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 1: 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 2: 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 3: 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 can be configured with an IPv4 address or dual stack enabled (IPv4 and IPv6) to support IPv6 clients over MRA. Starting from the X14.2 release, Expressway supports IPv6 clients over MRA.

Note To support IPv6 clients over MRA, enable dual network for CUCM and IMP-related configuration. Dual Networking does not necessarily mean configuring with both IPv4 and IPv6 **addresses**.

- **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 Certificate Requirements, on page 8.

Additional Requirements for ICE Media Path Optimization

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

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.
- IM and Presence can be configured with an IPv4 address or dual stack enabled (IPv4 and IPv6) to support IPv6 clients over MRA. Starting from the X14.2 release, Expressway supports IPv6 clients over MRA.

Note To support IPv6 clients over MRA, enable dual network for CUCM and IMP-related configuration. Dual Networking does not necessarily mean configuring with both IPv4 and IPv6 **addresses**.

- For information on certificate requirements, see Certificate Requirements, on page 8.

CUCM Servers Using Self-Signed Certificates

By default, a CUCM server comes with self-signed certificates. If these are in place, it is impossible to use both **TLS Verify** and **Secure Device Registrations** simultaneously. Either feature can be used independently. However, because the certificates are self-signed, it means *self-signed Tomcat* and *self-signed CallManager* certificates need to be uploaded to the trusted CA list on the Expressway C. When Expressway C searches its trust list to validate a certificate, it will stop once it finds one with a matching subject. Because of this, whichever is higher on the trust list, *tomcat* or *callmanager*, that feature will work. The lower one will fail just as if it was not present.

Solution: Sign your CUCM certificates with a CA (public or private) and trust that CA alone.

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 4: 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 (root and intermediatecertificates) 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 root and intermediate 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 5: 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.

Note Expressway uses mTLS for any MRA connections. mTLS is activated for all MRA connections once Activation Code Onboarding is enabled. This can alter the behavior of the Jabber Client depending on the Operating System.

If you are using Jabber on an Apple Computer, a pop-up will request you to select a certificate from the local *trust store*. If no certificate is chosen, the MRA login still works since mTLS does not need Jabber MRA logins. Only IP Phones need mTLS.

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 6: 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
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 7: MRA-Compatible Endpoints

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

Endpoints	MRA Support
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
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**:
  - When a CUCM node goes down, 78XX / 88XX series phones registered over MRA will continue communicating 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, the Cisco IP Phone forms two static server groups, not a full mesh of server groups for devices behind Expressway-E. Therefore, registration will fail if an Expressway-C and CUCM node goes down and the IP Phone does not have a valid server group.

    For example, Consider a Customer having Clusters E1 and E2, C1 and C2, CUCM sub, and CUCM pub. IP phones form two static server groups based on `getedgeconfigeresponse`:

    ```
    E1 > C1 > CUCM sub
    ```

    ```
    E2 > C2 > CUCM pub
    ```

    If the customer takes down C2 and CUCM sub, the registration fails since there are no valid server groups. The phone does not create full mesh server groups for devices behind Expressway-E.

- **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):

  - 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 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.
- 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.