this configuration to partition your main Production cluster off from a separate Staging cluster. See Assign Deployment Partitions for UC Services, on page 70.
Step 4	Configure Internal DNS entries: 1. Configure `_cisco-uds._tcp.<domain>` SRV records for each Unified CM domain. 2. Create forward and reverse lookups for each Unified CM and IM and Presence node. 3. Configure A and PTR records that point Expressway-C to Expressway-E. **Note** As of X12.6, the `_cisco_uds.tcp.example.com` internal SRV record is no longer mandatory for MRA endpoints to be able to reach the correct UC cluster. However, note that this SRV record is still required if you are deploying on-premises Cisco Jabber and Webex clients. See Local DNS (Internal Domains), on page 13.
Step 5	Configure Public DNS: 1. On Expressway-E, configure `_collab-edge._tls.<domain>` and `_sips_tcp.<domain>` DNS SRV records for each Edge domain. 2. Configure A records that point the Expressway-E hostname to the public IP address of Expressway-E. **Note** MRA endpoints must have connectivity to the Public DNS server so that they can reach Expressway-E. See Public DNS (External Domains), on page 13. **Warning** Expressway-E Fully Qualified Domain Name (FQDN) must match with the SRV A record to establish connectivity between MRA endpoints and the Public DNS server so that they can reach Expressway-E.
Step 6	Configure Expressway-E certificates. Make sure that the Expressway-E certificate includes each Unified CM registration domain. For details, see Certificate Requirements, on page 17.

Steps	Task
Step 7	If you are deploying SAML SSO, associate the appropriate domain to your Identity Provider: See Associate Domains with an IdP, on page 49.
Step 8	If you are using Device Activation Codes to provision MRA clients, provision a clusterwide MRA Activation Domain on Unified CM for MRA onboarding. In addition, provision any MRA Service Domains with the edge domains that you want users to use after their device activates. See MRA Device Onboarding Configuration Flow, on page 94.

(Optional) Using SRVs to create Alias FQDNs for Expressway-E

An optional approach if you have multiple Edge domains is to use SRV records to create an alias domain for Expressway-E, which would simulate multiple Expressway-E FQDNs. For example, if you have an Expressway-E server in example.com and you have two edge domains (example.com and staging.com):

- For each Edge domain, configure the _collab_edge SRV to point to the Expressway-E FQDN address as if it were a part of that Edge domain (for example, an SRV that points to expe.example.com and another that points to expe.staging.com).

- For each FQDN, configure A records that point to the public IP address of Expressway-E.

Session Persistency

Session Persistency enhances the user experience while roaming and allows Webex apps to do the following:

- Roam between different Access points in a network.

- Roam between different networks (For example, Wi-Fi, VPN over 3G/4G) without having to re-register.

- Maintain the SIP-based subscription status while roaming between different networks.

- Maintain registration in the case of network connectivity loss.

- Seamlessly transit both active and held calls from one network to another without call drops.

To facilitate connectivity during roaming between networks, Session Persistency allows dynamic IP address/port change via keep-alive registration. In addition, the feature includes a configurable TCP reconnect timer, which must be enabled at the product level, to allow Webex apps clients to remain connected in case of a temporary network connectivity loss or roaming. The timer is in effect only when the clients tear down the original TCP connection explicitly. To leverage the Session Persistency feature, you must comply with Cisco-defined SIP interfaces.

For example, if you are in an active Webex apps client call inside the office and walk outside the building losing Wi-Fi connectivity, the call would now continue as the client switches to Mobile and Remote Access through Expressway. Likewise, you will not see call drops if the client switches from Mobile and Remote Access through Expressway to the office Wi-Fi network.

Onboarding MRA Devices

MRA Device Onboarding via Activation Codes

Activation Codes provide a simple and secure way to onboard remote endpoints for Mobile and Remote Access (MRA). This feature eliminates the need for an MRA user to be on-premises the first time they use their phones. Remote users can plug in the phone, enter the activation code, and then start placing calls.

This feature leverages the Cisco cloud to handle onboarding. An administrator onboards Cisco Unified Communications Manager to the cloud, specifying the clusterwide MRA Activation Domain with the Expressway cluster to which all remote MRA users connect during device activation.

If you have multiple Expressway clusters, MRA Service Domains let you specify which Expressway your phones register. After the phone activates, the phone downloads its configuration file, which contains a redirect to the MRA Service Domain with the Expressway cluster that is assigned to that phone.

What is an Activation Code?

An activation code is a single-use, 16-digit value that a user must enter on a phone before registering the phone. The user must enter the correct code, or the phone does not register. Activation codes provide a secure method to onboard phones without requiring an administrator to collect and input the MAC Address for each phone manually.

Custom Certificates (Optional)

If you want to use your own certificates, you can use the cloud to distribute certificates to MRA phones so that they can establish trust with Expressway. With this option, you must upload your certificates first to Expressway, and then to the **PhoneEdge-trust** store on Cisco Unified Communications Manager. The certificates are uploaded to the Cisco cloud so that the phone can download them during the device activation process.

MRA Onboarding Process Flow

The below table contains the process flow for onboarding new MRA phones via Device Activation Code Onboarding in MRA mode. Match each numbered step to the subsequent graphic for an illustration of the process.

✎

Note When you start Device Activation Service on UCM publisher to on-board clients over Mobile and Remote Access, you need to start the UDS and CCM services as well. Moreover, delete and rediscover the UCM cluster in Unified Communications configuration in Expressway-C, as doing a refresh of servers will not work.

Process Step	Process Flow
0	Administrator configures Cloud Onboarding and specifies the MRA Activation Domain and any MRA Service Domains.
1	Administrator provisions full device configuration without specifying the MAC address. The device name will be a random BAT MAC address.
2	Administrator requests activation code for this device. Device Activation Service requests the code from the cloud-based device activation service.
3	Activation Code is sent to the user (either via email or via the Self-Care Portal).
4	User enters the activation code. Phone gets the MRA target from the cloud.
5	Phone learns the location of Expressway and authenticates using the MIC + activation code in an SRP handshake.
6	Device activation service updates the device configuration in the database with the phone MAC and sends success to the phone
7	The phone can register and gets its phone specific configuration file from TFTP and then register with Unified CM. If the phone is assigned to a different MRA Service Domain, a redirect is provided in the configuration file. The phone can then register using the MRA Service Domain.
8	Device Activation Service releases the activation code from the cloud. The code can be reused in the future.

