Cisco Expressway X12.5

Release Notes

First Published: January 2019

Last Updated: February 2019

Preview Features Disclaimer

Some features in this release are provided in “preview” status only, because they have known limitations or incomplete software dependencies. Cisco reserves the right to disable preview features at any time without notice. Preview features should not be relied on in your production environment. Cisco Technical Support will provide limited assistance (Severity 4) to customers who want to use preview features.

Contents

Preface

Change History

Table 1 Release Notes Change History

Date	Change	Reason
February 2019	Clarification of Hybrid Services upgrade not requiring release key. Clarify existing OAuth Token Authorization with Jabber item in *Limitations*. Add licensing issue for Jabber Guest versions before 11.1(2), to *Open and Resolved Issues*.	Documentation correction
January 2019	First publication.	X12.5

Supported Platforms

Table 2 Expressway Software Versions Supported by Platform

Platform name	Serial Numbers	Scope of software version support
Small VM (OVA)	(Auto-generated)	X8.1 onwards.
Medium VM (OVA)	(Auto-generated)	X8.1 onwards.
Large VM (OVA)	(Auto-generated)	X8.1 onwards.
CE1200 (Expressway pre-installed on UCS C220 M5L)	52E#####	X8.11.1 onwards
CE1100‡ (Expressway pre-installed on UCS C220 M4L)	52D#####	X8.6.1 onwards.
CE1000* (Expressway pre-installed on UCS C220 M3L)	52B#####	X8.1.1 to X8.10.x No support for any versions after X8.10.x on this hardware.
CE500* (Expressway pre-installed on UCS C220 M3L)	52C#####	X8.1.1 to X8.10.x No support for any versions after X8.10.x on this hardware.

‡ As of 13th November 2018, you cannot order the CE1100 appliance from Cisco. See the End-of-sale announcement for other important dates in the lifecycle of this platform.

Advance Notice - Hardware Service Support for CE500 and CE1000 Appliances to be Withdrawn

Cisco will withdraw support services for the Cisco Expressway CE500 and CE1000 appliance hardware platforms in a future release. More details are available in the End-of-sale announcement.

Related Documents

Table 3 Links to Related Documentation

Installation - virtual machines	*Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page
Installation - physical appliances	*Cisco Expressway CE1200 Appliance Installation Guide* on the Expressway installation guides page
Basic configuration for registrar / single systems	*Cisco Expressway Registrar Deployment Guide* on the Expressway configuration guides page
Basic configuration for firewall traversal / paired systems	*Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the Expressway configuration guides page
Administration and maintenance	*Cisco Expressway Administrator Guide* on the Cisco Expressway Series maintain and operate guides page *Cisco Expressway Serviceability Guide* on the Cisco Expressway Series maintain and operate guides page
Clustering	*Cisco Expressway Cluster Creation and Maintenance Deployment Guide* on the Cisco Expressway Series configuration guides page
Certificates	*Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page
Rest API	*Cisco Expressway REST API Reference Guide* on the Expressway configuration guides page
Unified Communications	*Mobile and Remote Access Through Cisco Expressway* on the Expressway configuration guides page
Cisco Meeting Server	*Cisco Meeting Server with Cisco Expressway Deployment Guide* on the Expressway configuration guides page *Cisco Meeting Server API Reference Guide* on the Cisco Meeting Server programming guides page Other Cisco Meeting Server guides are available on the Cisco Meeting Server configuration guides page
Cisco Webex Hybrid Services	Hybrid services knowledge base
Microsoft infrastructure	*Cisco Expressway with Microsoft Infrastructure Deployment Guide* on Expressway configuration guides page *Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet* on Expressway configuration guides page
Multiway Conferencing	Cisco TelePresence Multiway Deployment Guide on Expressway configuration guides page

Features in X12.5

Change in Software Version Numbering

To better align with other Cisco product versions, this first release after X8.11.x is numbered X12.5. There is no Expressway X12.0 release. And there are no other intermediate Expressway releases between X8.11.x and X12.5.

CAUTIONS - Please Read Before you Install X12.5

Release keys are required for upgrade (and to downgrade to old release), except for certain deployments of Cisco Webex Hybrid Services connectors.

- **Currently you need an X12 Release Key to install this software**, except for certain deployments where the Expressway is registered as a connector host for Hybrid Services (see below).
- If you need to revert for any reason to the old software, you will need an X8 Release Key to downgrade.

If Expressway is a Hybrid Services connector

Upgrading your connector host Expressway to X12.5.x (from X8.10.x or X8.11.x) does *not* require a release key if both these conditions apply to the Expressway:

- It was configured for Hybrid Services using the Service Select wizard (which disables the release key requirement).
- It does not already have a release key. That is, the Expressway is not being used as anything other than a connector host.

These conditions are met in most Hybrid Services deployments. However, if your deployment requires the Expressway connector host to have a release key, then you will need a new release key to upgrade to this release.

Expressways on X8.1.x or earlier need a two-stage upgrade.If you are upgrading a system on X8.1.x or earlier software, you must do an intermediate upgrade to X8.10 first, before you upgrade to this release (see Upgrade Prerequisites and Software Dependencies, page 21 for details). Otherwise there is a risk of data corruption.

Cisco Jabber 12.5 or later is needed if you want chat/messaging services over MRA with authentication using OAuth refresh (self-describing tokens) and you configure IM and Presence Service presence redundancy groups. With this release of Expressway, user login failures will occur in this scenario if Jabber versions before 12.5 are in use.

Withdrawn or Deprecated Features in this Release

These features or software **are no longer supported from Expressway version X12.5**.

- Cisco Advanced Media Gateway (AM Gateway)
- For VM deployments, VMware ESXi virtual hardware versions ESXi5.x

These features are deprecated from Expressway version X12.5, and **support will be withdrawn in a subsequent release**.

- FindMe device/location provisioning service
- Smart Call Home

Summary of New Features in this Release

IMPORTANT! New features in software version X12.5 and later are not supported for the Cisco TelePresence Video Communication Server product (VCS). They apply only to the Cisco Expressway Series product (Expressway). This software version is provided for the VCS for maintenance and bug fixing purposes only.

