Collaboration Edge Using Cisco BE6000

Cisco Validated Design Guide

August 2016

© 2016 Cisco Systems, Inc. All rights reserved.

Contents

Preface

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

Today's enterprises are looking for seamless access to rich collaborative services irrespective of the location .

This CVD discuss about the primary drivers for deploying the collaboration edge solution namely **the Remote and Mobile access** and **B2B collaboration**.

Related PA Guides

- Cisco Preferred Architecture for Midmarket Collaboration 11.x, Design Overview
- Cisco Preferred Architecture for Video 11.x, Design Overview

Related CVD Guides

Unified Communications using the Business Edition 6000 CVD

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd/collaboration

Documentation for Cisco Validated Designs

Cisco Preferred Architecture (PA) Design Overview guides – These documents help customers and sales teams to select the appropriate architecture based on an organization's business requirements; understand the products that are used within the architecture; and obtain general design best practices. These guides support sales processes.

Cisco Validated Design (CVD) guides – These documents provide detailed steps for deploying the Cisco Preferred Architectures. These guides support planning, design, and implementation of the Preferred Architectures.

Cisco Collaboration Solution Reference Network Design (SRND) guide – This document provides detailed design options for Cisco Collaboration. The Cisco Collaboration SRND should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

Scope

This guide covers the following areas of technology and products:

- Cisco Unified Communication Manager
- Desktop video endpoints and mobile clients
- Multipurpose room systems
- Cisco Expressway Series
- Cisco Unified Border Element
- Session Initiation Protocol (SIP) signaling

For more information, see the *Design Overview* section in this guide.

Proficiency

This guide is for people with technical proficiencies—or equivalent experience in **CCNA Collaboration**—1 to 3 years in designing, installing, and troubleshooting voice and unified communications applications, devices, and networks.

Comments and Questions

If you would like to comment on a guide or ask questions, please email: collab-mm-cvd@external.cisco.com.

Disclaimer

The IP address scheme used in this document is for representational purposes only.

Introduction

The rise in mobility has opened up new ways in which teams, employees and customers are connecting and collaborating with one another. The key to success in this new world is having open and accessible communications across environments—whether it be in a physical office, face-to-face through a video call, in a voice call, or in a converged connection through Cisco® Jabber. Today's organizations need to support mobile workers by providing them with collaboration technologies that are designed around mobility first.

Collaboration with video provides a higher level of user interaction. Providing functionality to mobile users by leveraging the Internet has increased significantly over the past few years, and for many organizations, connectivity is a fundamental requirement for conducting day-to-day activities. Moreover, securely connecting mobile workers and remote site workers to each other and to headquarters are critical functions that enable organizations to accomplish their business goals.

The Cisco solution for remote workers has classically relied upon VPN connections to provide a secure tunnel into the corporate network.

In addition, teleworkers can use their Cisco TelePresence devices without a VPN, making collaboration at home as easy as in the office. Cisco Expressway makes collaboration as easy outside the enterprise as it is inside by simplifying the end-user experience. Using secure mobile access based on Transport Layer Security (TLS), Jabber mobile users can access all their collaboration workloads (video, voice, content, instant messaging, and presence) without requiring the extra step of a VPN, leaving the flexibility for users to route all other traffic directly via the Internet.

Technology Use Case

Organizations are looking for a simple and efficient way to extend their rich collaborative services offered behind their firewall to users who are outside their firewalls. Clients like Cisco Jabber, which truly integrate multiple channel of communications within a single soft client, are very critical for enterprises. It enables enterprises to have their mobile workforce access the same set of rich collaborative features to streamline the business process and also make them productive irrespective of the location.

Collaboration edge portfolio consists of a broad range of solutions and components each of them which solves a particular business use-case.

Broadly speaking it extends access to the same set of rich collaborative services accessible by a user inside an enterprise to their mobile and remote workforce via the VPN-less mode thus making the experience more seamless and consistent irrespective of the location.

It also helps these users to engage in communication with the people who aren't part of their businesses for example partners, customers and other stakeholders of the communities via multi-modal format of communication (Video, Voice and IM&P).

Additionally, the collaboration edge solution also connects enterprise voice users to the provider SIP trunking services. With SIP Trunking, enterprises can lower costs, simplify the network and extend rich collaborative services.