Figure 27: MRA Device Onboarding Process Flow with Activation Codes
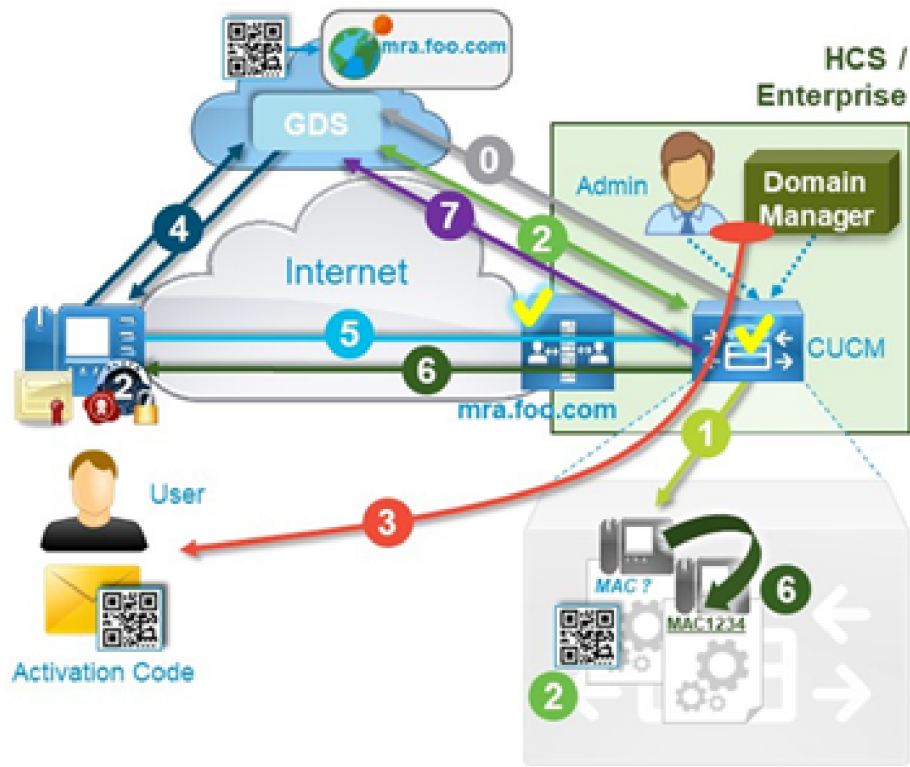
Device Onboarding Prerequisites

The following table has support information for Activation Code Onboarding for MRA endpoints:

Table 18: MRA Activation Code Onboarding Support Information

Support	Details
Minimum Releases	Expressway X12.5.1 Cisco Unified Communications Manager 12.5(1)SU1 Cisco IP Phone firmware 12.5(1)SR3
Supported Endpoints	Cisco IP Phones 7811, 7821, 7832, 7841, 7861, 8811, 8832, 8832NR, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR

Note   As of release X14.0, if you are onboarding supported Cisco IP Phone 78xx Series and 88xx Series phones for Mobile and Remote Access, the phones switch to MRA mode only if the **Allow Activation Code via MRA** checkbox is checked within the **Phone Configuration** window of **Cisco Unified Communications Manager**.

Using this approach, you must configure Activation Code onboarding for MRA phones. In addition, the MRA phone user must enter the correct activation code to activate and use the phone.

For details on configuring Activation Code Onboarding, see the "Device Onboarding via Activation Codes" chapter of *Feature Configuration Guide for Cisco Unified Communications Manager*.

In addition, the following prerequisites exist:

- If you've upgraded Expressway from a release prior to X12.5, refresh your Unified CM servers on Expressway-C before you configure this feature. On Expressway-C go to **Configuration** > **Unified Communications** > **Unified CM servers** and click **Refresh servers**.

- **Cisco Device Activation Service**—This service must be running on Cisco Unified Communications Manager (the service is running by default). Check the list of services in Cisco Unified Serviceability to verify the service is running.

- **OAuth Refresh Logins**—This feature must be enabled in Cisco Unified Communications Manager by setting the **OAuth Refresh Login Flow** enterprise parameter to **Enabled**.

- **Self-Care Portal**—If you want users to be able to use the Self-Care Portal to activate their phones:

  - The **Show Phones Ready to Activate** enterprise parameter must be set to **True** in Cisco Unified Communications Manager.

  - End users require login access to the portal. See the "Self-Care Portal" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager* for Self-Care configuration details.

  - The Self-Care Portal is not supported over MRA so remote users may need a VPN to access the portal.

- **DNS SRV records**—For the MRA Activation Domain and any MRA Service Domains, you must configure *_collab_edge* SRVs that point to the appropriate Expressway clusters.

MRA Device Onboarding Configuration Flow

Follow these procedures to configure MRA Device Onboarding using activation codes in MRA mode.

Steps	Procedures
Step 1	Enable OAuth Authentication in Cisco Unified Communications Manager and Expressway: 1. Enable OAuth on Cisco Unified Communications Manager: a. From Cisco Unified CM Administration, go to **System** > **Enterprise Parameters**. b. Set the **OAuth Refresh Login Flow** parameter to **Enabled**. c. Click **Save**. 2. Enable OAuth Refresh authentication on Expressway: a. Go to **Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**. b. Set **Authorize by OAuth token with refresh** to **On**. c. Click **Save**.
Step 2	Onboard Cisco Unified Communications Manager to the cloud for MRA activation code onboarding. 1. From Cisco Unified CM Administration, choose **Advanced Features** > **Cisco Cloud Onboarding**. 2. Click the **Generate Voucher** button. 3. Check the **Enable Activation Code Onboarding with Cisco Cloud** check box. 4. Specify the **MRA Activation Domain**. 5. Click **Save**. **Note** • Collab-edge DNS records must exist for the MRA Activation domain. • There is a limit of one MRA Activation Domain per cluster. The MRA Activation is added automatically to the list of MRA Service Domains.
Step 3	Configure MRA Service Domains. 1. From Cisco Unified CM Administration, choose **Advanced Features** > **MRA Service Domains**. 2. If you have multiple Expressway clusters, add each domain where your MRA endpoints will operate. 3. Check the **IsDefault** check box, if you want a domain to be applied as a clusterwide default MRA Service domain. 4. Click **Save**.