Table 4 Feature History by Release Number

Feature / change	X12.5 (Cisco Expressway Series)
Virtualized Systems - ESXi 6.0, 6.5, and 6.7 Qualification	Supported
ACME (Automated Certificate Management Environment) support on Expressway-E	Supported
Single SAML for Clusters	Supported
MRA: SIP UPDATE Method Support for Session Refresh	Supported
MRA: Media Path Optimization for ICE	Supported
MRA: Improved Handling of Dual Network Domains with no Split DNS	Supported
MRA: Device Onboarding with Activation Codes	Preview
MRA: OAuth with Refresh (Self-Describing) on Unified CM SIP Lines	Preview
MRA: Support for Encrypted iX	Preview
MRA: Support for Headset Management	Preview
SIP Proxy to Multiple Meeting Server Conference Bridges - Support for Cisco Meeting Server Load Balancing (Not new in X12.5. Included for information due to its preview status)	Preview
Cisco Meeting App can use Expressway-E TURN Server (Not new in X12.5. Included for information due to its preview status)	Preview
Multiple Presence Domains over MRA (Not new in X12.5. Included for information due to its preview status)	Preview
Smart Call Home (Not new in X12.5. Included for information due to its preview status)	Deprecated and Preview

Virtualized Systems - ESXi 6.0, 6.5, and 6.7 Qualification

This item applies to virtualized systems. The VMware ESXi virtual hardware versions required to host Expressway VMs have changed in this release and **the minimum required version is now ESXi 6.0** (ESXi 5.0 and ESXi 5.5 are no longer supported by VMware). The following ESXi versions have been successfully tested for Expressway X12.5:

- ESXi 6.0
- ESXi6.5 Update 2
- ESXi6.7 (the ESXi Side-Channel-Aware Scheduler is not supported with X12.5)

ACME Automatic Certificate Signing

From X12.5 the Cisco Expressway Series supports the ACME protocol (Automated Certificate Management Environment) which enables automatic certificate signing and deployment to the Cisco Expressway-E from a certificate authority such as Let's Encrypt. The main benefit of this feature is to generate low-cost server certificates to identify the Expressway-E, thereby reducing the cost of Expressway-based deployments like MRA (Mobile and Remote Access).

Due to the underlying validation mechanism this feature is most likely to be useful for MRA deployments. For Business to Business (B2B) applications, it's not always practical to include your primary domain in ACME certificates.

The configuration process is simple. You enter some information on the Cisco Expressway-E to create a certificate signing request (CSR), then the Expressway's ACME client interacts with the certificate authority to request the certificate. The Expressway downloads the certificate and you click a button to deploy it. After this manual step, you can schedule renewal so that the certificate does not expire—because ACME certificates are deliberately short-lived.

One compromise of the ACME protocol is that it requires an inbound HTTP connection to port 80 on the Cisco Expressway-E. You can manage this risk with the Expressway's security features or, for highly secure environments, you can disable ACME and use the traditional CSR procedure with your preferred certificate authority.

No Jabber Guest support with ACME

Currently Expressway does not support ACME with Jabber Guest deployments.

Single SAML for Clusters

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). Now, both cluster-wide and per-peer modes are supported. The settings are on **Configuration > Unified Communications > Configuration > SAML Metadata**.

For the cluster-wide mode, export the metadata file from the primary peer for the SAML agreement. You must not export it from the other peers. If you change the primary peer for any reason, you must again export the metadata file from the new primary peer, and then reimport the metadata file to the IdP.

Additionally for the cluster-wide mode, you must generate a self-signed certificate. The certificate is distributed among the peers for verifying SAML responses from the IdP. The metadata file exported from this cluster contains the public key of this certificate. The IdP uses the public key to sign the SAML responses.

MRA: Media Path Optimization for ICE

From X12.5, we support Interactive Connectivity Establishment (ICE) passthrough to allow MRA-registered endpoints to pass media directly between endpoints by bypassing the WAN and the Cisco Expressway Series.

A new **Status > ICE Passthrough metrics** page in the web user interface displays metrics data about completed ICE passthrough calls.

More information

Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway* guide on the Expressway Configuration Guides page.

Background information about ICE in Expressway is in *About ICE and TURN Services* in the *Cisco Expressway Administrator Guide* on the Expressway Maintain and Operate Guides page.

The ICE protocol is defined in RFC 5245.

MRA: Improved Handling of Dual Network Domains

The main application for this feature is for MRA deployments with separate internal and external network domains. It's no longer a requirement to add a *_cisco-UDS* SRV record to the internal 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.

Note that this feature is for MRA-connected devices. The *_cisco-uds* record is still required for local/internal Jabber clients.

Limitation: This case is not supported for CUCM 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.

There are no configuration or interface changes for this feature. More details about how to configure network domains and DNS records in Expressway for MRA are in the *Expressway Mobile and Remote Access Deployment Guide*.

MRA: SIP Update Method Support for Session Refresh

From X12.5, the Cisco Expressway Series supports the SIP UPDATE method over MRA connections for session refresh purposes only. That is, to send and receive session timers for a periodic session refresh (RFC 4028). SIP UPDATE for session refresh is not supported for Business-to-Business deployments.

CAUTION: Do not enable this method unless it is absolutely necessary. Only enable SIP UPDATE for session refresh if RE-INVITE based session refresh has issues between Expressway-C and Unified CM.

Expressway uses the re-INVITE method for session refresh by default. To use the SIP UPDATE method, the **SIP UPDATE for session refresh** setting must be enabled on the zones that traverse SIP signaling (**Configuration > Zones > Zones**). To configure SIP UPDATE as a preferred method for zones that are auto-generated, enable the **SIP UPDATE for the session refresh** setting when you discover each Unified CM node (**Configuration > Unified Communications > Unified CM Servers**).

SIP UPDATE for session refresh support over MRA has some limitations. For example, the following features that rely on the SIP UPDATE method (RFC 3311) will fail:

- 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.

(PREVIEW) MRA: OAuth with Refresh (Self-Describing) on Unified CM SIP Lines

Although this feature is in the Cisco Expressway Series from X12.5, **it has external software dependencies and may not work until these dependencies are satisfied**.

Subject to running supported versions of Unified CM and Jabber, Expressway X12.5 and later supports OAuth with refresh on the Unified CM SIP line interface, for Jabber clients only. When this option is enabled on the Unified CM SIP line and the Jabber client, on-premises clients are authorized using self-describing tokens instead of client certificates.

Support for OAuth with refresh on the Unified CM SIP line means that secure SIP and SRTP is possible without Certificate Authority Proxy Function (CAPF). It enables end-to-end encryption of ICE and ICE passthrough calls over MRA.

How to enable OAuth with refresh on the Unified CM SIP line interface

1. On the Unified CM node, do the following:
   a. Enable SIP OAuth Mode using the CLI command `utils sip-oauth enable`.
   b. Verify if SIP OAuth is set to listen on default ports (**System > Cisco Unified CM**).

      The default ports are 5090 for on-premises and 5091 for MRA. To avoid port conflicts, ensure that these ports are not configured to listen any existing SIP Trunk in Unified CM.

   The settings to enable SIP OAuth on the SIP line on Unified CM are summarized here for convenience. For detailed information, see the Cisco Unified Communications Manager documentation.