Design Overview

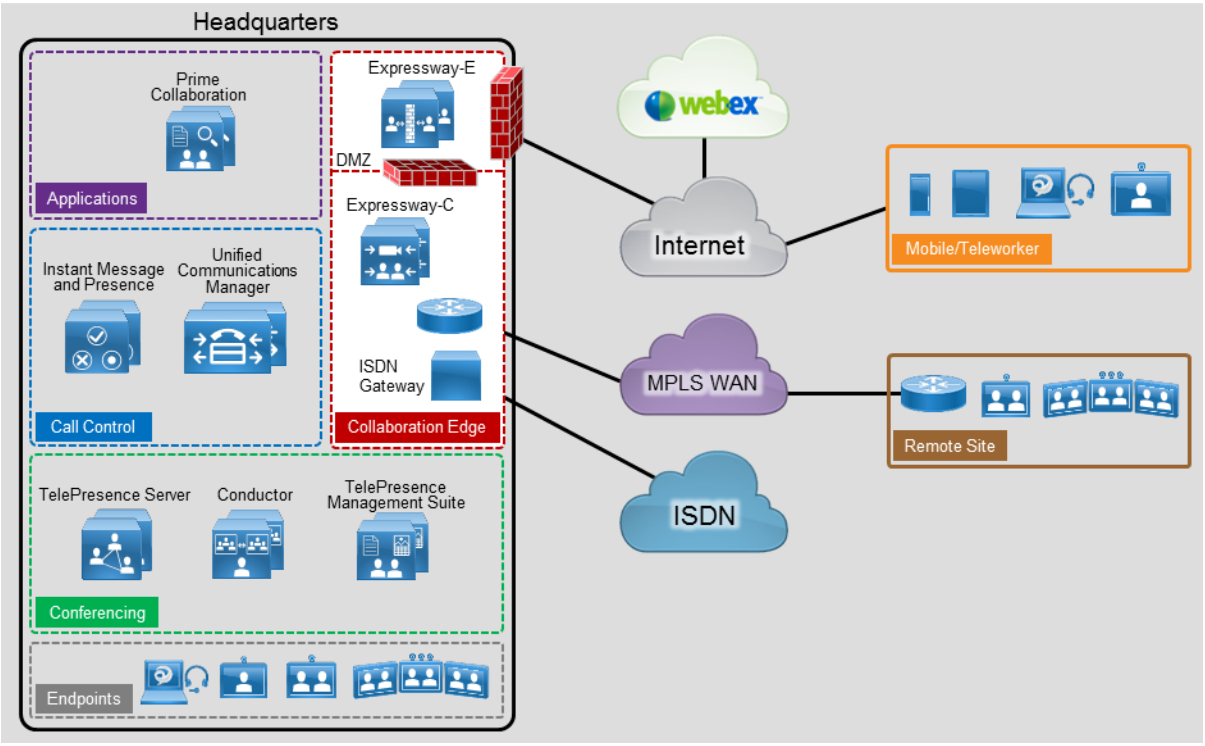
An end-to-end Cisco collaboration edge solution incorporates endpoints, infrastructure components, and centralized management tools.

Cisco Preferred Architecture

Cisco Preferred Architectures provide recommended deployment models for specific market segments based on common use cases. They incorporate a subset of products from the Cisco Collaboration portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive, out-of-the-box, and built to scale with an organization as its business needs change.This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

The Cisco Preferred Architecture (PA) delivers capabilities that enable organizations to realize immediate gains in productivity and add value to their current voice deployments.

Figure 1. Preferred Architecture

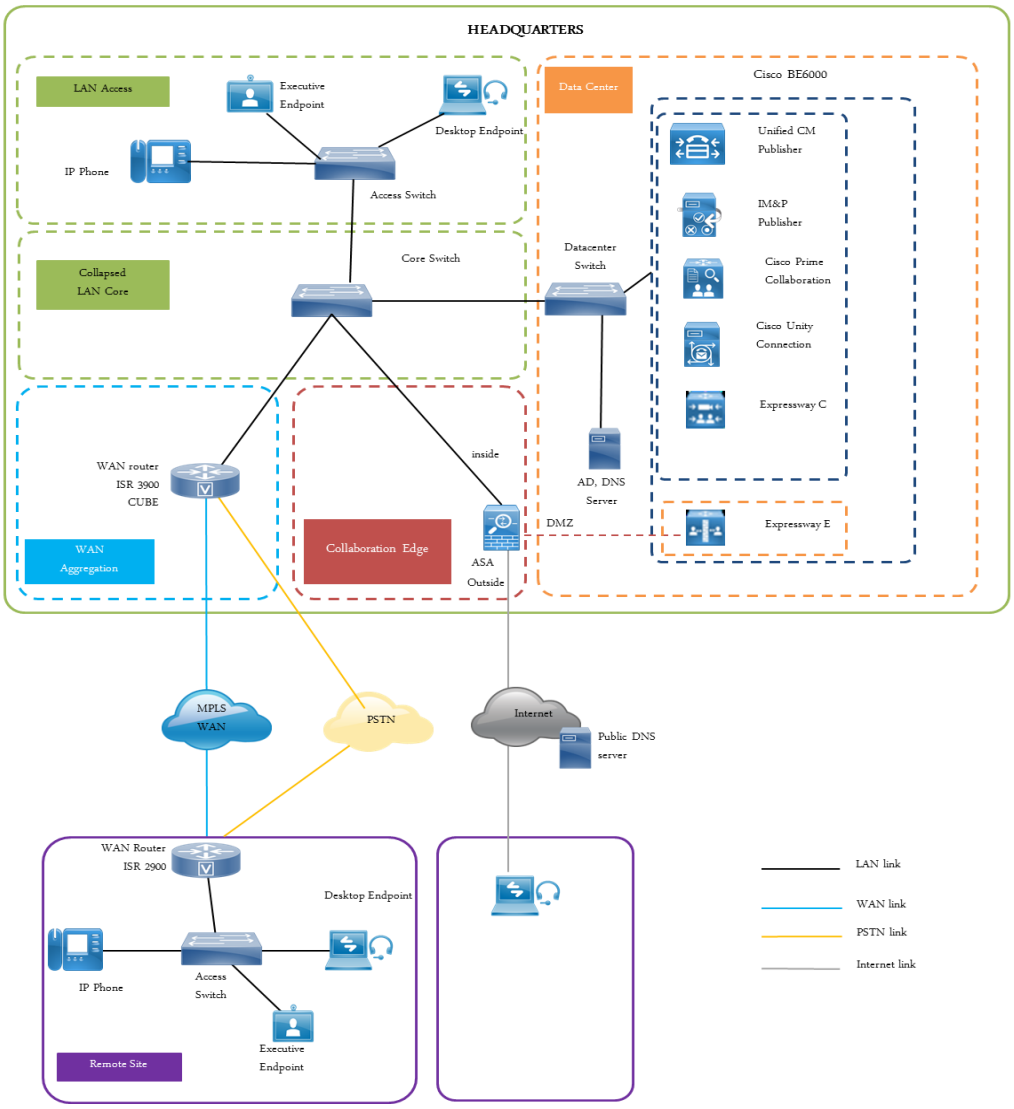


Solution Details

This *Collaboration Edge Using Cisco BE6000 Technology Design Guide* includes the following components:

