



Cisco Expressway SIP Trunk to Unified CM

Deployment Guide

First Published: December 2013

Last Updated: September 2019

Cisco Expressway X8.8

Unified CM 8.6.x, 9.x, 10.x, 11.x

Contents

Preface	5
Change History	5
Introduction	5
Deployment Scenario	5
Configuring Unified CM for an Expressway Trunk	7
Prerequisites	7
Configuration Summary	7
Configuring the SIP Profile for Expressway	7
Configuring the Region with an Appropriate Session Bit Rate for Video Calls	10
Configuring the SIP Profile for Phone Devices	10
Adding a Phone Device	10
Configuring the Device Directory Number	10
Configuring the SIP Trunk Security Profile	11
Configuring the SIP Trunk Device	11
Configuring the Cluster Fully Qualified Domain Name	13
Allowing Numeric Dialing from Cisco Phones to Expressway	14
Allowing Dialing to Expressway Domain from Cisco Phones	15
Checking the Message Size Limit on Unified CM	15
Configuring Expressway Routing	17
Prerequisites	17
Configuration Summary	17
Ensuring a Consistent URI Format	17
Creating a Neighbor Zone for Unified CM	18
Creating a Search Rule to Route Calls to the Unified CM Neighbor Zone	20
Creating a Transform that Converts number@<IP address of cucm> to number@exp.domain	21
Creating a Transform to Convert other Unified CM-supplied Domain Variants to number@exp.domain	22
Connecting Expressway to Unified CM Using TLS	25
Before you Begin	25
Process Summary	25
Ensure Certificate Trust Between Unified CM and Expressway	25
Set the Cluster Security Mode to Mixed Mode	27

Configure a SIP Trunk Security Profile on Unified CM	28
Update Unified CM Trunk to Expressway to Use TLS	28
Update Device Profiles to Encrypt Calls to Unified CM-registered Endpoints	29
Update Expressway Neighbor Zone to Unified CM to Use TLS	29
Verify That the TLS Connection is Operational	29
Appendix 1: Troubleshooting	31
Problems Connecting Expressway-C Local Calls	31
Check for Errors	32
Tracing Calls	32
Call Failures with Cisco TelePresence Server	32
In-call Problems	32
Taking a Trace on Unified CM Using RTMT	32
Call Failures	34
Appendix 2: Connecting Unified CM to an Expressway Cluster	35
Configuring the Trunk to Expressway to Specify the DNS SRV Address for the Expressway Cluster	35
Configuring the Trunk to Expressway to Specify a List of Expressway Peers	35
Appendix 3: Connecting Expressway to a Cluster of Unified CM Nodes	37
Option 1: Using a Single Neighbor Zone	37
Option 2: Using a DNS Zone	37
Appendix 4: Additional Information	41
IP Address Dialing	41
Characters Allowed in SIP URIs	41
Cisco Legal Information	41
Cisco Trademark	42

Preface

Change History

Table 1 Deployment Guide Change History

Date	Change	Reason
September 2019	Added advice not to configure multiple SIP trunks/neighbor zones with the same port (the UI does allow this but it is not recommended).	Clarification
August 2018	Clarified limitation on multiple TLS-enabled SIP trunks between the same Unified CM node and Expressway-C node.	Clarification
June 2016	Updated for X8.8.	X8.8 release
November 2015	New template applied. Version numbers updated. Republished for X8.7.	X8.7 release
July 2015	Updated for X8.6.	
April 2015	Updated for X8.5.2. Link to new IP address dialing article.	
December 2014	Updated for X8.5. IP address dialing information modified.	
June 2014	Republished for X8.2.	
December 2013	Initial release.	

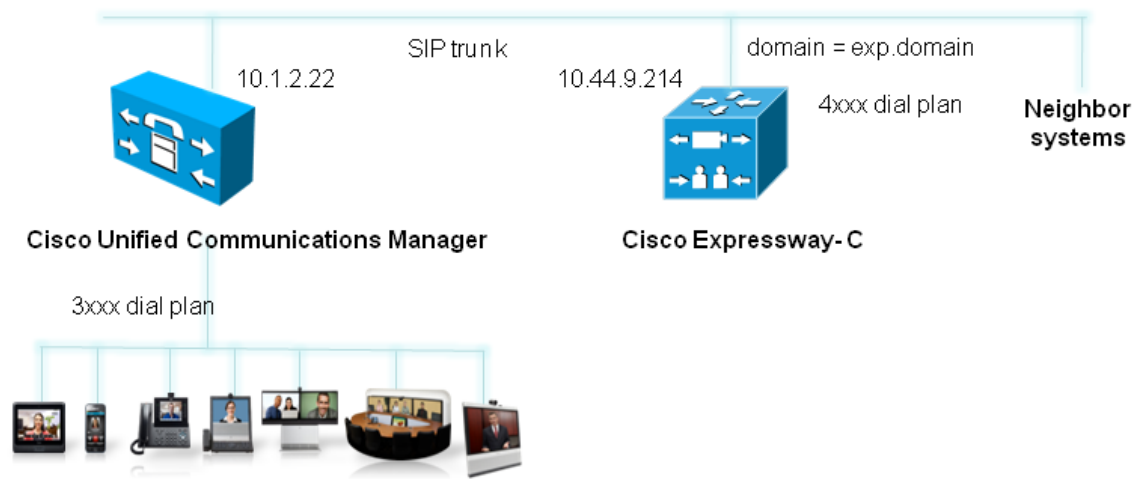
Introduction

This deployment guide provides guidelines on how to configure the Cisco Expressway (Expressway) version X8.8 and Cisco Unified Communications Manager (Unified CM) versions 8.6.x and later to interwork via a SIP trunk.

Deployment Scenario

A company already has Unified CM running their telephone/video system. They want to integrate this via a SIP trunk to an Expressway-C to provide further services such as integration with Jabber Guest servers or another Expressway managing integration to Microsoft Lync.

Introduction



For the purposes of this example, the existing Unified CM system uses telephone (digit-only) numbers to specify who to call:

- Endpoints connected to the Unified CM are identified by 3xxx extension numbers.
- Endpoints and systems that are contacted via the Expressway-C are identified by 4xxx extension numbers.

Note that more complicated dial plans can also be supported, including alphanumeric dialing; they would require additional transforms/routing configuration.

Unified CM and the Expressway-C are connected together using a SIP trunk across an IP network; the Expressway-C domain is exp.domain. Calls sent to Unified CM will have the domain portion set to the Expressway domain; calls from Unified CM to Expressway will arrive with the domain portion set as <FQDN of Expressway>:5060 for TCP and <FQDN of Expressway>:5061 for TLS.

This guide specifies how to configure both the Unified CM and the Expressway-C so that SIP calls can be routed between each system. It does not describe how to configure the onward routing, such as additional neighbor zones from the Expressway to other systems (such as another Expressway, Jabber Guest servers or a Cisco VCS).

Initially the configuration use non-secure TCP connections, as this allows for easier troubleshooting. It then describes how to secure the video network over TLS.