2. After you enable Unified CM for SIP OAuth, discover or refresh the Unified CM nodes in Expressway-C.

   A new CEOAuth (TLS) zone is created automatically in Expressway-C. For example, *CEOAuth <Unified CM name>*. A search rule is created to proxy the requests originating from the on-premises endpoints towards the Unified CM node. This zone uses TLS connections irrespective of whether Unified CM is configured with mixed mode. To establish trust, Expressway-C also sends the hostname and Subject Alternative Name (SAN) details to the Unified CM cluster
3. Upgrade the Jabber clients to Cisco Jabber 12.5 or later, which is required for MRA or on-premises clients to connect using OAuth with refresh.
4. Enable OAuth authorization on the Phone Security Profile (**System > Security > Phone Security Profile**) and apply the Phone Security Profile on the Jabber clients.

(PREVIEW) MRA: Device Onboarding with Activation Codes

Although this feature is in the Cisco Expressway Series from X12.5, **it has external software dependencies and cannot currently be used** until these dependencies are satisfied and the feature is fully implemented in the solution.

This feature optionally allows MRA-compliant devices to easily and securely register over MRA using an activation code. It's enabled with the **Allow activation code onboarding** setting on the **Configuration > Unified Communications > Configuration** page.

Onboarding with an activation code requires mutual TLS (mTLS) authentication. TLS is automatically enabled or disabled on the MRA port 8443, depending on whether onboarding with an activation code is enabled or disabled.

Existing deployments need to refresh CUCMs before this feature can be used

If you have upgraded an existing Expressway from an earlier release than X12.5, refresh the currently configured Unified CMs on Expressway before you use this feature. To do this, go to **Unified Communications > Configuration**, select all the configured Unified CMs and click **Refresh**. This task is not necessary for any Unified CMs that you add later.

(PREVIEW) MRA: Support for Headset Management

Although this feature is in the Cisco Expressway Series from X12.5, **it has external software dependencies and may not work until these dependencies are satisfied**.

Expressway supports user headset management by Cisco Unified Communications Manager administrators, over MRA connections. This means that MRA-connected users no longer have to do their own headset configuration.

Expressway does not currently support the */headset/metrics* API.

(PREVIEW) MRA: Support for Encrypted iX (for ActiveControl)

Although this feature is in the Cisco Expressway Series from X12.5, **it has external software dependencies and may not work until these dependencies are satisfied**.

ActiveControl over MRA is already supported with encrypted phone profiles. This feature will allow MRA video endpoints and Jabber clients with non-secure phone security profiles to negotiate ActiveControl so that users can see roster lists, layouts, and other iX-dependent ActiveControl features in video meetings.

There are no configuration or interface changes for this feature. However, you may need to rediscover your Cisco Unified Communications Manager servers after you upgrade the Expressway.

Cisco Webex Hybrid Services with Expressway X12.5

- Some Expressway-based Hybrid Services require that you configure the connector host as a cluster, even if there is only one peer in the cluster (" cluster of one"). **Be very careful when modifying the Clustering configuration that you do not clear all Peer N address fields and Save the configuration**, unless you intend to factory reset the Cisco Expressway. You will lose your registration, all your connectors, and all associated configuration. See Features in X12.5, page 6.

- The Management Connector must be up to date before you upgrade Expressway. Authorize and accept any Management Connector upgrades advertised by the Cisco Webex cloud before you try to upgrade Expressway. Failure to do so may cause issues with the connector after the upgrade.
- Expressways that will be used to host connectors for Cisco Webex Hybrid Services must be running a supported Expressway software version now, before you register them to Cisco Webex. (You can upgrade just the Management Connector component on the Expressway, without needing to upgrade the whole Expressway.)

  For details about which versions of Expressway are supported for hybrid connector hosting, see Connector Host Support for Cisco Webex Hybrid Services
- Upgrading your connector host Expressway to X12.5.x (from X8.10.x or X8.11.x) does *not* require a release key if both these conditions apply to the Expressway:
  - It was configured for Hybrid Services using the Service Select wizard (which disables the release key requirement).
  - It does not already have a release key. That is, the Expressway is not being used as anything other than a connector host.

  These conditions are met in most Hybrid Services deployments. However, if your deployment requires the Expressway connector host to have a release key, then you will need a new release key to upgrade to this release.

REST API Expansion

We continue to expand the REST API to simplify remote configuration. We are adding REST API access to configuration, commands, and status information when we add new features, but are also selectively retrofitting the REST API to features that were introduced in earlier versions.

For example, third party systems, such as Cisco Prime Collaboration Provisioning, can use the API to control the following features / services on the Expressway:

Configuration APIs	API introduced in version
Clustering	X8.11
Smart Call Home	X8.11
Microsoft Interoperability	X8.11
B2BUA TURN Servers	X8.10
Admin account	X8.10
Firewall rules	X8.10
SIP configuration	X8.10
Domain certificates for Server Name Identification	X8.10
MRA expansion	X8.9
Business to business calling	X8.9
MRA	X8.8

The API is self-documented using RESTful API Modeling Language (RAML). You can access the RAML definitions for your system at `https://<ip address>/api/provisioning/raml`. A high-level summary of how to access and use the API is available in *Cisco Expressway REST API Summary Guide* on the Expressway installation guides page.

All Preview Features Including from Earlier Releases

The following features are Preview status only. Some of them were originally introduced as Preview features in X8.11.x or earlier.

- Device Onboarding with Activation Codes over MRA
- OAuth on Unified CM SIP Lines over MRA
- Headset Management over MRA
- Encrypted iX (for ActiveControl) over MRA
- Support for Meeting Server Load Balancing (SIP Proxy to Multiple Meeting Server Conference Bridges)
- Multiple Presence Domains / Multiple IM Address Domains over MRA
- Cisco Meeting App with Expressway-E TURN Server
- (Now deprecated) Smart Call Home

(PREVIEW) SIP Proxy to Multiple Meeting Server Conference Bridges (Support for Meeting Server Load Balancing)

This feature is currently in preview status only. It is not supported with Cisco Meeting Server software version 2.3 or earlier. Also, a Limitation currently exists regarding support for dual-homed conferences with a Meeting Server cluster.

From X8.11, Cisco Expressway Series supports the mechanism that is used to load balance the calls between Meeting Servers that are in call bridge groups.

When Cisco Meeting Servers are in a call bridge group, and a participant tries to join a space on a server that has no capacity, that server rejects the call with the response code " 488 Not Acceptable Here" . This call is then rerouted to another server by the call control layer. That other server then sends a SIP INVITE to the call control layer, using the original call details. The participant is now in the correct space, on a different Meeting Server. In cases where there is capacity in the “second” server, but another Meeting Server has more capacity, it asks that Meeting Server in the group to send the SIP INVITE.

There is a new setting in the neighbor zone called Meeting Server load balancing which must be enabled (**Configuration > Zones > Zones > Zone Name > Advanced**). This allows the Cisco Expressway's B2BUA to process the INVITE from the " second" Meeting Server to enable the participant to connect.