Steps	Procedures
Step 4	Optional. Assign an MRA Service Domain to an existing device pool. This lets you assign a specific Expressway cluster to all MRA devices that use the device pool. 1. From Cisco Unified CM Administration, choose **System** > **Device Pool**. 2. Click **Find** and select the appropriate device pool. 3. From the **MRA Service Domain** drop-down, select the domain that you want to assign to devices that use this device pool. 4. Click **Save**.
Step 5	Configure MRA Access Control to allow activation code onboarding: 1. From Expressway-C, choose **Configuration** > **Unified Communications** > **Configuration**. 2. Set **Authorize by OAuth token with refresh** to **On**. 3. Set **Allow activation code onboarding** to **Yes**.
Step 6	Check Trusted Cisco manufacturing certificates (MICs) installed. They are required to access the activation code onboarding functionality: 1. On Expressway-E, choose **Maintenance** > **Security certificates** > **Trusted CA certificates**. 2. Click **Activate code onboarding trusted CA certificates**.
Step 7	Optional. If you want to use your own custom certificates (: 1. Upload the certificates to Expressway. 2. Upload certificates to PhoneEdge-trust on Unified Communications Manager. Unified Communications Manager uploads the certificates to the cloud. During the activation process, the phone downloads the certificates from the cloud, thereby ensuring that the phone can communicate with Expressway.

Step 8	Provision the phone in the Cisco Unified Communications Manager database using any accepted provisioning method. No matter which option you choose, make sure that both of the following check boxes are checked:
	
	    • **Requires Activation Code Onboarding**
	
	    • **Allow Activation Code via MRA**
	
	Note You can provision the phone with a dummy MAC address. The onboarding process updates the **Device Name** using the phone's actual MAC address.
	
	         For sample provisioning procedures using either the GUI or Bulk Administration, see the "Device Onboarding via Activation Codes" chapter of the *System Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1* or later.

Step 9	Ship the phone to the MRA users.

Activate Phones

Administrators have two options for sending activation codes to phone users:

- Self-Care Portal—Phone users can log in to the portal to view their phone's activation code and an accompanying barcode. They can either key the activation code onto the phone or use the phone's video camera to scan the barcode—both methods work. Review Device Onboarding Prerequisites for information about Self-Care requirements.

- CSV File Export—In Cisco Unified Communications Manager, administrators can export a csv file of outstanding activation codes and associated users. They can use the contents of this file to notify MRA users with their activation codes. To export a csv file:

  1. From Cisco Unified CM Administration, choose **Device** > **Phone**.

  2. From **Related Links**, select **Export Activation Codes** and click **Go**.

✎

Note   Activation Codes have a default lifetime of 168 hours (7 days). You can reconfigure this value via the **Activation Time to Live (Hours)** service parameter in Cisco Unified Communications Manager. If the activation code expires, the administrator can click **Release Activation Code** and then **Generate New Activation Code** from the **Phone Configuration** window in order to reset the activation code.

Entering the Activation Codes

When an MRA user plugs in their phone, they are prompted to enter the activation code. Once they enter the activation code, or scan the barcode that displays in Self-Care, the phone onboards, downloads its configuration file, and registers.

The phone is now ready to use.

Additional Options for Secure Onboarding

The following options slightly modify the configuration process for added security:

Option 1: Administrator provisions phone with actual MAC address

Rather than using a dummy MAC address, the administrator adds the phone to Cisco Unified Communications Manager with the actual MAC address. This method ties the activation code to the actual phone MAC address, enhancing security as the activation code works on that phone only. However, this method requires that the administrator collect and enter each phone MAC address individually.

Option 2: Administrator activates phone on-Premises before sending to Remote User for reonboarding in MRA mode

With this method, the administrator activates the phone in on-premises mode before resetting the activation code requirement and shipping to the MRA user, who will activate the phone in MRA mode.

- Administrator configures Activation Code Onboarding (On-Premises mode) and provisions the phone with a dummy MAC address.

- Administrator onboards and registers the phone in the on-premises environment. This process updates the **Device Name** in Cisco Unified Communications Manager with the actual phone MAC address and lets the phone updates its firmware load.

- The administrator configures Activation Code Onboarding for MRA mode, resets the activation code requirement thereby locking the phone until the new code is entered.

> **Note** In the **Phone Configuration** window, both of the following check boxes must be checked as they reset the activation code and lock the phone:
>
> - **Requires Activation Code Onboarding**
>
> - **Allow Activation Code via MRA**

- The administrator ships the phone to the MRA user and provides the user with the new activation code.

- The remote MRA user must enter the new activation code in order to use the phone.

This option provides the following benefits:

- Improves security as the activation code is tied to the MAC address and works for that phone only.

- Ensures that phone firmware is already up to date when the user receives the phone.

- Does not require the administrator to collect and input individual MAC addresses.

For information on how to configure activation code onboarding in On-Premises mode, see the On-Premises tasks in the "Device Onboarding via Activation Codes" chapter of the *System Configuration Guide for Cisco Unified Communications Manager.*

MRA Maintenance

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.

Figure 28: Maintenance Mode on Expressway-C

Limitation for CE endpoints

Maintenance mode is not supported over MRA for endpoints running CE software. The Expressway drops MRA calls from these endpoints when you enable maintenance mode.

MRA Registration Counts

From X12.6.1 onward, the **Status** > **Overview** page on Cisco Expressway-E lets you monitor up-to-date usage information for SIP devices that are registered over MRA. The **Overview** page contains the following fields:

MRA Registration:

- **Current**—The total number of devices that are currently registered over MRA.

- **Peak**—The peak count for MRA registrations since the last Expressway restart.

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.

Figure 29: Advanced Settings

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).

SIP Registration Failover for Cisco Jabber

The SIP registration failover for Cisco Jabber applies if you deploy Expressway with Mobile and Remote Access (MRA).