Configuring Unified CM for an Expressway Trunk

Prerequisites

Ensure that Unified CM contains a basic configuration and has already set up at least:

- System > Server
- System > Cisco Unified CM
- System > Cisco Unified CM Group
- System > Date / Time Group
- System > Presence Group
- System > Region Information
- System > Device Pool
- System > DHCP
- System > Location
- System > Physical location
- System > Enterprise parameters
- System > Licensing

Configuration Summary

The configuration on Unified CM contains the following tasks:

- Configuring the SIP Profile for Expressway (already exists if using version 9.x)
- Configuring the region with an appropriate session bit rate for video calls
- Configuring a SIP Profile for phone devices
- Adding a phone device: add the new phone device to the list of supported endpoints on Unified CM
- Configuring the device directory number: specify the telephone number that will cause this phone to ring
- Configuring the SIP Trunk security profile
- Configuring the SIP Trunk device
- Configuring the Cluster Fully Qualified Domain Name
- Allowing numeric dialing from Cisco phones to Expressway
- Allowing dialing to Expressway domain from Cisco phones
- Checking the message size limit on Unified CM

These tasks are explained in detail below.

Configuring the SIP Profile for Expressway

Note: This procedure does not apply to Unified CM versions 9.x and later, because the newer versions have a "Standard SIP Profile For Cisco VCS" (you can also use that profile for Expressway).

1. On Unified CM, go to **Device > Device Settings > SIP Profile**.

Configuring Unified CM for an Expressway Trunk

2. Click **Copy** against the **Standard SIP Profile**.

Find SIP Profile where Name ▼ begins with ▼ Find Clear Filter + −			
<input type="checkbox"/>	Name ▲	Description	Copy
	Standard SIP Profile	Default SIP Profile	

Configuring Unified CM for an Expressway Trunk

3. Configure the fields as follows (leave other fields as default values):

Name	"Standard SIP Profile For Cisco VCS" (the profile is named "for Cisco VCS" for consistency with other Unified CM versions)
Default MTP Telephony Event Payload Type	101
Redirect by Application	Select the check box
Use Fully Qualified Domain in SIP Requests	Select the check box
Allow Presentation Sharing using BFCP	Select the check box (in Unified CM 8.6.1 or later)
Timer Invite Expires	180
Timer Register Delta	5
Timer Register Expires	3600
Timer T1	500
Timer T2	Leave as default (typically 4000 or 5000)
Retry INVITE	6
Retry non-INVITE	10
Start Media Port	16384
Stop Media Port	32766
Call Pickup URI	x-cisco-serviceuri-pickup
Call Pickup Group Other URI	x-cisco-serviceuri-opickup
Call Pickup Group URI	x-cisco-serviceuri-gpickup
Meet Me Service URI	x-cisco-serviceuri-meetme
Timer Keep Alive Expires	120
Timer Subscribe Expires	120
Timer Subscribe Delta	5
Maximum Redirections	70
Off Hook To First Digit Timer	15000
Call Forward URI	x-cisco-serviceuri-cfwdall
Abbreviated Dial URI	x-cisco-serviceuri-abbrdial
Reroute Incoming Request to new Trunk based on	Never

4. Click **Save**.

Configuring the Region with an Appropriate Session Bit Rate for Video Calls

Ensure that your regions have an appropriate session bit rate for video calls:

1. Go to **System > Region Information > Region**.
2. Select the region (for example the **Default** region).
3. Set **Maximum Session Bit Rate for Video Calls** to a suitable upper limit for your system, for example 6000 kbps.
4. Click **Save** and then click **Apply Config**.

Configuring the SIP Profile for Phone Devices

This creates the SIP Profile that is to be applied to all phone devices.

1. On Unified CM, go to **Device > Device Settings > SIP Profile**.
2. Click **Copy** against the **Standard SIP Profile**.
3. Configure the following fields, leaving everything else as its default value:

Name	Standard SIP Profile – for phone devices
Use Fully Qualified Domain in SIP Requests	Select the check box
Allow Presentation Sharing using BFCP	Select the check box if BFCP (Dual video / presentation sharing) is required.

4. Click **Save**.

Adding a Phone Device

1. Go to **Device > Phone**.
2. Click **Add New**.
3. Select a **SIP Profile** of *Standard SIP Profile – for phone devices*.
4. Configure the other fields as required.
5. Click **Save** and click **OK**.
6. Click **Apply Config** and click **OK**.

Alternatively, if there is already another phone configured, copy its configuration by selecting “super copy”, entering the new phone’s MAC address and then changing the description (especially correct the MAC address part of the description).

Configuring the Device Directory Number

1. Go to **Device > Phone**.
2. Select the relevant device name.
3. On the left hand side, select a line.
4. Set up the required directory number (for this example use a 3xxx number).

Configuring the SIP Trunk Security Profile

1. Go to **System > Security > SIP Trunk Security Profile**.
2. (Before version 9.x) Click **Add New** and name the new profile.
3. (9.x onwards) Select **Non Secure SIP Trunk Profile**.
4. Configure the fields as follows:

Name	Non Secure SIP Trunk Profile
Device Security Mode	Non Secure
Incoming Transport Type	TCP+UDP
Outgoing Transport Type	TCP
Incoming Port	<p>5060</p> <p>If you deploy Mobile and Remote Access (MRA), note that MRA uses ports 5060 and 5061. Do not use these ports for other SIP trunks; use a different port (such as 5070 or 5071). The reason is to avoid potential issues with MRA if Unified CM receives registration requests on what it believes to be a SIP trunk. This applies to TCP or TLS connections.</p> <p>Use a unique port number for each SIP trunk between Unified CM and Expressway. The Expressway user interface does not stop you configuring multiple SIP trunks/neighbor zones to use the same port, but we do not recommend this configuration. In particular it will cause unexpected licensing behavior.</p>
Accept Unsolicited Notification	Select this check box
Accept Replaces Header	Select this check box

5. Click **Save**.

Configuring the SIP Trunk Device

1. On Unified CM, go to **Device > Trunk**.
2. Click **Add New**.
3. Select a **Trunk Type** of *SIP Trunk*.
 - **Device Protocol** displays *SIP*.
 - If asked for a **Trunk Service Type**, select *None (Default)*.
4. Click **Next**.