We recommend that Meeting Server load balancing is set to *On* regardless of whether endpoints are registered with Expressway or with Unified CM.

Supported and Unsupported Functionality

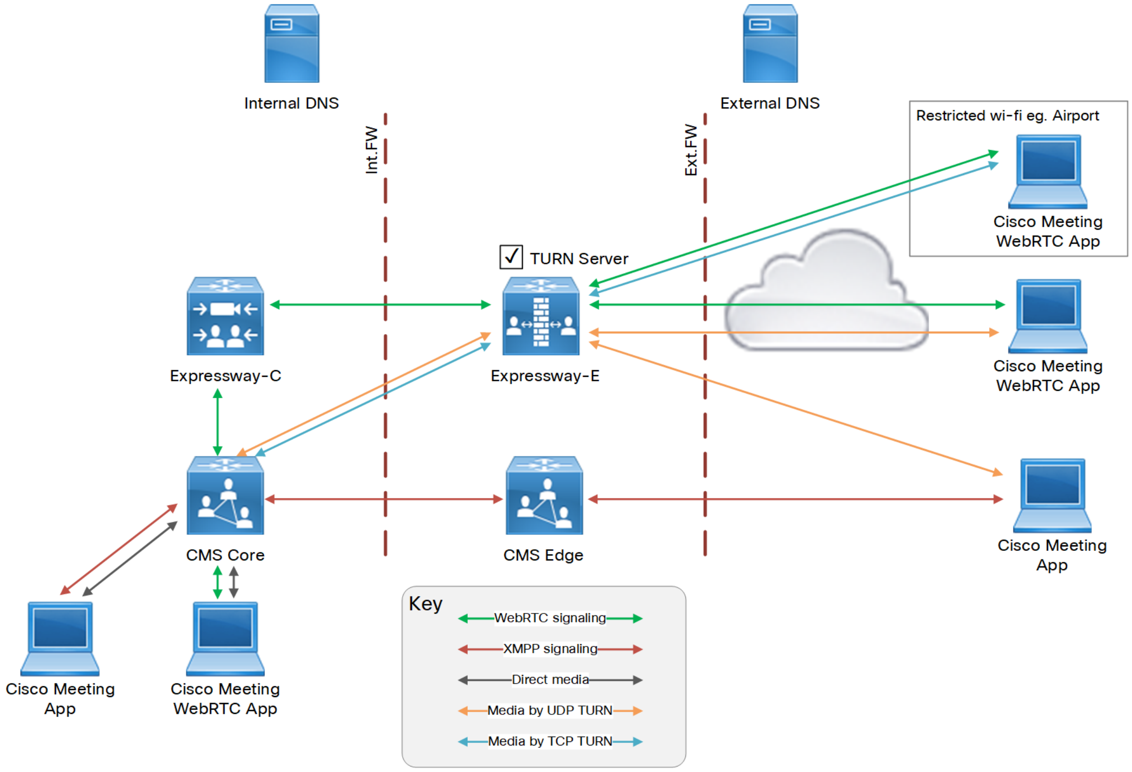
- Cisco Expressway invokes its B2BUA to process the call replacement.
- Load balancing of calls from registered H.323 endpoints is also supported.
- Different encryption modes can be applied on call legs to and from Cisco Expressway.
- Calls with DTLS-secured media are not supported.

(PREVIEW) Cisco Meeting App with Expressway-E TURN Server

This feature is currently in preview status only.

Owing to TURN server enhancements in X8.11, it is possible to use the Expressway-E TURN server for media path discovery and media relay between the Cisco Meeting App and the Cisco Meeting Server, even when that Expressway-E is being used to proxy WebRTC to the Meeting Server.

Figure 1 Cisco Meeting WebRTC App and Cisco Meeting App sharing a TURN server



In the diagram, the Expressway-E is configured to listen on TCP 443 for TURN requests and for WebRTC requests. The TURN clients (Meeting Server Core, Meeting App, and Cisco Meeting WebRTC App) will all try to use UDP 3478 for TURN requests.

If the WebRTC App cannot make the outbound connection to UDP 3478, it uses the TCP override port, which is 443 by default, to request media relays.

The Meeting Server Edge is still required to traverse the XMPP signalling for Cisco Meeting Apps. However, there is no need to use the TURN services of the Meeting Server Edge server.

(PREVIEW - now DEPRECATED) Smart Call Home

This feature is currently in preview status only. **It is deprecated from X12.5 and will not be supported in future.**

This feature is deprecated from Expressway X12.5, and **support will be withdrawn in a subsequent release**.

Smart Call Home is an embedded support capability for Expressway. It offers proactive diagnostics and real-time alerts, enabling higher network availability and increased operational efficiency. Smart Call Home notifies users of Schedule- and Event-based notifications.

- Schedule-based notifications: inventory, telemetry and configuration messages used to generate a Device Report and improve hardware and software quality by identifying failure trends. You can find these notifications posted on the first day of every month.
- Event-based notifications: ad hoc events already supported by Expressway such as alarms and ACRs. You will find these notifications posted to the Smart Call Home server as and when they occur.

Note: Although the web user interface includes an option for SMTP with Smart Call Home, currently this is not actually implemented in the Expressway.

(PREVIEW) Multiple Presence Domains / Multiple IM Address Domains over MRA

This feature is currently in preview status only.

Jabber 10.6 and later can be deployed into an infrastructure where users are organized into more than one domain, or into domains with subdomains (subject to IM and Presence Service 10.0.x or later).

Open and Resolved Issues

Bug Search Tool Links

Follow the links below to read the most recent information about the open and resolved issues in this release.

- All open issues, sorted by date modified (recent first)
- Issues resolved by X12.5

Notable Issues in this Version

Licensing issues with Jabber Guest calls in Single NIC deployments

Currently the software has some unexpected rich media session (RMS) licensing behavior for Jabber Guest calls in Single NIC deployments.

- The Expressway-E should count one RMS license for each Jabber Guest call, but it does not. This issue may cause confusion about the server's load, because usage appears low even when the server is processing multiple calls. CDETS CSCva36208 refers.
- **This issue only applies to users who have a Jabber Guest version earlier than release 11.1(2)**, users with 11.1(2) and later are not affected. In affected cases, although each Jabber Guest call ought to consume an RMS license on the Cisco Expressway-E, in reality the RMS licenses are consumed on the Cisco Expressway-C. This issue was identified in X8.10 and CDETS CSCvf34525 refers. Contact your Cisco representative if you are affected by it.

Note that we recommend the Dual NIC Jabber Guest deployment.

Limitations

Some Expressway Features are Preview or Have External Dependencies

Important: We aim to provide new Expressway features as speedily as possible. Sometimes it is not possible to officially support a new feature because it may require updates to other Cisco products which are not yet available, or known issues or limitations affect some deployments of the feature. If customers may still benefit from using the feature, we mark it as "preview" in the release notes. Preview features may be used, **but you should not rely on them in production environments** (see Preview Features Disclaimer, page 1). Occasionally, we may recommend that a feature is not used until further updates are made to Expressway or other products.