- Cisco Unified Communications Manager (CUCM), for call control and SIP endpoint registrations
- Cisco Unified Communications Manager Instant Messaging & Presence for Jabber Clients
- Cisco Expressway-C and Cisco Expressway-E, for VPN-less mobile and remote access
- Cisco Expressway-C and Cisco Expressway-E, for business to business collaboration
- Cisco Unified Border Element for SIP trunking to PSTN

Figure 2. Solution components block diagram



Cisco Unified Communications Manager (Cisco Unified CM)

Cisco Unified CM (formerly Cisco Unified CallManager) serves as the software-based, call-processing component of Cisco Unified Communications. CUCM extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through CUCM open-telephony application program interface (API).

CUCM is the primary call agent in this CVD. CUCM supports session initiation protocol (SIP), and the configurations in this document use SIP as signaling protocol for the endpoints.

Cisco Video and TelePresence Endpoints

Cisco video endpoints provide a wide range of features, functionality, and user experiences. Because endpoints range from desktop video phones and softclients to multiple-screen immersive TelePresence endpoints, an organization can deploy the right variety of endpoints to meet users' needs. Additionally, these devices enable users to access multiple communication services, such as:

- Voice calls
- Video calls
- Conferencing
- Presence
- Desktop sharing

Table 1. Cisco Telepresence and Video Endpoints

Product	Description
Cisco DX Series	Collaboration desk endpoint
Cisco MX Series	Collaboration room endpoint
Cisco SX Series	TelePresence integration solutions
Cisco IX Series	Immersive TelePresence room system
Cisco Unified IP Phones 8800/7800	General office phones (video)

Table 2. Cisco Jabber

Product	Description
Mobile: Jabber for Android Jabber for iPhone and iPad Desktop: Jabber for Mac Jabber for Windows	Soft client with integrated voice, video, voicemail, and instant messaging and presence functionality for mobile devices and personal computers

Table 3. Comparison of Endpoint features and Capabilities

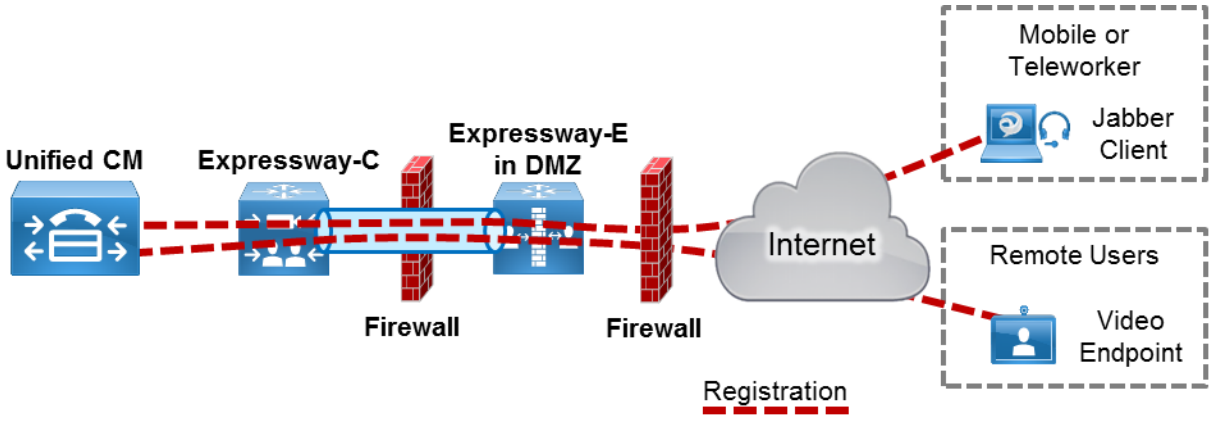
Product(s)	Audio	Video	Content Sharing	Unified CM High Availability	Mobile and Remote Access
Jabber Mobile	Y	Y	N	Y	Y
Jabber Desktop	Y	Y	Y	Y	Y
DX Series	Y	Y	Y[1]	Y	Y
EX Series	Y	Y	Y	Y	Y
MX Series	Y	Y	Y	Y	Y
SX Series	Y	Y	Y	Y	Y
IX Series	Y	Y	Y	Y	N
8800/7800	Y	Y	N	Y	Y

1 The DX series will be running the CE software.

Cisco Expressway-E and Expressway-C

Cisco Expressway Series is a firewall traversal solution that enables mobile and remote access to CUCM and other Cisco Collaboration Applications . The Expressway Mobile and Remote Access solution is complelementary to Cisco's Anyconnect, providing organizations an alternative to VPN for remote workers using Cisco Jabber or TelePresence endpoints.