Configuring Unified CM for an Expressway Trunk

5. Configure the **Device Information** fields as follows:

Device Name	As required, such as Expressway_system
Device Pool	(As set up in System > Device Pool)
Call classification	OnNet
Location	(As set up in System > Location)
Packet Capture Mode	None
Media Termination Point Required	Clear this check box if any video phones registered to Unified CM are to make or receive video calls with endpoints routed via Expressway. Select this check box if audio devices only are registered to Unified CM.
SRTP Allowed	Select this check box. For background, read Secure RTP between CUCM and VCS or Expressway Configuration Example
Run On All Active Unified CM Nodes	Select this check box

6. Configure the **Call Routing Information > Inbound Calls** fields as follows:


Significant digits	All
Connected Line ID Presentation	Default
Connected Name Presentation	Default
Calling Search Space	(As set up in Call Routing > Class of Control > Calling Search Space)
Prefix DN	<blank>
Redirecting Diversion Header Delivery - Inbound	Select this check box

7. Configure the **Call Routing Information > Outbound Calls** fields as follows:

Calling Party Selection	Originator
Calling Line ID Presentation	Default
Calling Name Presentation	Default
Caller ID DN	<blank>
Caller Name	<blank>

Configuring Unified CM for an Expressway Trunk

8. Configure the **SIP Information** fields as follows:

Destination address is an SRV	Select this check box if a domain is specified for the destination address, and the DNS server uses DNS SRV records to direct the domain to a cluster of Expressways. Do not select this check box if an IP address is specified as the Destination address .
Destination address	<FQDN of Expressway / Expressway cluster>. Alternatively you can enter the <IP address of Expressway>. If you are not using SRV records and need to specify multiple peers, click  to add extra Destination address rows.
Destination port	5060 (this displays as zero if you are using SRV records)
Presence Group	Standard Presence Group (or whichever presence group has been configured in System > Presence Group)
SIP Trunk Security Profile	Non Secure SIP Trunk Profile
SIP Profile	Standard SIP Profile for Cisco VCS
DTMF Signaling Method	RFC 2833
Normalization Script	vcs-interop (if available, the vcs-interop script may be used with Expressway) Note: You must apply SIP normalization to any trunk to Expressway, even if the trunk is only used for voice.

9. Click **Save**.
10. Click **Reset**.
11. Click **Reset**.

Configuring the Cluster Fully Qualified Domain Name

Unified CM must be configured with a **Cluster Fully Qualified Domain Name** so that it can receive calls to addresses in the format <address>@domain. (It is also required when Unified CM is clustered so that Expressway can send the call to any Unified CM node.)

- Go to **System > Enterprise parameters**, and find the **Clusterwide Domain Configuration** section.
- Set the **Cluster Fully Qualified Domain Name** to the same domain as the video network, for example exp.domain.

This parameter defines one or more Fully Qualified Domain Names (FQDNs) for this cluster. Multiple FQDNs must be separated by a space. Requests containing URLs (for example, SIP calls) whose host portion matches any of the FQDNs in this parameter will be recognized as a request destined for this cluster and/or devices attached to it.

- Click **Save**.

Clusterwide Domain Configuration	
Organization Top Level Domain	<input type="text"/>
Cluster Fully Qualified Domain Name	<input type="text" value="exp.domain"/>

Allowing Numeric Dialing from Cisco Phones to Expressway

Unified CM can be configured to take a prefix and route calls to a SIP trunk based on a specific prefix. Configure Unified CM to route calls dialed as 4xxx to the Expressway:

1. On Unified CM, go to **Call Routing > Route/Hunt > Route Pattern**.
2. Click **Add New**.
3. Configure a Route Pattern to route calls dialed 4xxx to the Expressway trunk (no change to dialed number).

Pattern Definitions	
Route Pattern	4XXX
Route Partition	(As set up in System > Device Pool)
Description	As required, for example "Route 4 xxx to Expressway SIP trunk"
Gateway/Route List	Required Trunk to route calls to the Expressway-C
Call Classification	<i>OnNet</i>
Provide Outside Dial Tone	Not selected
Called Party Transformations	
Discard Digits	< None >

Pattern Definition

Route Pattern* 4XXX
Route Partition LABCM6
Description Route 4 xxx to Expressway
Numbering Plan -- Not Selected --
Route Filter < None >
MLPP Precedence* Default
Gateway/Route List* Expressway_system (Edit)
Route Option
☒ Route this pattern
☐ Block this pattern No Error
Call Classification* OnNet
☐ Allow Device Override ☐ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgent Priority
☐ Require Forced Authorization Code
Authorization Level* 0
☐ Require Client Matter Code

Calling Party Transformations

☐ Use Calling Party's External Phone Number Mask
Calling Party Transform Mask
Prefix Digits (Outgoing Calls)
Calling Line ID Presentation* Default
Calling Name Presentation* Default

Connected Party Transformations

Connected Line ID Presentation* Default
Connected Name Presentation* Default

Called Party Transformations

Discard Digits < None >

Allowing Dialing to Expressway Domain from Cisco Phones

Configure a SIP route pattern that tells Unified CM that anything with, for example, a domain exp.domain needs to be sent down the Expressway SIP trunk. This is required to permit dialing from endpoints that support SIP URIs with domains, and also for enabling the reverse path to the Expressway for certain signaling.

1. On Unified CM, go to **Call Routing > SIP Route Pattern**.
2. Click **Add New**.
3. Configure the fields as follows:

Pattern Usage	<i>Domain Routing</i>
IPv4 Pattern	Domain for calls, for example exp.domain
Route Partition	Default is "<None>"; set according to dial plan restrictions
SIP Trunk	Required Trunk to route calls to the Expressway-C

4. Click **Save**.

Pattern Definition

Pattern Usage

Domain Routing

IPv4 Pattern*

exp.domain

IPv6 Pattern

Description

Expressway system

Route Partition

LABCM6

SIP Trunk/Route List*

Expressway_system

(Edit)

☐ Block Pattern

Calling Party Transformations

☐ Use Calling Party's External Phone Mask

Calling Party Transformation Mask

Prefix Digits (Outgoing Calls)

Calling Line ID Presentation*

Default

Calling Line Name Presentation*

Default

Connected Party Transformations

Connected Line ID Presentation*

Default

Connected Line Name Presentation*

Default

Save

Delete

Copy

Add New

When nnnn@exp.domain is dialed by an endpoint registered to Unified CM, Unified CM will route the call to the Expressway as nnnn@<FQDN of Expressway>:5060 (TCP) or nnnn@<FQDN of Expressway>:5061 (TLS). (The domain may alternatively be the IP address of Expressway, depending on what is configured as the SIP Trunk **Destination Address**.)

Checking the Message Size Limit on Unified CM

SIP messages for video are considerably larger than SIP messages for audio calls, in particular, when a Cisco TelePresence Server is used in the video network.

Ensure that the **SIP Max Incoming Message Size** on Unified CM is set to 11000:

1. Go to **System > Service Parameters**.
2. Select the appropriate server.
3. Select *Cisco CallManager (Active)* as the service.

Configuring Unified CM for an Expressway Trunk

4. Select **Advanced**.
5. In the **Clusterwide Parameters (Device - SIP)** configure the field as follows:

SIP Max Incoming Message Size

11000

6. Click **Save**.

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Service Parameter Configuration' page is displayed, with a 'Related Links' section showing 'Parameters for All Servers'. The 'SIP Max Incoming Message Size' parameter is highlighted with a red box, showing a value of 11000. Other parameters visible include 'SIP Station UDP Port Throttle Threshold' (50), 'SIP Trunk UDP Port Throttle Threshold' (200), 'SIP V.150 Outbound SDP Offer Filtering' (No Filtering), 'SIP Max Incoming Message Headers' (100), 'Send SIP Multicast TTL in SDP' (False), 'Default PUBLISH Expiration Timer' (3600), and 'Minimum PUBLISH Expiration Timer' (60).

