



Mobile and Remote Access Through Cisco Expressway Deployment Guide (X12.5)

First Published: 2014-04-15

Last Modified: 2020-04-08

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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 NON-INFRINGEMENT 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 of this document are considered uncontrolled. See the current online version for the latest version.

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

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](http://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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

About the Documentation 1

- Change History 1
- This Guide Does not Apply for the VCS 3
- Related Documents 3

CHAPTER 2

Mobile and Remote Access Overview 5

- About Mobile and Remote Access 5
- Core Components 6
- Mobile and Remote Access Ports 7
- Protocol Summary 7
- Jabber Client Connectivity Without VPN 8

CHAPTER 3

MRA Deployment Scenarios 9

- Deployment Scope 9
- Deployment Scenarios 9
 - MRA with Standalone Network Elements 10
 - MRA with Clustered Network 10
 - MRA with Multiple Clustered Networks 11
 - MRA as a Hybrid Deployment (using WebEx Cloud) 11
 - Jabber with Team Messaging Mode 12
- Unsupported Deployments 13
 - VPN Links 13
 - Traversal Zones Between VCS Series and Expressway Series 13
 - Unclustered or Many-to-One Traversal Connections 14
 - Nested Perimeter Networks 14
 - Expressway-C in DMZ with Static NAT 15

CHAPTER 4	Limitations and Unsupported Features	17
	Supported and Unsupported Features with Mobile and Remote Access	17
	Unsupported Client and Endpoint Features	17
	Unsupported Expressway Features and Limitations	19
	Partial Support for Cisco Jabber SDK	20

CHAPTER 5	MRA Infrastructure Requirements	21
	Required Versions	21
	Infrastructure Product Versions	21
	Configuration Recommendations and Requirements	22
	IP Addresses	22
	Network Domain	22
	DNS	22
	SRV Records	23
	Public DNS (External Domains)	23
	Local DNS (Internal Domains)	23
	Firewall Configuration	24
	Bandwidth Restrictions	25
	IM and Presence Service	25

CHAPTER 6	Endpoint and Client Requirements	27
	MRA-Compatible Endpoints	27
	EX, MX, and SX Series Endpoints (Running TC Software)	28
	Considerations for Android-based DX650, DX80, and DX70 Devices and Supported IP Phone 7800 and 8800 models	28
	MRA-Compatible Clients	28
	Which MRA Features Are Supported	29

CHAPTER 7	Expressway Fundamentals	31
	Maintenance Mode on the Expressway	31
	Secure Communications Configuration	32
	Media Encryption	33
	Clustered Expressway Systems and Failover Considerations	33

Authorization Rate Control	33
Credential Caching	33
Expressway Automated Intrusion Protection	34

CHAPTER 8**Unified CM Requirements 37**

Unified CM Dial Plan	37
Unified CM and Expressway in Different Domains Deployment	37
Server Certificate Requirements for Unified Communications Manager	37
Cisco Unified Communications Manager Certificates	37
IM and Presence Service Certificates	38
Expressway Certificates	38
Expressway-C Server Certificate Requirements	38
Expressway-E Server Certificate Requirements	39
Unified CM Denial of Service Threshold	39

CHAPTER 9**Install MRA 41**

Expressway Configuration Summary	41
Installation Requirements	42
Expressway-C for Mobile and Remote Access Setup	42
Configure DNS and NTP Settings on Expressway-C	42
Enable SIP Protocol During Installation	42
[Recommended] Disable Automated Intrusion Protection on Expressway-C	43
Enable the Expressway-C for Mobile and Remote Access	43
Configure the Domains to Route to Unified CM	43
Enable Shared Line and Multiple Lines for MRA Endpoints	44
Discover Unified Communications Servers and Services for Mobile and Remote Access	45
Trust the Certificates Presented to the Expressway-C	46
Discover Unified CM Servers	46
Discover IM and Presence Service Nodes	48
Discover Cisco Unity Connection Servers	49
Automatically Generated Zones and Search Rules	49
Why You Need to Refresh the Discovered Nodes?	50

CHAPTER 10**Configure MRA 51**

Configure MRA Access Control	51
Authorization and Authentication Comparison	51
Expressway (Expressway-C) Settings for Access Control	52
Configure Cisco Unified Communications Manager for OAuth with Refresh	55
Check Unified CM Support	55
Configure OAuth with Refresh (Self-Describing) on Unified CM SIP Lines	55
Refresh Servers on the Expressway-C	56
Check the Unified Communications Services Status	56
Working With the Allow List	57
Automatic Inbound Rules	58
Edit the HTTP Allow List	58
Upload Rules to the HTTP Allow List	60
Expressway-E for Mobile and Remote Access Configuration Workflow	60
Configure DNS and NTP Settings on Expressway-E	60
Enable SIP Protocol During Configuration	61
Enable the Expressway-E for Mobile and Remote Access	61
SAML SSO Authentication Over the Edge	61
About Simple OAuth Token Authorization	62
About Self-Describing OAuth Token Authorization with Refresh	63
OAuth Token Authorization Prerequisites	64
On the Expressway Pair	64
On Cisco Jabber Clients	64
On Unified CM	65
On the Identity Provider	65
Identity Provider Selection	65
High Level Task List	65
Import the SAML Metadata from the IdP	66
Associate Domains with an IdP	67
Export the SAML Metadata from the Expressway-C	67
IdPs Configurations	68
Active Directory Federation Services 2.0	68
Activation Code Onboarding Through MRA	69
Dial via Office-Reverse through MRA	71
Dial via Office-Reverse through MRA Prerequisites	71

Call Flows	71
How DVO-R Works with Expressway Mobile and Remote Access	72
Notes	73
Configuration Checklist for DVO-R	73
More DVO-R Information	73
Built-in-Bridge Recording through MRA	73
Built-in-Bridge Recording through MRA Prerequisites	74
Configure BiB over MRA	74
Configure a Secure Traversal Zone Connection for Unified Communications	75
Install Expressway Security Certificates	75
Configure Encrypted Expressway Traversal Zones	76

CHAPTER 11**Unified CM Configuration 79**

SIP Trunks Between Unified CM and Expressway-C	79
Configure Line Registration Listening Ports on Unified CM	79
Configure SIP Trunk Listening Ports on Unified CM	80
Configure SIP Trunk Listening Ports on Expressway	80
Unified Communications Services Deployment Partitions	80
Create a New Deployment	81
Associate a Domain with a Deployment	82
Associate a Unified CM or Other Server/Service with the Deployment	82

CHAPTER 12**APNS Support (Optional) 83**

Apple Push Notifications (APNS) Prerequisites and Recommendations	83
Push Notifications in Unified Communications Products	85
Configure Apple Push Notifications in Expressway	85

CHAPTER 13**ICE Passthrough Support (Optional) 87**

ICE Passthrough for Media Optimization	87
How ICE Passthrough Works	87
Supported Deployments	89
Supported Components	90
Supported Endpoints	90
ICE Passthrough Configuration	90

Prerequisites	91
Set Up Unified CM for ICE Passthrough	91
Verify the Unified CM Cluster Security Mode	91
Apply Phone Security Profile with Encrypted TLS on Endpoints	92
Apply a Common Phone Profile with ICE Configuration on Endpoints	92
Set Up Cisco Expressway-C for ICE Passthrough Workflow	93
Install Server Certificates	94
Change CEtcp Neighbor Zones to CEtls Neighbor Zones	94
Set Up the UC Traversal Zone for ICE Passthrough Support	95
Set Up the UC Neighbor Zone for ICE Passthrough Support	95
Use CLI to Configure ICE Passthrough on Cisco Expressway Zones	95
Set Up Cisco Expressway-E as TURN Server	96
Signaling Path Encryption Between Expressway-C and Unified CM	97
ICE Passthrough Metrics Use	98
View ICE Passthrough Metrics in Expressway-C	98
Metric Collection with the collectd Daemon	100
View Call Types in the Call History	100
Bandwidth Manipulation	101

CHAPTER 14
Troubleshooting 103

General Techniques	103
Alarms and Status Messages	103
Use the Collaboration Solutions Analyzer	104
Diagnostic Logs	104
Jabber for Windows Diagnostic Logs	104
Configure Cisco Expressway Diagnostic Log Levels	104
Create a Diagnostic Log Capture	105
After You Create Logs	105
Check DNS Records	105
Check that the Cisco Expressway-E is Reachable	106
Check Call Status	106
Mobile and Remote Access Call Identification	107
Rich Media Sessions (Cisco Expressway Only)	107
Devices Registered to Unified CM via Cisco Expressway	107

Identify Devices in Unified CM	107
Identify Provisioning Sessions in Cisco Expressway-C	107
Ensure that Cisco Expressway-C is Synchronized to Unified CM	108
Check MRA Authentication Status and Tokens	108
Cisco Expressway Certificate and TLS Connectivity Issues	108
CiscoSSL 5.4.3 Rejects Diffie-Hellman Keys with Fewer than 1024 Bits	109
Cisco Jabber Sign In Issues	109
Jabber Triggers Automated Intrusion Protection	109
Jabber Popup Warns About Invalid Certificate When Connecting from Outside the Network	110
Jabber Doesn't Register for Phone Services	110
Jabber Cannot Sign In Due to XMPP Bind Failure	110
Jabber Cannot Sign In Due to SSH Tunnels Failure	111
Jabber Cannot Signin When Connecting to Different Peers in a Cluster of Cisco Expressway-Es	111
Cisco Expressway Returns "401 Unauthorized" Failure Messages	111
Call Failures due to "407 Proxy Authentication Required" or "500 Internal Server Error" Errors	111
Call Bit Rate is Restricted to 384 kbps or Video Issues when Using BFCP (Presentation Sharing)	112
Endpoints Can't Register to Unified CM	112
IM and Presence Service Realm Changes	112
No Voicemail Service ("403 Forbidden" Response)	112
"403 Forbidden" Responses for Any Service Requests	113
Client HTTPS Requests are Dropped by Cisco Expressway	113
Failed: Address is not a IM and Presence Server	113
Invalid SAML Assertions	113
"502 Next Hop Connection Failed" Messages	113
MRA calls fail if the called endpoint is more than 15 hops away from the Expressway-E	114

APPENDIX A

Allow List Formats	115
Allow List Rules File Reference	115
Example List Rules CSV File	116
Allow List Tests File Reference	116
Example List Tests CSV File	117



CHAPTER 1

About the Documentation

- [Change History](#), on page 1
- [This Guide Does not Apply for the VCS](#), on page 3
- [Related Documents](#), on page 3

Change History

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

Date	Change	Reason
April 2020	Various clarifications and corrections to the guide.	Document corrections & enhancements
December 2019	Various clarifications to the guide: <ul style="list-style-type: none">• Reverse DNS requirement updates• TLS verify subject name requirement• Minimum TLS version pre-11.5(1)SU3• No call preservation if node fails	Document corrections & enhancements
March 2019	Clarify that from X12.5, local DNS no longer requires <code>_cisco-uds._tcp.<domain></code> SRV records (still recommended).	Document correction
February 2019	Clarify UID mapping is mandatory on IdP for single, cluster-wide SAML agreement.	Content enhancement
February 2019	Add Jabber 12.5 clients to supported endpoints for ICE passthrough (subject to Unified CM 12.5).	Software dependency change

Date	Change	Reason
January 2019	<ul style="list-style-type: none"> • Fixed CE version for ICE support in MRA to 9.6.1 or later. • Removed Jabber endpoints from ICE for MRA supported components. • Correction to section Unsupported Expressway Features and Limitations, on page 19 for ICE for MRA with Static NAT. 	Document correction
January 2019	Updated for X12.5.	X12.5 release
September 2018	Updated for X8.11.2 (change to Unsupported Expressway Features and Limitations, on page 19 for chat/messaging if user authentication by OAuth refresh).	X8.11.2 release
September 2018	<p>Updated for Webex and Spark platform rebranding, and for X8.11.1 maintenance release.</p> <p>Added, to Unsupported Expressway Features and Limitations, on page 19 section, a known issue with chat/messaging services over MRA if user authentication is by OAuth refresh (self-describing tokens).</p>	X8.11.1 release Clarification
July 2018	Included Hunt Group support, subject to Cisco Unified Communications Manager 11.5(1)SU5 or later fixed version.	Software dependency change
July 2018	Updated for X8.11. Also removed port reference topic, which is now available in the <i>Cisco Expressway IP Port Usage Guide</i> .	X8.11 release
May 2018	Clarify MFT over MRA is not supported when using an unrestricted version of IM and Presence Service.	Clarification
March 2018	Clarify no Jabber support for redundant UDS services.	Clarification
December 2017	Added configuration step to enable SIP protocol (disabled by default on new installs).	Content defect
November 2017	Clarified which Cisco IP Phones in the 88xx series support MRA (Configuration Overview section).	Content defect
September 2017	Added links to information about supported features for MRA-connected endpoints. Add information about Collaboration Solutions Analyzer.	Content enhancement
August 2017	Deskphone control functions bullet removed from “Unsupported Contact Center Features” as not applicable.	Content defect
July 2017	Clarify required versions for Unified Communications software. Corrected duplicated prerequisites for Push Notifications feature.	Content defect

Date	Change	Reason
July 2017	Updated.	X8.10 release
April 2017	Added details on partial support for Cisco Jabber SDK features.	Content defect
January 2017	Updated section on unsupported features when using MRA. Added description of Maintenance Mode. Clarified that Expressway-C and Expressway-E need separate IP addresses.	X8.9.1 release
December 2016	Updated.	X8.9 release
September 2016	Unsupported deployments section updated. Minimum versions note about TLS added.	Clarification to avoid misconfiguration
August 2016	Updated DNS prerequisite to create reverse lookup entries for Expressway-E.	Customer found defect
June 2016	HTTP Allow list feature updates.	X8.8 release
	Entries before X8.8 are removed for clarity	

This Guide Does not Apply for the VCS



Important

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

From version X12.5 onwards, this guide applies only to the Cisco Expressway Series product (Expressway) and no longer applies to the Cisco VCS product (VCS).

Related Documents

The following documents may help with setting up your environment:

- [Expressway Basic Configuration \(Expressway-C with Expressway-E\) Deployment Guide](#)
- [Expressway Cluster Creation and Maintenance Deployment Guide](#)
- [Certificate Creation and Use With Expressway Deployment Guide](#)
- [Cisco Expressway IP Port Usage Configuration Guide](#), on the [Cisco Expressway Series configuration guides page](#).
- [Expressway Administrator Guide](#)

- *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*, at [Cisco Unified Communications Manager Configuration Guides](#)
- “Directory Integration and Identity Management” chapter in the *Cisco Collaboration System 10.x Solution Reference Network Designs (SRND)* document
- *SAML SSO Deployment Guide for Cisco Unified Communications Applications*, at [Cisco Unified Communications Manager Maintain and Operate Guides](#)
- Jabber client configuration details:
 - *Cisco Jabber for Windows*
 - *Cisco Jabber for iPad*
 - *Cisco Jabber for Android*
 - *Cisco Jabber for Mac*



CHAPTER 2

Mobile and Remote Access Overview

- [About Mobile and Remote Access, on page 5](#)

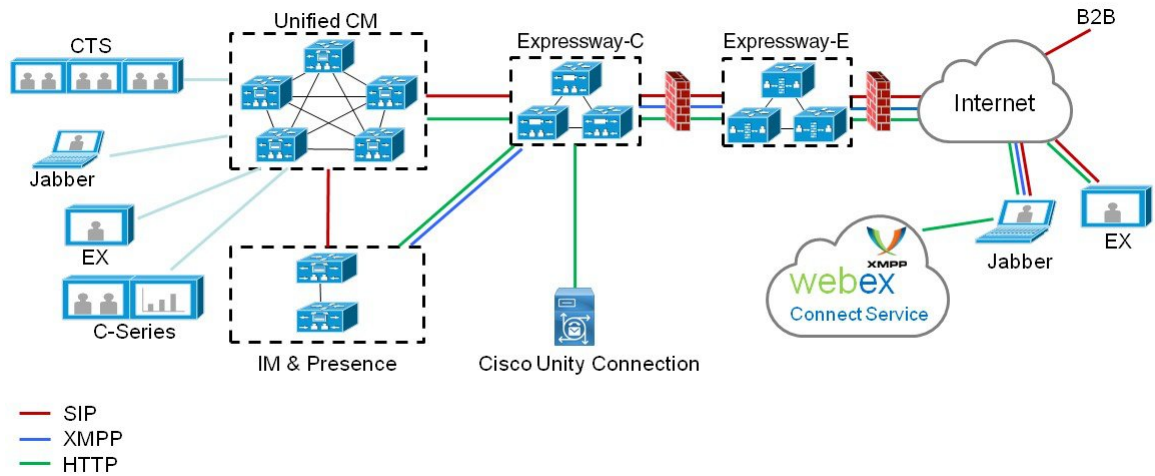
About Mobile and Remote Access

Cisco Unified Communications Mobile and Remote Access (MRA) is part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is outside the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The MRA solution provides the following functions:

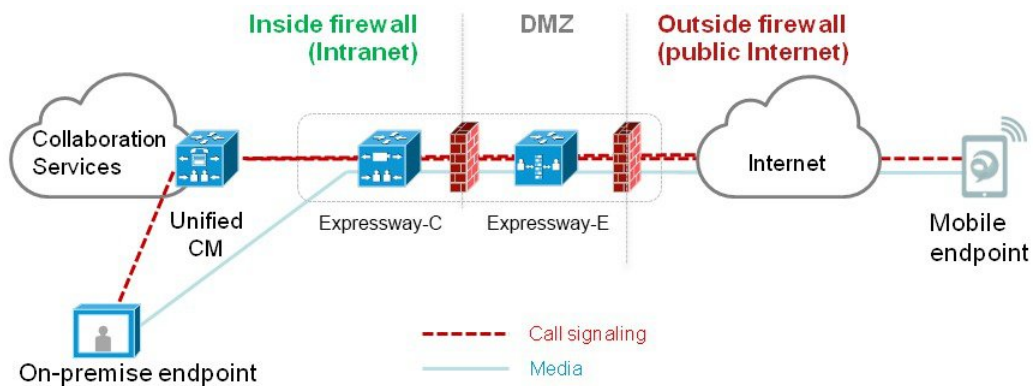
- **Off-premises access:** a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- **Security:** secure business-to-business communications
- **Cloud services:** enterprise grade flexibility and scalable solutions providing rich Cisco Webex integration and service provider offerings
- **Gateway and interoperability services:** media and signaling normalization, and support for non-standard endpoints

Figure 1: Unified Communications: Mobile and Remote Access



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

Figure 2: Typical Call Flow - Signalling and Media Paths



Unified CM provides call control for both mobile and on-premises endpoints. Signaling traverses the Expressway solution between the mobile endpoint and Unified CM. Media traverses the Expressway solution and is relayed between endpoints directly. All media is encrypted between the Expressway-C and the mobile endpoint.

Core Components

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

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

- Unified CM and IM and Presence Service are configured as specified in the configuration and management guides for your version, at [Cisco Unified Communications Manager Configuration Guides](#).
- If used, IM and Presence Service and/or Unity Connection are similarly configured as specified in the relevant [Cisco Unified Communications Manager Configuration Guides](#).

Mobile and Remote Access Ports

Information about MRA ports is available in the *Cisco Expressway IP Port Usage Configuration Guide* at the [Cisco Expressway Series Configuration Guides](#) page. This includes ports that can potentially be used between the internal network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located), and between the DMZ and the public internet.