Expressway features which are provided in preview status only in this release, are listed in the Feature History table earlier in these notes.

Unsupported Functionality

- The Expressway does not terminate DTLS. We do not support DTLS for securing media and SRTP is used to secure calls. Attempts to make DTLS calls through Expressway will fail. The DTLS protocol is inserted in the SDP but only for traversing the encrypted iX protocol.
- From X12.5, Expressway provides limited SIP UPDATE support over MRA connections for session refresh purposes only, as specified by RFC 4028. However, you should not switch this on unless you have a specific requirement to use this capability. Any other use of SIP UPDATE is not supported and features that rely on this method will not work as expected.
- Audio calls may be licensed as video calls in some circumstances. Calls that are strictly audio-ONLY consume fewer licenses than video calls. However, when audio calls include non-audio channels, such as the iX channel that enables ActiveControl, they are treated as video calls for licensing purposes.

Mobile and Remote Access Limitations

Important: If you use Expressway for Mobile and Remote Access (MRA), various unsupported features and limitations currently exist. These are detailed in *Supported and Unsupported Features with Mobile and Remote Access* in the X8.11 *Mobile and Remote Access Through Cisco Expressway* guide.

Some recent Cisco IP Phones in both the 8800 Series and 7800 Series do not currently support MRA at all. For details of which 7800/8800 Series phones support MRA, see the *Prerequisites* section of the *Mobile and Remote Access Through Cisco Expressway* guide, or ask your Cisco representative.

SIP UPDATE for session refresh support over MRA has some limitations. For example, the following features that rely on the SIP UPDATE method (RFC 3311) will fail:

- 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.

Spurious Alarms when Adding or Removing Peers in a Cluster

When a new peer is added to a cluster, the system may raise multiple 20021 Alarms (*Cluster communication failure: Unable to establish...*) even if the cluster is in fact correctly formed. The alarms appear on the existing peers in the cluster. The unnecessary alarms are typically lowered after at least 5 minutes elapses from the time that the new peer is successfully added.

These alarms also occur if a peer is removed from a cluster. This is generally valid alarm behavior in the case of removing a peer. However, as in the case of adding a peer, the alarms may not be lowered for 5 minutes or more.

CE1200 Appliance

- In certain scenarios, issues exist with restores of an Expressway-E onto a CE1200 appliance from a CE1100 or earlier appliance backup. More details are provided in the upgrade instructions, including how to resolve each issue:
  - The CE1200 appliance may restore as an Expressway-C.
  - An incorrect banner may display in the web user interface.
- The CE1200 appliance requires Expressway minimum software version X8.11.1 or later. Although the system does not prevent downgrades to an earlier software version, Cisco does not support appliances on earlier versions.
- The Expressway allows you to add or delete Traversal Server or Expressway Series keys through the CLI, but in practice these keys have no effect in the case of CE1200 appliances. The service setup wizard (Type setting) manages whether the appliance is an Expressway-C or an Expressway-E, rather than the Traversal Server key as for earlier appliances.

Virtual Systems

With physical Expressway appliances, the **Advanced Networking** option allows the speed and duplex mode to be set for each configured Ethernet port. You cannot set port speeds for virtual machine-based Expressway systems.

Also, virtual machine-based systems always show the connection speed between Expressway and Ethernet networks as 10000 Mb/s, regardless of the actual physical NIC speed. This is due to a limitation in virtual machines, which cannot retrieve the actual speed from the physical NIC(s).

Medium Appliances with 1 Gbps NIC - Demultiplexing Ports

If you upgrade a Medium appliance with a 1 Gbps NIC to X8.10 or later, Expressway automatically converts the system to a Large system. As a result, Expressway-E listens for multiplexed RTP/RTCP traffic on the default demultiplexing ports for Large systems (36000 to 36011); instead of on the demultiplexing ports that are configured for Medium systems. In this case, the Expressway-E drops the calls because ports 36000 to 36011 are not open on the firewall. From X8.11.3 you can manually change the system size back to Medium, through the **System > Administration settings** page (select *Medium* from the **Deployment Configuration** list). If you encounter this issue in a release earlier than X8.11.3, the workaround is to open the default demultiplexing ports for Large systems on the firewall.

Language Packs

If you translate the Expressway web user interface, new Expressway language packs are available from X8.10.3. Older language packs do not work with X8.10.*n* software (or X8.9.*n*). Instructions for installing or updating the packs are in the *Expressway Administrator Guide*.

Option Keys Only Take Effect for 65 Keys or Fewer

If you try to add more than 65 option keys (licenses), they appear as normal in the Expressway web interface (**Maintenance > Option keys)**. However, only the first 65 keys take effect. Additional keys from 66 onwards appear to be added, but actually the Expressway does not process them. CDETS CSCvf78728 refers.

XMPP Federation-Behavior on IM&P Node Failure

If you use XMPP external federation, be aware that if an IM and Presence Service node fails over to a different node after an outage, the affected users are not dynamically moved to the other node. Expressway does not support this functionality, and it has not been tested.

Cisco Webex Calling May Fail with Dual-NIC Expressway

This issue applies if you deploy Expressway with a dual-NIC Expressway-E. Cisco Webex Calling requests may fail if the same (overlapping) static route applies to both the external interface and the interface with the Expressway-C. This is due to current Expressway-E routing behavior, which treats Webex INVITES as non-NAT and therefore extracts the source address directly from the SIP Via header.

We recommend that you make static routes as specific as possible, to minimize the risk of the routes overlapping, and this issue occurring.

Microsoft Federation with Dual Homed Conferencing-SIP Message Size

If you use dual homed conferencing through Expressway and Meeting Server with an AVMCU invoked on the Microsoft side, the maximum SIP message size must be set to 32768 bytes (the default) or greater. It's likely that you will need a greater value for larger conferences (that is, from around nine or more participants upwards). Defined via **SIP max size** on **Configuration > Protocols > SIP**.

Intradomain Microsoft Interop with Expressway and Cisco Meeting Server

If you use Meeting Server for Microsoft interoperability, a limitation currently applies to the following intradomain/intracompany scenario:

*You deploy separate Microsoft and standards-based SIP networks in a **single domain** and in a configuration that has an Expressway-E **directly facing** a Microsoft front end server (because you use internal firewalls between subnetworks, or for any other reason). For example, Cisco Unified Call Manager in one (sub)network and Microsoft in a second (sub)network, inside the same domain.*

In this case we do not generally support Microsoft interoperability between the two networks, and calls between Meeting Server and Microsoft will be rejected.