Parameter	Value
SIP Station UDP Port Throttle Threshold *	50
SIP Trunk UDP Port Throttle Threshold *	200
SIP V.150 Outbound SDP Offer Filtering *	No Filtering
SIP Max Incoming Message Size *	11000
SIP Max Incoming Message Headers *	100
Send SIP Multicast TTL in SDP *	False
Default PUBLISH Expiration Timer *	3600
Minimum PUBLISH Expiration Timer *	60

Configuring Expressway Routing

Prerequisites

The Expressway-C must be configured with IP address, DNS and NTP information, and is accessible for management via its web interface (see [Expressway Basic Configuration Deployment Guide](#)).

Rich media session licenses must be installed.

Configuration Summary

The configuration on Expressway-C contains the following tasks:

- Creating a transform to ensure a consistent URI format
- Configuring a neighbor zone that contains the Unified CM
- Configuring a search rule to route calls to that zone
- Configuring a transform that converts number@<IP address of cucm> to number@exp.domain
- Configuring a transform to convert other Unified CM-supplied domain variants to number@exp.domain

These tasks are explained in detail below.

Ensuring a Consistent URI Format

In this deployment scenario, users want to be able to route calls via the Expressway to other devices or endpoints (not registered to Unified CM) that have a 4xxx extension number. Unified CM endpoints are to be dialed using a 3xxx number. This dialing model can be supported by H.323 (if the endpoint registers the 4-digit E.164 alias), however, SIP does not support dialing by numbers alone. If a number (without a domain appended) is dialed from a SIP endpoint the endpoint will automatically append its own domain.

For consistency with both SIP and H.323 dialing, this deployment scenario always uses the URI form for routing calls (that is, dialed_digits@domain). When the Expressway receives a call request, the dialed number:

- will contain the 4 digit extension number that identifies the specific endpoint to route to
- may or may not include a domain (only included when a SIP endpoint is making the call)

Thus, a transform is needed to ensure that the dialed number is transformed into a consistent form, in this case to add the domain (exp.domain) if required. To achieve this, a regex is used: `([^\@]*)` transforms to `\1@exp.domain` (any dialed information which does not contain a domain – does not contain an '@' – has the '@exp.domain' added.)

See the Regular Expression Reference in the Appendices section of [Expressway Administrator Guide](#) for further details, or alternatively search the internet for the term “Regular Expression”.

To create the transform:

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.

Configuring Expressway Routing

3. Configure the fields as follows:

Priority	2
Description	"Add domain where none exists" for example
Pattern type	<i>Regex</i>
Pattern string	<i>([^\@]*)</i>
Pattern behavior	<i>Replace</i>
Replace string	<i>\1@exp.domain</i>
State	<i>Enabled</i>

4. Click **Create transform**.

Create transform You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

Configuration

Priority	<input type="text" value="2"/>	
Description	<input type="text" value="Add domain where none exists"/>	
Pattern type	<input type="text" value="Regex"/>	
Pattern string	<input type="text" value="* ([^\@]*)"/>	
Pattern behavior	<input type="text" value="Replace"/>	
Replace string	<input type="text" value="\1@exp.domain"/>	
State	<input type="text" value="Enabled"/>	

Creating a Neighbor Zone for Unified CM

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.

Configuring Expressway Routing

3. Configure the fields as follows (you can leave other fields with default values unless you have specific needs for your deployment):

Name	CUCM Neighbor
Type	<i>Neighbor</i>
Hop count	15
H.323 mode	<i>Off</i> (H.323 is not supported between Expressway and Unified CM)
SIP mode	<i>On</i>
SIP port	5060 for TCP or 5061 for TLS (must match the port set on the SIP trunk)
Transport	<i>TCP</i> or <i>TLS</i> . Choose <i>TLS</i> if you want secure transport and encrypted media
Media encryption mode	<i>Auto</i>
SIP authentication trust mode	<i>Off</i>
Peer 1 address	IP address of Unified CM, or the FQDN of Unified CM. If you are planning to ultimately use a TLS connection, then typically you will need to specify the FQDN of Unified CM here as this is the name that will be used to authenticate the certificate presented by Unified CM.
Zone profile (Advanced section)	Select the following option depending on your Unified CM version: <ul style="list-style-type: none"> – <i>Cisco Unified Communications Manager</i> for versions earlier than 8.6.1. – <i>Cisco Unified Communications Manager (8.6.1 or 8.6.2)</i> for 8.6.1 or 8.6.2 – <i>Cisco Unified Communications Manager (9.x or later)</i> for versions from or after 9.x Unified CM 8.6.1 or later is required for BFCP (dual video / presentation sharing).
SIP UDP/iX filter mode (Advanced section)	This toggle filters out the iX protocol. You must set it <i>On</i> if the neighbor zone is to Unified CM versions before 9.0(1). Support for iX was added in 9.0(1), so you can leave the default <i>Off</i> for this parameter for Unified CM versions after that. You should also check Allow iX Application Media on the SIP profile of the trunk from Unified CM to Expressway-C.

This configures the Expressway to use SIP over TCP to communicate with the Unified CM. To use TLS, complete the configuration as described here for TCP and then see [Connecting Expressway to Unified CM Using TLS, page 25](#).

4. Click **Create zone**.

Configuring Expressway Routing

Edit zone

Type

Neighbor

Hop count

*

15

i

H.323

Mode

Off

i

SIP

Mode

On

i

Port

*

5060

i

Transport

TCP

i

Accept proxied registrations

Deny

i

Media encryption mode

Auto

i

ICE support

Off

i

Authentication

Authentication policy

Do not check credentials

i

SIP authentication trust mode

Off

i

Location

Peer 1 address

10.50.157.22

i

Peer 2 address

i

Peer 3 address

i

Peer 4 address

i

Peer 5 address

i

Peer 6 address

i

Advanced

Zone profile

Custom

i

Monitor peer status

Yes

i

Call signaling routed mode

Always

i

Creating a Search Rule to Route Calls to the Unified CM Neighbor Zone

Search rules specify the range of telephone numbers / URIs to be handled by this neighbor Unified CM. They can also be used to transform URIs before they are sent to the neighbor.

Configuring Expressway Routing

In this example deployment, the transforms set up in [Ensuring a Consistent URI Format, page 17](#) ensure that dial strings are in URI format number@exp.domain.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields as follows to route the call to Unified CM:

Rule name	Route to CUCM
Description	For example: Send 3xxx@exp.domain calls to CUCM
Priority	100
Protocol	<i>Any</i>
Source	<i>Any</i>
Request must be authenticated	Configure this setting according to your authentication policy
Mode	<i>Alias pattern match</i>
Pattern type	<i>Regex</i>
Pattern string	(3\d{3})@exp.domain(.*)
Pattern behavior	<i>Leave</i> (@domain formatted addresses will work in Unified CM due to the Cluster Fully Qualified Domain Name enterprise parameter)
On successful match	<i>Stop</i>
Target zone	<i>CUCM Neighbor</i>
State	<i>Enabled</i>

4. Click **Create search rule**.

See the “Zones and Neighbors” section of [Expressway Administrator Guide](#) for further details.