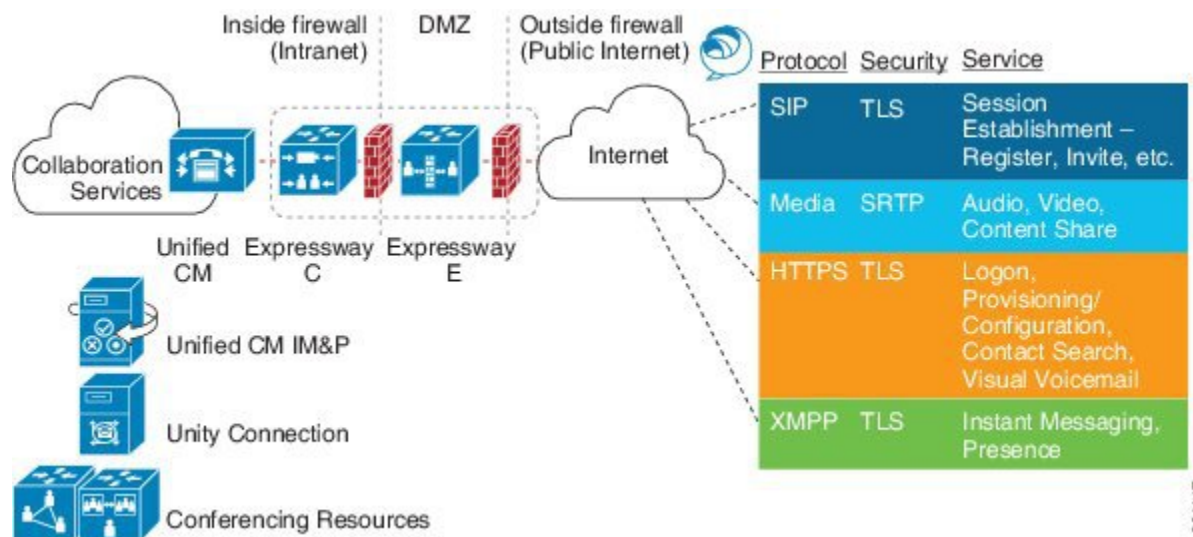
Protocol Summary

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

Table 2: Protocols and Associated Services

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

Figure 3: Protocol Workload Summary



394117

Jabber Client Connectivity Without VPN

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

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

- Use Instant Messaging and Presence services
- Make voice and video calls
- Search the corporate directory
- Share content
- Launch a web conference
- Access visual voicemail



Note

Cisco Jabber Video for TelePresence (Jabber Video) does not work with MRA.



CHAPTER 3

MRA Deployment Scenarios

- [Deployment Scope, on page 9](#)
- [Deployment Scenarios, on page 9](#)
- [Unsupported Deployments, on page 13](#)

Deployment Scope

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

- Mobile and Remote Access
- Microsoft interoperability, using the Expressway-C-based B2BUA
- Jabber Guest services

Deployment Scenarios

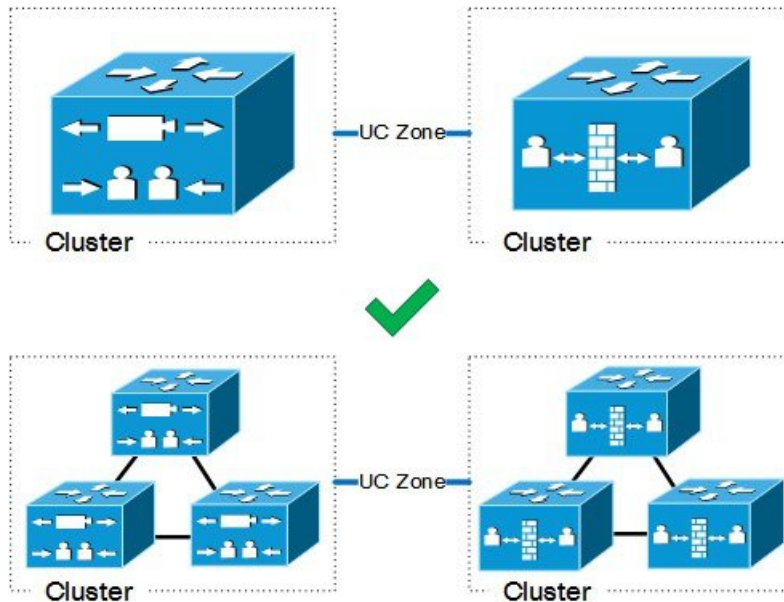
This section describes the supported deployment environments:

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



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

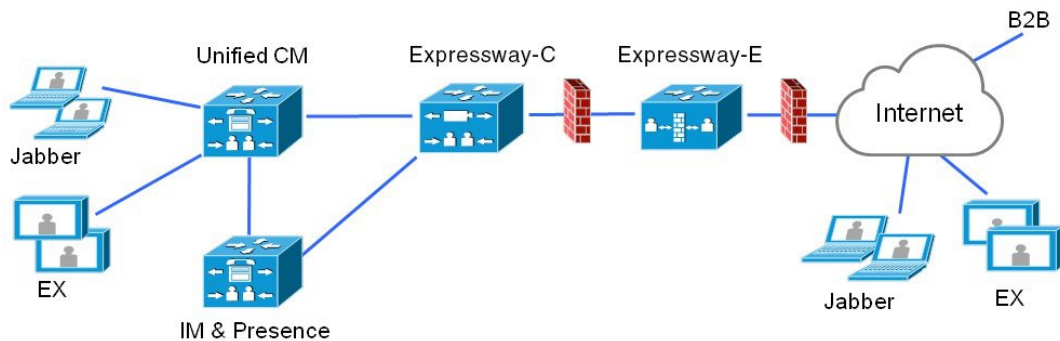
Figure 4: Supported MRA Traversal Connections 433240



MRA with Standalone Network Elements

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

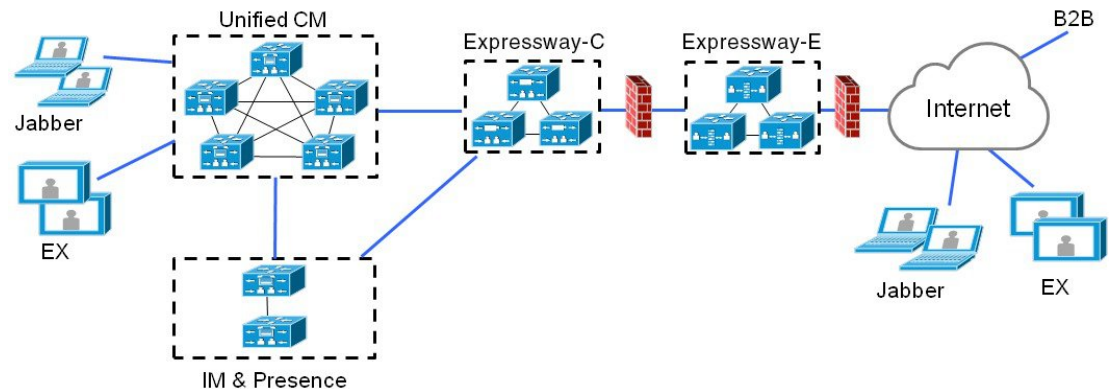
Figure 5: Single Clustered Network Elements



MRA with Clustered Network

In this scenario each network element is clustered.

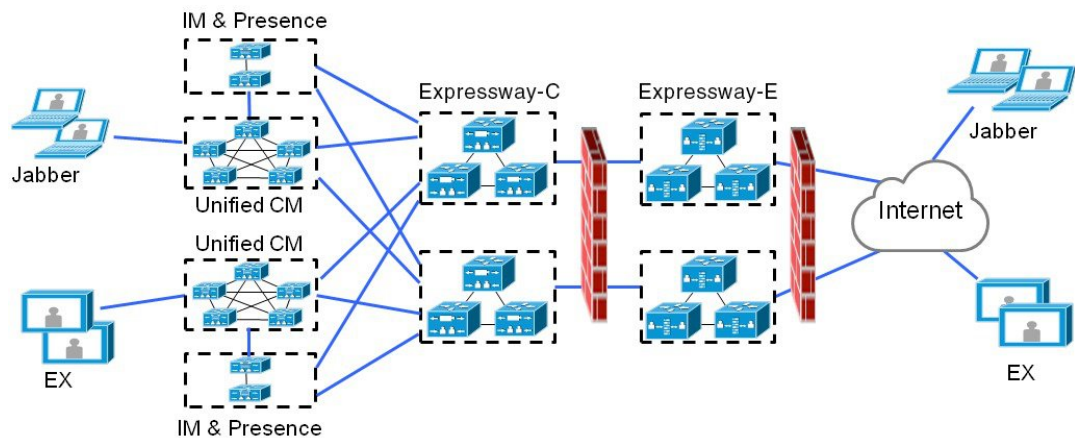
Figure 6: Single Clustered Network Elements



MRA with Multiple Clustered Networks

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

Figure 7: Multiple Clustered Network Elements

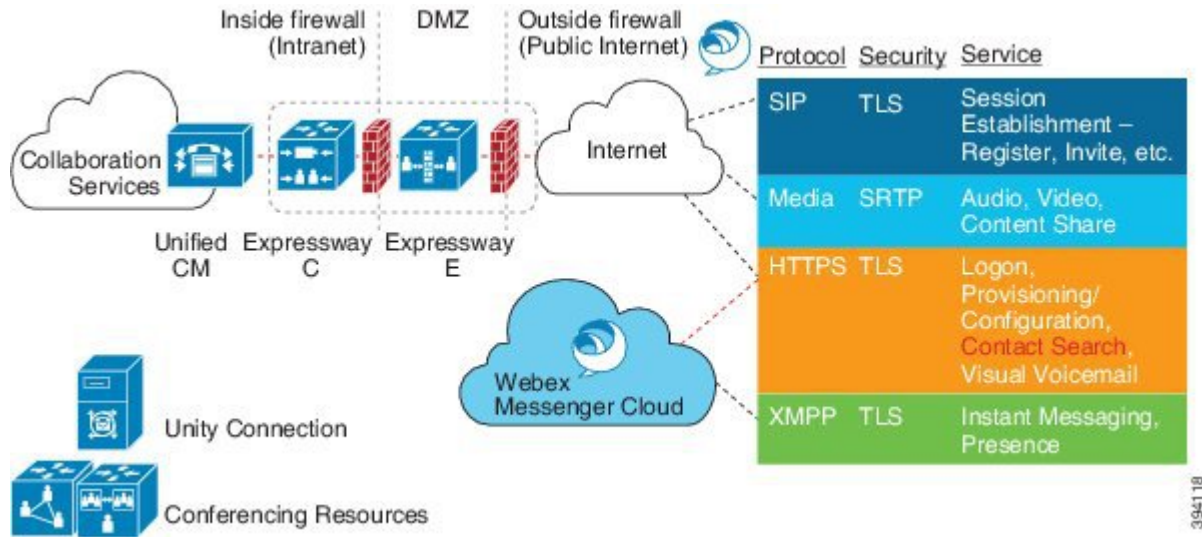


- Jabber clients can access their own cluster through any route.
- Expressway-C uses round robin to select a node (publisher or subscriber) when routing home cluster discovery requests.
- Each combination of Unified CM and IM and Presence Service clusters must use the same domain.
- Intercluster Lookup Service (ILS) must be active on the Unified CM clusters.
- Intercluster peer links must be configured between the IM and Presence Service clusters, and the Intercluster Sync Agent (ICSA) must be active.

MRA as a Hybrid Deployment (using WebEx Cloud)

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

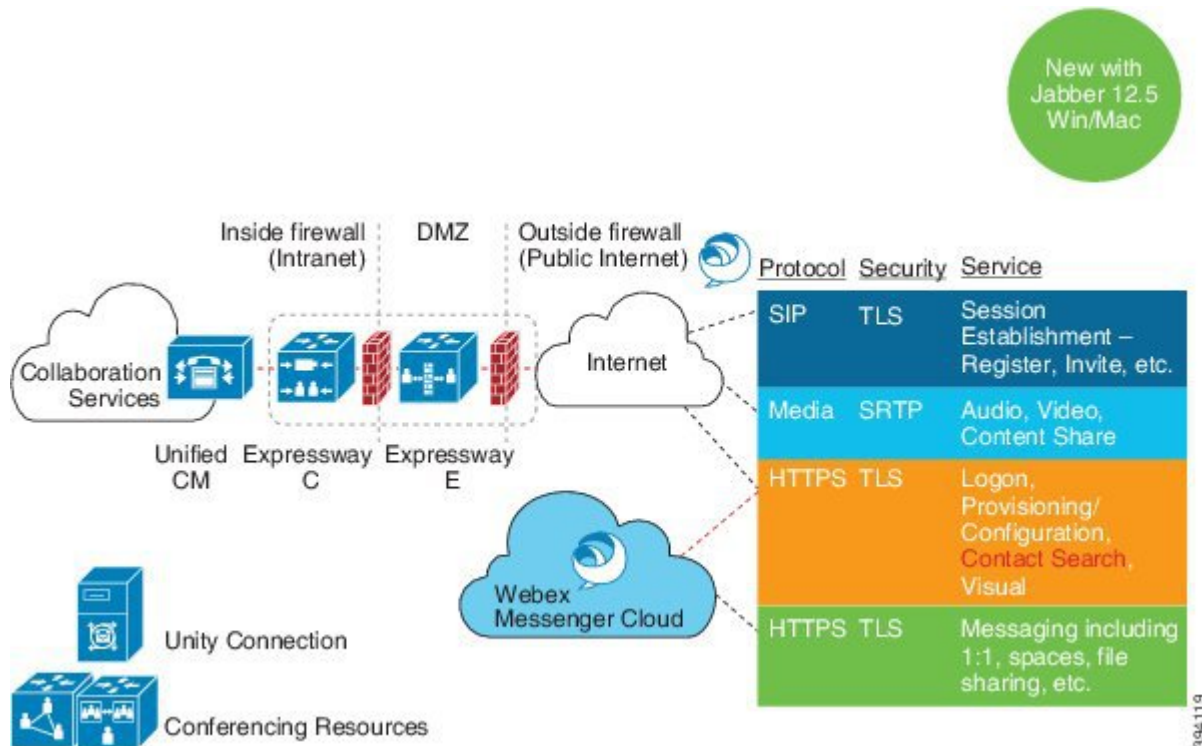
Figure 8: Hybrid Deployment



394118

Jabber with Team Messaging Mode

Figure 9: Jabber with Team Messaging Mode



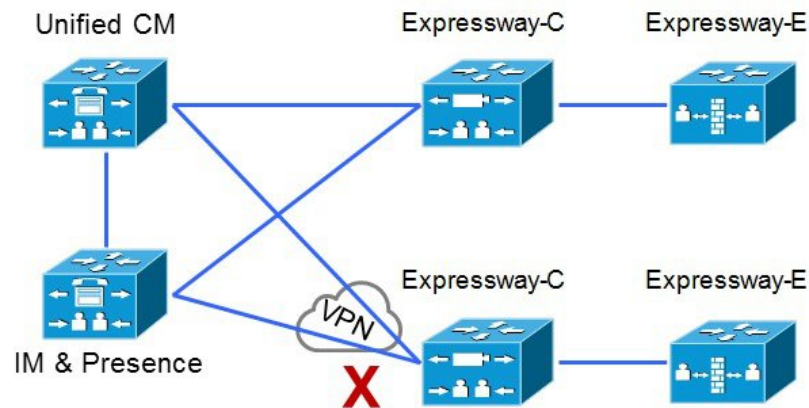
394119

Unsupported Deployments

VPN Links

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

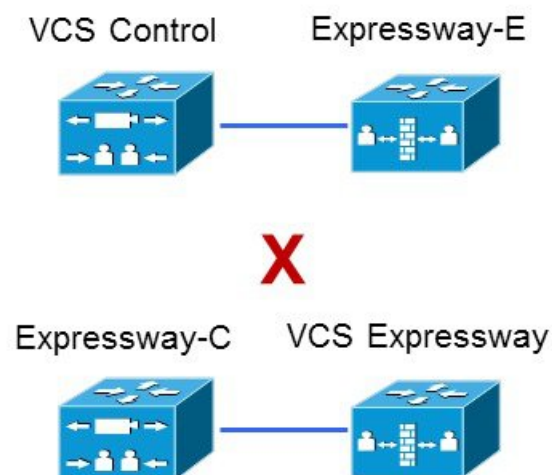
Figure 10: VPN Links Unsupported



Traversal Zones Between VCS Series and Expressway Series

“Mixed” traversal connections are not supported. That is, we do not support traversal zones, or Unified Communications traversal zones, between Cisco VCS and Cisco Expressway *even though it is possible to configure these zones*.

Figure 11: Mixed Traversal Zones



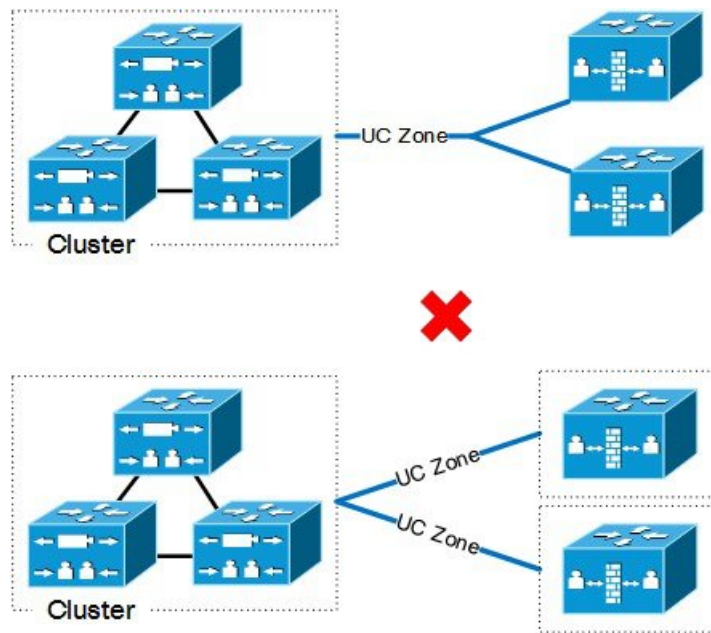
Explicitly, we do not support VCS Control traversal to Expressway-E, nor do we support Expressway-C traversal to VCS Expressway.

Unclustered or Many-to-One Traversal Connections

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

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

Figure 12: Unclustered or Many-to-One Traversal Connections

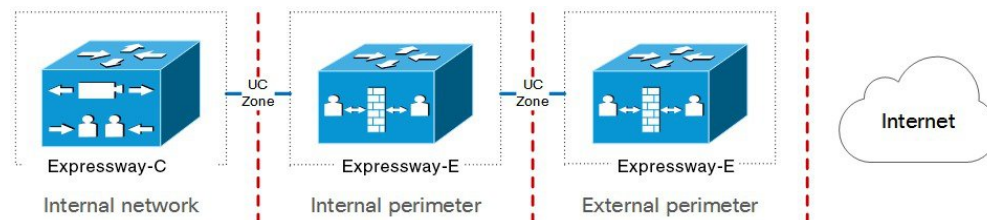


Nested Perimeter Networks

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

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

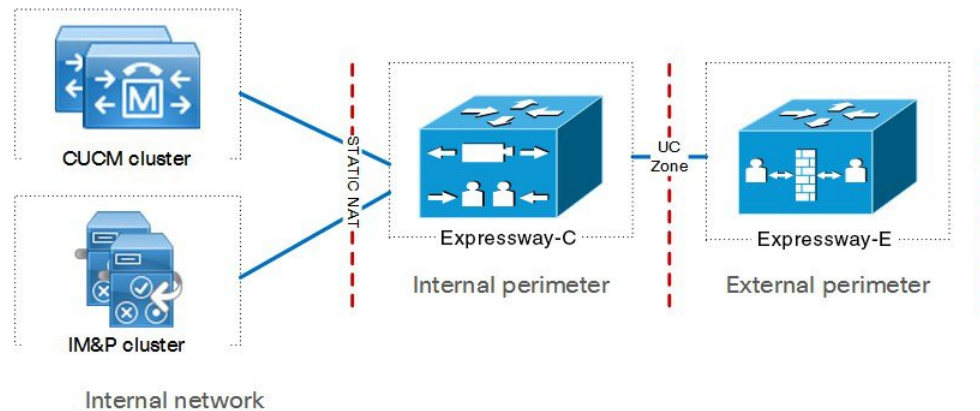
Figure 13: Nested Perimeter Networks



Expressway-C in DMZ with Static NAT

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

Figure 14: Expressway-C in DMZ with Static NAT



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



CHAPTER 4

Limitations and Unsupported Features

- [Supported and Unsupported Features with Mobile and Remote Access](#), on page 17

Supported and Unsupported Features with Mobile and Remote Access

Not all features are supported in every deployment scenario when using Mobile and Remote Access (MRA). This section provides information about:

- Key unsupported features for clients and endpoints. Lists client and endpoint features that are known not to work in certain MRA situations.

This is not an exhaustive list and for full details please refer to the documentation for the endpoint or client concerned.
- Unsupported Expressway features that are known not to work in certain MRA situations.