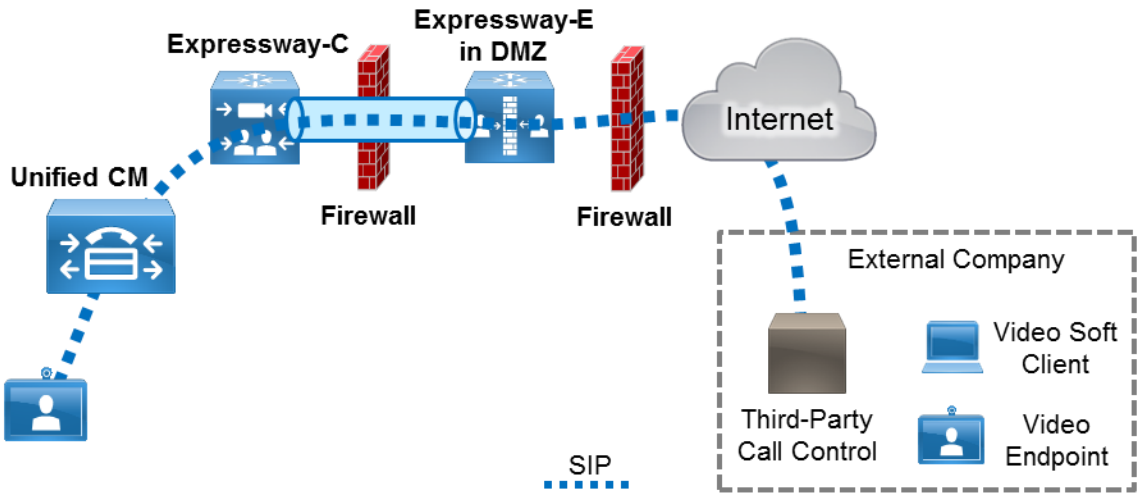
Figure 3. Mobile & Remote Access



The Cisco Expressway series also offers Business-to-Business (B2B) collaboration. This enables for an enterprise to seamlessly communicate with other businessess for instance partner organizations, vendors,

etc thus, extending the rich media services beyond the boundaries of the enterprise. Cisco Expressway Series consists of Cisco Expressway-E and Cisco Expressway-C.

Figure 4. Business to Business Collaboration



Cisco Expressway-E acts as a traversal server and allows secure communication through to your business and provides other services, such as DNS SRV lookup.

Cisco Expressway-C acts as the traversal client for Cisco Expressway-E (required in all Cisco Expressway E deployments). It acts as a video gateway providing interworking with third party industry standard H.264 SVC, H.323, AVC devices & systems (including Microsoft Lync 2013).

In this design, you create separate traversal zones one for mobile and remote access and for business-to-business video communications.

Cisco Unified Border Element (CUBE)

Cisco Unified Border Element (CUBE) is Cisco's session border controller (SBC) helping enterprises connect to Service Provider SIP trunking services. CUBE provides session control, security, interworking and demarcation to interconnect unified communications networks and enable end-to-end voice. Deploying CUBE is essential for routing voice calls beyond the enterprise through the IP PSTN to customers and partners. With SIP Trunking, CUBE lowers costs, simplifies the network and extends rich collaborative services.

Cisco Adaptive Security Appliance (Cisco ASA)

This design uses Cisco Adaptive Security Appliance as the security appliance. The appliance is deployed in three-port firewall mode, in which one port is connected to the inside network, another to an outside interface, and the third to the DMZ interface. Cisco Expressway-E is connected to the DMZ interface of Cisco ASA. Expressway-C and other collaboration components are on the inside of the Cisco ASA

appliance. Expressway-E is static-NATed to a public IP. All communication to the Expressway-E is based on the NATed IP. This means that Cisco ASA allows traffic from inside to reach the DMZ by using the NATed IP. This is also known as *NAT reflection*.

SIP and H.323 ALGs are disabled on the Cisco ASA appliance carrying network traffic to or from the Cisco Expressway-E. When enabled, this is frequently found to negatively affect the built in traversal functionality of the Cisco Expressway-E, because much of the SIP messaging is encrypted and Cisco ASA cannot inspect the payload.

Dial Plan

This design follows a single-cluster centralized call processing model. The endpoints use a seven-digit phone number for dialing, which preserves the capability to receive calls from devices that only support numeric dialing. The numbers are in the following pattern:

800xxxx

For URI dialing, the endpoints are assigned the URI in the following pattern:

800xxxx@mmcvd.ciscolabs.com

For business-to-business calls, the example external domain used is:

cisco.com

Deployment Details

This guide is divided into two sections:

1. Deployment tasks for MRA and B2B Collaboration
2. Deployment tasks for SIP trunking to IP PSTN (CUBE)

Section1: Deploy MRA & B2B Collaboration

Core Tasks

Before beginning service-specific configuraiton, complete the following tasks:

1. Installing Cisco Expressway-C and Cisco Expressway-E
2. Configuring CUCM for Expressway

Mobile and Remote access Configuration

For Mobile and Remote access-specific configuration, complete the following tasks:

1. Cisco Expressway-E specific installation tasks
2. Deploying Mobile and Remote access

Business to Business (B2B) Configuration

For B2B specific configuration, complete the following tasks:

3. Deploying B2B

Pre-deployment Checklists and Tasks

Fill in the Easy access configuration sheet for your reference during the deployment process.	**Yes/No**
Establish network connectivity for BE6K server to application and DMZ networks – Refer http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/BE6000/InstallationGuide/10_01/Deploying_Expressway_with_Business_Edition.pdf.	Yes/No
Define the required DNS records on the appropriate DNS servers as specified under the Easy access configuration sheet_DNS records requirements.	Yes/No
Open the firewall ports mentioned as per the Easy access configuration sheet firewall ports requirements	**Yes/No**
Follow the guidelines specified as part of Expressway certificate requirements to be ready to generate and sign the certificates at later stage of deployment process. In addition, arrange for the purchase of a public certificate so that you are ready to generate certificates immediately during the deployment process later.	Yes/No

Easy Access Configuration Sheet

The following tables provide you with a place to capture all the information you may need during the configuration of Cisco Expressway related services. Each table is comprised of the information items needed, references the example values used in this CVD, and provides a column into which you may enter your own particular site-specific values in an easy-reference format.