Expressway X12.7 and later versions build on existing failover capabilities for clustered Expressways with a few MRA failover updates that improve substantially the failover time for Cisco Jabber clients that connect over MRA. Among the updates include adaptive routing, STUN keepalive support, and improved error reporting.

These new capabilities will allow Jabber clients to support MRA High Availability (failover) for voice and video.

Adaptive routing

Adaptive routing updates in Expressway X12.7 and later versions allows Expressway to alter the routing path dynamically. If a node failure is detected, packets are rerouted to a peer node that is up and running. For example, assume that a remote Jabber client sends a SIP REGISTER that is intended to be routed through a specific Expressway-E (EXWY-E1), Expressway-C (EXWY-C1) and Unified CM (CUCM1) combination, but the designated Expressway-C node is either down or is in maintenance mode. In this case, the message is rerouted to a peer Expressway-C node (EXWY-C2) and then on to the intended Unified CM destination. After the registration, Cisco Jabber also updates its routing table so that future SIP messages use the registration path.

Note **Notes**

- Failover does not include call preservation. The Jabber registration fails over to the new registration path, but active calls at the time of the failure are dropped.

STUN keepalive support

In addition to adaptive routing, Expressway X12.7 and later versions support the use of STUN keepalives by MRA connected Jabber clients. Remote Jabber clients send STUN keepalives into the enterprise network via Expressway-E to learn of connection issues ahead of time. As a result, if a node in the registration path fails, Jabber will learn of the failure after receiving the STUN response and can select a different route path for future SIP messages.

Settings

The STUN keepalive setting is configurable in the **Advanced** section of the **Configuration** > **Unified Communications** > **Configuration** page. See Figure 29: Advanced Settings.

Field	Description
STUN keepalive	Enable STUN keepalive for Unified CM High Availability. Default: *On*

Requirements

No specific configuration is required (subject of course to the necessary clustering/backup nodes existing). However, you must be running the following minimum releases:

Routing Feature	Minimum Releases Required
Adaptive routing	1. Expressway X12.7 2. Cisco Jabber 12.9 MR 3. Cisco Webex App

Routing Feature	Minimum Releases Required
STUN keepalives	1. Expressway X12.7 2. Cisco Unified Communications Manager 14 3. Cisco Jabber 12.9 MR 4. Cisco Webex App

Note **Notes**

-
- STUN Keepalive is sent every 30 seconds from the client (Jabber) and if it didn't get the response within 3 seconds, then the client initiates failover.

- When Expressway is configured with a different domain from CUCM, the CUCM admin needs to update Exp-C Hostname entry manually to FQDN, by appending the relevant system domain of Exp-C.

Load Balance After Node Recovery

With MRA-HA, whenever there is a node(s) failure the load of the failed node(s) will be shifted to the other available nodes in the cluster. The following sections describe the load balancing procedure after the node(s) became active in the cluster.

Load Balance Expressway-C nodes

From X14.1 release, Expressway-C node load balancing is achieved by using Adaptive Routing on Expressway-E node.

After an Expressway-C node failure, the traffic/registrations will be handled by other nodes in the cluster. Once the failure node gets recovered and becomes active, even though new registrations go through that node, the existing load won't be handled by that node. To load balance the Expressway-C cluster in that scenario, we are introducing AR mechanism on Expressway-E.

There is a keep alive mechanism between Expressway-E nodes and Expressway-C nodes, in a mesh architecture. Within the keep alive message, Expressway-C sends resource usage/active registrations to Expressway-E. Then, Expressway-E evaluates the active registrations across all the nodes in Expressway-C and if it identifies an unbalanced load on the node, it triggers load balancing.

The load balancing is achieved by adaptively routing the Register messages (New/Refresh) to least loaded node. This will be done to the clients which supports Adaptive Routing. Once the load is balanced Expressway-E will stop the process. This ensures no node is idle and load is balanced.

Load Balance Expressway-E nodes

Expressway-E node maintains the count of total number of registrations of all nodes in the cluster. Whenever there is an imbalance in the cluster, the node with high number of registrations will respond to register messages with a warning header in the 200-response message, indicating load is imbalanced.

> **Note**   The load balance will not be shared equally or in a fixed ratio but will try to avoid the 0-100 share situation for a node.

Benefits with all software requirements

When all three components - clients, Expressway, Unified CM - are running updated software with MRA registration failover capabilities, the following benefits apply:

- No user action required for failover

- Faster failover times - down to 30-60 seconds from the previous standard of 120 seconds

- Route path updates dynamically to handle server failures

- More routes are available to reach the intended destination

- Remote Jabber clients can learn of server failures via STUN keepalives and adjust routing ahead of time

Adaptive routing benefit without Unified CM upgrade

Even without new Unified CM software (but with new Expressway and Jabber software), this feature has the benefit of allowing Jabber clients to detect path failures.

> **Note**   This action will take over 2 minutes, and Expressway may flag Unified CM servers as inactive in some scenarios where actually the server is just idle or has low use at the time.

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 and Presence Service servers on Expressway-C, you must do this on the primary peer.

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. 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.

Configure Exemptions

If you have Automated Intrusion Protection configured, use this procedure to configure exemptions for IP address ranges from one or more protection categories.

One example where you may need an exemption is if you have multiple MRA users connected behind a NAT using the same public IP address. This may trigger protection due to the incoming traffic from the single IP address.

Note   This procedure assumes you have the Automated Intrusion Protection enabled on Expressway-E and disabled on Expressway-C, which is the recommended deployment.

Step 1   On Expressway-E, go to **System** > **Protection** > **Automated detection** > **Exemptions**.
Step 2   Click on the **Address** that you want to configure or click **New** to configure a new address.
Step 3   Enter the **Address** and **Prefix Length** to define the IP address range that you want to exempt.

Step 4   Select from the categories to which you want to apply the exemption. For the example situation where you have multiple users behind a NAT, the following categories would apply:

> • HTTP Proxy Authentication Failure
> • HTTP Proxy Resource Access Failure
> • SIP Authentication Failure

Step 5   Click **Add Address**.

Check the Unified Communications Services Status

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

Step 1   Go to **Status** > **Unified Communications**.