Unsupported Client and Endpoint Features

This section lists some key client and endpoint features which we know do not work with MRA-connected devices.

- This item applies if you have multiple IM and Presence Service clusters configured on Cisco Expressway-C, and some of them run software earlier than version 11.5*n*. In this case, because Cisco Expressway-C may select any cluster (round robin approach), it might select a cluster on an older software version. If so, IM and Presence Service features that require 11.5 are unavailable for endpoints connected over MRA.
- In Expressway-E systems that use dual network interfaces, XCP connections (for IM&P XMPP traffic) always use the non-external (i.e. internal) interface. So XCP connections may fail in deployments where the Expressway-E internal interface is on a separate network segment and is used for system management purposes only, and where the traversal zone on the Expressway-C connects to the Expressway-E's external interface.
- For supported Cisco Jabber clients connected over MRA, the E911NotificationURL feature requires a static HTML page for the notification to ensure that the web page renders correctly. Scripts and link tags are not supported.

- Directory access mechanisms other than the Cisco User Data Service (UDS) are not supported for Cisco Jabber clients over MRA.
- Some Cisco Unified Contact Center Express features are not supported over MRA. Please see the Unified Contact Center Express documentation for details.
- Endpoint failover behavior:
 - Cisco Jabber clients support IM and Presence Service failover over MRA. However, they do not support any other type of MRA-related redundancy or failover—including SIP, voicemail, and User Data Services (UDS). Clients use single UDS server only.



Note This also applies on premises, and not just over MRA.

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

SIP registration failover is supported over MRA, for Cisco IP Phones and devices running TC or CE software. This includes failure of Cisco Expressway-C, Cisco Expressway-E, or a Cisco Unified Communications Manager (Unified CM) node. SIP registration failover is subject to a requirement that if an Expressway node fails, another active node must be available in the Expressway cluster.

To support Unified CM failover over MRA, Cisco IP Phones need clustered Expressway-C and Expressway-E servers. Devices running TC or CE software do not need clustered Expressway servers for this case. You need at least the same number of Expressway-C and Expressway-E servers in the cluster as the number of Unified CMs in the Call Manager group configured on the IP phone.

- 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 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.
- These limitations exist for recording over MRA connections:
 - Recording only works for direct person-to-person calls, not for conferences. This includes Built-in-Bridge (BiB) recording.
 - Recording is not currently supported for the Silent Monitoring and Whisper Coaching features.
 - In the case of call recording for Cisco Jabber endpoints, Jabber does not support injecting recording tones into the media streams. Also, be aware that Unified CM 12.5(1)SU1 or later is needed to allow Jabber mobile devices to be CTI-monitored.
- The Expressway does not encrypt the iX protocol on behalf of other entities. So iX must be encrypted end to end, with the endpoints and conferencing server doing the encryption, or it must be unencrypted end to end.



Note For iX to work over MRA, the conferencing server must be configured with an encrypted trunk to Unified CM and the endpoints/Jabber must be running a suitable, iX-capable software version.

- Certificate provisioning to remote endpoints is not supported over MRA. For example, the Certificate Authority Proxy Function (CAPF). If you can do the first-time configuration on premises (inside the firewall) including CAPF enrolment, then these endpoints can use encrypted TFTP configuration files over MRA. But you can't do the CAPF enrolment over MRA, so you must bring the endpoints back on-premises for subsequent certificate operations.
- 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.
- Peer-to-peer file transfer when using IM and Presence Service and Jabber is not supported over MRA.
- Managed File Transfer (MFT) over MRA is supported when using IM and Presence Service 10.5.2 and later and Jabber 10.6 and later clients. MFT over MRA is not supported when using an unrestricted version of IM and Presence Service.
- File transfer with Webex Messenger Service and Cisco Jabber is supported.
- Additional Mobility features including Session Handoff are not supported over MRA.
- Hunt groups (including hunt pilots and hunt lists) are supported over MRA when using Unified CM version 11.5(1)SU5, or any later version that has the relevant change.
- The Cisco Unified Communications Self Care Portal is not supported over MRA.

Unsupported Expressway Features and Limitations

- Currently, if one Expressway node in a clustered deployment fails or loses network connectivity for any reason (including if the Unified CM restarts or fails), all active calls going through the affected node will fail. The calls are not handed over to another cluster peer. Bug ID [CSCtr39974](#) refers. This is not an MRA-specific issue and applies to all call types.
- We don't support third-party network load balancers between MRA clients and Expressway-E.
- The Expressway cannot be used for Jabber Guest when it's used for Mobile and Remote Access (MRA).
- The Expressway-C used for MRA cannot also be used for Microsoft gateway service. Microsoft gateway service requires a dedicated Expressway-C.
- Maintenance mode is not supported over MRA for endpoints running CE software. The Expressway drops MRA calls from these endpoints when you enable maintenance mode.
- As Expressway only supports IPv4 mode for MRA connections, the IP configuration settings "IPv6 only" or "Both" are not supported. In the case of "Both", as Expressway does not proxy IPv6 MRA traffic from clients, intermittent issues may arise if clients send IPv6 instead of IPv4.
- Endpoint management capability (SNMP, SSH/HTTP access) is not supported.
- Multidomain and multicustomer support is limited as follows:
 - Before X8.5, each Expressway deployment supported only one IM&P domain. (Even though IM and Presence Service 10.0 and later supports Multiple Presence Domains.)

- As of X8.5, you can create multiple deployments on the Expressway-C, but this feature is still limited to one domain per deployment.
- As of X8.5.1, a deployment can have Multiple Presence Domains. However, this feature is in preview status only, and we currently recommend that you do not exceed 50 domains.
- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM.
- The Expressway does not support some Cisco Unified Contact Center Express features for contact center agents or other users who connect over MRA. Jabber for Mac and Jabber for Windows cannot provide deskphone control over MRA, because the Expressway pair does not traverse the CTI-QBE protocol.
However, if these Jabber applications, or other CTI applications, can connect to Unified CM CTIManager (directly or through the VPN) they can provide deskphone control of MRA-connected clients.
- For ICE passthrough calls, if Host and Server-reflexive addresses cannot negotiate successfully, endpoints can utilize relay address of the TURN server to establish optimized media path. However, when Expressway is used as a TURN server and if static NAT is configured on the Expressway-E, the media cannot be passed using the relay address (CDETS CSCvf85709 refers). In this case, default traversal path is used to traverse the media. That is, the media passes through Expressway-C and Expressway-E.
- The Expressway-E does not support TURN relay over TCP for ICE passthrough calls.

Partial Support for Cisco Jabber SDK

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

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

For more information, see the [Getting Started Guide for Cisco Jabber SDK](#).



CHAPTER 5

MRA Infrastructure Requirements

- [Required Versions, on page 21](#)
- [Configuration Recommendations and Requirements, on page 22](#)

Required Versions

MRA through Cisco Expressway requires the following components. These are *minimum* requirements, and some individual MRA features need later software versions which are specified, where applicable, in the relevant part of the guide.

Infrastructure Product Versions

Table 3: Infrastructure Product Versions

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

Configuration Recommendations and Requirements

IP Addresses

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

Network Domain

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



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

DNS

Single Domain with Split DNS - Recommended

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

Dual Domain without Split DNS

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

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

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

Single Domain without Split DNS

Deployments that require Jabber clients to always connect over MRA also benefit from the X12.5 update that no longer requires the Expressway-C to resolve the `_cisco-uds` DNS SRV record. So administrators only need

to configure the `_collab-edge` DNS SRV record, and Jabber clients using service discovery will only have the option of connecting over MRA.

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

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

- MRA domain(s). The domain(s) configured on Expressway and enabled for Unified CM registration
- CMS Web Proxy URL link. Defined in the Expressway “Guest account client URI” setting on the **Expressway > Configuration > Unified Communications > Cisco Meeting Server** page.

SRV Records

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

Public DNS (External Domains)

The public, external DNS must be configured with `_collab-edge._tls.<domain>` SRV records so that endpoints can discover the Expressway-Es to use for Mobile and Remote Access. You also need SIP service records for general deployment (not specifically for MRA).

Table 4: Example: Cluster of 2 Expressway-E Systems

Domain	Service	Protocol	Priority	Weight	Port	Target host
example.com	collab-edge	tls	10	10	8443	expe1.example.com
example.com	collab-edge	tls	10	10	8443	expe2.example.com
example.com	sips	tcp	10	10	5061	expe1.example.com
example.com	sips	tcp	10	10	5061	expe2.example.com

Local DNS (Internal Domains)

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



Important

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

Table 5: Example: Local DNS

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

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

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

Firewall Configuration

- Ensure that the relevant ports are configured on your firewalls between your internal network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located) and between the DMZ and the public internet.

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

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

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

- Do not use a shared address for the Expressway-E and the Expressway-C, as the firewall cannot distinguish between them. If you use static NAT for IP addressing on the Expressway-E, make sure that any NAT operation on the Expressway-C does not resolve to the same traffic IP address. We do not support shared NAT addresses between Expressway-E and Expressway-C.
- The traversal zone on the Expressway-C points to the Expressway-E through the **Peer address** field on the traversal zone, which specifies the address of the Expressway-E server.
 - For dual NIC deployments, you can specify the Expressway-E address using a FQDN that resolves to the IP address of the internal interface. With split DNS you can optionally use the same FQDN as is available on the public DNS. If you don't use split DNS you must use a different FQDN.
 - For single NIC with static NAT (this deployment is NOT recommended), you must specify the Expressway-E address using a FQDN that resolves to the public IP address. This also means that the external firewall must allow traffic from the Expressway-C to the external FQDN of the Expressway-E. This is known as NAT reflection, and may not be supported by all types of firewalls.

For more information, see the “Advanced networking deployments” appendix in the [Expressway Basic Configuration \(Expressway-C with Expressway-E\) Deployment Guide](#)

Bandwidth Restrictions

The **Maximum Session Bit Rate for Video Calls** on the default region on Cisco Unified Communications Manager is 384 kbps by default. The **Default call bandwidth** on Expressway-C is also 384 kbps by default. These settings may be too low to deliver the expected video quality for MRA-connected devices.

IM and Presence Service



Note If you are using an IM&P server that is earlier than 11.5(1)SU3, make sure the minimum TLS version for the XMPP service is 1.0 (on newer Expressway installations the default is TLS 1.2). Instructions for configuring TLS versions and cipher suites are in the Expressway Administrator Guide.

Ensure that the **Cisco AXL Web Service** is active on the IM and Presence Service publishers that discovers other IM and Presence Service nodes for remote access. To check this, select the Cisco Unified Serviceability application and go to **Tools > Service Activation**.

If you are deploying Mobile and Remote Access with multiple IM and Presence Service clusters, you must configure Intercluster peer links between the clusters, and the Intercluster Sync Agent (ICSA) must be active on all clusters. This ensures that the user database is replicated between clusters, allowing Expressway-C to correctly route XMPP traffic.

For details of the correct configuration, refer to the chapter “Intercluster Peer Configuration” in *Configuration and Administration of IM and Presence Service* on Cisco Unified Communications Manager. You can find the correct document for your version at <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>.



CHAPTER 6

Endpoint and Client Requirements

- [MRA-Compatible Endpoints, on page 27](#)
- [EX, MX, and SX Series Endpoints \(Running TC Software\), on page 28](#)
- [Considerations for Android-based DX650, DX80, and DX70 Devices and Supported IP Phone 7800 and 8800 models, on page 28](#)
- [MRA-Compatible Clients, on page 28](#)
- [Which MRA Features Are Supported, on page 29](#)

MRA-Compatible Endpoints

Table 6: MRA-Compatible Endpoints

Endpoints	MRA Support
Cisco IP Phone 7800 Series	11.0(1)
Cisco IP Phone 8800 Series except Cisco Wireless IP Phone 8821 and 8821-EX and Cisco Unified IP Conference Phone 8831	11.0(1)
Cisco IP Conference Phone 7832	12.1(1)
Cisco IP Conference Phone 8832	12.1(1)
Cisco TelePresence endpoints: SX Series, EX Series, MX Series, Profile Series, C Series	TC7.0.1
Cisco TelePresence and Cisco WebEx endpoints: DX70, DX80, MX700, MX800, MX800 Dual, SX10, SX20, SX80, MX200 G2, MX300 G2	CE8 or CE9
Cisco WebEx endpoints: Cisco WebEx Room Kit, Cisco WebEx Codec Plus, Cisco WebEx Room 55, Cisco WebEx Room 70 Single, Cisco WebEx Room 70 Dual	CE 9.0
Android-based Cisco DX650, DX70, and DX80 devices	10.2.4(99)

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

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

These devices must verify the identity of the Expressway-E they are connecting to by validating its server certificate. To do this, they must have the certificate authority that was used to sign the Expressway-E's server certificate in their list of trusted CAs.

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

Mutual authentication is optional, and these devices are not required to provide client certificates. If you do want to configure mutual TLS, you cannot use CAPF enrolment to provision the client certificates. Instead, manually apply the certificates to the devices. The client certificates must be signed by an authority that is trusted by the Expressway-E.

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

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

- **Trust list:** You cannot modify the root CA trust list on Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series devices. Make sure that the Expressway-E's server certificate is signed by one of the CAs that the devices trust, and that the CA is trusted by the Expressway-C and the Expressway-E.
- **Off-hook dialing:** The way KPML dialing works between these devices and Unified CM means that you need Cisco Unified Communications Manager 10.5(2)SU2 or later to be able to do off-hook dialing via MRA. You can work around this dependency by using on-hook dialing.

MRA-Compatible Clients

Table 7: MRA-Compatible Client Versions

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

Jabber	MRA Support	Legacy Authentication (LDAP)	Legacy Authentication with SSO	OAuth with Refresh	OAuth Refresh with SSO	APNS
Cisco Jabber for iPhone and iPad	9.6.1	-	10.6	11.9	11.9	11.9
Cisco Jabber for Android	9.6	-	10.6	11.9	11.9	NA
Cisco Jabber for Mac	9.6	-	10.6	11.9	11.9	NA

Jabber clients verify the identity of the Expressway-E they are connecting to by validating its server certificate. To do this, they must have the certificate authority that was used to sign the Expressway-E's server certificate in their list of trusted CAs.

Jabber uses the underlying operating system's certificate mechanism:

- Windows: Certificate Manager
- MAC OS X: Key chain access
- IOS: Trust store
- Android: Location & Security settings

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

- [Cisco Jabber for Windows](#)
- [Cisco Jabber for iPhone and iPad](#)
- [Cisco Jabber for Android](#)
- [Cisco Jabber for Mac](#) (requires X8.2 or later)

Which MRA Features Are Supported

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

- Jabber clients
 - See “Supported Services in the Remote Access” section, *Planning Guide for Cisco Jabber* (for your version) on the [Install and Upgrade Guides](#) page.
- Cisco IP Phone 7800 Series (desk phones)

See “Phone Features Available for Mobile and Remote Access Through Expressway” in the “Phone Features and Setup” chapter, *Cisco IP Phone 7800 Series Administration Guide for Cisco Unified Communications Manager* on the [Maintain and Operate Guides](#) page.

- Cisco IP Conference Phone 7832

See “Phone Features Available for Mobile and Remote Access Through Expressway” in the “Phone Features and Setup” chapter, *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager* on the [Maintain and Operate Guides](#) page.

- Cisco IP Phone 8800 Series (desk phones)

See “Phone Features Available for Mobile and Remote Access Through Expressway” in the “Phone Features and Setup” chapter, *Cisco IP Phone 8800 Series Administration Guide for Cisco Unified Communications Manager* on the [Maintain and Operate Guides](#) page.

- Cisco IP Conference Phone 8832

See “Phone Features Available for Mobile and Remote Access Through Expressway” in the “Phone Features and Setup” chapter, *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager* on the [Maintain and Operate Guides](#) page.



CHAPTER 7

Expressway Fundamentals

- [Maintenance Mode on the Expressway, on page 31](#)
- [Secure Communications Configuration, on page 32](#)
- [Media Encryption, on page 33](#)
- [Clustered Expressway Systems and Failover Considerations, on page 33](#)
- [Authorization Rate Control, on page 33](#)
- [Credential Caching, on page 33](#)
- [Expressway Automated Intrusion Protection, on page 34](#)

Maintenance Mode on the Expressway

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

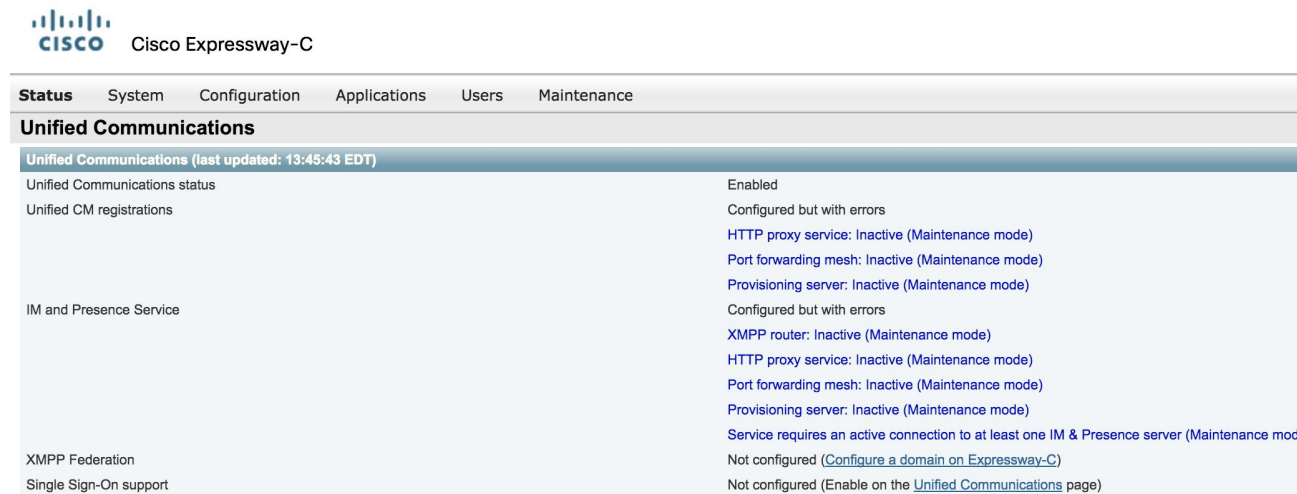
When you engage maintenance mode, the Expressway stops accepting new calls or proxy (MRA) traffic. Existing calls and chat sessions are not affected.

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

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

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

Figure 15: Maintenance Mode on Expressway-C



The screenshot shows the Cisco Expressway-C web interface. At the top, there is a navigation bar with tabs for Status, System, Configuration, Applications, Users, and Maintenance. Below this is a section titled 'Unified Communications' with a sub-header 'Unified Communications (last updated: 13:45:43 EDT)'. The main content area is a table with two columns: the left column lists various services and their status, and the right column provides details for each service.

Service	Status
Unified Communications status	Enabled
Unified CM registrations	Configured but with errors
	HTTP proxy service: Inactive (Maintenance mode)
	Port forwarding mesh: Inactive (Maintenance mode)
	Provisioning server: Inactive (Maintenance mode)
IM and Presence Service	Configured but with errors
	XMPP router: Inactive (Maintenance mode)
	HTTP proxy service: Inactive (Maintenance mode)
	Port forwarding mesh: Inactive (Maintenance mode)
	Provisioning server: Inactive (Maintenance mode)
	Service requires an active connection to at least one IM & Presence server (Maintenance mode)
XMPP Federation	Not configured (Configure a domain on Expressway-C)
Single Sign-On support	Not configured (Enable on the Unified Communications page)

Limitation for CE endpoints

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

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 host name then:

- It needs to be routable using that name.
- This is the name that the Expressway expects to see in the Unified CM's server certificate.

If you are using secure profiles, ensure that the root CA of the authority that signed the Expressway-C certificate is installed as a CallManager-trust certificate (**Security > Certificate Management** in the Cisco Unified OS Administration application).

Media Encryption

Media encryption is enforced on the call legs between the Expressway-C and the Expressway-E, and between the Expressway-E and endpoints located outside the enterprise.

The encryption is physically applied to the media as it passes through the B2BUA on the Expressway-C.

Clustered Expressway Systems and Failover Considerations

You can configure a cluster of Expressway-Cs and a cluster of Expressway-Es to provide failover (redundancy) support as well as improved scalability.