Table 4. Expressway-C network configuration

Item	CVD Configuration	Site Specific configuration
	Expressway C	Expressway C
IPV4 LAN 1 address	10.106.170.148	
IPV4 LAN 1 subnet	255.255.255.0	
IPV4 gateway	10.106.170.6	
System host name	EXPc1	
Default DNS servers (Local)	10.106.170.130 (Local DNS)	
Domain name	mmcvd.ciscolabs.com	
NTP servers	10.106.170.130	
Time zone	Asia/Calcutta	
IPv4 Static NAT address	NA	

Table 5. Expressway-E Network Configuration

Item	CVD Configuration	Site-specific configuration
	Expressway E	Expressway E
IPV4 LAN 1 address	10.126.69.50	
IPV4 LAN 1 subnet	255.255.255.0	
IPV4 t gateway	10.126.69.49	
System host name	EXPc1	
Default DNS servers (Public DNS)	10.126.69.38 (Public DNS)	
Domain name	mmcvd.ciscolabs.com	
NTP servers	10.106.170.130	
Time zone	Asia/Calcutta	
IPv4 Static NAT address	10.126.69.37	

Table 6. CUCM and CUCM IM&P references

Item	CUCM	Site-specific details
Unified CM publisher address	10.106.170.135	
System name	CUCM-Pub	
Domain name	mmcvd.ciscolabs.com	

Item	CUCM IM&P	Site-specific details
IM and Presence Service database publisher node	10.106.170.194	
IM and Presence publisher System name	IMP2	
Domain name	mmcvd.ciscolabs.com	

DNS SRV Records

Table 7. DNS SRV records (Inside DNS)

Item	CVD Configuration	Site-specific configuration
Domain	mmcvd.ciscolabs.com	
Service	cisco-uds	cisco-uds
Protocol	tcp	Tcp
Priority	10	10
Weight	10	10
Port	8443	8443
Service	cucm-pub.mmcvd.ciscolabs.com	

Table 8. DNS SRV records (Public DNS)

Item	CVD Configuration		Site-specific configuration	
Domain	mmcvd.ciscolabs.com			
Service	collab-edge	sip	collab-edge	sip
Protocol	tls	tcp/udp	Tls	tcp/udp
Priority	10	10	10	10
Weight	10	10	10	10
Port	8443	5060	8443	5060
Service	EXPe1.mmcvd.cisco.com	EXPe1.mmcvd.ciscolabs.com		

i	Tech Tip

SIP SRV records should be defined one each for TCP and UDP and specific to B2B use case only as described in above table 8

The SRV record of Expressway-E on public DNS should reference to DNS A record Expressway-E's statically Nat'ed public IPv4 address.

Firewall port requirements

Table 9. Firewall ports to be opened outbound from Inside to DMZ

Purpose	Protocol	Expressway-C (source)	Expressway-E (listening)
XMPP (IM and Presence)	TCP	Ephemeral port	7400
SSH (HTTP/S tunnels)	TCP	Ephemeral port	2222
Traversal zone SIP signaling	TLS	25000 to 29999	7001
Traversal zone SIP media	UDP	36012 to 59999	36000 to 36001
SIP TCP/TLS	TCP/TLS	25000 to 2999	7011
H323 RAS Assent	UDP	1719	6011
Q.931/H.225 & H.245	TCP	15000 to 19999	2776

Table 10. Firewall ports to be opened outbound from DMZ to public internet

Purpose	Protocol	Expressway-E (source)	Internet endpoint (listening)
SIP media	UDP	36012 to 59999	>=1024
SIP signaling	TLS	25000 to 29999	>=1024

Table 11. Firewall ports to be opened inbound Internet to DMZ

Purpose	Protocol	Internet endpoint (source)	Expressway-E (listening)
XMPP (IM and Presence)	TCP	>=1024	5222
UDS (provisioning/phonebook)	TCP	>=1024	8443
Media	UDP	>=1024	36012 to 59999
SIP signaling	TLS	>=1024	5061

Table 12. Expressway-E management ports to be opened

Purpose	Transport Protocol	Management device source port (inside)	Expressway Destination port
Management	TCP	>=1024	80 / 443 / 22 / 23
SNMP Monitoring	UDP	>=1024	161
Purpose	**Transport Protocol**	**Expressway-E source port**	**PC listening port (inside)**
NTP	UDP	123	123
Syslog	UDP	30000 to 35999	514
DNS	UDP	>=1024	53

Expressway MRA Certificates requirements

The Expressway certificates can be generated using the Certificate Sign Request (CSR) option available on both the Expressway-C and Expressway-E devices. After completing the Installing Cisco Telepresence Expressway C/E tasks below, the administrator can log into the expressway server via web interface and using the CSR utility can generate the certificates. Once the certificates are generated it could be downloaded and be signed by the appropriate Certificate Authority for authentication purposes.

Expressway-C server certificates can be signed by an private CA or optionally by third party public trusted CA

Expressway-E server certificate must be signed by a third party public trusted CA only. Additionally if a DX or 7800/8800 series phone is used for MRA then need to ensure that Expressway-E server certifcate is mandatorily signed by one of the third party public trusted root CA's that's embedded into the endpoint device platform OS certifcate store.

Below table shows Expressway certificate signing request tool prompts for and incorporates the relevant Subject Alternate Name (SAN) as appropriate for the Unified Communications feature to be deployed on the Expressway.