Step 2   Review the list and status of domains, zones and (Expressway-C only) Unified CM and IM and Presence Service servers.

The page displays any configuration errors along with links to the relevant configuration page that you access to address the issue.

Why You Need to 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.** 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 is likely to cause some kind of failure.

The information that the Expressway-C reads from the Unified Communications node is different for each node type/role. These are 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 (such as adding or removing a node)
>
> • Changing security parameters (such as enabling Mixed Mode)
>
> • Changing connection sockets (such as SIP port configuration)
>
> • Changing TFTP server configuration
>
> • Upgrading node software

Devices cannot connect during the refresh

It takes some time to restore services after a server refresh and while the refresh is in progress, Jabber clients and other endpoints are unable to connect over MRA. It is not possible to provide accurate timings as they

vary depending on the deployment. For straightforward deployments the refresh typically takes 5 to 10 seconds, but very complex configurations may take upwards of 45 seconds.

Refresh Servers on the Expressway-C

You must refresh the Cisco Unified Communications Manager and Cisco Unity Connection nodes defined on the Expressway-C. This fetches keys that the Expressway needs to decrypt the tokens.

Step 1 For Unified CM, go to **Configuration** > **Unified Communications** > **Unified CM servers** and click **Refresh servers**.

Step 2 For Unity Connection, go to **Configuration** > **Unified Communications** > **Unity Connection servers** and click **Refresh servers**.

Refresh Servers on the Expressway-C

MRA Troubleshooting

General Techniques

Alarms and Status Messages

When troubleshooting, first check if any alarms have been raised (**Status** > **Alarms**). If alarms exist, follow the instructions in the **Action** column. Check the alarms on both Cisco Expressway-C and Cisco Expressway-E.

Next, review the status summary and configuration information (**Status** > **Unified Communications**). Check the status page on both Cisco Expressway-C and Cisco Expressway-E. If any required configuration is missing or invalid, an error message and a link to the relevant configuration page is shown.

You may see invalid services or errors if you change the following items on Cisco Expressway, for which a system restart is required to be sure the configuration changes take effect:

- Server or CA certificates

- DNS configuration

- Domain configuration

Use the Collaboration Solutions Analyzer

The Collaboration Solutions Analyzer (CSA) tool set provided by TAC, can be used to help with deploying and troubleshooting MRA. (See the Cisco Expressway release notes for instructions about how to access the CSA.)

Step 1   Use the CollabEdge **validator tool** to validate your MRA deployment.

It simulates a Jabber client sign in process and provides feedback on the result.

Step 2   If the CollabEdge validator cannot identify the issue, we suggest that you collect logs from the Cisco Expressway while attempting to sign in. Then use the **log analysis** component in the CSA to analyze the logs.

Diagnostic Logs

Jabber for Windows Diagnostic Logs

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

Configure Cisco Expressway Diagnostic Log Levels

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

Before you begin

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

Step 1   Go to **Maintenance** > **Diagnostics** > **Advanced** > **Support Log configuration**.

Step 2   Select the recommended logs for the problem you are experiencing. You can find these using the Log Advisor Tool: https://logadvisor.cisco.com/logadvisor/collaboration/unifiedcommunications/mra.

Step 3   Click **Set to debug**.

Create a Diagnostic Log Capture

After you configure the Cisco Expressway diagnostic log levels, you can start the diagnostic log capture.

Step 1   Go to **Maintenance** > **Diagnostics** > **Diagnostic logging**.

Step 2   (Optional) Select **Take tcpdump while logging**.

Step 3   Click **Start new log**.

Step 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.

Step 5   Reproduce the system issue you want to trace in the diagnostic log.

Step 6   Click **Stop logging**.

Step 7   Click **Collect log**.

Step 8   When the log collection completes, 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 Create Logs

If you want to download the logs again, you can re-collect them by using the **Collect log** button. If the button is grayed out, first refresh the page in 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.

Check DNS Records

You can use the Cisco Expressway's DNS lookup tool to assist in troubleshooting system issues.

Go to **Maintenance** > **Tools** > **Network utilities** > **DNS lookup**.

The SRV record lookup includes those specific to H.323, SIP, Unified Communications and TURN services.

Note   Performing the DNS lookup from the Cisco Expressway-C returns the view from within the enterprise, and that performing it on the Cisco Expressway-E returns 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

Check that the Cisco Expressway-E is Reachable

This procedure describes how to check that the Cisco Expressway-E is reachable.

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

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

Check Call Status

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

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

If the Cisco 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.

Step 1 If you wish to get information about the current calls, go to the **Call status** page (**Status** > **Calls** > **Calls**).

The **Call status** page lists all the calls currently taking place to or from devices registered with the Cisco Expressway, or that are passing through the Cisco Expressway.

Step 2 If you wish to get information about the completed calls, go to the **Call history** page (**Status** > **Calls** > **History**).

The **Call history** page 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 Cisco Expressway was last restarted.

Mobile and Remote Access Call Identification

The call status and call history pages show all call types—Unified CM remote sessions (if Mobile and Remote Access is enabled) as well as Cisco Expressway RMS sessions.

To distinguish between the call types, you must drill down into the call components. Mobile and Remote Access calls have different component characteristics depending on whether the call is being viewed on the Cisco Expressway-C or Cisco Expressway-E:

- On the Cisco Expressway-C, a Unified CM remote session has three components (as it uses the B2BUA to enforce media encryption). One of the Cisco Expressway components routes the call through one of the automatically generated neighbor zones (with a name prefixed by either **CEtcp** or **CEtls**) between Cisco Expressway and Unified CM.

- On the Cisco 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 (Cisco Expressway Only)

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.

Devices Registered to Unified CM via Cisco Expressway

Identify Devices in Unified CM

This procedure describes how to identify devices registered to Unified CM via Cisco Expressway.

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

Step 2 Check the **IP Address** column.

Devices that are registered via Cisco Expressway will display the IP Address of the Cisco Expressway-C it is registered through.

Identify Provisioning Sessions in Cisco Expressway-C

This procedure describes how to identify sessions that have been provisioned via Cisco Expressway-C.

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

Step 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.