Creating a Transform that Converts number@<IP address of cucm> to number@exp.domain

When a call is made from Unified CM to Expressway, the callback address is presented as number@<ip address of cucm>. If the destination endpoint returns the call, the Expressway needs to be able to route it back to Unified CM. To enable this, the domain portion of the address must have the IP address removed and the video domain added (so that the existing search rule can route the call to Unified CM). A transform is required:

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.

Configuring Expressway Routing

3. Configure the fields as follows:

Priority	3
Description	"CUCM IP to domain" for example
Pattern type	<i>Regex</i>
Pattern string	(.*)@<ip address of Unified CM>(: ; .)*? If a Unified CM cluster is in use, the regex must cater for the IP address of every possible node, for example (.*)(10\.\.1\.\.2\.\.22 10\.\.1\.\.2\.\.23)(: ; .)*?
Pattern behavior	<i>Replace</i>
Replace string	\1@exp.domain\2
State	<i>Enabled</i>

4. Click **Create transform**.

Create transform You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

Configuration

Priority	<input type="text" value="3"/>
Description	<input type="text" value="CUCM IP to domain"/>
Pattern type	Regex
Pattern string	<input type="text" value="(*)@<ip address of CUCM>(: ; .)*?"/>
Pattern behavior	Replace
Replace string	<input type="text" value="\1@exp.domain\2"/>
State	Enabled

Creating a Transform to Convert other Unified CM-supplied Domain Variants to number@exp.domain

This transform converts URIs received from Unified CM to the format used in the Expressway's neighbor zones.

The domain portion of the URI received from Unified CM depends on its SIP Trunk configuration (see [Configuring the SIP Trunk Device, page 11](#)). Thus, this could be the IP address:port of the Expressway or the FQDN of the Expressway or Expressway cluster.

In this example, it is matching URIs received from Unified CM in the form 4xxx@exp-name.exp.domain:<port> and converting it into 4xxx@exp.domain.

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.

Configuring Expressway Routing

3. Configure the fields as follows:

Description	Convert Unified CM supplied domain information to the Expressway SIP domain
Priority	Enter a high priority such as 5 (the priority of this transform should be before any transforms that need to be applied for searching neighbor zones)
Pattern type	<i>Regex</i>
Pattern string	For example: (4\d{3})@exp-name.exp.domain(:.*)?
Pattern behavior	Replace
Replace string	For example: \1@exp.domain
State	Enabled

4. Click **Create transform**.

Create transform You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

Configuration

Priority	<input type="text" value="5"/>
Description	<input type="text" value="Convert Unified CM supplied domain information to the"/>
Pattern type	<input type="text" value="Regex"/>
Pattern string	<input type="text" value="(4\d{3})@exp-"/>
Pattern behavior	<input type="text" value="Replace"/>
Replace string	<input type="text" value="\1@exp.domain"/>
State	<input type="text" value="Enabled"/>

Connecting Expressway to Unified CM Using TLS

These instructions explain how to take a system that is already configured and working using a TCP interconnection between Expressway and Unified CM, and to convert that trunk to use TLS instead.

Before you Begin

Limitation on multiple TLS-enabled Expressway Neighbor Zones with Cisco Unified Communications Manager

Cisco Unified Communications Manager versions which are affected by CDETS [CSCus63305](#) (*Intermittent calls to Destination fails via TLS trunk*) cannot have multiple TLS-enabled SIP trunks between the same Cisco Unified Communications Manager node and Expressway-C node. Only one TLS-enabled Cisco Unified Communications Manager SIP trunk is supported in this case.

No SSL interop with versions 9.x and earlier

CiscoSSL was upgraded to version 5.4.3 in Expressway X8.7.2. Cisco SSL version 5.4.3 rejects keys with fewer than 1024 bits when doing Diffie-Hellman (DH) key exchange. As a result, **SSL interoperability is prevented with versions 9.x and earlier of Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service**. This is because those products generate 768 bit keys for D-H key exchange.

Process Summary

This table summarizes the process to convert to TLS:

Table 2 Overview of Tasks to Create SIP TLS Trunk Between Expressway and Unified CM

Command or Action
Ensure Certificate Trust Between Unified CM and Expressway, page 25
Set the Cluster Security Mode to Mixed Mode, page 27
Configure a SIP Trunk Security Profile on Unified CM, page 28
Update Device Profiles to Encrypt Calls to Unified CM-registered Endpoints, page 29
Update Unified CM Trunk to Expressway to Use TLS, page 28
Update Expressway Neighbor Zone to Unified CM to Use TLS, page 29
Verify That the TLS Connection is Operational, page 29

Ensure Certificate Trust Between Unified CM and Expressway

For Unified CM and Expressway to establish a TLS connection with each other:

- Expressway and Unified CM must both have valid server certificates loaded (you must replace the Expressway's default server certificate with a valid server certificate)
- Expressway must trust Unified CM's server certificate (the root CA of the Unified CM server certificate must be loaded onto Expressway)
- Unified CM must trust Expressway's server certificate (the root CA of the Expressway server certificate must be loaded onto Unified CM)

See [Expressway Certificate Creation and Use Deployment Guide](#) for full details about loading certificates and how to generate CSRs on Expressway to acquire certificates from a Certificate Authority (CA).

Note: In a clustered environment, you must install CA and server certificates on each peer/node individually.

Connecting Expressway to Unified CM Using TLS

We strongly recommend that you do not use self-signed certificates in a production environment.

Load Server and Trust Certificates on Expressway

Expressway Server Certificate

Expressway has only one server certificate. By default, this is a certificate signed by a temporary certificate authority. We recommend that it is replaced by a certificate generated by a trusted certificate authority.

To upload a server certificate:

1. Go to **Maintenance > Security > Server certificate**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the **server certificate** PEM file.
3. If you used an external system to generate the Certificate Signing Request (CSR) you must also upload the **server private key** PEM file that was used to encrypt the server certificate. (The private key file will have been automatically generated and stored earlier if the Expressway was used to produce the CSR for this server certificate.)
 - The **server private key** PEM file must not be password protected.
 - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload server certificate data**.

Note: If you are using Unified CM version 8.5(1) or earlier and are having problems establishing a TLS connection between Expressway and Unified CM, we recommend adding the following x509 extended key attributes into the CSR:

- serverAuth (1.3.6.1.5.5.7.3.1) -- TLS Web server authentication
- clientAuth (1.3.6.1.5.5.7.3.2) -- TLS Web client authentication
- ipsecEndSystem (1.3.6.1.5.5.7.3.5) -- IP security end system

Expressway Trusted CA Certificate

The **Trusted CA certificate** page (**Maintenance > Security > Trusted CA certificate**) allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway. When a TLS connection to Expressway mandates certificate verification, the certificate presented to the Expressway must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

The root CA of the Unified CM server certificate must be loaded into the Expressway's trusted CA certificate list.

To upload a new file containing one or more CA certificates, **Browse** to the required PEM file and click **Append CA certificate**. This will append any new certificates to the existing list of CA certificates. If you are replacing existing certificates for a particular issuer and subject, you have to manually delete the previous certificates.

Repeat this process on every Expressway that will communicate with this Unified CM.

Load Server and Trust Certificates on Unified CM

Certificate management for Unified CM is performed in the **Cisco Unified OS Administration** application.