Workaround

If you are not able to deploy the intradomain networks without an intervening Expressway-E (you cannot configure Meeting Server <> Expressway-C <> Microsoft), a workaround is to deploy an Expressway-C in each subnet, with an Expressway-E to traverse between them. That is:

Meeting Server <> Expressway-C <> Firewall <> Expressway-E <> Firewall <> Expressway-C <> Microsoft

Licensing Behavior with Chained Expressway-Es

If you chain Expressway-Es to traverse firewalls (from X8.10), be aware of this licensing behavior:

- If you connect through the firewall to the Cisco Webex cloud, each of the *additional* Expressway-Es which configure a traversal zone with the traversal client role, will consume a Rich Media Session license (per call). As before, the original Expressway-C and Expressway-E pair do not consume a license.
- If you connect through the firewall to a third-party organization (Business to Business call), *all* of the Expressway-Es in the chain, including the original one in the traversal pair, will consume a Rich Media Session license (per call). As before, the original Expressway-C does not consume a license.

OAuth Token Authorization with Jabber

Regardless of any MRA access policy settings configured on Cisco Unified Communications Manager, if you have Jabber users running versions before 11.9 (no token authentication support) and Expressway is configured to allow non-token authentication methods, then those users are able to authenticate by username and password or by traditional single sign-on.

Note: If your deployment opts to strictly enforce MRA policy, then endpoints that don't support self-describing tokens (" OAuth with Refresh") cannot use MRA. This includes Cisco TelePresence TC and CE endpoints, and Cisco IP Phone 7800 or 8800 Series endpoints that don’t have the onboarding with activation codes feature.

Expressway Forward Proxy

CAUTION: At present the built-in Expressway forward proxy is not suitable for use with Cisco Unified Communications Manager and/or IM and Presence Service, and is not supported for those products. The forward proxy is in the Expressway user interface, but it should not be used. This means that if you require a forward proxy deployment, you need to use a suitable third-party HTTPS proxy.

TURN Servers

Currently, the TCP 443 TURN service and TURN Port Multiplexing are not supported through the CLI. Use the Expressway web interface to enable these functions (**Configuration > Traversal > TURN**).

Interoperability

Test Results

The interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco TelePresence products.

Notable Interoperability Concerns

X8.7.x (and earlier versions) of Expressway are not interoperable with Cisco Unified Communications Manager IM and Presence Service 11.5(1) and later. This is caused by a deliberate change in that version of IM and Presence Service, which has a corresponding change in Expressway X8.8 and later.

To ensure continuous interoperability, you must upgrade the Expressway systems *before* you upgrade the IM and Presence Service systems. The following error on Expressway is a symptom of this issue:

```
Failed Unable to Communicate with <IM&P node address>. AXL query HTTP error "'HTTPError:500'"
```

Which Expressway Services Can Run Together?

The *Cisco Expressway Administrator Guide* on the Cisco Expressway Series maintain and operate guides page details which Expressway services can coexist on the same Expressway system or cluster. See the table " *Services That Can be Hosted Together*" in the Introduction section. For example, if you want to know if MRA can coexist with CMR Cloud (it can) the table will tell you.

Upgrading to X12.5

Upgrade Prerequisites and Software Dependencies

CAUTION: This section has important information about issues that may prevent the system working properly after an upgrade. Before you upgrade, please review this section and complete any tasks that apply to your deployment.

Release keys are required for upgrade (and to downgrade to old release), except for certain deployments of Cisco Webex Hybrid Services connectors.

- **Currently you need an X12 Release Key to install this software**, except for certain deployments where the Expressway is registered as a connector host for Hybrid Services (see below).
- If you need to revert for any reason to the old software, you will need an X8 Release Key to downgrade.

If Expressway is a Hybrid Services connector

Upgrading your connector host Expressway to X12.5.x (from X8.10.x or X8.11.x) does *not* require a release key if both these conditions apply to the Expressway:

- It was configured for Hybrid Services using the Service Select wizard (which disables the release key requirement).
- It does not already have a release key. That is, the Expressway is not being used as anything other than a connector host.

These conditions are met in most Hybrid Services deployments. However, if your deployment requires the Expressway connector host to have a release key, then you will need a new release key to upgrade to this release.

Expressway systems on X8.1.x or earlier need a two-stage upgrade.

If you are upgrading a system which is running software older than version X8.2, **you must first upgrade to an intermediate release before you install this X12.5 software.** Otherwise there is a **risk of data corruption**, due to database format changes in our later software versions. We recommend upgrading to X8.10.x (latest maintenance release) as the intermediate release. However, if you have specific reasons to prefer an earlier software version, you can upgrade to any version from and including X8.2, before you install this X12.5 software. (Version X8.2 is not affected by this issue—only versions from X8.1.x and earlier.)

- Version X8.10.n release notes are available here: https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-release-notes-list.html
- Version X8.10.n software is available here:https://software.cisco.com/download/type.html?mdfid=286255326&flowid=77866

All Deployments

We do not support downgrades. Do not install a previous Expressway version onto a system that is running a newer version. If you do so, the system configuration will not be preserved.

From X8.11.1, when the system restarts after the upgrade it uses a new encryption mechanism. This is due to the unique root of trust for every software installation, introduced in X8.11.1.

X8.8 and later versions are more secure than earlier versions. Upgrading could cause your deployments to stop working as expected, and you must check for the following environmental issues before you upgrade to X8.8 or later:

- Certificates: Certificate validation was tightened up in X8.8.
  - Try the secure traversal test before and after upgrade (**Maintenance > Security > Secure traversal test**) to validate TLS connections.
  - Are your Unified Communications nodes using valid certificates that were issued by a CA in the Expressway-Cs' trust list?

  - If you use self-signed certificates, are they unique? Does the trusted CA list on Expressway have the self-signed certificates of all the nodes in your deployment?
  - Are all entries in the Expressway's trusted CA list unique? You must remove any duplicates.
  - If you have TLS verify enabled on connections to other infrastructure (always on by default for Unified Communications traversal zone, and optional for zones to Unified Communications nodes) you must ensure that the hostname is present in the CN or SAN field of the host's certificate. We do not recommend disabling TLS verify mode, even though it may be a quick way to resolve a failing deployment.
- DNS entries: Do you have forward and reverse DNS lookups for all infrastructure systems that the Expressway interacts with? From X8.8, you must create forward and reverse DNS entries for all Expressway-E systems, so that systems making TLS connections to them can resolve their FQDNs and validate their certificates.

  If the Expressway cannot resolve hostnames and IP addresses of systems, your complex deployments (eg. MRA) could stop working as expected after you upgrade.
- Cluster peers: Do they have valid certificates? If they are using default certificates you should replace them with (at least) internally generated certificates and update the peers' trust lists with the issuing CA. From X8.8, clustering communications use TLS connections between peers instead of IPSec. TLS verification is not enforced (by default) after you upgrade, and you'll see an alarm reminding you to enforce TLS verification.