Ensure that Cisco Expressway-C is Synchronized to Unified CM

Changes to Unified CM cluster or node configuration can lead to communication problems between Unified CM and Cisco 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 Cisco Expressway-C. To do this:

Step 1   On Cisco Expressway, go to **Configuration** > **Unified Communications**.

Step 2   Rediscover all Unified CM and IM and Presence Service nodes.

Check MRA Authentication Status and Tokens

This procedure describes how to check MRA authentication status and tokens.

Step 1   (Optional) To check and clear standard (non-refresh) OAuth user tokens, go to **Users** > **View and manage OAuth without refresh token holders**.

This could help identify problems with a particular user's OAuth access.

Step 2   (Optional) To check statistics for MRA authentication, go to **Status** > **Unified Communications** > **View detailed MRA authentication statistics**.

Any unexpected requests or responses on this page could help identify configuration or authorization issues.

Registration Issues

Endpoints Can't 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 Cisco 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, on page 75 for more information.

- Secure registrations may fail ('`Failed to establish SSL connection`' messages) if the server certificate on the Cisco 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 Cisco Expressway's certificate — must be in FQDN format.

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

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

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

✎

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

Cisco Expressway Certificate and TLS Connectivity Issues

Modifications to the Cisco Expressway's server certificate or trusted CA certificates need a Cisco 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 Cisco 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 and Presence Service, with Cisco Expressway version X8.7.2 or later, then the SSL handshake between the two systems will fail by default.

The symptom is that all MRA endpoints fail to register or make calls after you upgrade to Cisco 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.

You must either upgrade your infrastructure or consult the Cisco Technical Assistance Center to check whether it is possible to modify the default configurations for Unified CM and/or Unified CM IM and Presence Service to support TLS (refer CSCuy59366).

Cisco Jabber Sign In Issues

Jabber Triggers Automated Intrusion Protection

Conditions

- Your MRA solution is configured for authorization by OAuth token (with or without refresh)

- The Jabber user's access token has expired

- Jabber does one of these:

    - Resumes from desktop hibernate

    - Recovers network connection

    - Attempts fast login after it has been signed out for several hours

Behavior

- Some Jabber modules attempt to authorize at Cisco Expressway-E using the expired access token.

- The Cisco Expressway-E (correctly) denies these requests.

- If there are more than 5 such requests from a particular Jabber client, the Cisco Expressway-E blocks that IP address for ten minutes (by default).

Symptoms

The affected Jabber clients' IP addresses are added to the Cisco Expressway-E's **Blocked addresses** list, in the *HTTP proxy authorization failure* category. You can see these on **System** > **Protection** > **Automated detection** > **Blocked addresses**.

Workaround

There are two ways you can work around this issue; you can increase the detection threshold for that particular category, or you can create exemptions for the affected clients. We describe the threshold option here because the exemptions may well be impractical in your environment.

1. Go to **System** > **Protection** > **Automated detection** > **Configuration**.

2. Click **HTTP proxy authorization failure**.

3. Change the **Trigger level** from *5* to *10*. 10 should be enough to tolerate the Jabber modules that present expired tokens.

4. Save the configuration, which takes effect immediately.

5. Unblock any affected clients.

Jabber Popup Warns About Invalid Certificate When Connecting from Outside the Network

This is a symptom of an incorrectly configured server certificate on the Cisco 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 Certificate Requirements, on page 17.

Jabber Doesn't Register for Phone Services

There is a case handling mismatch between the Cisco Expressway and the User Data Service (UDS) 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 information in the *Cisco Unified Communications Manager Configuration Guides* at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

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 Cisco Expressway-C and Cisco Expressway-E will work normally in all other respects. Cisco Expressway will report 'Application failed - An unexpected software error was detected in portforwarding.pyc'.

This can occur if the Cisco 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 Cisco Expressway-Es

Jabber sign in failures have been seen when there is inconsistency of the DNS domain name between Cisco 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.

Specific Issues

Cisco Expressway Returns "401 Unauthorized" Failure Messages

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

- Note that the solution must be configured to userid of the IDP that is provided in the SAML assertion should match the sAMAccountName of CUCM userid to validate against the tokens (access/refresh).

- The client is supplying an unknown username or the wrong password.

- Intercluster Lookup Service (ILS) has not been set up on all the Unified CM clusters. This may result in intermittent failures, depending upon which Unified CM node is being used by Cisco 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 Cisco 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 or 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.

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 Cisco 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 Cisco 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 Cisco Expressway-C.

"403 Forbidden" Responses for Any Service Requests

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

Client HTTPS Requests are Dropped by Cisco Expressway

This can be caused by the automated intrusion protection feature on the Cisco 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.

Failed: Address is not a IM and Presence Server

This error can occur when trying to configure the IM and Presence Service servers used for remote access (via **Configuration** > **Unified Communications** > **IM and Presence servers**). It is due to missing CA certificates on the IM and Presence Service servers and applies to systems running 9.1.1. More information and the recommended solution is described in 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 Cisco 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 Cisco Expressway-C. In this case you will see `No uid Attribute in Assertion from IdP` in the log.

The Cisco 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 Cisco Expressway-E indicates that the next hop failed (typically to the Cisco Expressway-C). Try the following steps:

1. Go to the **Status** > **Unified Communications** page on the Cisco Expressway-E. Did the Cisco 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 Cisco Expressway-C node is down, that is probably causing the 502 error.

MRA calls fail if the called endpoint is more than 15 hops away from the Expressway-E

The Unified Communications traversal zone has a default hop count of 15. If you suspect this is a contributing factor, sign in to all your MRA Expressways, raise the hop count to a significantly larger number, for example, 70 and test.

MRA calls fail if the called endpoint is more than 15 hops away from the Expressway-E

PART I

Appendix

HTTP Allow List Formats

This appendix contains information that can be used to generate and test HTTP Allow Lists.

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 19: 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, for example:`8443` • /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		Optional	Comma-delimited list of HTTP methods, optionally in double-quotes, for example: `"GET,PUT"`
3		Optional	`exact` or `prefix`. Default is `prefix`.
4		Optional	Text description of the rule. Enclose with double quotes if there are spaces.

Example List Rules 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 20: 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 for example, **PUT**. Defaults to **GET** if not supplied.