All existing certificates are listed under **Security > Certificate Management**. Server certificates are of type *certs* and trusted CA certificates are of type *trust-certs*.

Unified CM Server Certificate

By default, Unified CM has a self-signed server certificate **CallManager.pem** installed. We recommend that this is replaced with a certificate generated from a trusted certificate authority.

Unified CM Trusted CA Certificate

To load the root CA certificate of the authority that issued the Expressway certificate (if it is not already loaded):

Connecting Expressway to Unified CM Using TLS

1. Click **Upload Certificate/Certificate chain**.
2. Select a **Certificate Name** of *CallManager-trust*.
3. Click **Browse** and select the file containing the root CA certificate of the authority that issued the Expressway certificate.
4. Click **Upload File**.

Repeat this process on every Unified CM server that will communicate with Expressway. Typically this is every node that is running the CallManager service.

Set the Cluster Security Mode to Mixed Mode

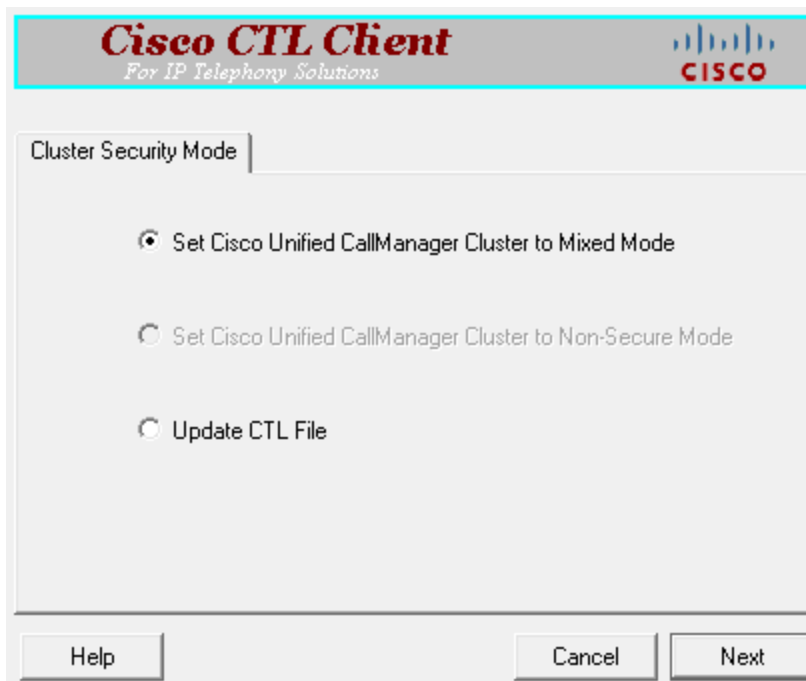
The Cisco Unified Communications Manager cluster must be in Mixed Mode to allow the registration of both secure devices and non-secure devices. This allows for best effort encryption between the Expressway and the Cisco Unified Communications Manager. Read [Secure RTP between CUCM and VCS or Expressway Configuration Example](#) for background on best effort encryption between Expressway and Unified CM.

Note: This requirement relates to media encryption. Unified CM does **not** need to be in Mixed Mode to support TLS SIP trunks.

As of version 10.0, you can use the CLI to change the cluster security mode. On earlier versions, you must use the Cisco CTL Client plugin to change the cluster security mode. The security mode change updates the CTL file, so you must restart the Cisco CallManager and Cisco Tftp services after the change.

The process is summarized below, but you should refer to the *Cisco Unified Communications Manager Security Guide* for your version, which you can find on the [Cisco Unified Communications Manager \(CallManager\) Maintain and Operate Guides](#) page.

1. Obtain access to the Unified CM publisher node, including hardware security tokens (if using the CTL Client plugin).
2. (Pre 10.0) Download and install the Cisco CTL Client plugin from Unified CM.
3. Run the CTL Client plugin to enable Mixed Mode. On 10.0 or later, you can use `utils ctl set-cluster mixed-mode` at the CLI.



Connecting Expressway to Unified CM Using TLS

4. Update the CTL file (via the plugin or `utils ctl update CTLFile`).
5. Restart the Cisco CallManager and Cisco Tftp services (via Cisco Unified Serviceability).

Configure a SIP Trunk Security Profile on Unified CM

On Unified CM:

1. Select **Cisco Unified CM Administration**, click **Go** and log in.
2. Go to **System > Security > SIP Trunk Security Profile**.
3. Click **Add New**.
4. Configure the fields as follows:

Name	A name indicating that this is an encrypted profile.
Description	Enter a textual description as required.
Device Security Mode	<i>Encrypted.</i>
Incoming Transport Type	<i>TLS.</i>
Outgoing Transport Type	<i>TLS.</i>
Enable Digest Authentication	Leave unselected.
X.509 Subject Name	The subject name or a subject alternate name provided by the Expressway in its certificate. For Expressway clusters, ensure that this list includes all of the names contained within all of the peers' certificates. To specify multiple X.509 names, separate each name by a space, comma, semicolon or colon.
Incoming Port	5061 Use a different port (such as 5070 or 5071) if you are using 5061 for MRA registrations. The reason is to avoid potential issues with MRA if Unified CM receives registration requests on what it believes to be a SIP trunk. This applies to TCP or TLS connections.
Accept Unsolicited Notification	Select this check box
Accept Replaces Header	Select this check box
Other parameters	Leave all other parameters unselected.

5. Click **Save**.

Update Unified CM Trunk to Expressway to Use TLS

On Unified CM:

1. Go to **Device > Trunk**.
2. Using Find, select the **Device Name** previously set up for the trunk to the Expressway.

Connecting Expressway to Unified CM Using TLS

3. Configure the following fields:

SIP Information section	
Destination Port	5061 (unless using DNS SRV, in which case ensure the SRV records are set up correctly).
SIP Trunk Security Profile	Select the trunk profile set up above.

Leave other parameters as previously configured.

4. Click **Save**.
5. Click **Reset**.

Update Device Profiles to Encrypt Calls to Unified CM-registered Endpoints

Endpoints registered to Unified CM need to be configured with a "SIP Secure profile" to provide encrypted media and call negotiation. If such profiles are not available by default, create them at **System > Security > Phone Security**. On the secure profiles, you must set **Device Security Mode** to *Encrypted*.

See [Securing Cisco TelePresence Products](#) for further information on using the Cisco CTL Client and configuring Unified CM for secure communications.

Update Expressway Neighbor Zone to Unified CM to Use TLS

Expressway will report that the Unified CM zone is active even while it is communicating with Unified CM over TCP. The changes below are necessary to enable communications over TLS.

On Expressway:

1. Go to **Configuration > Zones > Zones**, then select the zone to Unified CM.
2. Configure the following fields:

SIP section	
Port	5061
Transport	<i>TLS</i>
TLS verify mode	<i>On</i>
Authentication trust mode	<i>Off</i>

Leave other parameters as previously configured.

3. Click **Save**.

Verify That the TLS Connection is Operational

To verify correct TLS operation, check that the Expressway zone reports its status as active and then make some test calls.

1. Check the Expressway zone is active:
 - a. Go to **Configuration > Zones > Zones**.
 - b. Check the **SIP status** of the zone.