Details about how to set up Expressway clusters are contained in [Expressway Cluster Creation and Maintenance Deployment Guide](#) and information about how to configure Jabber endpoints and DNS are contained in “Configure DNS for Cisco Jabber”.

Note that when discovering Unified CM and IM and Presence Service servers on Expressway-C, you must do this on the primary peer.

Authorization Rate Control

The Expressway can limit the number of times that any user's credentials can be used, in a given configurable period, to authorize the user for collaboration services. This feature is designed to thwart inadvertent or real denial of service attacks, which can originate from multiple client devices authorizing the same user, or from clients that reauthorize more often than necessary.

Each time a client supplies credentials to authorize the user, the Expressway checks whether this attempt would exceed the **Maximum authorizations per period** within the previous number of seconds specified by the **Rate control period**.

If the attempt would exceed the chosen maximum, then the Expressway rejects the attempt and issues the HTTP error 429 “Too Many Requests”.

The authorization rate control settings are configurable in the **Advanced** section of the **Configuration > Unified Communications > Configuration** page.

Credential Caching



Note These settings do not apply to clients that are using SSO (common identity) for authenticating via MRA.

The Expressway caches endpoint credentials which have been authenticated by Unified CM. This caching improves overall performance because the Expressway does not always have to submit endpoint credentials to Unified CM for authentication.

The caching settings are configurable in the **Advanced** section of the **Configuration > Unified Communications > Configuration** page.

Credentials refresh interval specifies the lifetime of the authentication token issued by the Expressway to a successfully authenticated client. A client that successfully authenticates should request a refresh before this token expires, or it will need to re-authenticate. The default is 480 minutes (8 hours).

Credentials cleanup interval specifies how long the Expressway waits between cache clearing operations. Only expired tokens are removed when the cache is cleared, so this setting is the longest possible time that an expired token can remain in the cache. The default is 720 minutes (12 hours).

Expressway Automated Intrusion Protection

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

- http-ce-auth
- http-ce-intrusion
- sshpfd-auth
- sshpfd-intrusion
- xmpp-intrusion

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

On Expressway-C

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

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

On Expressway-E

You should enable the Automated protection service (**System > System administration**) if it is not yet running.

To protect against malicious attempts to access the HTTP proxy, you can configure automated intrusion protection on the Expressway-E (**System > Protection > Automated detection > Configuration**).

We recommend that you enable the following categories on the Expressway-E:

- HTTP proxy authorization failure and HTTP proxy protocol violation. Do not enable the HTTP proxy resource access failure category.
- XMPP protocol violation



Note The Automated protection service uses Fail2ban software. It protects against brute force attacks that originate from a single source IP address.



CHAPTER 8

Unified CM Requirements

- [Unified CM Dial Plan, on page 37](#)
- [Unified CM and Expressway in Different Domains Deployment, on page 37](#)
- [Server Certificate Requirements for Unified Communications Manager, on page 37](#)
- [Unified CM Denial of Service Threshold, on page 39](#)

Unified CM Dial Plan

The Unified CM dial plan is not impacted by devices registering via Expressway. Remote and mobile devices still register directly to Unified CM and their dial plan will be the same as when it is registered locally.

Unified CM and Expressway in Different Domains Deployment

Unified CM nodes and Expressway peers can be located in different domains. For example, your Unified CM nodes may be in the `enterprise.com` domain and your Expressway system may be in the `edge.com` domain.

In this case, Unified CM nodes must use IP addresses or FQDNs for the **Server host name / IP address** to ensure that Expressway can route traffic to the relevant Unified CM nodes.

Unified CM servers and IM and Presence Service servers must share the same domain.

DNS Host Name / FQDN

The first character of the DNS host name defined for the Unified CM must be a letter (do not start with a digit or special character).

Server Certificate Requirements for Unified Communications Manager

Cisco Unified Communications Manager Certificates

Two Cisco Unified Communications Manager certificates are significant for Mobile and Remote Access:

- *CallManager* certificate
- *Tomcat* certificate

These certificates are automatically installed on the Cisco Unified Communications Manager and by default they are self-signed and have the same common name (CN).

We recommend using CA-signed certificates. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. So if the *CallManager* and *tomcat* self-signed certificates have the same CN in the Expressway's trusted CA list, the Expressway can only trust one of them. This means that either secure HTTP or secure SIP, between Expressway-C and Cisco Unified Communications Manager, will fail.

Also, when generating tomcat certificate signing requests for any products in the Cisco Collaboration Systems Release 10.5.2, you need to be aware of [CSCus47235](#). You need to work around this issue to ensure that the FQDNs of the nodes are in the certificates as Subject Alternative Name (SAN) entries. The *Expressway X8.5.3 Release Note* on the [Release Notes page](#) has details of the workarounds.

IM and Presence Service Certificates

Two IM and Presence Service certificates are significant if you use XMPP:

- *cup-xmpp* certificate
- *tomcat* certificate

We recommend using CA-signed certificates. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. If the *cup-xmpp* and *tomcat* (self-signed) certificates have the same CN, Expressway only trusts one of them, and some TLS attempts between Cisco Expressway-E and IM and Presence Service servers will fail. For more details, see [CSCve56019](#).

Expressway Certificates

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

A table that lists which CSR alternative name elements apply to which Unified Communications features, is provided in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway configuration guides page](#).

Expressway-C Server Certificate Requirements

The Expressway-C server certificate must include the following elements in its list of subject alternate names:

- **Unified CM phone security profile names**
- **IM and Presence chat node aliases (federated group chat)**

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

We recommend that you use DNS format for the chat node aliases when generating the CSR. You must include the same chat node aliases in the Expressway-E server certificate's alternative names.

More details, including the process to generate the CSR, are provided in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway configuration guides page](#).

Expressway-E Server Certificate Requirements

The Expressway-E server certificate needs to include the following elements in its list of subject alternative names (SAN):

- **Unified CM registrations domains**
- **XMPP federation domains**
- **IM and Presence chat node aliases (federated group chat)**

More details, including the process to generate the CSR, are provided in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway configuration guides page](#).

Unified CM Denial of Service Threshold

High volumes of Mobile and Remote Access calls may trigger denial of service thresholds on Unified CM. This is because all the calls arriving at Unified CM are from the same Expressway-C (cluster).

If necessary, we recommend that you increase the level of the **SIP Station TCP Port Throttle Threshold** (**System > Service Parameters**, and select the **Cisco CallManager** service) to 750 KB/second.



CHAPTER 9

Install MRA

- [Expressway Configuration Summary, on page 41](#)
- [Installation Requirements, on page 42](#)
- [Expressway-C for Mobile and Remote Access Setup, on page 42](#)
- [Discover Unified Communications Servers and Services for Mobile and Remote Access, on page 45](#)

Expressway Configuration Summary

The following steps summarize the configuration required on the Expressway-C and Expressway-E.

Procedure

- Step 1** Make sure that **System host name** and **Domain name** are specified for every Expressway and that each Expressway is synchronized to a reliable NTP service. The hostname can contain only letters, digits, hyphens, and underscores. The first character must be a letter, and the last character must be a letter or a digit.
- Step 2** Enable SIP on the Expressway-E and Expressway-C. (SIP is disabled by default on new installs.)
- Step 3** [Recommended] Disable automated intrusion protection on the Expressway-C and configure it on the Expressway-E. (From X8.9, this feature is enabled by default on new installations. See [Expressway Automated Intrusion Protection, on page 34](#))
- Step 4** Set **Unified Communications mode** to *Mobile and Remote Access*.
- Step 5** Configure the Unified CM, IM and Presence Service, and Cisco Unity Connection servers on the Expressway-C.
- Step 6** Configure the domains on the Expressway-C for which services are to be routed to Unified CM.
- Step 7** [Optional] Create additional deployments and associate domains, and UC services with them.
- Step 8** Install appropriate server certificates and trusted CA certificates.
- Step 9** Configure a Unified Communications traversal zone connection between Expressway-E and Expressway-C.
- Step 10** If required, configure the HTTP server allow list for any web services inside the enterprise that need to be accessed from remote Jabber clients.
- Step 11** [Optional] Configure SSO over collaboration edge, to allow for common identity between external Jabber clients and the users' Unified CM profiles.

Configuration changes on Expressway generally take immediate effect. A banner message or alarm will prompt you if a system restart or other action is required.

Installation Requirements

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

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

For information about how to do this, see:

- [Secure Communications Configuration, on page 32](#) (if your system does not already have a secure traversal zone in place).
- [Server Certificate Requirements for Unified Communications Manager, on page 37](#).

If you want to use XMPP federation, the IM and Presence Service servers must be discovered on the Expressway-C. So that all relevant information is available when generating certificate signing requests.

Expressway-C for Mobile and Remote Access Setup

This section describes the configuration steps required on the Expressway-C for Mobile and Remote Access.

Configure DNS and NTP Settings on Expressway-C

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

If you have a cluster of Expressways, you must do this for every peer.

Procedure

- Step 1** Access **System** > **DNS**, and set the **System host name** and **Domain name**.
 - Step 2** Set the local DNS servers.
 - Step 3** Access **System** > **Time** and ensure that a reliable NTP service is configured.
All Expressway systems must be synchronized to a reliable NTP service.
 - Step 4** Set the **Authentication method** in accordance with your local policy.
-

Enable SIP Protocol During Installation

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

Procedure

- Step 1** On the Expressway-C, go to **Configuration > Protocols > SIP**.
- Step 2** Set **SIP mode** to **On** and **Save** the page.
-

[Recommended] Disable Automated Intrusion Protection on Expressway-C

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

See [Expressway Automated Intrusion Protection, on page 34](#).

Procedure

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

Enable the Expressway-C for Mobile and Remote Access

To enable Mobile and Remote Access functionality:

Procedure

- Step 1** Go to **Configuration > Unified Communications > Configuration**.
- Step 2** Set **Unified Communications mode** to **Mobile and Remote Access**.
- You must select **Mobile and Remote Access** before you can configure the relevant domains and traversal zones.
- Step 3** Click **Save**.
-

Configure the Domains to Route to Unified CM

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

The available services are:

- **SIP registrations and provisioning on Expressway:** the Expressway is authoritative for this SIP domain. The Expressway acts as a SIP registrar for the domain and accepts registration requests for any SIP endpoints attempting to register with an alias that includes this domain.

- **SIP registrations and provisioning on Unified CM:** Endpoint registration, call control and provisioning for this SIP domain is serviced by Unified CM. The Expressway acts as a Unified Communications gateway to provide secure firewall traversal and line-side support for Unified CM registrations.
- **IM and Presence Service:** Instant messaging and presence services for this SIP domain are provided by the Unified CM IM and Presence Service.
- **XMPP federation:** Enables XMPP federation between this domain and partner domains.
- **Deployment:** Associates the domain with the selected deployment, if there are multiple deployments. This setting is absent if there is only one deployment (there is always at least one).

Turn **On** all of the applicable services for each domain. For example, the same domain may be used by endpoints such as Jabber or EX Series devices that require line-side Unified Communications support, and by other endpoints such as third-party SIP or H.323 devices that require Expressway support. (In this scenario, the signaling messages sent from the endpoint indicate whether line-side unified communications or Expressway support is required.)

Note that these settings are not entirely independent. You cannot disable SIP registration and provisioning on Unified CM while using IM and Presence Service. You can disable IM and Presence Service while SIP registrations and provisioning on Unified CM is **On**, but the reverse is not true. So, if you switch IM and Presence Service **On**, then your setting for SIP registrations and provisioning on Unified CM is ignored and the Expressway-C behaves as though it was **On**.

Figure 16: Domains

The screenshot shows the 'Domains' configuration page in Cisco Expressway. At the top right, it says 'You are here: Configuration > Domains > Edit'. Below this is a 'Configuration' section with a 'Domain name' field containing 'example.com'. Underneath is a 'Supported services for this domain' section with four rows of settings:

Service	Setting	Info
SIP registrations and provisioning on Expressway-C	Off	i
SIP registrations and provisioning on Unified CM	On	i
IM and Presence Service	On	i
XMPP federation	Off	i

At the bottom of the configuration area are buttons for 'Save', 'Delete', and 'Cancel'.

Procedure

- Step 1** On Expressway-C, go to **Configuration > Domains**.
- Step 2** Select the domains (or create a new domain, if not already configured) for which services are to be routed to Unified CM.
- Step 3** For each domain, turn **On** the services for that domain that Expressway is to support.

Enable Shared Line and Multiple Lines for MRA Endpoints

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

only enable SIP Path headers if you are running Unified CM version 11.5(1)SU3 or later (CDETS CSCvd84831 refers).

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

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

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

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

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

Before you begin

Requires Unified CM 11.5(1)SU3 or later.

Procedure

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

Step 2 Change **SIP Path headers** to **On**.

Step 3 Click **Save**.

The Expressway-C puts its address in the Path headers of registrations from now on, and preserves the Contact header.

Step 4 Go to **Configuration > Unified Communications > Unified CM servers**.

Step 5 Click **Refresh servers**.

Discover Unified Communications Servers and Services for Mobile and Remote Access

The Expressway-C must be configured with the address details of the Unified Communications services/nodes that are going to provide registration, call control, provisioning, voicemail, messaging, and presence services to MRA users.

IM and Presence Service configuration is not required if you're deploying the hybrid model, as these services are provided by the Cisco Webex cloud.

The connections configured in this procedure are static. You must refresh the configuration on the Expressway-C after you reconfigure or upgrade any of the discovered Unified Communications nodes. For more details, see [Why You Need to Refresh the Discovered Nodes?](#), on page 50. Be aware that as described in that section, Jabber and other endpoints cannot connect during the refresh.

Procedure

- Step 1** Go to **Configuration > Unified Communications** and select the **UC server type**.
- Step 2** Click **Refresh servers**.
-

Trust the Certificates Presented to the Expressway-C

If **TLS verify mode** is **On** when discovering Unified Communications services, then you must configure the Expressway-C to trust the certificates presented by the IM and Presence Service nodes and Unified CM servers.

Procedure

- Step 1** Determine the relevant CA certificates to upload:
- If the servers' tomcat and CallManager certificates are CA-signed, the Expressway-C's trusted CA list must include the root CA of the certificate issuer.
 - If the servers are using self-signed certificates, the Expressway-C's trusted CA list must include the self-signed certificates from all discovered IM and Presence Service nodes, Cisco Unity Connection servers, and Unified CM servers.
- Step 2** Go to **Maintenance > Security > Trusted CA certificate** and upload the required certificates.
- Step 3** Go to **Maintenance > Restart options** and restart Expressway-C.
-

Discover Unified CM Servers

Procedure

- Step 1** On Expressway-C, go to **Configuration > Unified Communications > Unified CM servers**.
The page lists any Unified CM nodes that have already been discovered.
- Step 2** Add the details of a Unified CM publisher node:
- a) Click **New**.
 - b) Enter the Unified CM publisher address.
You must enter an FQDN when TLS verify mode is On.
 - c) Enter the **Username** and **Password** of an account that can access this server.

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

- d) [Recommended] Leave **TLS verify mode** switched **On** to ensure Expressway verifies the node's certificates.

The Unified CM node presents its tomcat certificate for AXL and UDS queries, and its CallManager certificate for subsequent SIP traffic. If the Unified CM server is using self-signed certificates, the Expressway-C's trusted CA list must include a copy of the tomcat certificate and the CallManager certificate from every Unified CM server.

- e) (Optional) To enable support for AES GCM media encryption, set AES GCM support to On.
f) (Optional) Select which deployment this node/cluster will belong to.

The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.

- g) Click **Add address**.

If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.

If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

Figure 17: Configuration Example

The screenshot shows the 'Unified CM servers' configuration page. The breadcrumb trail is 'Configuration > Unified Communications > Unified CM servers > New'. The main heading is 'Unified CM server lookup'. The form contains the following fields:

- Unified CM publisher address: (with an information icon)
- Username: (with an information icon)
- Password: (with an information icon)
- TLS verify mode: (with a dropdown arrow and an information icon)

At the bottom of the form are two buttons: 'Add address' and 'Cancel'.

- Step 3** Repeat the discovery procedure for other Unified CM nodes/clusters, if required.
- Step 4** Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.
- Step 5** Deleting Unified CM Servers from the Discovered List. **Only do this step if you need to remove existing Unified CMs from the Expressway configuration for any reason:**
- In the **Currently found Unified CM nodes** list, check the **Publisher address** entries that you want to remove from the list of discovered nodes and click **Delete**.

Discover IM and Presence Service Nodes

Procedure

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

The page lists any IM and Presence Service nodes that have already been discovered.

Step 2 Add the details of an IM and Presence Service database publisher node:

- a) Click **New**.
- b) Enter the address of the IM and Presence Service database publisher node .

You must enter an FQDN when **TLS verify mode** is **On**.

- c) Enter the **Username** and **Password** of an account that can access this server.

These credentials are stored permanently in the Expressway database. The corresponding IM and Presence Service user must have the *Standard AXL API Access* role.

- d) [Recommended] Leave TLS verify mode switched **On** to ensure Expressway verifies the node's tomcat certificate (for XMPP-related communications).
- e) (Optional) Select which deployment this node/cluster will belong to.

The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.

- f) Click **Add address**.

If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.

If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

Figure 18: IM and Presence Service Example

The status of the discovered node will be Inactive unless a valid traversal zone connection exists between the Expressway-C and the Expressway-E (may not yet be configured).

Step 3 Repeat the discovery procedure for other IM and Presence Service nodes/clusters, if required.

Step 4 Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

Discover Cisco Unity Connection Servers

Procedure

- Step 1** On Expressway-C, go to **Configuration > Unified Communications > Unity Connection servers**.
The page lists any Cisco Unity Connection nodes that have already been discovered.
- Step 2** Add the details of a Cisco Unity Connection publisher node:
- Click **New**.
 - Enter the **Unity Connection address**.
You must enter an FQDN when **TLS verify mode** is **On**.
 - Enter the **Username** and **Password** of an account that can access this server.
These credentials are stored permanently in the Expressway database. The corresponding Cisco Unity Connection user must have the System Administrator or Remote Administrator role.
 - [Recommended] Leave **TLS verify mode** switched **On** to ensure Expressway verifies the node's tomcat certificate.
 - (Optional) Select which deployment this node/cluster will belong to.
The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.
 - Click **Add address**.
If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.
If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.
- Step 3** Repeat the discovery procedure for other Cisco Unity Connection nodes/clusters, if required.
- Step 4** Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.
-

Automatically Generated Zones and Search Rules

Expressway-C automatically generates non-configurable neighbor zones between itself and each discovered Unified CM node. A TCP zone is always created, and a TLS zone is created also if the Unified CM node is configured with a Cluster Security Mode (**System > Enterprise Parameters > Security Parameters**) of 1 (*Mixed*) (so that it can support devices provisioned with secure profiles). The TLS zone is configured with its **TLS verify mode** set to **On** if the Unified CM discovery had TLS verify mode enabled. This means that the Expressway-C will verify the CallManager certificate for subsequent SIP communications. Each zone is created with a name in the format 'CEtcp-<node name>' or 'CETls-<node name>'.

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 OAuth with Refresh \(Self-Describing\) on Unified CM SIP Lines, on page 55](#).

A non-configurable search rule, following the same naming convention, is also created automatically for each zone. The rules are created with a priority of 45. If the Unified CM node that is targeted by the search rule has a long name, the search rule will use a regex for its address pattern match.

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

Why You Need to Refresh the Discovered Nodes?

When the Expressway-C discovers a Unified Communications node, it establishes a connection to read the information required to create zones and search rules to proxy requests originating from outside of the network in towards that node. **This configuration information is static.** Expressway only reads it when you manually initiate discovery of a new node, or when you refresh the configuration of previously discovered nodes. If any related configuration has changed on a node after you discover it, the mismatch between the new configuration and what the Expressway-C knows of that node is likely to cause some kind of failure.

The information that the Expressway-C reads from the Unified Communications node is different for each node type/role. These are examples of UC configuration that you can expect to require a refresh from the Expressway. The list is not exhaustive. If you suspect that a configuration change on a node is affecting MRA services, you should refresh those nodes to eliminate one known source of potential problems.