Example List Tests 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

Post-Upgrade Tasks for MRA Deployments

To Reconfigure the MRA Access Control Settings

☞

Important

- The **Check for internal authentication availability** setting will be off after the upgrade. Depending on the authentication settings on the Unified CM, this may prevent remote login by some Cisco Jabber users.

- The *Exclusive* option in X8.9 is now configured by setting **Authentication path** to *SAML SSO authentication*. This has the effect of prohibiting authentication by username and password.

Before you begin

After the system restarts you need to reconfigure the MRA access control settings.

Step 1 On the , go to **Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**.

Step 2 Do one of the following:

- To take advantage of the new MRA access control methods from X8.10, set the appropriate values on this page for your chosen methods. See the first table below for help about which values to apply.

- Or to retain your pre-upgrade authentication approach, set the appropriate values on this page to match your previous settings on the . See the second table below for help about how to map the old settings to their new equivalents on the .

Step 3 If you configure self-describing tokens (**Authorize by OAuth token with refresh**), refresh the Unified CM nodes: Go to **Configuration** > **Unified Communications** > *<UC server type>* and click **Refresh servers**.

Settings for MRA Access Control

The fields you actually see in the Web UI depend on whether MRA is enabled (**Unified Communications mode** set to *Mobile and remote access*) and on the selected authentication path. Not all the fields in the table are necessarily displayed.

Table 21: Settings for MRA access control

Field	Description	Default
Authentication path	Hidden field until MRA is enabled. Defines how MRA authentication is controlled. *SAML SSO authentication*: Clients are authenticated by an external IdP. *UCM/LDAP basic authentication*: Clients are authenticated locally by the Unified CM against their LDAP credentials. *SAML SSO and UCM/LDAP*: Allows either method. *None*: No authentication is applied. This is the default setting until MRA is first enabled. The "None" option is needed (rather than just leaving MRA turned off) because some deployments must turn on MRA to allow functions which are not actually MRA. (Such as the Web Proxy for Meeting Server, or XMPP Federation.) Only these customers should use "None". **Note** Do not use it in other cases.	None before MRA turned on UCM/LDAP after MRA turned on
Authorize by OAuth token with refresh	This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them. Only Jabber clients are currently capable of using this authorization method. Other MRA endpoints do not currently support it. The clients must also be in OAuth token with refresh authorization mode.	On
Authorize by OAuth token (previously SSO Mode)	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. This option requires authentication through the IdP. Currently, only Jabber clients are capable of using this authorization method, which is not supported by other MRA endpoints.	Off

Field	Description	Default
Authorize by user credentials	Available if **Authentication path** is *UCM/LDAP* or *SAML SSO and UCM/LDAP*. Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices.	Off
Check for internal authentication availability	Available if **Authorize by OAuth token with refresh** or **Authorize by OAuth token** is enabled. The default is No, for optimal security and to reduce network traffic. Controls how the Expressway-E reacts to remote client authentication requests by selecting whether or not the Expressway-C should check the home nodes. The request asks whether the client may try to authenticate the user by OAuth token, and includes a user identity with which the Expressway-C can find the user's home cluster: *Yes*: The *get_edge_sso* request will ask the user's home Unified CM if OAuth tokens are supported. The home Unified CM is determined from the identity sent by the Jabber client's *get_edge_sso* request. *No*: If the Expressway is configured not to look internally, the same response will be sent to all clients, depending on the Edge authentication settings. The option to choose depends on your implementation and security policy. If all Unified CM nodes support OAuth tokens, you can reduce response time and overall network traffic by selecting *No*. Or select *Yes* if you want clients to use either mode of getting the edge configuration - during rollout or because you can't guarantee OAuth on all nodes. **Caution** Setting this to *Yes* has the potential to allow rogue inbound requests from unauthenticated remote clients. If you specify *No* for this setting, the Expressway prevents rogue requests.	No

Field	Description	Default
Identity providers: Create or modify IdPs	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. **Selecting an Identity Provider** Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services. 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	-
Identity providers: Export SAML data	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. For details about working with SAML data, see *SAML SSO Authentication Over the Edge*.	-

Field	Description	Default
Allow Jabber iOS clients to use embedded Safari	By default the IdP or Unified CM authentication page is displayed in an embedded web browser (not the Safari browser) on iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices.	No
	This setting optionally allows 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 OAuth deployment.	
	A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the 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.	
SIP token extra time to live	Available if **Authorize by OAuth token** is *On*.	0 seconds
	Optionally extends the time-to-live for simple OAuth tokens (in seconds). Gives users a short window to accept calls after their credentials expire. However, it increases the potential security exposure.	

MRA Access Control Values Applied by the Upgrade

Table 22: MRA access control values applied by the upgrade

Option	Value after upgrade	Previously on...	Now on...

Authentication path	Pre-upgrade setting is applied
	
	Note **SSO mode**=*Off* in X8.9 is two settings in X8.10:
	     • **Authentication path**=*UCM/LDAP*
	     • **Authorize by user credentials**=*On*
	
	    SSO Mode=*Exclusive* in X8.9 is two settings in X8.10:
	     • **Authentication path**=*SAML SSO*
	     • **Authorize by OAuth token**=*On*
	
	    SSO Mode=*On* in X8.9 is three settings in X8.10:
	     • **Authentication path**=*SAML SSO/and UCM/LDAP*
	     • **Authorize by OAuth token**=*On*
	     • **Authorize by user credentials**=*On*
		Both	Expressway-C

Authorize by OAuth token with refresh	On	-	Expressway-C
Authorize by OAuth token (previously SSO Mode)	Pre-upgrade setting is applied	Both	Expressway-C
Authorize by user credentials	Pre-upgrade setting is applied	Both	Expressway-C
Check for internal authentication availability	No	Expressway-E	Expressway-C
Identity providers: Create or modify IdPs	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)

Option	Value after upgrade	Previously on...	Now on...
Identity providers: Export SAML data	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)
Allow Jabber iOS clients to use embedded Safari	No	Expressway-E	Expressway-C
SIP token extra time to live	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)

Configuring HSM Devices on Expressway

Important: Read this First

HSM failure. If an Expressway is configured to use HSM and the HSM subsequently fails, **all services that require encryption will become unavailable**. This includes MRA, calls, web access, and so on.