Connecting Expressway to Unified CM Using TLS

If the zone is not active, try resetting or restarting the trunk again on Unified CM.

2. Make test calls from Expressway registered endpoints to a Unified CM phone.
3. Make test calls from a Unified CM phone to Expressway registered endpoints.

Appendix 1: Troubleshooting

Problems Connecting Expressway-C Local Calls

Look at “Search history” to Check the Applied Transforms

Search history entries report on any searches initiated from a SETUP/ARQ /LRQ in H323 and from an INVITE/OPTIONS in SIP.

1. Go to **Status > Search history**.
The summary shows the source and destination call aliases, and whether the destination alias was found.
2. Select the relevant search attempt.

The search history for that search attempt shows:

- the incoming call’s details
- any transforms applied by admin or user policy or CPL
- and in priority order, zones which matched the required (transformed) destination, reporting on:
 - any transforms the zone may apply
 - found or not found status
 - if not found, the error code as seen in the zone’s search response
 - repeated until a zone is found that can accept the call, or all zone matches have been attempted (the search may be “not found” due to lack of bandwidth or because the search from the zone resulted in an H.323 rejection reason or a non 2xx response to a SIP request)

If the search indicates:

- Found: False
- Reason: 480 Temporarily Not Available

this could be because the Expressway zone links are not correctly set up. From the command line execute `xcommand DefaultLinksAdd` to set up the required links for the Expressway’s default zones; also check the links for other zones that have been created.

Note that each H.323 call will have two entries in the search history:

- The first for an ARQ to see if the endpoint can be found.
- The second for the Setup to actually route the call.

The ARQ search does not depend on links or link bandwidth, and so if links do not exist or link bandwidth is insufficient it may still pass, even though the Setup search will subsequently fail.

Each SIP call will usually have only a single search history entry for the SIP INVITE.

Look at Call History to Check How the Call Progressed

1. Go to **Status > Calls > History**.
The summary shows the source and destination call aliases, call duration and protocol (including any interworking).
2. Select the relevant call attempt and then the relevant call components.
This shows the incoming and outgoing call leg details and the zone and subzone routing.

Check for Errors

Check the Event Log which is accessible from the web browser: **Status > Logs > Event Log**.

Tracing Calls

Tracing Calls at SIP / H.323 Level in Expressway

1. Go to **Maintenance > Diagnostics > Diagnostic logging**.
2. Optionally, select **Take tcpdump while logging**.
3. Click **Start new log**.
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.
5. Reproduce the system issue you want to trace in the diagnostic log.
6. Click **Stop logging**.
7. 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).

Call Failures with Cisco TelePresence Server

SIP messages from Cisco TelePresence Server can be > 5,000 bytes (which is the default **SIP Max Incoming Message Size** configured in Unified CM).

Increase the **SIP Max Incoming Message Size** – see [Checking the Message Size Limit on Unified CM, page 15](#).

In-call Problems

Calls Clear Down when a Call Transfer from a Video Phone on Unified CM Transfers a Call to Expressway

Even if use of a media termination point (MTP) is not requested on the SIP trunk between Unified CM and Expressway, if DTMF signaling method is configured as “No preference” on the SIP trunk on Unified CM, Unified CM will try and use a Media Transfer Point and the call will fail.

To resolve this, ensure that DTMF signaling method is configured as *RFC 2833* on Unified CM on the SIP trunk from Unified CM to Expressway.

Poor Video Quality from Unified CM

Ensure that your Unified CM region has an appropriate session bit rate for video calls as described in [Configuring the Region with an Appropriate Session Bit Rate for Video Calls, page 10](#).

Taking a Trace on Unified CM Using RTMT

RTMT is a tool that lets you monitor system health, view graphs and collect logs from Unified CM. There are versions for both Linux and Windows. Unified CM must also be configured to specify what can be traced.

Appendix 1: Troubleshooting

Configure Unified CM to Enable Tracing

1. Log in to Unified CM.
2. In the **Navigation** drop-down select **Cisco Unified Serviceability** and click **Go**.
3. Go to the **Troubleshooting Trace Settings** page (**Trace > Troubleshooting Trace Settings**).
4. Select the **Check All Services** check box.
5. Click **Save**.

Installing RTMT – Real Time Monitoring Tool

1. Log in to Unified CM using a Linux or Windows PC.
2. Go to **Application > Plugins**.
3. Select **Find** with 'Name begins with <blank>' and 'Plugin Type equals Installation'.
4. Scroll down to the entry for 'Cisco Unified CM Real-Time Monitoring Tool – Linux' or 'Cisco Unified CM Real-Time Monitoring Tool – Windows', as required.
5. Click on the **Download** link.
6. When downloaded, run the downloaded install file.
7. Follow the instructions in the install wizard.
8. When complete, click **Done** to exit the installer.

Running RTMT

1. Run RTMT. (For example, under windows this is in **Start > All Programs > Cisco > CallManager Serviceability > Real-Time Monitoring Tool**.)
2. In the Login window enter the **Host IP Address**, **User Name** and **Password**.
3. Click **OK**.

Taking a Trace Using RTMT

1. Select **Trace & Log Central**.
2. Double-click on **Real Time Trace**.
3. Double-click **View Real Time Data**.
4. Select a Node – the Unified CM instance that is to have the trace run on it.
5. Click **Next >**.
6. Select the following:
 - **Products** = *UCM*
 - **Services** = *Cisco CallManager*
 - **Trace File Type** = *sdi*
7. Click **Finish**.

Note:

- Logs can take a while to download.
- The sdi (System Diagnostic Interface) trace contains alarms, error information and SIP stack trace information.

Appendix 1: Troubleshooting

Call Failures

Registrations Received on a SIP Trunk Rejected by Unified CM

REGISTER requests received on a SIP trunk are rejected by Unified CM with a 405 error response. With a warning that the SIP trunk does not allow registrations. The error response is likely to include this text:

- SIP/2.0 405 Method Not Allowed
- SIP trunk disallows REGISTER

TLS Calls Fail when Unified CM uses SRV Trunk Destinations

Calls from Unified CM may fail if they use a TLS trunk security profile and SRV trunk destinations (requiring "_sips._tcp" SRV record lookups in DNS).

See bug CSCue37440 in the [Cisco Bug Search Tool](#) for up-to-date information regarding the versions of Unified CM in which this issue has been fixed.

If you need to address one or more Expressway peers you can work around this problem by not using SRV records. Instead, in the SIP trunk, specify each Expressway **Destination Address** individually using DNS A-records or static IP addresses. However, note that these addresses affect the domain portion of the URI received by Expressway from Unified CM. You may need to set up appropriate transforms on the Expressway to cater for this (see [Creating a Transform to Convert other Unified CM-supplied Domain Variants to number@exp.domain](#), page 22).

Appendix 2: Connecting Unified CM to an Expressway Cluster

From Unified CM version 8.5, to connect Unified CM with a cluster of Expressway peers there are 2 methods of providing Unified CM with the addresses of the Expressway cluster peers:

- the trunk to Expressway specifies the DNS SRV address for the Expressway cluster
- the trunk to Expressway specifies a list of Expressway peers

Prior to Unified CM 8.5, the trunk to Expressway had to specify the DNS SRV address for the Expressway cluster.