- Changing cluster (such as adding or removing a node)
- Changing security parameters (such as enabling Mixed Mode)
- Changing connection sockets (such as SIP port configuration)
- Changing TFTP server configuration
- Upgrading node software

Devices cannot connect during the refresh

It takes some time to restore services after a server refresh and while the refresh is in progress, Jabber clients and other endpoints are unable to connect over MRA. It is not possible to provide accurate timings as they vary depending on the deployment. For straightforward deployments the refresh typically takes 5 to 10 seconds, but very complex configurations may take upwards of 45 seconds.



CHAPTER 10

Configure MRA

- [Configure MRA Access Control, on page 51](#)
- [Check the Unified Communications Services Status, on page 56](#)
- [Working With the Allow List, on page 57](#)
- [Expressway-E for Mobile and Remote Access Configuration Workflow, on page 60](#)
- [SAML SSO Authentication Over the Edge, on page 61](#)
- [Activation Code Onboarding Through MRA, on page 69](#)
- [Dial via Office-Reverse through MRA, on page 71](#)
- [Built-in-Bridge Recording through MRA, on page 73](#)
- [Configure a Secure Traversal Zone Connection for Unified Communications, on page 75](#)

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.

Procedure

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

Authorization and Authentication Comparison

We use the concepts “authorization” and “authentication” in documentation and the user interface. At a high level, these terms can be explained using a hotel analogy:

- **Authentication:** Equates to hotel registration by a visitor. Defines the initial check-in process to allow you access into the hotel, where you prove who you are by presenting credentials like a passport or driving license.

- **Authorization:** Equates to a hotel key card given to a visitor. Controls the specific hotel room and other services that you are allowed to use during your stay.

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.

Expressway (Expressway-C) Settings for Access Control

Table 8: Settings for MRA Access Control

Field	Description	Default
Authentication path	<p>Hidden field until MRA is enabled. Defines how MRA authentication is controlled.</p> <p><i>SAML SSO authentication:</i> Clients are authenticated by an external IdP.</p> <p><i>UCM/LDAP basic authentication:</i> Clients are authenticated locally by the Unified CM against their LDAP credentials.</p> <p><i>SAML SSO and UCM/LDAP:</i> Allows either method.</p> <p><i>None:</i> 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.</p>	None before MRA turned on UCM/LDAP after MRA turned on
Authorize by OAuth token with refresh	<p>This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them.</p> <p>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.</p> <p>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.</p> <p>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.</p>	On

Field	Description	Default
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 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.	Off
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 65 .	—
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: <ul style="list-style-type: none"> • Cluster: Generates a single cluster-wide 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 61 .	—

Field	Description	Default
Allow Jabber iOS clients to use embedded Safari	<p>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.</p> <p>This setting optionally allows Jabber on iOS devices to use the native Safari browser. Because the Safari browser <i>is</i> able to access the device trust store, you can now enable password-less authentication or two-factor authentication in your OAuth deployment.</p> <p>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.</p> <p>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.</p>	No
Check for internal authentication availability	<p>Available if Authorize by OAuth token with refresh or Authorize by OAuth token is enabled.</p> <p>The default is No, for optimal security and to reduce network traffic.</p> <p>Controls how the Expressway-E reacts to remote client authentication requests by selecting whether or not the Expressway-C should check the home nodes.</p> <p>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:</p> <ul style="list-style-type: none"> • <i>Yes</i>: The <code>get_edge_sso</code> 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 <code>get_edge_sso</code> request. • <i>No</i>: If the Expressway is configured not to look internally, the same response will be sent to all clients, depending on the Edge authentication settings. <p>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 <i>No</i>. Or select <i>Yes</i> 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.</p> <p>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.</p>	No

Field	Description	Default
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.	No
SIP token extra time to live	Available if Authorize by OAuth token is <i>On</i> . 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

Configure Cisco Unified Communications Manager for OAuth with Refresh

To use self-describing tokens on Expressway (**Authorize by OAuth token with refresh**), you must also enable OAuth with refresh on Unified CM, and on Unity Connection if you use it. The settings are summarized here for convenience. For details, refer to the Cisco Unified Communications Manager or Cisco Unity Connection documentation.

Procedure

Do one of the following actions.

- For Unified CM, enable **OAuth with Refresh Login Flow** and **Caching**, in the **System > Enterprise Parameters**.
- For Unity Connection, enable **OAuth with Refresh Login Flow** and add **CUCM Publisher** to the **Authz server** settings.

Check Unified CM Support

You can check what authorization methods your Unified CM servers support. This displays the version numbers in use.

Procedure

On the Expressway, select **Configuration > Unified Communications > Unified CM servers**.

Configure OAuth with Refresh (Self-Describing) on Unified CM SIP Lines

From version X12.5, OAuth is supported on the Unified CM SIP line interface for Jabber clients only. When OAuth is enabled on the Unified CM SIP line and Jabber client, on-premises clients are authorized using self-describing tokens instead of client certificates.

Support for OAuth on the Unified CM SIP line from X12.5 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.

Procedure

Step 1 On 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.

Step 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

Step 3 Upgrade the Jabber clients to 12.5. Cisco Jabber 12.5 or later is required for either MRA or on-premises clients to connect using OAuth.

Step 4 Enable OAuth authorization on the Phone Security Profile (**System > Security > Phone Security Profile**) and apply the Phone Security Profile on the Jabber clients.

Refresh Servers on the Expressway-C

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

Procedure

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

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

Check the Unified Communications Services Status

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

Procedure

- Step 1** Go to **Status > Unified Communications**.
- Step 2** Review the list and status of domains, zones and (Expressway-C only) Unified CM and IM and Presence Service servers.
- The page displays any configuration errors along with links to the relevant configuration page that you access to address the issue.
-

Working With the Allow List

Expressway-C automatically adds rules (inbound and outbound) to the HTTP allow list.

For example, it adds inbound rules to allow external clients to access the Unified Communications nodes discovered during MRA configuration. These include Unified CM nodes (running CallManager and TFTP service), IM and Presence Service nodes, and Cisco Unity Connection nodes.

- Inbound rules are viewable at **Configuration > Unified Communications > HTTP allow list > Automatic inbound rules**.
- Outbound rules are viewable at **Configuration > Unified Communications > HTTP allow list > Automatic outbound rules**.

Can I edit the allow list?

- You can't add outbound rules to the list.
- You can add your own inbound rules, if clients from outside need to access other web services inside the enterprise. For example, these services may require you to configure the allow list.
 - Jabber Update Server
 - Cisco Extension Mobility
 - Directory Photo Host
 - Advanced File Transfer (AFT)
 - Problem Report Tool server
- You can't edit or delete auto-added rules in the list.

AFT feature

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

Automatic Inbound Rules

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

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

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

Table 9: Properties of Automatically Added Allow List Rules

Column	Description
Type	This rule affects all nodes of the listed type: <ul style="list-style-type: none"> • Unified CM servers: Cisco Unified Communications Managernodes • IM and Presence Service nodes: Cisco Unified Communications Manager IM and Presence Service nodes • Unity Connection servers: Cisco Unity Connection nodes • TFTP: TFTP nodes
Protocol	The protocol on which the rule allows clients to communicate with these types of nodes.
Ports	The ports on which the rule allows clients to communicate with these types of nodes.
Match type	<i>Exact</i> or <i>Prefix</i> . Depends on the nature of the service the clients access with the help of this rule.
Path	The path to the resource that clients access with the help of this rule. This may not be present, or may only be a partial match of the actual resource, if the rule allows <i>Prefix</i> match.
Methods	The HTTP methods that will be allowed through by this rule (such as GET).

Edit the HTTP Allow List

Procedure

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

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

Step 2 (Optional) Use the check boxes to modify the set of default HTTP methods, then click **Save**.

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

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

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

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

Step 5 Configure the rule to your requirements.

Here is some advice for each of the fields.

Table 10: Properties of Manually Added Allow List Rules

Column	Description
Description	Enter a meaningful description for this rule, to help you recognize its purpose.
Url	Specify a URL that MRA clients are allowed to access. For example, to allow access to <code>http://www.example.com:8080/resource/path</code> , just type it in exactly like that. <ul style="list-style-type: none"> The protocol the clients are using to access the host must be <code>http://</code> or <code>https://</code> Specify a port when using a non-default port e.g. <code>:8080</code> (Default ports are 80 (http) and 443 (https)) Specify the path to limit the rule scope (more secure), e.g. <code>/resource/path</code> <p>If you select Prefix match for this rule, you can use a partial path or omit the path. Be aware that this could be a security risk if the target resources are not resilient to malformed URLs.</p>
Allowed methods	Select Use defaults or Choose methods . If you choose specific HTTP methods for this rule, they will override the defaults you chose for all rules.
Match type	Select Exact match or Prefix match . Your decision here depends on your environment. It is more secure to use exact matches, but you may need more rules. It is more convenient to use prefix matches, but there is some risk of unintentionally exposing server resources.
Deployment	If you are using multiple deployments for your MRA environment, you also need to choose which deployment uses the new rule. You won't see this field unless you have more than one deployment.

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

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

Upload Rules to the HTTP Allow List



Note You cannot upload outbound rules.

Procedure

-
- Step 1** Go to **Configuration > Unified Communications > HTTP allow list > Upload rules**.
- Step 2** Browse to and select the CSV file containing your rule definitions.
See [Allow List Rules File Reference](#), on page 115.
- Step 3** Click **Upload**.
The Expressway responds with a success message and displays the **Editable inbound rules** page.
-

Expressway-E for Mobile and Remote Access Configuration Workflow

This section describes the configuration steps required on the Expressway-C for Mobile and Remote Access.

Procedure

Configure DNS and NTP Settings on Expressway-E

If you have a cluster of Expressways, you must do this for every peer.



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

If you have a cluster of Expressway-Es, make sure that the Domain name is identical on each peer. The name is case-sensitive .

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

Before you begin

All Expressway systems are synchronized to a reliable NTP service (**System > Time**).

Procedure

- Step 1** Access **System** > **DNS**.
 - Step 2** Set **System host name** and **Domain name**.
 - Step 3** Set Public DNS servers.
 - Step 4** Set an **Authentication** method in accordance with your local policy.
-

Enable SIP Protocol During Configuration

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

Procedure

- Step 1** On the Expressway-C, go to **Configuration** > **Protocols** > **SIP**.
 - Step 2** Set **SIP mode** to **On** and **Save** the page.
-

Enable the Expressway-E for Mobile and Remote Access

To enable Mobile and Remote Access functionality:

Procedure

- Step 1** Go to **Configuration** > **Unified Communications** > **Configuration**.
 - Step 2** Set **Unified Communications mode** to **Mobile and Remote Access**.
 - Step 3** Click **Save**.
-

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

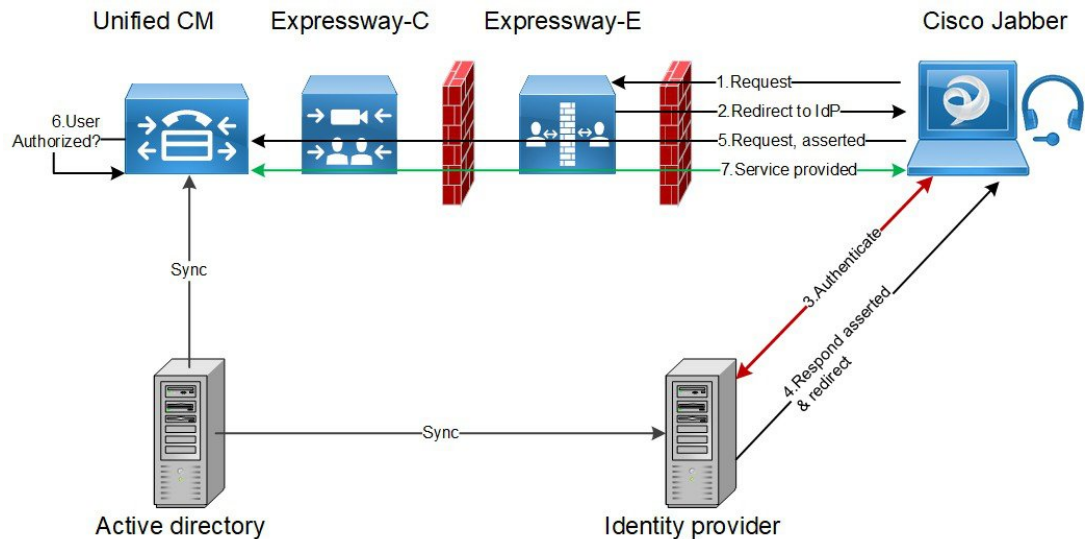
How it works

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 19: Simple OAuth token-based authorization for on-premises UC services



About Self-Describing OAuth Token Authorization with Refresh

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

- Token refresh capability, so users do not have to repeatedly re-authenticate.
- Fast authorization.
- Access policy support. The Expressway can enforce MRA access policy settings applied to users on the Unified CM.
- Roaming support. Tokens are valid on-premises and remotely, so roaming users do not need to re-authenticate if they move between on-premises and off-premises.

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

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

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

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

Prerequisites

- Expressway is already providing Mobile and Remote Access for Cisco Jabber.
- All other devices in the call flow are similarly enabled.
- You have the following minimum product versions installed, or later:
 - Expressway X8.10.1
 - Cisco Jabber iOS 11.9

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

 - Cisco Unified Communications Manager 11.5(SU3)
 - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
 - Cisco Unity Connection 11.5(SU3)
- Make sure that self-describing authentication is enabled on the Cisco Expressway-C (**Authorize by OAuth token with refresh** setting) and on Unified CM and/or IM and Presence Service (**OAuth with Refresh Login Flow** enterprise parameter).
- You must refresh the Unified CM nodes defined on the Expressway. This fetches keys from the Unified CM that the Expressway needs to decrypt the tokens.

OAuth Token Authorization Prerequisites

On the Expressway Pair

- An Expressway-E and an Expressway-C are configured to work together at your network edge.
- A Unified Communications traversal zone is configured between the Expressway-C and the Expressway-E.
- The SIP domain that will be accessed via 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

High Level Task List

1. If you intend to use self-describing token authorization (**Authorize by OAuth token with refresh**) we recommend getting it working on-premises first, before attempting to enable it for MRA clients.
2. Configure a synchronizable relationship between the identity provider and your on-premises directory so that authentication can securely be owned by the IdP. See “Directory Integration and Identity Management” in the [Cisco Collaboration System 11.x Solution Reference Network Designs \(SRND\)](#) document.
3. Export SAML metadata file from the IdP. Check the documentation on your identity provider for the procedure. For example, see “Enable SAML SSO through the OpenAM IdP” in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.
4. Import the SAML metadata file from the IdP to the Unified CM servers and Cisco Unity Connection servers that will be accessed by single sign-on. See the Unified Communications documentation or help for more details.

5. Export the SAML metadata files from the Unified CM servers and Cisco Unity Connection servers. For example, see “High-Level Circle of Trust Setup” in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.
6. Create the Identity Provider on the Expressway-C, by importing the SAML metadata file from the IdP.
7. Associate the IdP with SIP domain(s) on the Expressway-C.
8. Export the SAML metadata file(s) from the (primary) Expressway-C; ensure that it includes the externally resolvable address of the (primary) Expressway-E.

The SAML metadata file from the Expressway-C contains the X.509 certificate for signing and encrypting SAML interchanges between the edge and the IdP, and the binding(s) that the IdP needs to redirect clients to the Expressway-E (peers).
9. Import the SAML metadata files from the Unified CM servers and Cisco Unity Connection servers to the IdP. An example using OpenAM is in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.
10. If you intend to use a single, cluster-wide metadata file for SAML agreement, configure the mandatory attribute uid on the IdP. A Service Provider identifies the identity of an authenticated user through this attribute (for information about attribute mapping, refer to the IdP product documentation).



Note This uid attribute must match the LDAP synchronized user id attribute that is used in Unified Communications applications.

11. Similarly, import the SAML metadata file from the Expressway-C to the IdP. See the IdP documentation for details.
12. Turn on SAML SSO at the edge, on the Expressway-C. See [Configure MRA Access Control, on page 51](#).

Import the SAML Metadata from the IdP

Procedure

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.

Procedure

- 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.
-

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). 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.



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

Procedure

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.

IdPs Configurations

This topic covers any known additional configurations that are needed when using a particular IdP for OAuth token-based authorization over MRA.

These configuration procedures are required in addition to the prerequisites and high level tasks already mentioned, some of which are outside of the document's scope.

Active Directory Federation Services 2.0

After creating Relying Party Trusts for the Expressway-Es, you must set some properties of each entity, to ensure that Active Directory Federation Services (ADFS) formulates the SAML responses as Expressway-E expects them.

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

These procedures were verified on AD FS 2.0, although the same configuration is required if you are using AD FS 3.0.

You need to:

- Sign the whole response (message and assertion)
- Add a claim rule to send identity as `uid` attribute

Sign the Whole Response

Procedure

In Windows PowerShell®, run the following command for each Expressway-E's <EntityName> once per Relying Party Trust created on ADFS:

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

where <EntityName> must be a display name for the Relying Party Trust of Expressway-E as set in ADFS.

Add a Claim Rule for Each Relying Party Trust

Procedure

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

Activation Code Onboarding Through MRA

This feature optionally allows MRA-compliant devices to easily and securely register over MRA using an activation code. It is 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 Unified CMs before this feature can be used

If you have upgraded an existing Cisco Expressway from an earlier release than X12.5, refresh the currently configured Unified CMs on Cisco 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.

Prerequisites

Ensure the phone has been created and activation enabled on CUCM, for more information [see](#)

1. In Cisco CUCM Enterprise Parameters, Verify OAuth with Refresh login flow parameter is enabled.
Go to **Cisco Unified CM Administration** > **Enterprise Parameters** > **SSO and OAuth Configuration**
2. Check the cloud Onboarding page
 - To authorize the cluster (CCMAct service) to connect to the cloud-based device activation service, generate the voucher by clicking the Generate Voucher button.

Check Enable Activation Code onboarding with Cisco Cloud



Note Collab-edge DNS SRV record(s) need to exist for this domain

MRA Activation domain should be provided. MRA activation domain provided to Cisco Cloud to redirect phones to customer Expressway-E(s).



Note One MRA activation domain per CUCM cluster

3. Go to **Cisco Unified CM Administration** > **Advanced Features** > **MRA Service Domain** menu to create and manage MRA service domains



Note There will be one system level default MRA service domain, plus the option to establish MRA service domains at the device pool and device level. The MRA activation domain can also be used as a service domain. Different service domains can be used to direct phones to regional Expressway C/E pairs.

4. Check MRA access control on Expressway
 - Go to **Expressway C** > **Configuration** > **Unified Communications** > **Configuration**
 - Check Authorize by OAuth token with refresh is set to On
 - Allow activation code onboarding set to Yes



Note Enabling Activation Code Onboarding forces the Expressway-E to request a client certificate for any connections to TCP 8443

5. Check Trusted Cisco manufacturing certificates (MICs) installed. They are required to access the activation code onboarding functionality
 - Go to **Expressway E** > **Maintenance** > **Security certificates** > **Trusted CA certificate**

- Click Activate code onboarding trusted CA certificates

Dial via Office-Reverse through MRA

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

DVO-R handles call signaling and voice media separately. Call signaling, including the signaling for Mobile and Remote Access on Expressway, traverses the IP connection between the client and Cisco Unified Communications Manager. Voice media traverses the cellular interface and hairpins at the enterprise Public Switched Telephone Network (PSTN) gateway. Moving audio to the cellular interface ensures high-quality calls and securely maintained audio even when the IP connection is lost.