Deployments that use CE1200 appliances

When you restore an Expressway-E onto a CE1200 appliance from a CE1100 or earlier appliance backup, the CE1200 appliance may restore as an Expressway-C. This issue occurs if the service setup wizard was used in the CE1100 or earlier appliance to change the type to Expressway-C, and the wizard was not completed for the entire configuration. To avoid this issue, do the following before you back up the appliance:

1. Run the service setup wizard and change the type to Expressway-E.
2. Complete the wizard to the end.

Also, if you restore the Expressway-E configuration onto a CE1200 appliance from a CE1100 backup, the CE1200 appliance restores as an Expressway-E (as expected). However, depending on how the CE1100 type was previously configured, the web interface banner may display as Expressway-C. If you encounter this issue, go to the service setup wizard (**Status > Overview** page) and change **Type** to *Expressway-E*, then restart the system. This issue only occurs if the Traversal Server option key was used on the CE1100 to change the type to Expressway-E. If you used the service setup wizard, you will not encounter the issue.

Deployments that use MRA

This section only applies if you use the Expressway for MRA (mobile and remote access with Cisco Unified Communications products).

- Minimum versions of Unified Communications infrastructure software apply - some versions of Unified CM, IM and Presence Service, and Cisco Unity Connection have been patched with CiscoSSL updates. Check that you are running the minimum versions described in the Expressway MRA deployment guide, before you upgrade Expressway (see *Mobile and Remote Access Through Cisco Expressway* on the Expressway configuration guides page).

  IM and Presence Service 11.5 is an exception. You must upgrade Expressway to X8.8 or later *before* you upgrade IM and Presence Service to 11.5.
- Expressway-C and Cisco Expressway-E **should be upgraded together**. We don't recommend operating with Expressway-C and Expressway-E on different versions for an extended period.

- This item applies if you are upgrading a Expressway that is used for MRA, with clustered Unified CMs and endpoints running TC or Collaboration Endpoint (CE) software. In this case you must install the relevant TC or CE maintenance release listed below (or later) *before* you upgrade the Expressway. This is required to avoid a known problem with failover. If you do not have the recommended TC/CE maintenance release, an endpoint will not attempt failover to another Unified CM if the original Unified CM to which the endpoint registered fails for some reason. CDETS CSCvh97495 refers.
  - TC7.3.11
  - CE8.3.3
  - CE9.1.2

Note: Versions from X8.10.n move the MRA authentication (access control) settings from Expressway-E to Expressway-C, and apply default values where it is not possible to retain your existing settings. For correct system operation, after you upgrade **you must reconfigure the access control settings on the Expressway,** as described later in these upgrade instructions.

Deployments that use X8.7.x or earlier with Cisco Unified Communications Manager IM and Presence Service 11.5(1)

X8.7.x (and earlier versions) of Expressway are not interoperable with Cisco Unified Communications Manager IM and Presence Service 11.5(1) and later. And you must upgrade the Expressway software before the IM and Presence Service software. More details are in Interoperability, page 20.

Deployments that use Cisco Webex Hybrid Services

The Management Connector must be up to date before you upgrade Expressway. Authorize and accept any Management Connector upgrades advertised by the Cisco Webex cloud before you try to upgrade Expressway. Failure to do so may cause issues with the connector after the upgrade.

For details about which versions of Expressway are supported for hybrid connector hosting, see Connector Host Support for Cisco Webex Hybrid Services

Upgrade Instructions

Before You Begin

- Do the upgrade when the system has low levels of activity.
- Make sure all relevant tasks in Upgrade Prerequisites and Software Dependencies, page 21 are complete.
- Note your MRA authentication settings before upgrading. This item only applies if you use the Expressway for MRA and you upgrade from X8.9.x or earlier to X8.10 or later. From version X8.10 we moved the MRA authentication (access control) settings from the Expressway-E to the Expressway-C. The upgrade does not preserve the existing Cisco Expressway-E settings, so after the upgrade you need to review the MRA access control settings on the Expressway-C and adjust them as necessary for your deployment. To access existing MRA authentication settings:
  a. On the Expressway-E, go to **Configuration > Unified Communications > Configuration** and locate **Single Sign-on support**. Note the existing value (On, Exclusive, or Off)
  b. If **Single Sign-on support** is set to On or Exclusive, also note the current values of these related fields:
     - **Check for internal authentication availability**
     - **Allow Jabber iOS clients to use embedded Safari**

Clustered systems

To upgrade a clustered system, you should use the upgrade instructions in the *Expressway Cluster Creation and Maintenance Deployment Guide* on the Cisco Expressway Series configuration guides page. The following important requirement for upgrading clusters is explained in that guide, but for convenience it is also repeated here:

CAUTION: For clustered systems, to avoid the risk of configuration data being lost and to maintain service continuity, it is ESSENTIAL TO UPGRADE THE PRIMARY PEER FIRST and then upgrade the subordinate peers ONE AT A TIME IN SEQUENCE.

Process

This process does not apply if you are upgrading a clustered system, or a Expressway that uses device provisioning (Cisco TMSPE), or FindMe (with Cisco TMS managing Expressway). In those cases, follow the directions in the *Expressway Cluster Creation and Maintenance Deployment Guide* instead.

1. Backup the Expressway system before you upgrade (**Maintenance > Backup and restore**).
2. Enable maintenance mode:
   a. Go to **Maintenance > Maintenance mode**.
   b. Set **Maintenance mode** to *On*.
   c. Click **Save** and click **OK** on the confirmation dialog.
3. Wait for all calls to clear and registrations to timeout.
   – If necessary, manually remove any calls that do not clear automatically (**Status > Calls**, click **Select all** and then click **Disconnect**).
   – If necessary, manually remove any registrations that do not clear automatically (**Status > Registrations > By device**, click **Select all** and then click **Unregister**).
4. Upgrade and restart the Expressway (**Maintenance > Upgrade**).

   If you are upgrading to a new *major* release, for example from X7.x to X8.x, you first need to obtain a new release key from Cisco. The key is required during the upgrade process.

   The web browser interface may timeout during the restart process, after the progress bar has reached the end. This may occur if the Expressway carries out a disk file system check – which it does approximately once every 30 restarts.

5. This step depends on whether or not you use the Expressway for MRA:
   - If you don't use MRA, the upgrade is now complete and all Expressway configuration should be as expected.
   - If you do use MRA, go on to the next section and reconfigure your MRA access control settings.

Upgrade Expressway-C and Expressway-E Systems Connected Over a Traversal Zone

We recommend that Expressway-C (traversal client) and Expressway-E (traversal server) systems that are connected over a traversal zone both run the same software version.

However, we do support a traversal zone link from one Expressway system to another that is running the previous feature release of Expressway (for example, from an X8.11 system to an X8.10 system). This means that you do not have to simultaneously upgrade your Expressway-C and Expressway-E systems.