Table 13. CSR SAN Elements

CSR SAN element	Mobile & Remote Access	XMPP federation
Unified CM Registration domains	Expressway-E only	NA
XMPP federation domains	**NA**	**Expressway-E only**
IM & Presence chat node aliases (Federated group chat)	NA	Required
Unified CM phone security phone profile names	Expressway-C only	NA

Table 14. CVD specific CSR SAN Configuration

CSR SAN element	Mobile & Remote Access CVD Configuration		Site Specific Configuration	
	Expressway-C CSR SAN	Expressway-E CSR SAN	Expressway-C CSR SAN	Expressway-E CSR SAN
Additional Alternative names	NA	NA		
Unified CM Registration domains [1]	NA	mmcvd.cisco.com		

IM & Presence chat node aliases (Federated group chat) [2]	NA	NA		
Unified CM phone security phone profile names [3]	NA	NA		

i **Tech Tip**

[1]**Unified CM Registration domains** – you can have FDDN's seperated by commas if you want multiple domains. Select the DNS format and manually specifcy FQDN's. You may optionally chose CollabEdgeDns format if you are not able to include top level company domain. Doing so collab-edge will be prefixed to the top level FQDN.

[2]**IM & Presence chat node aliases** – requred for federated group chat using TLS. A new certificate must be produced if new chat node aliases are added or renamed for both Expressway-C and Expressway-E. Expressway-E certificate should have the same set of chat node aliases entered in its Additional Alternative names field that matches the ones defined on Expressway-C's cetificate

[3]**Unified CM Phone security profile** – This is the phone security profiles defined on Unified CM configured for encrypted TLS and used by the device for remote access. This should be specified in the FQDN format. This enables secure communication between the Unified CM and the Expressway-C. However, for this deployment the traffic between CUCM and Expressway-C is TCP based and hence not required.

Core Tasks

Install Cisco Expressway

Repeat procedures 1 to 5 for Expressway-C and Expressway-E.

PROCESS

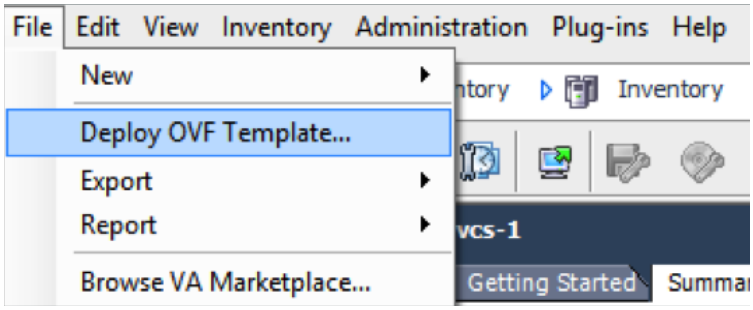
1. Deploy OVA to host
2. Configure the VM guest
3. Obtain Licenses
4. Apply licenses
5. Configure system name, DNS and NTP settings

Procedure 1 Deploy OVA to host

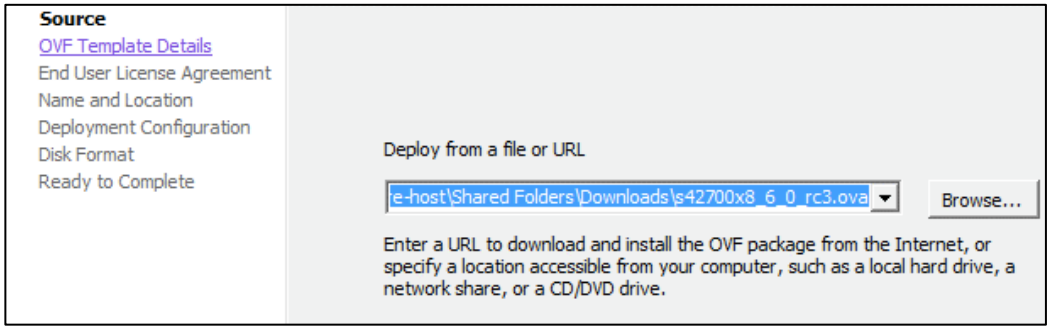
This procedure represents a typical installation. The Deploy OVF Template dynamically changes to reflect host configuration.

Step 1. Log into vSphere to access the ESXi host.

Step 2. Select **File > Deploy OVF Template**.



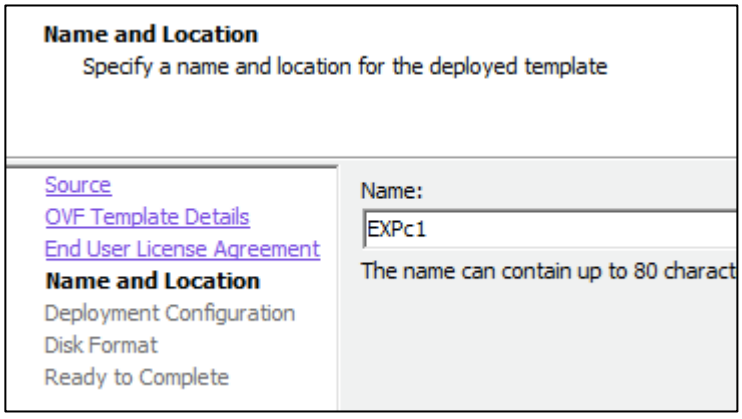
Step 3. Click **Browse**, find the location of the .ova file, click **Open**, and then click **Next**.