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

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

Dial via Office-Reverse through MRA Prerequisites

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

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

Call Flows

Figure 20: DVO-R calling

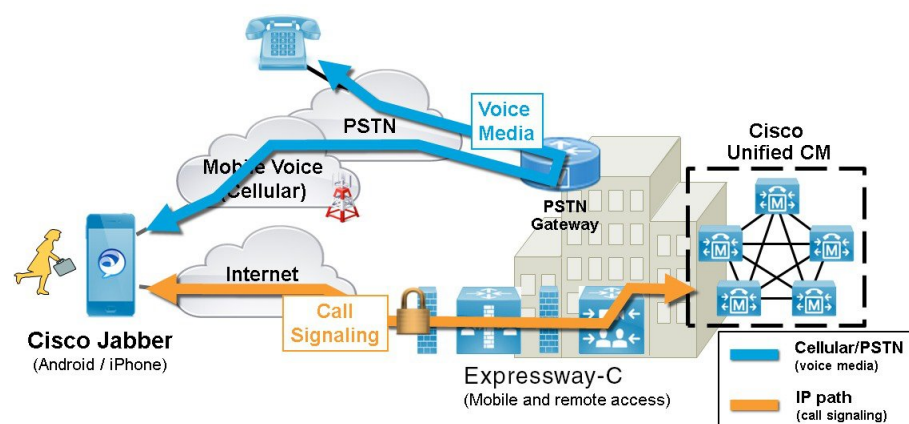


Figure 21: DVO-R using Mobility Identity

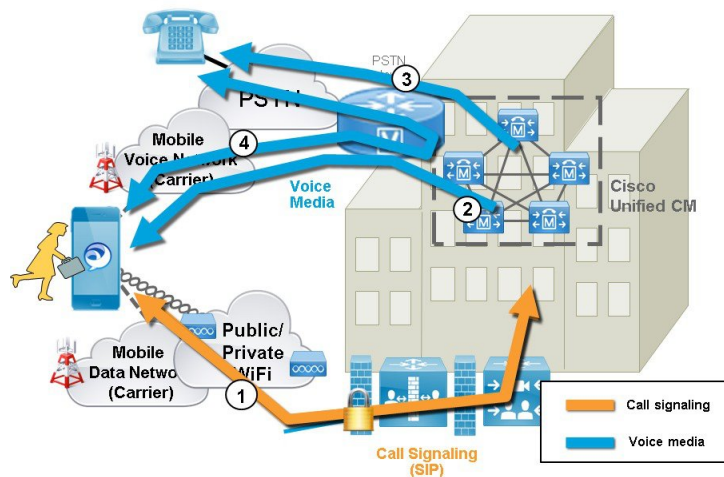
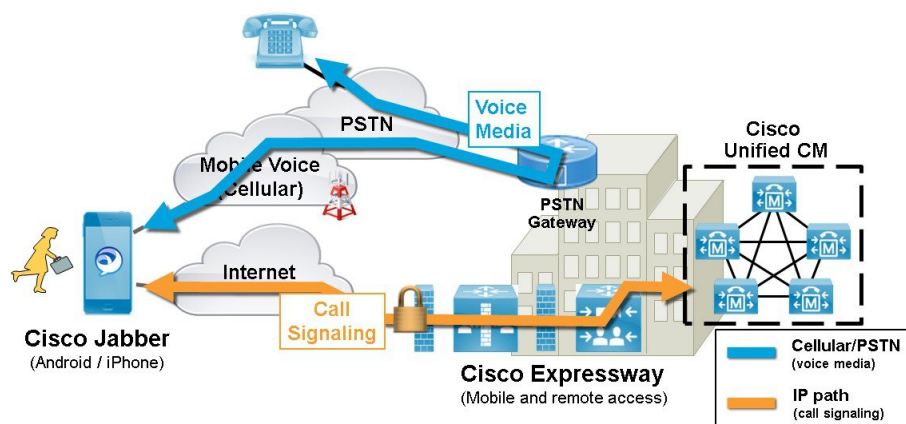


Figure 22: DVO-R using Alternate Number



How DVO-R Works with Expressway Mobile and Remote Access

When you dial a number, a signal is sent to Cisco Unified Communications Manager over the IP path (WLAN or mobile network). See stage 1 of [Figure 21: DVO-R using Mobility Identity, on page 72](#) or [Figure 22: DVO-R using Alternate Number, on page 72](#).

Cisco Unified Communications Manager calls your mobile number or the Alternate Number you set (see stage 2 of [Figure 21: DVO-R using Mobility Identity, on page 72](#) or [Figure 22: DVO-R using Alternate Number, on page 72](#).)

When you answer, Cisco Unified Communications Manager extends the call to the number you dialed and you hear ring back (see stage 3 of [Figure 21: DVO-R using Mobility Identity, on page 72](#) or [Figure 22: DVO-R using Alternate Number, on page 72](#)).

When the person answers, the ongoing call is hairpinned at the enterprise PSTN gateway.

If you made the call using a Mobile Identity, your call is anchored at the enterprise gateway. The call is active on your mobile and desk phone, so you can switch between the two (see stage 4 of [Figure 21: DVO-R using Mobility Identity, on page 72](#)).

If you specified an Alternate Number, your ongoing call is not anchored and you cannot pick up on your desk phone (see stage 4 of [Figure 22: DVO-R using Alternate Number, on page 72](#)).

Notes

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



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

Configuration Checklist for DVO-R

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

More DVO-R Information

More information on this subject is available in the article *Configuring Dial via Office-Reverse to Work with Mobile and Remote Access* at <http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-configuration-examples-list.html>.

Built-in-Bridge Recording through MRA

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

How it works

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

BiB is always enabled on the Expressway.

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

Bandwidth and call capacity impacts

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

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

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

Built-in-Bridge Recording through MRA Prerequisites

BiB over MRA requires the following components, or later:

- Any compatible clients:
 - Cisco Jabber for Windows 11.9
 - Cisco Jabber for Mac 11.9
 - Cisco Jabber for iPhone and iPad 11.9
 - Cisco Jabber for Android 11.9
 - Cisco IP Phone 7800 Series, Cisco IP Conference Phone 7832, or Cisco IP Phone 8800 Series devices which support MRA (not all these phones are MRA-compatible)

The phones which currently support MRA are listed in the [MRA Infrastructure Requirements, on page 21](#) section of this guide, or ask your Cisco representative for details.
- Registrar/call control agent: Cisco Unified Communications Manager 11.5(1)SU3 BiB is not supported on Expressway-registered endpoints.
- Edge traversal: Expressway X8.11.1
- Recording server: Out of scope for this document. (Information about configuring recording for Cisco Unified Communications Manager is available in the [Feature Configuration Guide for Cisco Unified Communications Manager](#).)

Configure BiB over MRA



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

Procedure

-
- Step 1** Verify that the BiB recording system in the Unified CM works correctly, before you configure BiB for MRA.
- Step 2** Make sure that the prerequisites listed above are in place.
- Step 3** SIP Path headers must be enabled on Cisco Expressway-C:
- a) On the Cisco Expressway-C, go to **Configuration > Unified Communications > Configuration**.
 - b) Set **SIP Path headers** to **On**.
- Step 4** Go to **Configuration > Unified Communications > Unified CM servers**.
- Step 5** Click **Refresh servers**.
-

Configure a Secure Traversal Zone Connection for Unified Communications

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

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

Use this workflow to set up a secure traversal zone connection.

Procedure

	Command or Action	Purpose
Step 1	Install Expressway Security Certificates, on page 75	Install suitable security certificates on Expressway-C and Expressway-E.
Step 2	Configure Encrypted Expressway Traversal Zones, on page 76	Configure a Unified Communications traversal zone between Expressway-C and Expressway-E.

Install Expressway Security Certificates

You must set up trust between the Expressway-C and the Expressway-E with a suitable server certificate on both Expressways. The certificate must include the Client Authentication extension. The system will not let you upload a server certificate without this extension when Unified Communications features are enabled.

The Expressway includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR:

- Ensure that the CA that signs the request does not strip out the client authentication extension.

- The generated CSR includes the client authentication request and any relevant subject alternate names for the Unified Communications features that have been enabled (see [Server Certificate Requirements for Unified Communications Manager, on page 37](#)).

Install on both Expressways the trusted Certificate Authority (CA) certificates of the authority that signed the Expressway's server certificates.

There are additional trust requirements, depending on the Unified Communications features being deployed.

- For Mobile and Remote Access deployments:
 - The Expressway-C must trust the Unified CM and IM&P tomcat certificate.
 - If appropriate, both the Expressway-C and the Expressway-E must trust the authority that signed the endpoints' certificates.
- For Jabber Guest deployments:
 - When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the Expressway-C either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server's certificate.

For more details, see the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway configuration guides page](#).

Procedure

-
- Step 1** Go to **Maintenance > Security > Server certificate** to generate a CSR and to upload a server certificate to the Expressway.
 - Step 2** Go to **Maintenance > Security > Trusted CA certificate** and upload trusted Certificate Authority (CA) certificates to the Expressway.
 - Step 3** Restart the Expressway for the new trusted CA certificate to take effect.
-

Configure Encrypted Expressway Traversal Zones

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

- The Expressway-C and Expressway-E must be configured with a zone of type Unified Communications traversal. This automatically configures an appropriate traversal zone (a traversal client zone when selected on Expressway-C or a traversal server zone when selected on Expressway-E) that uses SIP TLS with TLS verify mode set to On, and Media encryption mode set to Force encrypted.
- Both Expressways must trust each other's server certificate. As each Expressway acts both as a client and as a server you must ensure that each Expressway's certificate is valid both as a client and as a server.
- 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.

To set up a secure traversal zone, configure your Expressway-C and Expressway-E.

Procedure

- Step 1** Go to **Configuration > Zones > Zones**.
- Step 2** Click **New**.
- Step 3** Configure the fields as follows (leave all other fields with default values):

	Expressway-C	Expressway-E
Name	“Traversal zone” for example	“Traversal zone” for example
Type	Unified Communications traversal	Unified Communications traversal
Connection credentials section		
Username	“exampleauth” for example	“exampleauth” for example
Password	“ex4mpl3.c0m” for example	Click Add/Edit local authentication database . 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 <i>Cisco Expressway IP Port Usage Configuration Guide</i> , 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.	Not applicable

	Expressway-C	Expressway-E
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**.



CHAPTER 11

Unified CM Configuration

- [SIP Trunks Between Unified CM and Expressway-C](#), on page 79
- [Unified Communications Services Deployment Partitions](#), on page 80

SIP Trunks Between Unified CM and Expressway-C

Expressway deployments for Mobile and Remote Access do not require SIP trunk connections between Unified CM and Expressway-C. Note that the automatically generated neighbor zones between Expressway-C and each discovered Unified CM node are not SIP trunks.

However, you may still configure a SIP trunk if required. (For example, to enable B2B callers or endpoints registered to Expressway to call endpoints registered to Unified CM.)

If a SIP trunk is configured, you must ensure that it uses a different listening port on Unified CM from that used for SIP line registrations to Unified CM. An alarm is raised on Expressway-C if a conflict is detected.

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

See the [Cisco TelePresence Cisco Unified Communications Manager with Expressway \(SIP Trunk\) Deployment Guide](#) for more information about configuring a SIP trunk.

See [Configure Cisco Unified Communications Manager for OAuth with Refresh](#), on page 55 for information about OAuth-based authorization on SIP trunks.

Configure Line Registration Listening Ports on Unified CM

There are two ports that are used for line registrations to Unified CM:

- **SIP Phone Port:** the TCP port.
- **SIP Phone Secure Port:** the TLS port.

Procedure

- Step 1** Access **System > Cisco Unified CM**.
- Step 2** Set the **SIP Phone Port** to **5060**.

- Step 3** Set the **SIP Phone Secure Port** to 5061.
-

Configure SIP Trunk Listening Ports on Unified CM

Procedure

- Step 1** Go to **System > Security > SIP Trunk Security Profile** and select the profile used for the SIP trunk.
If this profile is used for connections from other devices, you may want to create a separate security profile for the SIP trunk connection to Expressway.
- Step 2** Configure the **Incoming Port** to be different from that used for line registrations.
- Step 3** Click **Save** and then click **Apply Config**.
-

Configure SIP Trunk Listening Ports on Expressway

Procedure

- Step 1** Go to **Configuration > Zones > Zones** and select the Unified CM neighbor zone used for the SIP trunk.
(Note that the automatically generated neighbor zones between Expressway-C and each discovered Unified CM node for line side communications are non-configurable.)
- Step 2** Configure the **SIP Port** to the same value as the **Incoming Port** configured on Unified CM.
- Step 3** Click **Save**.
-

Unified Communications Services Deployment Partitions

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

We recommend that you do not exceed ten deployments.

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

One primary deployment (called "Default deployment" unless you rename it) automatically encloses all domains and services until you create and populate additional deployments. This primary deployment cannot be deleted, even if it is renamed or has no members.

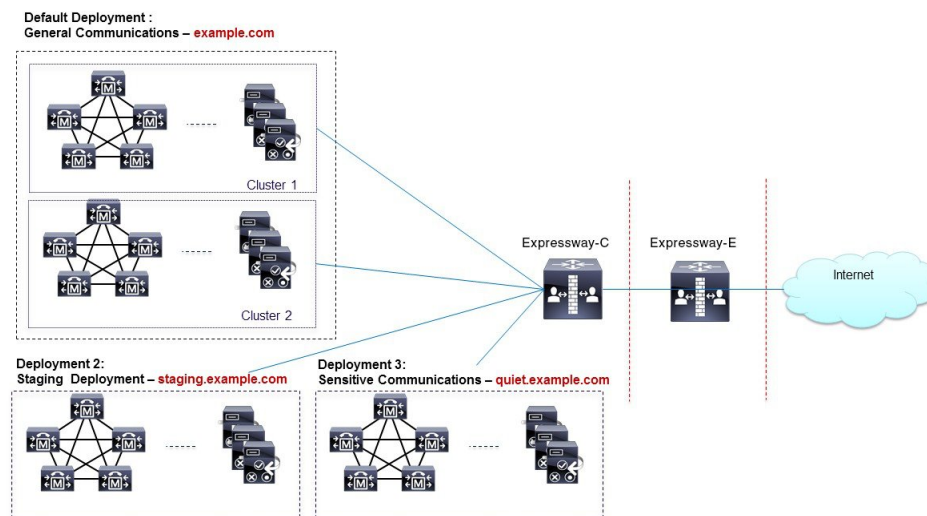
To partition the services that you provide through Mobile and Remote Access, create as many deployments as you need. Associate a different domain with each one, and then associate the required Unified Communications resources with each deployment.

You cannot associate one domain with more than one deployment. Similarly, each Unified Communications node may only be associated with one deployment.

Example

Consider an implementation of two sets of Unified Communications infrastructure to provide a live MRA environment and a staging environment, respectively. This implementation might also require an isolated environment for sensitive communications, as a third set.

Figure 23: Multiple Deployments to Partition Unified Communications Services Accessed from Outside the Network



Create a New Deployment

Procedure

- Step 1** Log in to the Expressway-C.
- Step 2** Go to **Configuration > Unified Communications > Deployments** and click **New**.
- Step 3** Give the deployment a name and click **Create deployment**.

The new deployment is listed on the Deployments page and is available to select when editing domains or UC services.

Associate a Domain with a Deployment

Procedure

- Step 1** Go to **Configuration > Domains**.
- The domains and their associated services are listed here. The deployment column shows where the listed domains are associated.
- Step 2** Click the domain name, or create a new domain.
- Step 3** In the **Deployment** field, select the deployment which will enclose this domain.
- Step 4** Click **Save**.
-

Associate a Unified CM or Other Server/Service with the Deployment

Procedure

- Step 1** Go to **Configuration > Unified Communications** and select one of the following entries:
- **Unified CM servers**
 - **IM and Presence Service nodes**
 - **Unity Connection servers**
- Any previously discovered service nodes of the selected type are listed here. The deployment column shows where the listed nodes are associated.
- If the list is not properly populated, see [Discover Unified Communications Servers and Services for Mobile and Remote Access, on page 45](#).
- Step 2** Click the server / service node name.
- Step 3** In the **Deployment** field, select which deployment will enclose this server / service node.
- Step 4** Click **Save**.
- When you save this change, the Expressway-C refreshes the connection to the node, which may temporarily disrupt the service to the connected users.
- Step 5** Repeat for any other Unified Communications services that will belong to the deployment.
-



CHAPTER 12

APNS Support (Optional)

- [Apple Push Notifications \(APNS\) Prerequisites and Recommendations, on page 83](#)
- [Push Notifications in Unified Communications Products, on page 85](#)
- [Configure Apple Push Notifications in Expressway, on page 85](#)

Apple Push Notifications (APNS) Prerequisites and Recommendations

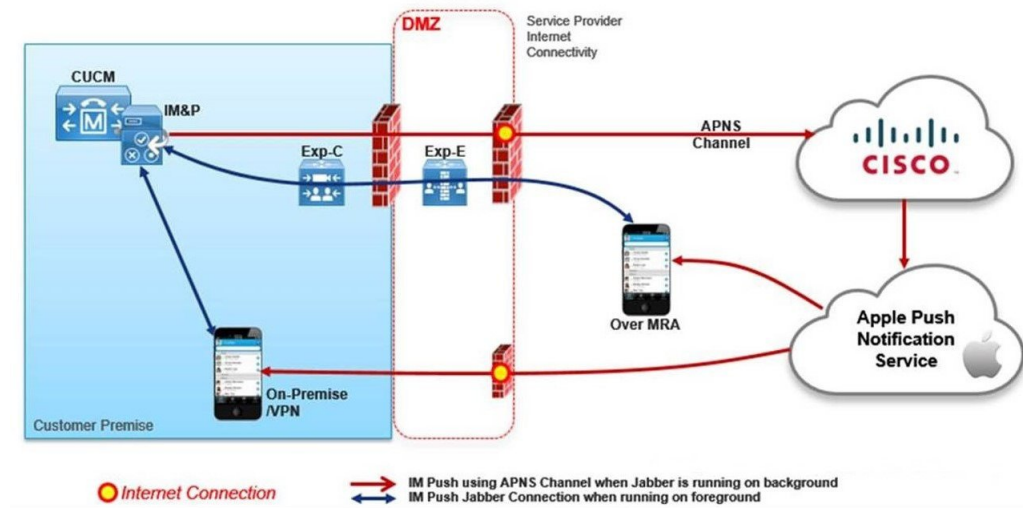
Apple Push Notifications apply for users with compatible Cisco Jabber iOS devices who sign in remotely. Expressway deployments that are configured for MRA can support Apple's cloud-based Push Notification Service (APNS). From X8.9.1, we support Push Notifications for IM and Presence Service instant messages. From X8.10, we support voice and video calls too.

Push Notifications are only used for Jabber for iPhone and iPad (and Cisco Jabber for Android clients from X12.6). Windows, and Mac users are unaffected.



Note If Unified CM detects a remote or mobile Jabber for iPhone and iPad connection, it always sends a Push Notification as well as a SIP Invite.

Figure 24: Push Notifications Architecture



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

- Push Notifications in the Expressway require a network connection between Cisco Jabber and the Push Notification servers in the Apple cloud. They cannot work in a private network, with no internet connection.
- Expressway is already providing Mobile and Remote Access for Jabber for iPhone and iPad. MRA must be fully configured (domain, zone, server settings).
- Depending on your Unified CM configuration, you may need a forward proxy to send Push Notifications to the Cisco Collaboration Cloud.
- We recommend using self-describing token authorization.
- Expressway-E restart required for Push Notifications with instant messages. After you enable Push Notifications on the IM and Presence Service you need to restart the Expressway-E. Until the restart, Expressway-E cannot recognize the push capability on IM and Presence Service, and does not send PUSH messages to the Jabber clients.
- You need the following Push Notification-enabled software versions, or later:
 - Expressway X8.10.1
 - Cisco Jabber iOS 11.9
 - Cisco Unified Communications Manager 11.5(SU3)
 - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
 - Cisco Unity Connection 11.5(SU3)

Why Have We Implemented Support for Push Notifications?

Apple now deprecates the VoIP Background Mode that allows Jabber iOS to keep a SIP session open even when the app is running in the background. Push Notifications allow Unified CM to tell Jabber about incoming calls and messages. Then Jabber can reconnect to Unified CM to retrieve the message or answer the call. Jabber uses the new self-describing token feature to help it to do this quickly.

Push Notifications in Unified Communications Products

For information about Push Notifications in Unified CM and IM and Presence Service, see *Deploying Push Notifications for Cisco Jabber on iPhone and iPad with Cisco Unified Communication Manager* available from the [Cisco Unified Communications Manager](#) documentation pages on Cisco.com.

Configure Apple Push Notifications in Expressway



Caution Although the built-in forward proxy is in the Expressway interface, it is not currently supported and it should not be used.

Procedure

- Step 1** Configure OAuth token validation on the Expressway (see [Configure MRA Access Control](#), on page 51).
- Step 2** Configure Unified CM to use a forward proxy server (depending on your requirements for external requests from iOS devices) and make HTTPS connections with Cisco's cloud services.
-



CHAPTER 13

ICE Passthrough Support (Optional)

- [ICE Passthrough for Media Optimization, on page 87](#)
- [How ICE Passthrough Works, on page 87](#)
- [Supported Deployments, on page 89](#)
- [Supported Components, on page 90](#)
- [Supported Endpoints, on page 90](#)
- [ICE Passthrough Configuration, on page 90](#)

ICE Passthrough for Media Optimization

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.