Some services, like Mobile and Remote Access, require both the Expressway-C and Expressway-E systems to be running the same software version.

Post-Upgrade Tasks for MRA Deployments

This section only applies if you use the Expressway for Mobile and Remote Access and you upgrade from X8.9.x or earlier to X8.10 or later. After the system restarts you need to reconfigure the MRA access control settings:

1. On the Expressway-C, go to **Configuration > Unified Communications > Configuration > MRA Access Control**.
2. Do one of the following:
   - To take advantage of the new MRA access control methods from X8.10, set the appropriate values on this page for your chosen methods. See the first table below for help about which values to apply.
   - Or to retain your pre-upgrade authentication approach, set the appropriate values on this page to match your previous settings on the Expressway-E. See the second table below for help about how to map the old Expressway-E settings to their new equivalents on the Expressway-C.
3. If you configure self-describing tokens (**Authorize by OAuth token with refresh**), refresh the Unified CM nodes: Go to **Configuration > Unified Communications > *<UC server type>*** and click **Refresh servers**.

Important!

- The **Check for internal authentication availability** setting will be off after the upgrade. Depending on the authentication settings on the Unified CM, this may prevent remote login by some Cisco Jabber users.
- The *Exclusive* option in X8.9 is now configured by setting **Authentication path** to *SAML SSO authentication*. This has the effect of prohibiting authentication by username and password.

The fields you actually see in the Web UI depend on whether MRA is enabled (**Unified Communications mode** set to *Mobile and remote access*) and on the selected authentication path. Not all the fields in the table are necessarily displayed.

Table 5 Settings for MRA access control

Field	Description	Default
Authentication path	Hidden field until MRA is enabled. Defines how MRA authentication is controlled. *SAML SSO authentication*: Clients are authenticated by an external IdP. *UCM/LDAP basic authentication*: Clients are authenticated locally by the Unified CM against their LDAP credentials. *SAML SSO and UCM/LDAP*: Allows either method. *None*: No authentication is applied. This is the default setting until MRA is first enabled. The " None" option is needed (rather than just leaving MRA turned off) because some deployments must turn on MRA to allow functions which are not actually MRA. (Such as the Web Proxy for Meeting Server, or XMPP Federation.) Only these customers should use " None" . **Do not use it in other cases.**	None before MRA turned on UCM/LDAP after MRA turned on
Authorize by OAuth token with refresh	This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them. Only Jabber clients are currently capable of using this authorization method. Other MRA endpoints do not currently support it. The clients must also be in OAuth token with refresh authorization mode. (missing or bad snippet)	On
Authorize by OAuth token (previously SSO Mode)	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. This option requires authentication through the IdP. Currently, only Jabber clients are capable of using this authorization method, which is not supported by other MRA endpoints.	Off
Authorize by user credentials	Available if **Authentication path** is *UCM/LDAP* or *SAML SSO and UCM/LDAP*. Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices.	Off

Table 5 Settings for MRA access control (continued)

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

Table 5 Settings for MRA access control (continued)

Field	Description	Default
Identity providers: Create or modify IdPs	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. **Selecting an Identity Provider** Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services. If you choose SAML-based SSO for your environment, note the following: ▪ SAML 2.0 is not compatible with SAML 1.1 and you must select an IdP that uses the SAML 2.0 standard. ▪ SAML-based identity management is implemented in different ways by vendors in the computing and networking industry, and there are no widely accepted regulations for compliance to the SAML standards. ▪ The configuration of and policies governing your selected IdP are outside the scope of Cisco TAC (Technical Assistance Center) support. Please use your relationship and support contract with your IdP Vendor to assist in configuring the IdP properly. Cisco cannot accept responsibility for any errors, limitations, or specific configuration of the IdP. Although Cisco Collaboration infrastructure may prove to be compatible with other IdPs claiming SAML 2.0 compliance, only the following IdPs have been tested with Cisco Collaboration solutions: ▪ OpenAM 10.0.1 ▪ Active Directory Federation Services 2.0 (AD FS 2.0) ▪ PingFederate® 6.10.0.4	–
Identity providers: Export SAML data	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. For details about working with SAML data, see SAML SSO Authentication Over the Edge, page 1.	–

Table 5 Settings for MRA access control (continued)

Field	Description	Default
Allow Jabber iOS clients to use embedded Safari	By default the IdP or Unified CM authentication page is displayed in an embedded web browser (not the Safari browser) on iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices. 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.	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.	0 seconds

Table 6 MRA access control values applied by the upgrade

Option	Value after upgrade	Previously on…	Now on…
Authentication path	Pre-upgrade setting is applied **Notes:** **SSO mode**=*Off* in X8.9 is two settings in X8.10: - **Authentication path**=*UCM/LDAP* - **Authorize by user credentials**=*On* **SSO Mode**=*Exclusive* in X8.9 is two settings in X8.10: - **Authentication path**=*SAML SSO* - **Authorize by OAuth token**=*On* **SSO Mode**=*On* in X8.9 is three settings in X8.10: - **Authentication path**=*SAML SSO/and UCM/LDAP* - **Authorize by OAuth token**=*On* - **Authorize by user credentials**=*On*	Both	Expressway-C
Authorize by OAuth token with refresh	Off	–	Expressway-C
Authorize by OAuth token (previously SSO Mode)	Pre-upgrade setting is applied	Both	Expressway-C
Authorize by user credentials	Pre-upgrade setting is applied	Both	Expressway-C
Check for internal authentication availability	No	Expressway-E	Expressway-C
Identity providers: Create or modify IdPs	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)
Identity providers: Export SAML data	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)
Allow Jabber iOS clients to use embedded Safari	No	Expressway-E	Expressway-C
SIP token extra time to live	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)

Using Collaboration Solutions Analyzer

Collaboration Solutions Analyzer is created by Cisco Technical Assistance Center (TAC) to help you with validating your deployment, and to assist with troubleshooting by analyzing Expressway log files. For example, you can use the Business to Business Call Tester to validate and test calls, including Microsoft interworked calls.

Note: You need a customer or partner account to use Collaboration Solutions Analyzer.

Getting started

1. If you plan to use the log analysis tool, first collect the logs from your Expressway.
2. Sign in to https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/
3. Click the tool you want to use. For example, to work with logs:
   a. Click **Log analysis**.
   b. Upload the log file(s).
   c. Select the files you want to analyze.
   d. Click **Run Analysis**.

      The tool analyzes the log files and displays the information in a format which is much easier to understand than the raw logs. For example, you can generate ladder diagrams to show SIP calls.

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com username and password.
3. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

Obtaining Documentation and Submitting a Service Request

Use the Cisco Notification Service to create customized flexible notification alerts to be sent to you via email or by RSS feed.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)