Factory reset. If the HSM is permanently unavailable for any reason, **you will need to do a factory reset** for the Expressway and then configure a new HSM on the Expressway. A factory reset **reinstalls the software image and resets the Expressway configuration** to the default, functional minimum (see the *Expressway Administrator Guide* for instructions about doing a reset.)

How to Enable and Manage HSM

Use the **HSM configuration** page (**Maintenance** > **Security** > **HSM configuration**) to configure the information needed for Expressway.

Settings are replicated across a cluster.

The **HSM configuration** page settings replicate across all peers in an Expressway cluster. So if you add or remove any settings on one peer, the change replicates to all other peers.

Task 1: Configure Prerequisites

Do the following before you enable Hardware Security Module (HSM) functionality on Expressway:

a.	Add an HSM option key.	**i.** Go to **Maintenance** > **Option keys**.
		ii. In the **Software option** section, enter the option key.
		iii. Click **Add option**. The key appears in the list at the top of the page.

b.	Install the HSM TLP package. You can get this from the same download site as the Expressway software image. The HSM TLP is an archive of HSM provider-specific binaries that are needed for the Expressway to use the HSM.	**i.** Go to **Maintenance** > **Upgrade**. **ii.** In the **Upgrade component** section, click **Choose File** to select the TLP file from your local machine. **iii.** Click **Upgrade**. A message, *Component installation succeeded*, appears at the top of the page and the HSM TLP also appears at the top of the page. You can check the list of all installed modules in the drop-down. **Note** You must add the option key and install the TLP on each peer in the cluster. You cannot enable HSM Mode on a cluster unless all peers have the option key and the TLP.
c.	Deploy an HSM box on the Expressway	To configure an nShield Connect XC HSM: **i.** Set up a Security World and Remote File System (RFS) according to the *nShield Connect User Guide*. **ii.** Configure RFS to an nShield Connect that contains master copies of all the files that the HSM needs. RFS normally resides on a client computer, but it can be located on any computer that is accessible on the network. **iii.** After you deploy RFS and the nShield Connect box, run the following command on RFS: `/opt/nfast/bin/rfs-setup --gang-client --write-noauth <Expressway_ip_address>` HSM certificate management will not work properly on the Expressway if this command is not run.
d.	Have access to a certificate signing authority.	-
e.	Create an HSM-compatible certificate.	See the *Expressway Administrator Guide*, *Security* chapter for instructions.

Task 2: Enable HSM on Expressway

This is the recommended procedure to enable HSM use on Expressway:

Step 1 Go to **Maintenance** > **Security** > **HSM configuration**.

Step 2 In **HSM Settings**, choose the HSM provider from the **HSM Mode** drop-down list.

Step 3 Configure the nShield settings:

a. Enter the RFS IP address and RFS Port. The default port is 9004.

b. Click **Save Configuration**.

The following message is displayed at the top of the page.

```
An HSM Settings updated
```

c. In the **Add Module** section, enter the IP address, Port, ESN (Electronic Serial Number), and KNETI (Network Integrity Key) of the device.

d. Click **Add Module**.

The following message is displayed at the top of the page.

```
An HSM Module successfully added
```

e. The device is now displayed in a table below the **HSM Mode** tab.

f. Repeat the Add Module steps to add more devices.

Step 4 Set the **HSM Mode** to *On* and click **Set Mode**.

The following message is displayed at the top of the page.

```
An HSM Mode successfully updated
```

Note Toggling the HSM Mode to *On/Off* may cause the web to become unavailable. If this happens, reload the browser page.

Results: HSM use is now enabled on the Expressway.

What to do next

To check the HSM operating status see the next section Task 3: Monitor HSM Status Check.

Task 3: Monitor HSM Status Check

After you enable HSM mode, an **HSM Status check** section displays on the **HSM configuration** page. This section displays information about the HSM server and HSM certificate for all Expressway cluster peers, and for all modules on each peer:

HSM server running

1. **TRUE**, after HSM mode is enabled on Expressway, if processes responsible for communicating with the HSM boxes are running on the Expressway.

2. **FALSE**, if processes are not running on the Expressway and an HSM failure alarm is raised.

HSM certificate in use

1. TRUE, when an HSM certificate and private key are in use by Expressway.

2. FALSE, when an HSM certificate and private key are not being used by Expressway. Default state is FALSE. An alarm, `HSM certificate is not used`, is raised on the Expressway - to warn that you are not using an HSM certificate and private key.

After the HSM certificate and private key are deployed to the Expressway, this alarm is lowered and the displayed status changes to TRUE.

The ESN section lists HSM modules that are added during the HSM configuration and are distinguished by their ESN. The other columns define **Connection Status** and **Hardware Status**.

Connection Status

1. OK, if no network issues exist between the Expressway and HSM module.

2. Failed, if network or HSM server connectivity issues exist and an alarm is raised.

Hardware Status

1. OK, if no hardware issues are detected on the HSM box itself.

2. Failed, if there are any hardware or an HSM box configuration issue and an alarm is raised.

Task 4: Next Steps - Generate and Install the HSM Private Key

When HSM is enabled and operating properly, you need to generate and install the HSM private key and certificate on Expressway. For details, see *Managing the Expressway Server Certificate with HSM*, in the *Expressway Administrator Guide*.

How to Delete Modules

✎

| Note | You cannot remove the last device while HSM mode is enabled. You first need to disable HSM mode.

To optionally delete devices (modules) from the Expressway HSM configuration:

Step 1   Go to **Maintenance** > **Security** > > **HSM configuration**.

Step 2   Choose the required device from the list and click **Delete**.

How to Disable HSM

If you decide to disable HSM for any reason, the recommended procedure is:

Step 1   Go to **Maintenance** > **Security** > **HSM configuration**.

Step 2   Set **HSM Mode** to *Off* and click **Set Mode**. This disables HSM usage on the Expressway.

Step 3   Check an individual device or click **Select all** to choose all the modules in the table to delete. (Click **Unselect all** to de-select all devices in the table.)

Step 4   Click **Delete** and then **OK** in the confirmation dialog.