ICE passthrough can be used with the currently supported MRA features. See [Supported and Unsupported Features with Mobile and Remote Access, on page 17](#) section for more information on supported MRA features.

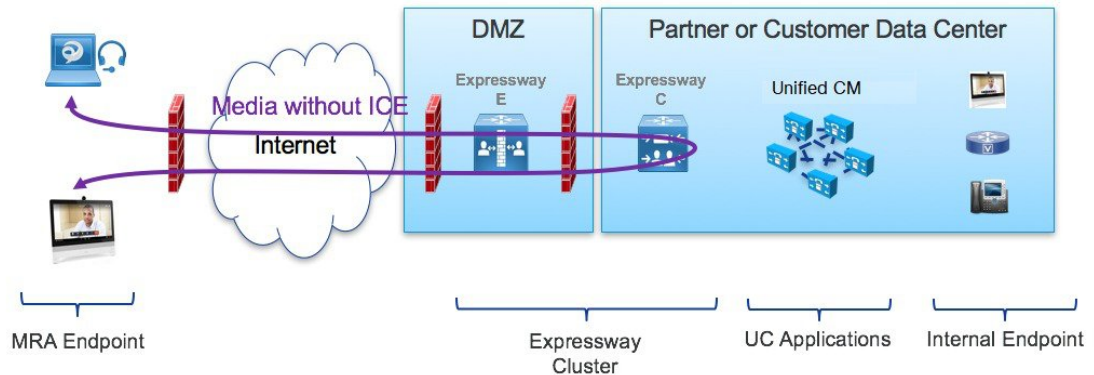
This feature uses the ICE protocol ([RFC 5245](#)). Background information about ICE is provided in the *About ICE and TURN Services* section of the *Cisco Expressway Administrator Guide* at <https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html>.

How ICE Passthrough Works

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

The following figure shows the MRA call without ICE passthrough. The media traverses through both the Cisco Expressway-E and the Cisco Expressway-C.

Figure 25: MRA Call Flow without ICE Passthrough



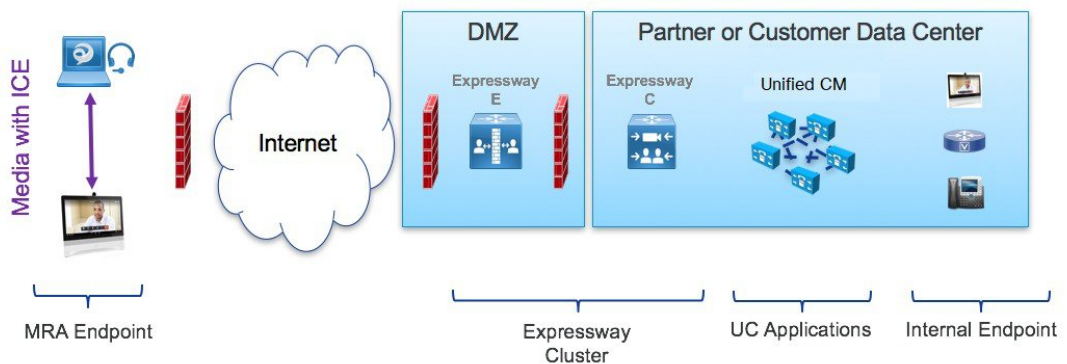
With ICE passthrough introduced in Cisco Expressway X12.5, each endpoint can pass the ICE candidates to the other endpoint through zones that traverse the SIP signaling. As a result, endpoints use the ICE protocol to negotiate the most optimal path for media. The most optimal path may be one of the following:

- **Host address:** Represents the host IP address of the endpoint which is behind the NAT device.
- **Server-reflexive address:** Represents the publicly accessible address of the endpoint on the NAT device.
- **Relay address:** Represents the relay address of the endpoint configured on the TURN server.

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

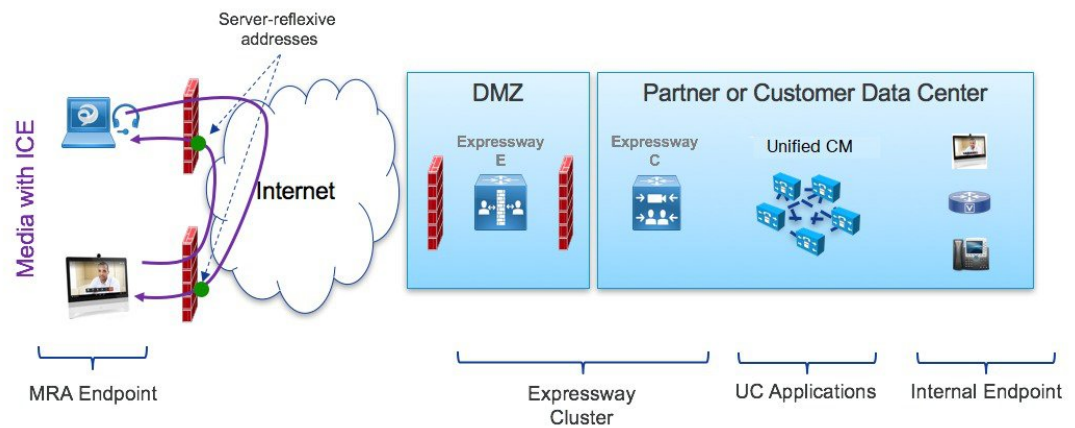
The following figure shows the MRA call with ICE passthrough. The media directly passes between the endpoints using the Host address, because the endpoints reside in the same network with no firewall between them.

Figure 26: MRA Call Flow with ICE Passthrough (using Host Address)



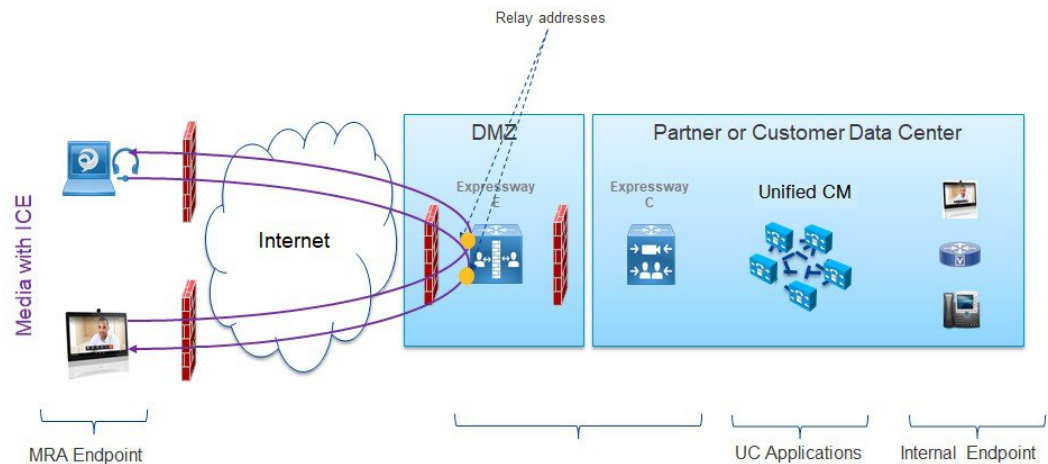
The following figure shows the MRA call with ICE passthrough where endpoints are behind a firewall. The media passes between the endpoints using Server-reflexive addressing, because the endpoints are behind different firewalls.

Figure 27: MRA Call Flow with ICE Passthrough (using Server-reflexive Address)



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

Figure 28: MRA Call Flow with ICE Passthrough (using Relay Address)



Supported Deployments

Cisco Expressway-based Deployments

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

- Cisco Webex Hybrid Services
- Jabber Guest
- Microsoft Gateway

- Collaboration Meeting Room (CMR) Cloud
- Business to Business Calling

HCS Deployments

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

- HCS Shared Architecture
- HCS Dedicated Server and HCS Dedicated Instance
- Customer-owned Collaboration Architecture



Note HCS Contact Center does not support ICE passthrough.

Supported Components

- HCS 11.5 or later
- Cisco Unified Communications Manager (Unified CM) 11.5 or later
- Cisco Expressway-C and Cisco Expressway-E X12.5 or later

Supported Endpoints

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

- Cisco Jabber clients, version 12.5 or later subject to using Unified Communications Manager 12.5 or later
- Cisco IP Conference Phone 7832, version 12.5(1) or later
- Cisco IP Phone 7800 Series (MRA-compatible models only), version 12.5(1) or later
- Cisco IP Phone 8800 Series (MRA-compatible models only), version 12.5(1) or later
- Cisco TelePresence DX, MX, SX Series, CE version 9.6.1 or later

ICE Passthrough Configuration

This section summarizes the steps to configure the following MRA components for ICE passthrough:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Expressway-C

- Cisco Expressway-E

Prerequisites

Before you start, make sure the following conditions are in place:

- Standard MRA configuration is done on Unified CM, Cisco Expressway-C, and Cisco Expressway-E.
- Endpoints are registered using MRA, and can make calls.

Set Up Unified CM for ICE Passthrough

The following steps summarize the configuration required on the Unified CM:

Procedure

- Step 1** Verify the Unified CM cluster security mode.
See [Verify the Unified CM Cluster Security Mode, on page 91](#).
- Step 2** Create a phone security profile with encrypted TLS and associate with the endpoints.
See [Apply Phone Security Profile with Encrypted TLS on Endpoints, on page 92](#).
- Step 3** Create a common phone profile with the configuration required for ICE Passthrough and associate with the endpoints.
See [Apply a Common Phone Profile with ICE Configuration on Endpoints, on page 92](#).
-

Verify the Unified CM Cluster Security Mode

The ICE MRA call path must be encrypted end-to-end. See [Signaling Path Encryption Between Expressway-C and Unified CM](#) for more details. For end-to-end encryption, Unified CM must be in mixed mode for physical endpoints. For Cisco Jabber clients, Unified CM is not required to be in mixed mode but must enable SIP OAuth.

For more information on how to enable OAuth, see [Configure Cisco Unified Communications Manager for OAuth with Refresh](#).

You cannot change the Unified CM security mode from Cisco Unified Communications Manager Administration. To change the security mode, use the Cisco CTL Client or the `utils ctl` CLI command, as follows:

Procedure

Do one of the following actions.

- To use the Cisco CTL client to set the cluster security mode to Mixed mode, see the “Update Cisco Unified Communications Manager Security Mode” section in the *Security Guide for Cisco Unified Communications Manager* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.
- To use the **utils ctl** CLI command to set the cluster security mode to Mixed mode, see the “utils ctl” section in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

Note A new license key is required on Unified CM for Mixed mode. You can order this license through Product Upgrade Tool (PUT) tool and install the license on Unified CM.

Apply Phone Security Profile with Encrypted TLS on Endpoints

After you create a phone security profile with encrypted TLS, you must associate the profile with the endpoints.

Procedure

Step 1 Create a phone security profile (**System > Security > Phone Security Profile**) with encrypted TLS for endpoints participating in ICE. Ensure that the following settings are configured in the phone security profile:

- **Device Security Mode** is set to *Encrypted*.
- **Transport Type** is set to *TLS*.

Caution If endpoints are not configured with secure mode, ICE Passthrough calls fail even if ICE is configured on the endpoints.

Step 2 Associate the phone security profile with the endpoints participating in ICE.

Step 3 Verify that the endpoints can register over MRA with the phone security profile and make calls.

For more information on how to create and associate phone security profile to the endpoints, see the *Security Guide for Cisco Unified Communications Manager* at: <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

Apply a Common Phone Profile with ICE Configuration on Endpoints

After you create a common phone profile with the configuration required for ICE Passthrough, you must associate the profile with the endpoints.

Procedure

Step 1 Create a common phone profile (**Device > Device Settings > Common Phone Profile > Standard Common Phone Profile**) with the following ICE configuration under **Interactive Connectivity Establishment (ICE)**:

- **ICE:** Choose *Enabled* so that endpoints can support ICE calls.
- **Default candidate type:** Choose *Host*. The host address is signaled in the initial endpoint Session Description Protocol (SDP) offer or answer.

Note For ICE for MRA calls, we do not support *Relay* as a default candidate type.
- **Server Reflexive Address:** Choose *Enabled* so that the endpoints include server reflexive candidates in the initial SDP offer or answer.
- **Primary TURN Server Host Name or IP Address:** Enter the FQDN of the first Cisco Expressway-E node in the MRA Cisco Expressway cluster.
- **Secondary TURN Server Host Name or IP Address:** Enter the FQDN of the second Cisco Expressway-E node in the MRA Cisco Expressway cluster.

Note Endpoints currently ignore the secondary TURN server.
- **TURN Server Transport Type:** Choose *Auto*.
- **TURN Server Username:** Enter the user ID configured on the Cisco Expressway-E TURN server.
- **TURN Server Password:** Enter the password configured on the Cisco Expressway-E TURN server.

Step 2 Go to **Device > Phone** and associate the endpoints with the common phone profile. Currently, you must manually configure the ICE on the endpoints running Collaboration Edge (CE) software.

Set Up Cisco Expressway-C for ICE Passthrough Workflow

The following workflow summarize the configuration required on Cisco Expressway-C.

Procedure

	Command or Action	Purpose
Step 1	Install Server Certificates, on page 94	Generate a new CSR and install appropriate server certificates and trusted CA certificates on Cisco Expressway-C.
Step 2	Change CEtcp Neighbor Zones to CETls Neighbor Zones, on page 94	Change the existing CEtcp neighbor zone to CETls neighbor zones.
Step 3	Set Up the UC Traversal Zone for ICE Passthrough Support, on page 95	Set up the UC Traversal Zone.

	Command or Action	Purpose
Step 4	Set Up the UC Neighbor Zone for ICE Passthrough Support, on page 95	Set up the UC Neighbor Zone.
Step 5	Use CLI to Configure ICE Passthrough on Cisco Expressway Zones, on page 95	Configure ICE Passthrough on the Unified Communication traversal zone and CEtlS neighbor zone.

Install Server Certificates

This procedure describes how to install server certificates.

Procedure

-
- Step 1** Generate a new CSR for the server certificate (**Maintenance > Security > Server Certificate**).
For more information, see the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway configuration guides page](#).
- Step 2** While generating the CSR, include the name of the phone security profile that you have associated with the endpoints in the Subject Alternate Names (SAN).
For more information, see [Server Certificate Requirements for Unified Communications Manager, on page 37](#).
- Step 3** Install the server certificate that is signed from the trusted certificate authority on Cisco Expressway-C.
This certificate allows the endpoints using the phone security profile to register over the TLS connection between Cisco Expressway-C and Unified CM.
-

Change CEtcp Neighbor Zones to CEtlS Neighbor Zones

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

Before you begin

Ensure that Unified CM is in Secure mode.

Procedure

-
- Step 1** Go to **Configuration > Unified Communications > Unified CM servers**.
- Step 2** Select the Unified CM Servers that you already discovered, and click **Refresh Servers** to update the configuration.
- Step 3** Verify that the Unified CM status shows *TLS: Active*.

If there is not already a CEtcp neighbor zone created for MRA, discover new Unified CM servers (**Configuration > Unified Communications > Unified CM servers**). For more information, see [Discover Unified Communications Servers and Services for Mobile and Remote Access, on page 45](#).

Cisco Expressway-C automatically generates non-configurable CEtIs neighbor zones between itself and each discovered Unified CM node if Unified CM68 node cluster is in Secure mode. For more information, see [Automatically Generated Zones and Search Rules, on page 49](#).

Set Up the UC Traversal Zone for ICE Passthrough Support

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

Procedure

- Step 1** In Cisco Expressway-C, go to **Configuration > Zones > Zones**.
- Step 2** Choose the Unified Communications traversal zone to Cisco Expressway-E.
- Step 3** In the SIP pane, set **ICE Passthrough support** to *On* and **ICE Support** to *Off*.

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

Set Up the UC Neighbor Zone for ICE Passthrough Support

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

Procedure

- Step 1** In Cisco Expressway-C, go to **Configuration > Unified Communications > Unified CM Servers**.
 - Step 2** Choose a server.
 - Step 3** In the Unified CM server lookup pane, set **ICE Passthrough support** to *On*.
-

Use CLI to Configure ICE Passthrough on Cisco Expressway Zones

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

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

Procedure

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

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

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

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

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

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

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

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

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

Set Up Cisco Expressway-E as TURN Server

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

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

Procedure

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

- **TURN services:** Set to *On*.
- **TCP 443 TURN service:** Set to *Off*.
- **TURN port multiplexing:** Set to *Off*. This option is available only on Large system.
- **TURN requests port:** Retain the default values. On Small and Medium systems, the default port is 3478. On Large systems, the default port range is 3478 to 3483.

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

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

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

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

- **Authentication realm:** Retain the default value. The default value is TANDBERG.
- **Media port range start:** Retain the default value. The default value is 24000.
- **Media port range end:** Retain the default value. The default value is 29999.

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

Step 3 Click **Save**.

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

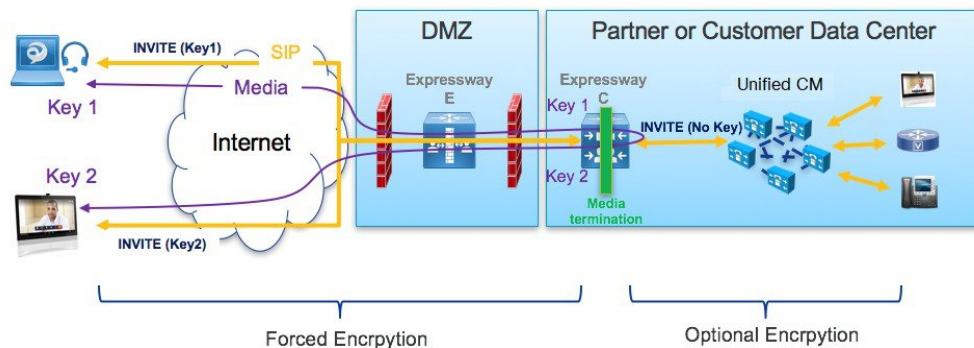
For more information on the steps to configure TURN services on Cisco Expressway-E, see *Configuring TURN Services* section in the *Cisco Expressway Administrator Guide* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

Signaling Path Encryption Between Expressway-C and Unified CM

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

The following figure shows the encryption without ICE Passthrough where encryption is forced between MRA endpoints and Expressway-C, and optional in the internal network. On an MRA call, a different encryption key is exchanged on each leg (Key 1 and Key 2), and the Expressway-C decrypts and re-encrypts the media between the 2 legs. The invite to Unified CM does not need a key if the internal leg is not encrypted.

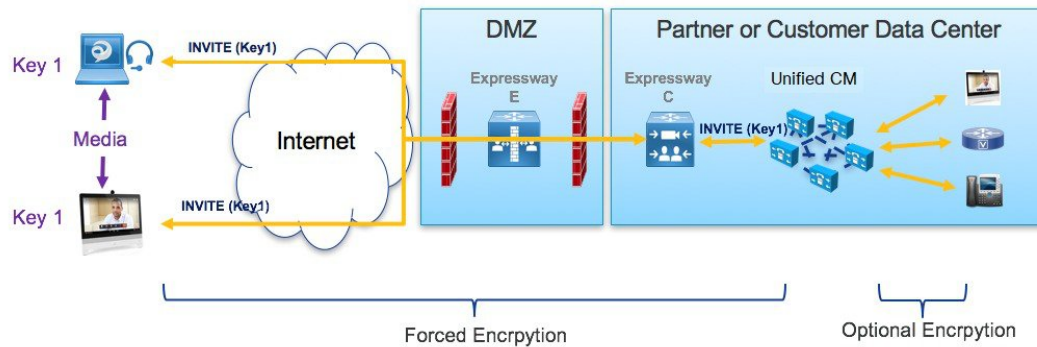
Figure 29: Encryption without ICE Passthrough



However, with ICE passthrough mode, the endpoints must be able to exchange their crypto keys end-to-end because the media packets are sent to each other directly and not through the Expressway-C. Whenever crypto keys are included in a SIP message, the message must be sent over TLS to protect the key. Because the SIP signaling path must be encrypted end-to-end to send the crypto keys end-to-end, the internal leg between the Expressway-C and Unified CM must be encrypted. If the signaling path is unencrypted, the crypto keys are dropped during call setup.

