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

Procedure

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

	Command or Action	Purpose
Step 5	Add Domains, on page 5	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 9	Configure settings for MRA Access Control, including OAuth authentication and SAML SSO settings.
Step 8	Configure OAuth on UC Applications, on page 17	Recommended. If your system supports it, configure OAuth authentication.
Step 9	SAML SSO Configuration, on page 18	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 22	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—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—Refer to this chapter for information on MRA features and optional configurations.
- Onboarding MRA Devices—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.

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.

Enable IPv6 Over MRA

Set up the Expressway-E external LAN to support dual addressing. This configuration will ensure that Expressway supports MRA over IPv6.

Expressway X14.2 release now officially supports MRA client over IPv6. This support was not available earlier. However, to provide this support, a few configuration changes are needed on Expressway, CUCM and other network components.

- Enable Expressway-Edge with dual networking option as "Both".
- Configure the interface used for Outside communication with MRA Client with a Global Unicast IPv6 address.
- DNS needs a valid AAAA record to resolve the IPv6 address of Exp-E. The MRA client will return this during "collab-edge_tls" dns srv query.
- Configure CUCM/IMP Servers for Dual Networking. Setting up an IPv6 address on those servers is not necessary.

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.

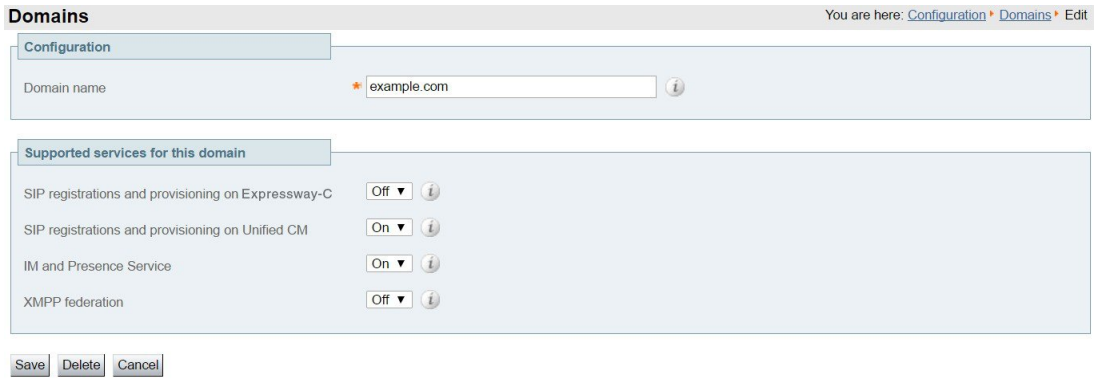
- **SIP registrations and provisioning on Expressway**—Expressway acts as a SIP registrar and accepts registration requests for any SIP domain.
- **SIP registrations and provisioning on Unified CM**—End registration and call control is handled by Unified CM. Expressway acts as a gateway for UC services.
- **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 1: 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

- The Expressway-C uses ICMP to contact the CUCM when using TLS verify mode ON. Ensure that ICMP is allowed on your network between CUCM and Expressway-C.
- 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.
- Currently, there is no published amount of maximum supported Cisco Unified CM/IM and Presence/Cisco Unity Connection server cluster limit for MRA. A single Expressway node cannot handle more than 400 UCM nodes. CUCM supports 20 clusters on a Single Medium OVA Expressway. This does not include different deployment sizes.