Configuring the Trunk to Expressway to Specify the DNS SRV Address for the Expressway Cluster

Ensure that in the DNS server used by Unified CM a DNS SRV record exists for the cluster of Expressway peers; in the DNS SRV record each peer should be set with equal priority and equal weight.

1. On Unified CM, go to **Device > Trunk**.
2. Select the previously configured Trunk.
3. Scroll down and configure the **SIP Information** section fields as follows:

Destination address	<DNS SRV name of Expressway cluster>
Destination address is an SRV	Select this check box.

4. Click **Save**.
5. Click **Reset**.
6. Click **Reset**.
7. On Expressway, ensure that the cluster name is configured as a SIP domain (**Configuration > Domains**).

SIP Information

Destination

☒ Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1 * exp-name.exp.domain		0

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile

DTMF Signaling Method* RFC 2833

Configuring the Trunk to Expressway to Specify a List of Expressway Peers

1. On Unified CM, go to **Device > Trunk**.
2. Select the previously configured Trunk.

Appendix 2: Connecting Unified CM to an Expressway Cluster

3. Scroll down and configure the **SIP Information** fields as follows:

(Click + to obtain additional destination address entries.)

Destination address is an SRV	Ensure that this check box is not selected
Destination address 1 and Destination port 1	IP address or DNS name of Expressway peer 1 5060 or 5061 depending on connectivity (TCP/TLS)
Destination address 2 and Destination port 2	IP address or DNS name of Expressway peer 2 5060 or 5061 depending on connectivity (TCP/TLS)
Destination address 3 and Destination port 3	IP address or DNS name of Expressway peer 3 – if it exists 5060 or 5061 depending on connectivity (TCP/TLS)
... up to Destination address 6 and Destination port 6	... repeat up to IP address or DNS name of Expressway peer 6 – where they exist

4. Click **Save**.
5. Click **Reset**.
6. Click **Reset**.

Appendix 3: Connecting Expressway to a Cluster of Unified CM Nodes

When connecting Expressway to a cluster of Unified CM nodes, Expressway needs to be able to route calls to each Unified CM node.

This can be done in 2 ways, in order of preference:

1. With a single neighbor zone in Expressway with the Unified CM nodes listed as location peer addresses.
2. By using DNS SRV records and an Expressway DNS zone.

Note that both options ensure that the Expressway to Unified CM call load is shared across Unified CM nodes.

Option 1: Using a Single Neighbor Zone

Unified CM Configuration

When in a cluster, Unified CM needs to accept calls routed to number@domain (instead of number@<ip address of Unified CM>) so that Expressway can send the call to any Unified CM node without having to make sure that the domain portion matches the IP address of the node that the call is being sent to.

Ensure that the **Cluster Fully Qualified Domain Name (System > Enterprise parameters, in the Clusterwide Domain Configuration section)** is set to the same domain as the video network, for example exp.domain.

Expressway-C Configuration

The Expressway configuration requires an update to the neighbor zone:

1. Go to **Configuration > Zones**.
2. Select the Unified CM neighbor zone.
3. Configure the fields as follows:

Peer 1 address	IP address of Unified CM node 1, or the domain of Unified CM node 1.
Peer 2 address	IP address or the domain of Unified CM node 2.
Peer 3 address	IP address or the domain of Unified CM node 3, or blank if no Unified CM node 3.
.... up to Peer 6 address	... repeat up to the IP address or the domain of Unified CM node 6, or leaving it blank if there is no Unified CM node.

Option 2: Using a DNS Zone

Unified CM Configuration

Ensure that the **Cluster Fully Qualified Domain Name (System > Enterprise parameters, in the Clusterwide Domain Configuration section)** is set to the same domain as the video network, for example exp.domain.

DNS Server Configuration

Configure the DNS server (that is used by the Expressway) with DNS SRV records for the Unified CM cluster.

- `_sips._tcp.fqdn_of_cucm_clusterrecords` for TLS connectivity (one record for each Unified CM node); or
- `_sip._tcp.fqdn_of_cucm_clusterrecords` for TCP connectivity (one record for each Unified CM node)

Appendix 3: Connecting Expressway to a Cluster of Unified CM Nodes

Expressway-C Configuration

Expressway configuration requires 3 steps:

- Create a Unified CM DNS zone
- Adjust search rule to use the DNS zone
- Delete the old Unified CM neighbor zone

Creating a Unified CM DNS Zone

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows:

Name	CUCM Cluster Neighbor DNS Zone
Type	<i>DNS</i>
Hop count	15
H.323 mode	<i>Off</i> H.323 access is not required for communication with Unified CM
SIP mode	<i>On</i>
TLS verify mode	<i>Off</i>
Media encryption mode	<i>Auto</i>
Include address record	<i>Off</i>
Zone profile	Select <i>Cisco Unified Communications Manager</i> or <i>Cisco Unified Communications Manager (8.6.1 or later)</i> as appropriate.

4. Click **Create zone**.

Appendix 3: Connecting Expressway to a Cluster of Unified CM Nodes

Create zone You are here: [Configuration](#) > [Zones](#) > [Zones](#) > Create zone

Configuration

Name * CUCM Cluster Neighbor DNS Zone i

Type * DNS v i

Hop count * 15 i

H.323

Mode Off v i

SIP

Mode On v i

TLS verify mode Off v i

Media encryption mode Auto v i

Advanced

Include address record Off v i

Zone profile Cisco Unified Communications Manager v i

Create zone Cancel

Adjusting the Search Rule

Change the search rule to point to this Unified CM DNS zone.

1. Go to **Configuration > Dial plan > Search rules**.
2. Select the existing “Route to Unified CM” search rule.
3. Update the **Target zone** to use the *CUCM Cluster Neighbor DNS Zone* created above.
4. Click **Save**.

Deleting the Old Unified CM Neighbor Zone

Delete the now unused neighbor zone “Unified CM Neighbor”.

1. Go to **Configuration > Zones > Zones**.
2. Select the check box next to the “CUCM Neighbor” zone.
3. Click **Delete**.

Appendix 4: Additional Information

IP Address Dialing

Unified CM cannot dial out to IP addresses, but the Expressway can. To support IP address dialing from endpoints registered to Unified CM, we recommend following the procedure in the knowledge base article [Dial IP Addresses from Endpoints Registered to CUCM with VCS/Expressway](#).

Characters Allowed in SIP URIs

The following character set is allowed in SIP URIs (further details may be found in RFC 3261):

a-z / A-Z / 0-9 / "-" / "_" / "." / "!" / "~" / "*" / "'" / "(" / ")" / "&" / "=" / "+" / "\$" / "," / ";" / "?" / "/"

If other characters are needed they must be “escaped” using “%” followed by a pair of hexadecimal digits that represents the ASCII value for the required character.

For example, “alice smith@example.com” must be encoded as `alice%20smith@example.com` (where %20 represents the space character).

Cisco Legal Information

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

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

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

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

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

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

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

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

© 2016 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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