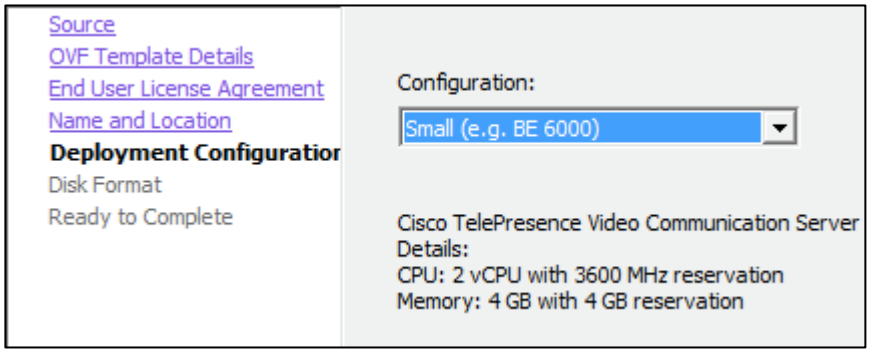
Step 4. On the OVF Template Details page, click **Next**.

Step 5. If an End User License Agreement page appears, read the EULA, click **Accept**, and then **Next**.

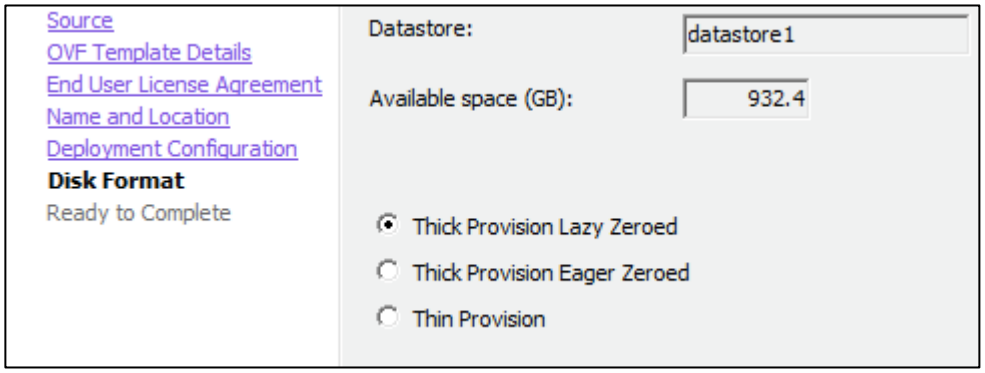
Step 6. On the Name and Location page, enter **the name for the server.**



Step 7. On the Deployment Configuration page, select **Small (e.g. BE 6000)** as the configuration option.

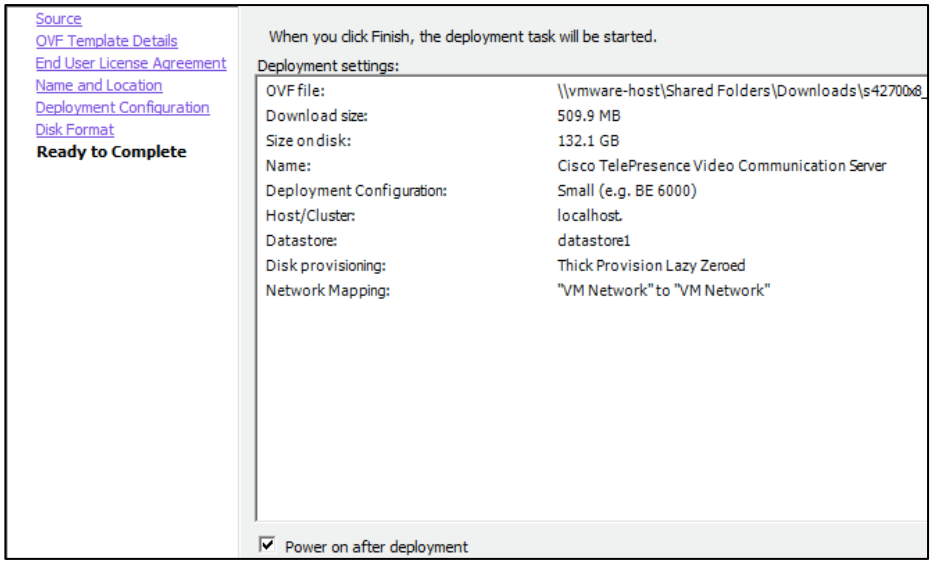


Step 8. On the Disk Format page, ensure that the default disk format of Thick Provision Lazy Zeroed is selected, and then click **Next**.



i	Tech Tip
Because the VM performance may degrade during the resizing of a partition, Thin Provision is not recommended.	

Step 9. On the **Ready to Complete** page, confirm deployment settings. Enable the power on after deployment option and Click **Finish.**



Procedure 2 Configure the VM guest

Step 1. Right-click the VM guest and click **Open Console**. The VM guest will take some time to boot.

Step 2. At the login prompt, enter the username **admin**, and the password **TANDBERG**.

Step 3. At the Install Wizard prompt, type **y**, and then press **Enter**.

Step 4. Using the Install Wizard, enter the information

- Run install wizard- **y**
- Do you wish to change the system password-**y**
- Password- **[Password]**
- IP Protocol- **IPv4**
- IP Address LAN1- **10.106.170.148**
- Subnet Mask LAN1- **255.255.255.128**
- Default Gateway Address-**10.106.170.6**
- Ethernet Speed-**auto**
- Run ssh daemon- **y**

Step 5. Next login as a **root** user and change the default root password. The default root password is **TANDBERG**

The configuration is applied and the Expressway-C/E restarts with the new configuration applied. The system is now ready to be accessed via the web interface for further management and monitoring.

Procedure 3 Obtain Licenses

Step 1. You will need to access Expressway-C and E in turn via a web browser to identify and record the Serial Number

Step 2. Using the serial numbers and the license PAK provided, obtain your licenses via the licensing portal (www.cisco.com/go/license). This will provide your Release and Option keys for the next Procedure.