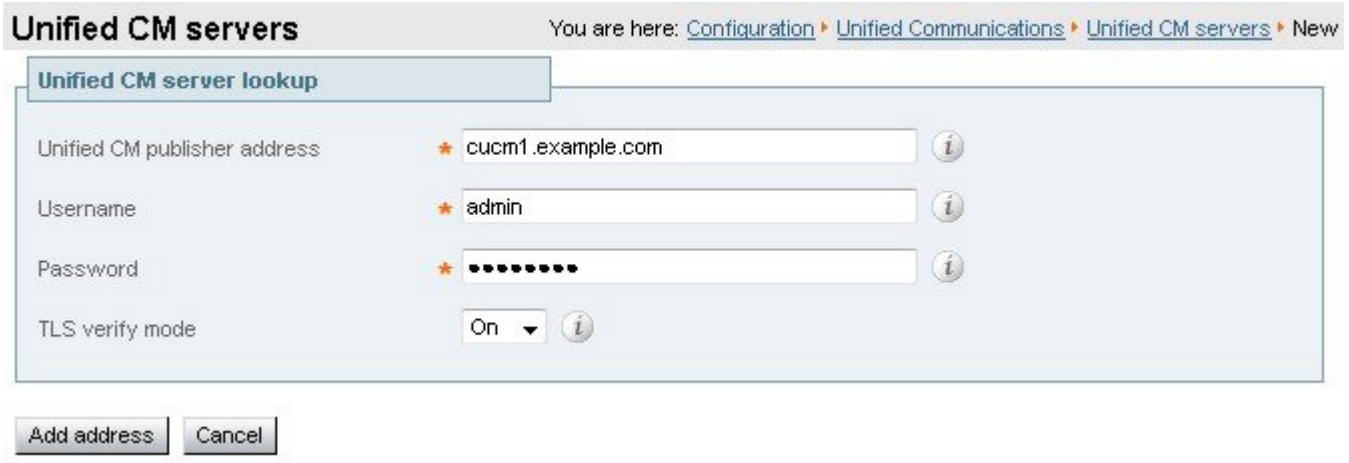
Step 1 On the Expressway-C primary peer, go to **Configuration** > **Unified Communications** > **Unified CM servers**.

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 17.

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 9

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 1: 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 16.
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 13.
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

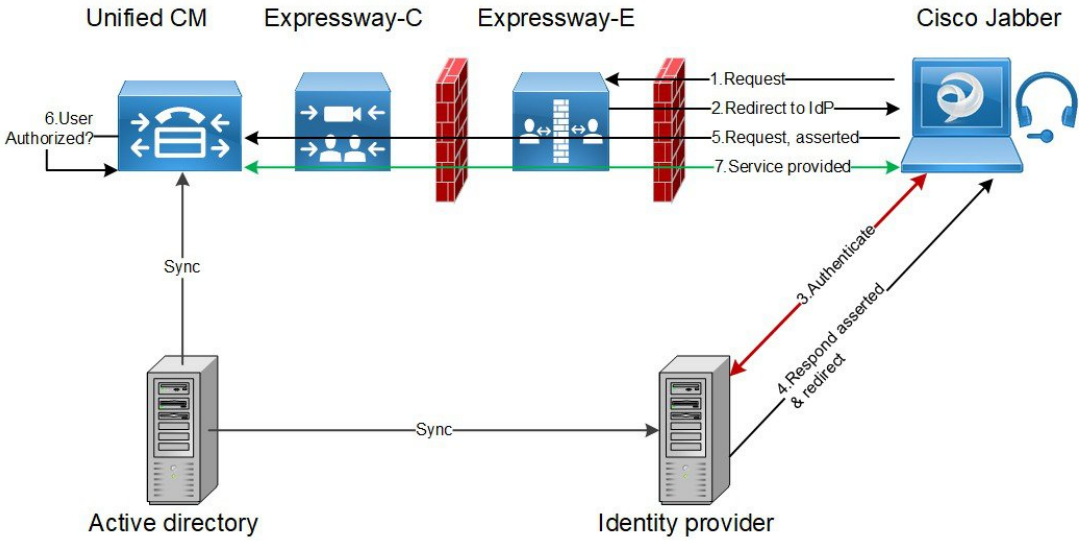
How it works

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 2: 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.
- Although Expressway-C provides its hostname, Unified CM can resolve the Expressway-C FQDN (as issued in the Expressway-C certificate CN/SAN). This is particularly relevant in split DNS environments. In Unified CM **Admin** > **Device** > **Expressway-C**, ensure they are defined as FQDN. Also, verify if the local DNS can resolve Expressway C's FQDN.

  If Unified CM servers are refreshed from Expressway C at any time, it will re-insert the hostname. You will have both FQDN and Hostname, which will cause issues. So, remove the hostname.

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
- Okta, Azure, F5 BIG IP

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 19	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 21	Import the Idp metadata to Expressway-C and complete the configuration.
Step 4	Associate Domains with an IdP, on page 21	In Expressway-C, associate the domain to the Identity Provider.
Step 5	Configure ADFS for SAML SSO, on page 22	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
- The Expressway-C must have a valid connection to the Expressway-E before you can export the Expressway-C's SAML metadata.
- If you have redeployed your Expressway onto a new appliance or Virtual Machine and restored the backup from the original Expressway, it will raise an alarm advising that the "SAML metadata is modified." Select **Download** to clear the alarm. An update to your IDP is not needed, provided you have not performed any other changes.

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.
- 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 2: 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.)
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.