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

Figure 30: Encryption with ICS Passthrough



ICE Passthrough Metrics Use



















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

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

View ICE Passthrough Metrics in Expressway-C

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

Figure 31: Metrics Example

ICE Passthrough metrics	
Metrics	
Peer 	127.0.0.1
Start time 	2018-10-22 20:43:45
End time 	2018-10-23 20:43:45
B2BUA connected calls 	4
Calls with optimized ICE media paths 	2
% of calls with optimized ICE media paths 	50%
Call types	
Host to host 	100%
Host to server reflexive 	0%
Host to relay 	0%
Server reflexive to server reflexive 	0%
Server reflexive to relay 	0%
Relay to relay 	0%
Advanced	
Calls with required Expressway ICE configuration 	100%
Calls attempted with offered ICE candidates 	100%
Calls with ICE candidates offered by one endpoint 	0%
Calls without ICE candidates 	0%
Calls with non-optimized media paths 	50%
Calls with ICE candidates offered but without required Expressway ICE configuration 	0%

- The **Peer** field shows the IP address or hostname of each node.
- The most recent 24-hour interval of data is shown.
- Each peer address is a link that takes you to the history for that node.
- The interval start time reflects the time of day of the most recent server restart.
- Each column shows information for a separate cluster.

Procedure

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

The page is organized into these sections:

- **Metrics:** For each peer, the time interval for which metrics are shown. For this interval, the number of B2BUA connected calls, the number of ICE calls, and the percentage of ICE vs total B2BUA calls. N/A values result when no ICE calls were processed during this 24-hour interval.
- **Call types:** For each call type, the percentage of placed ICE calls with each call type.
- **Advanced:** Other metrics that can help with troubleshooting.

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

- Step 3** To sort, click a column name and then the **Up** or **Down** arrow, to sort the data by that column.
- Step 4** Click **Export to CSV** to create a spreadsheet of the values on the page you are displaying.
- Step 5** Click the IP address or hostname for a cluster to display the **ICE Call Metrics History** page, which shows a history of values for that cluster.
- Each column shows a separate parameter.
 - Each row shows the values for a different interval, with the most recent shown first.
 - Each value is a raw value, not a percentage.
 - The page can display up to 60 records (that is, the 60 most recent 24-hour intervals).

Metric Collection with the collectd Daemon

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

View Call Types in the Call History

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

Procedure

- Step 1** In Cisco Expressway-C, navigate to **Status > Calls > History**.
- Step 2** Choose one of the following actions.
- Click the value in the **Start time** column to view the call detail record (CDR).
 - Choose **View** in the **Actions** column.
- Step 3** Examine the value in the **ICE Passthrough call type** field.
- Possible values are:
- *none*: Indicates optimized media path was not used for the call. The call is processed and connected using Cisco Expressway B2BUA.
 - *host_to_host*: Indicates optimized media path for the call was established using the host addresses of the endpoints.
 - *host_to_srvrflx*: Indicates optimized media path for the call was established between the host address of one of the endpoints and the server-reflexive address of the other endpoint.
 - *host_to_relay*: Indicates optimized media path for the call was established between the host address of one of the endpoints and the TURN relay address of the other endpoint.
 - *srvrflx_to_srvrflx*: Indicates optimized media path for the call was established using the server-reflexive addresses of the endpoints.

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

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

Bandwidth Manipulation

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



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



CHAPTER 14

Troubleshooting

- [General Techniques](#), on page 103
- [Cisco Expressway Certificate and TLS Connectivity Issues](#), on page 108
- [Cisco Jabber Sign In Issues](#), on page 109
- [Cisco Expressway Returns “401 Unauthorized” Failure Messages](#), on page 111
- [Call Failures due to “407 Proxy Authentication Required” or “500 Internal Server Error” Errors](#), on page 111
- [Call Bit Rate is Restricted to 384 kbps or Video Issues when Using BFCP \(Presentation Sharing\)](#), on page 112
- [Endpoints Can't Register to Unified CM](#), on page 112
- [IM and Presence Service Realm Changes](#), on page 112
- [No Voicemail Service \(“403 Forbidden” Response\)](#), on page 112
- [“403 Forbidden” Responses for Any Service Requests](#), on page 113
- [Client HTTPS Requests are Dropped by Cisco Expressway](#), on page 113
- [Failed: Address is not a IM and Presence Server](#), on page 113
- [Invalid SAML Assertions](#), on page 113
- [“502 Next Hop Connection Failed” Messages](#), on page 113
- [MRA calls fail if the called endpoint is more than 15 hops away from the Expressway-E](#), on page 114

General Techniques

Alarms and Status Messages

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

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

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

- Server or CA certificates
- DNS configuration

- Domain configuration

Use the Collaboration Solutions Analyzer

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

Procedure

- Step 1** Use the CollabEdge **validator tool** to validate your MRA deployment.
It simulates a Jabber client sign in process, and provides feedback on the result.
- Step 2** If the CollabEdge validator cannot identify the issue, we suggest that you collect logs from the Cisco Expressway while attempting to sign in. Then use the **log analysis** component in the CSA to analyze the logs.
-

Diagnostic Logs

Jabber for Windows Diagnostic Logs

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

Configure Cisco Expressway Diagnostic Log Levels

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

Before you begin

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

Procedure

- Step 1** Go to **Maintenance > Diagnostics > Advanced > Support Log configuration**.
- Step 2** Select the following logs:
- `developer.edgeconfigprovisioning`
 - `developer.trafficserver`
 - `developer.xcp`

Step 3 Click **Set to debug**.

Create a Diagnostic Log Capture

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

Procedure

- Step 1** Go to **Maintenance > Diagnostics > Diagnostic logging**.
- Step 2** (Optional) Select **Take tcpdump while logging**.
- Step 3** Click **Start new log**.
- Step 4** (Optional) Enter some **Marker** text and click **Add marker**.
- The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
 - You can add as many markers as required, at any time while the diagnostic logging is in progress.
 - Marker text is added to the log with a "**DEBUG_MARKER**" tag.
- Step 5** Reproduce the system issue you want to trace in the diagnostic log.
- Step 6** Click **Stop logging**.
- Step 7** Click **Collect log**.
- Step 8** When the log collection completes, click **Download log** to save the diagnostic log archive to your local file system.
- You are prompted to save the archive (the exact wording depends on your browser).
-

After You Create Logs

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

After you have completed your diagnostic logging, return to the **Support Log configuration** page and reset the modified logging modules back to *INFO* level.

Check DNS Records

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

Procedure

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

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

Note Performing the DNS lookup from the Cisco Expressway-C returns the view from within the enterprise, and that performing it on the Cisco Expressway-E returns what is visible from within the DMZ which is not necessarily the same set of records available to endpoints in the public internet.

The DNS lookup includes the following SRV services that are used for Unified Communications:

- `_collab-edge._tls`
- `_cisco-uds._tcp`

Check that the Cisco Expressway-E is Reachable

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

Procedure

Ensure that the FQDN of the Cisco Expressway-E is resolvable in the public DNS.

The FQDN is configured at **System > DNS** and is built as `<System host name>.<Domain name>`.

Check Call Status

Call status information can be displayed for both current and completed calls.

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

If the Cisco Expressway is part of a cluster, all calls that apply to any peer in the cluster are shown, although the list is limited to the most recent 500 calls per peer.

Procedure

Step 1 If you wish to get information about the current calls, go to the **Call status** page (**Status > Calls > Calls**).

The **Call status** page lists all the calls currently taking place to or from devices registered with the Cisco Expressway, or that are passing through the Cisco Expressway.

Step 2 If you wish to get information about the completed calls, go to the **Call history** page (**Status > Calls > History**).

The **Call history** page lists all the calls that are no longer active. The list is limited to the most recent 500 calls, and only includes calls that have taken place since the Cisco Expressway was last restarted.

Mobile and Remote Access Call Identification

The call status and call history pages show all call types—Unified CM remote sessions (if Mobile and Remote Access is enabled) as well as Cisco Expressway RMS sessions.

To distinguish between the call types, you must drill down into the call components. Mobile and Remote Access calls have different component characteristics depending on whether the call is being viewed on the Cisco Expressway-C or Cisco Expressway-E:

- On the Cisco Expressway-C, a Unified CM remote session has three components (as it uses the B2BUA to enforce media encryption). One of the Cisco Expressway components routes the call through one of the automatically generated neighbor zones (with a name prefixed by either **CEtcp** or **CEtls**) between Cisco Expressway and Unified CM.
- On the Cisco Expressway-E, there is one component and that routes the call through the **CollaborationEdgeZone**.

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

Rich Media Sessions (Cisco Expressway Only)

If your system has a rich media session key installed and thus supports business-to-business calls, and interworked or gatewayed calls to third-party solutions and so on, those calls are also listed on the call status and call history pages.

Devices Registered to Unified CM via Cisco Expressway

Identify Devices in Unified CM

This procedure describes how to identify devices registered to Unified CM via Cisco Expressway.

Procedure

Step 1 In Unified CM, go to **Device > Phone** and click **Find**.

Step 2 Check the **IP Address** column.

Devices that are registered via Cisco Expressway will display the IP Address of the Cisco Expressway-C it is registered through.

Identify Provisioning Sessions in Cisco Expressway-C

This procedure describes how to identify sessions that have been provisioned via Cisco Expressway-C.

Procedure

Step 1 In Cisco Expressway-C, go to **Status > Unified Communications**.

Step 2 In the **Advanced status information** section, click **View provisioning sessions**.

This shows a list of all current and recent (shown in red) provisioning sessions.

Ensure that Cisco Expressway-C is Synchronized to Unified CM

Changes to Unified CM cluster or node configuration can lead to communication problems between Unified CM and Cisco Expressway-C. This includes changes to the following items:

- Number of nodes within a Unified CM cluster
- Host name or IP address of an existing node
- Listening port numbers
- Security parameters
- Phone security profiles

You must ensure that any such changes are reflected in the Cisco Expressway-C. To do this:

Procedure

- Step 1** On Cisco Expressway, go to **Configuration > Unified Communications**.
- Step 2** Rediscover all Unified CM and IM and Presence Service nodes.
-

Check MRA Authentication Status and Tokens

This procedure describes how to check MRA authentication status and tokens.

Procedure

- Step 1** (Optional) To check and clear standard (non-refresh) OAuth user tokens, go to **Users > View and manage OAuth without refresh token holders >** .
- This could help identify problems with a particular user's OAuth access.
- Step 2** (Optional) To check statistics for MRA authentication, go to **Status > Unified Communications > View detailed MRA authentication statistics**.

Any unexpected requests or responses on this page could help identify configuration or authorization issues.

Cisco Expressway Certificate and TLS Connectivity Issues

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

If you are using secure profiles, ensure that the root CA of the authority that signed the Cisco Expressway-C certificate is installed as a CallManager-trust certificate (**Security > Certificate Management** in the **Cisco Unified OS Administration** application).

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

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

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

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

You must either upgrade your infrastructure or consult the Cisco Technical Assistance Center to check whether it is possible to modify the default configurations for Unified CM and/or Unified CM IM and Presence Service to support TLS (refer [CSCuy59366](#)).

Cisco Jabber Sign In Issues

Jabber Triggers Automated Intrusion Protection

Conditions

- Your MRA solution is configured for authorization by OAuth token (with or without refresh)
- The Jabber user's access token has expired
- Jabber does one of these:
 - Resumes from desktop hibernate
 - Recovers network connection
 - Attempts fast login after it has been signed out for several hours

Behavior

- Some Jabber modules attempt to authorize at Cisco Expressway-E using the expired access token.
- The Cisco Expressway-E (correctly) denies these requests.
- If there are more than 5 such requests from a particular Jabber client, the Cisco Expressway-E blocks that IP address for ten minutes (by default).

Symptoms

The affected Jabber clients' IP addresses are added to the Cisco Expressway-E's **Blocked addresses** list, in the *HTTP proxy authorization failure* category. You can see these on **System > Protection > Automated detection > Blocked addresses**.

Workaround

There are two ways you can work around this issue; you can increase the detection threshold for that particular category, or you can create exemptions for the affected clients. We describe the threshold option here because the exemptions may well be impractical in your environment.

1. Go to **System > Protection > Automated detection > Configuration**.
2. Click **HTTP proxy authorization failure**.
3. Change the **Trigger level** from *5* to *10*. 10 should be enough to tolerate the Jabber modules that present expired tokens.
4. Save the configuration, which takes effect immediately.
5. Unblock any affected clients.

Jabber Popup Warns About Invalid Certificate When Connecting from Outside the Network

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

This is expected behavior from Jabber. We recommend that you install a certificate issued by a CA that Jabber trusts, and that the certificate has the domains Jabber is using included in its list of SANs. See [Server Certificate Requirements for Unified Communications Manager, on page 37](#).

Jabber Doesn't Register for Phone Services

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

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

Users can recover from this issue by signing out and resetting Jabber. See [CSCux16696](#).

Jabber Cannot Sign In Due to XMPP Bind Failure

The Jabber client may be unable to sign in ("Cannot communicate with the server" error messages) due to XMPP bind failures.

This will be indicated by resource bind errors in the Jabber client logs, for example:

```
XmppSDK.dll #0, 201, Recv:<iq id='uid:527a7fe7:00000cfe:00000000' type='error'><bind
xmlns='urn:ietf:params:xml:ns:xmpp-bind'><error code='409' type='cancel'><conflict
xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'></error></iq>
```

```
XmppSDK.dll #0, CXmppClient::onResourceBindError
```

```
XmppSDK.dll #0, 39, CTriClient::HandleDisconnect, reason:16
```

This typically occurs if the IM and Presence Intercluster Sync Agent is not working correctly. See IM and Presence information in the *Cisco Unified Communications Manager Configuration Guides* at

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>.

Jabber Cannot Sign In Due to SSH Tunnels Failure

Jabber can fail to sign in due to the SSH tunnels failing to be established. The traversal zone between the Cisco Expressway-C and Cisco Expressway-E will work normally in all other respects. Cisco Expressway will report 'Application failed - An unexpected software error was detected in portforwarding.pyc'.

This can occur if the Cisco Expressway-E DNS hostname contains underscore characters. Go to **System > DNS** and ensure that the **System host name** only contains letters, digits and hyphens.

Jabber Cannot Signin When Connecting to Different Peers in a Cluster of Cisco Expressway-Es

Jabber sign in failures have been seen when there is inconsistency of the DNS domain name between Cisco Expressway-E peers. The domain names must be identical, even with respect to case, on all peers in the cluster.

Go to **System > DNS** on each peer to make sure that Domain name is identical on all peers.

Cisco Expressway Returns “401 Unauthorized” Failure Messages

A “401 Unauthorized” failure message can occur when the Cisco Expressway attempts to authenticate the credentials presented by the endpoint client. The reasons for this include:

- The client is supplying an unknown username or the wrong password.
- Intercluster Lookup Service (ILS) has not been set up on all of the Unified CM clusters. This may result in intermittent failures, depending upon which Unified CM node is being used by Cisco Expressway for its UDS query to discover the client's home cluster.

Call Failures due to “407 Proxy Authentication Required” or “500 Internal Server Error” Errors

Call failures can occur if the traversal zones on Cisco Expressway are configured with an **Authentication policy** of *Check credentials*. Ensure that the **Authentication policy** on the traversal zones used for Mobile and Remote Access is set to *Do not check credentials*.

Call Bit Rate is Restricted to 384 kbps or Video Issues when Using BFCP (Presentation Sharing)

This can be caused by video bit rate restrictions within the regions configured on Unified CM.

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

Endpoints Can't Register to Unified CM

Endpoints may fail to register for various reasons:

- Endpoints may not be able to register to Unified CM if there is also a SIP trunk configured between Unified CM and Cisco Expressway-C. If a SIP trunk is configured, you must ensure that it uses a different listening port on Unified CM from that used for SIP line registrations to Unified CM. See [SIP Trunks Between Unified CM and Expressway-C, on page 79](#) for more information.
- Secure registrations may fail ('Failed to establish SSL connection' messages) if the server certificate on the Cisco Expressway-C does not contain in its Subject Alternate Name list, the names of all of the Phone Security Profiles in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Note that these names — in both Unified CM and in the Cisco Expressway's certificate — must be in FQDN format.

IM and Presence Service Realm Changes

Provisioning failures can occur when the IM and Presence Service realm has changed and the realm data on the Cisco Expressway-C has not been updated.

For example, this could happen if the address of an IM and Presence Service node has changed, or if a new peer has been added to an IM and Presence Service cluster.

The diagnostic log may contain an INFO message like "Failed to query auth component for SASL mechanisms" because the Cisco Expressway-C cannot find the realm.

Go to **Configuration > Unified Communications > IM and Presence Service nodes** and click **Refresh servers** and then save the updated configuration. If the provisioning failures persist, verify the IM and Presence Service nodes configuration and refresh again.

No Voicemail Service ("403 Forbidden" Response)

Ensure that the Cisco Unity Connection (CUC) hostname is included on the HTTP server allow list on the Cisco Expressway-C.

"403 Forbidden" Responses for Any Service Requests

Services may fail ("403 Forbidden" responses) if the Cisco Expressway-C and Cisco Expressway-E are not synchronized to a reliable NTP server. Ensure that all Cisco Expressway systems are synchronized to a reliable NTP service.

Client HTTPS Requests are Dropped by Cisco Expressway

This can be caused by the automated intrusion protection feature on the Cisco Expressway-E if it detects repeated invalid attempts (404 errors) from a client IP address to access resources through the HTTP proxy.

To prevent the client address from being blocked, ensure that the **HTTP proxy resource access failure** category (**System > Protection > Automated detection > Configuration**) is disabled.

Failed: Address is not a IM and Presence Server

This error can occur when trying to configure the IM and Presence Service servers used for remote access (via **Configuration > Unified Communications > IM and Presence servers**). It is due to missing CA certificates on the IM and Presence Service servers and applies to systems running 9.1.1. More information and the recommended solution is described in [CSCul05131](#).

Invalid SAML Assertions

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

Check the logs for `Invalid SAML Response`.

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

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

"502 Next Hop Connection Failed" Messages

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

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

MRA calls fail if the called endpoint is more than 15 hops away from the Expressway-E

The Unified Communications traversal zone has a default hop count of 15. If you suspect this is a contributing factor, sign in to all your MRA Expressways, raise the hop count to a significantly larger number, e.g. 70, and test.



APPENDIX **A**

Allow List Formats

- [Allow List Rules File Reference](#), on page 115
- [Allow List Tests File Reference](#), on page 116

Allow List Rules File Reference

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

Table 11: Allow List Rule Arguments

Argument index	Parameter name	Required/Optional	Sample value
0	Url	Required	<code>protocol://host[:port][/path]</code> where <ul style="list-style-type: none"> • protocol is http or https • host may be a DNS name or IP address • :port is optional, and may only be : followed by one number in the range 0-65535, for example: 8443 • /path is optional and must conform to HTTP specification
1	Deployment	Optional	Name of the deployment that uses this rule. Required when you have more than one deployment, otherwise supply an empty argument.
2		Optional	Comma-delimited list of HTTP methods, optionally in double-quotes, for example: " GET , PUT "
3		Optional	exact or prefix . Default is prefix .
4		Optional	Text description of the rule. Enclose with double quotes if there are spaces.

Example List Rules CSV File

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

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

Allow List Tests File Reference

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

Table 12: Allow List Test Arguments

Argument index	Parameter name	Required/Optional	Sample value
0	Url	Required	protocol://host[:port] [/path] Where: <ul style="list-style-type: none"> • protocol is http or https • host may be a DNS name or IP address • :port is optional, and may only be : followed by one number in the range 0-65535 • /path is optional and must conform to HTTP specification
1	ExpectedResult	Required	allow or block . Specifies whether the test expects that the rules should allow or block the specified URL.
2	Deployment	Optional	Name of the deployment to test with this URL. If you omit this argument, the test will use the default deployment.
3	Description	Optional	Text description of the rule. Enclose with double quotes if there are spaces.
4	HttpMethod	Optional	Specify one HTTP method to test for example, PUT . Defaults to GET if not supplied.

Example List Tests CSV File

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

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