Procedure 4 Apply licenses

i	Tech Tip
To obtain licenses Refer Appendix 2 of the link - http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/install_guide/Cisco-Expressway-Virtual-Machine-Install-Guide-X8-6.pdf	

Step 1. Navigate to **Maintenance > Option keys**, enter the provided release key, and then click **Set release key**.

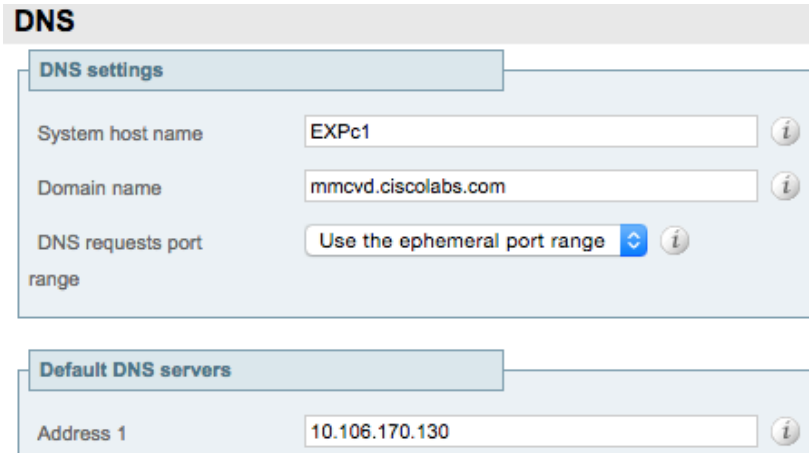
Step 2. For each option key provided, in **Add option key**, enter the option key value, and then click **Add option**.

Step 3. Navigate to **Maintenance > Restart options** and click **Restart**.

Procedure 5 Configure system name, DNS, and NTP settings

Step 1. Navigate to **System > DNS** and in the **DNS settings** section, enter the following values using the Easy Access Configuration Table 1 and Table 2 Leave the other fields as their default values.

- System host name-**EXPc1**
- Domain name-**mmcvd.cisco.com**
- Default DNS servers-**10.106.170.130**



Step 2. Click **Save**.

Step 3. Navigate to **System > Time** and using the Easy access configuration sheet enter the NTP server details:

- NTP servers–**10.106.170.130**

Cisco Expressway-E specific installation tasks

PROCESS

1. Configure static NAT

Expressway-E sits in the DMZ network and is NATed to a publically routable IP. Once NAT is configured on the Expressway-E, all communication to and from Expressway-E will use the NATed IP.

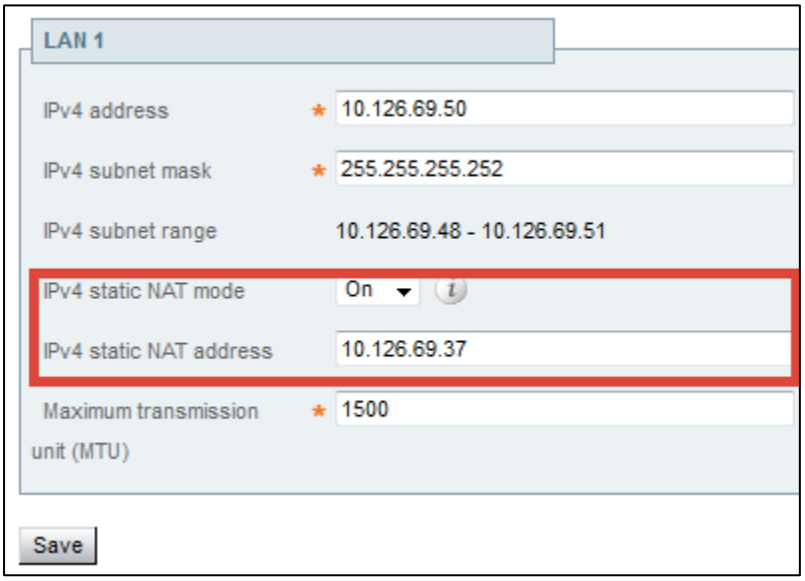
Expressway-E points to a public DNS server on the Internet.

Procedure 1 Configure static NAT

The advanced networking key is needed to enable NAT functionality on Expressway-E.

Step 4. Navigate to **System > IP** and enter the following into the relevant fields. Leave the other fields at their default values.

- Use Dual Network Interfaces–**No**
- IPv4 static NAT mode–**On**
- IPv4 static NAT address*– **10.126.69.37**



Step 5. Click **Save**.

i	Tech Tip
*The static NAT IPv4 address needs to be a publicly routable IPv4 address.	

Configure CUCM for Expressway

PROCESS

1. Configure region for video
2. Configure device pool in CUCM for video and add the video region
3. Select the above device pool for all video endpoints

For the installation and basic configuration of Cisco Unified Communications Manager (CUCM), please refer the Unified Communications Using BE6000 Technology Design Guide.

This process lists the prerequisite configuration on the CUCM before you can start configuring either, mobile and remote access or business-to-business communications.

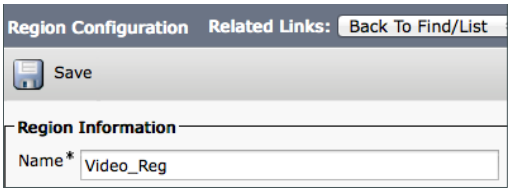
Procedure 1 Configure region for video

First, you log in to Cisco Unified Communications Manager Administration page and create a separate region for video traffic to allow more bandwidth for intra or inter region calls.

Step 1. Navigate to **System > Region Information > Region** and click **Add New**.

Step 2. Enter the following:

- Name—**Video_Reg**

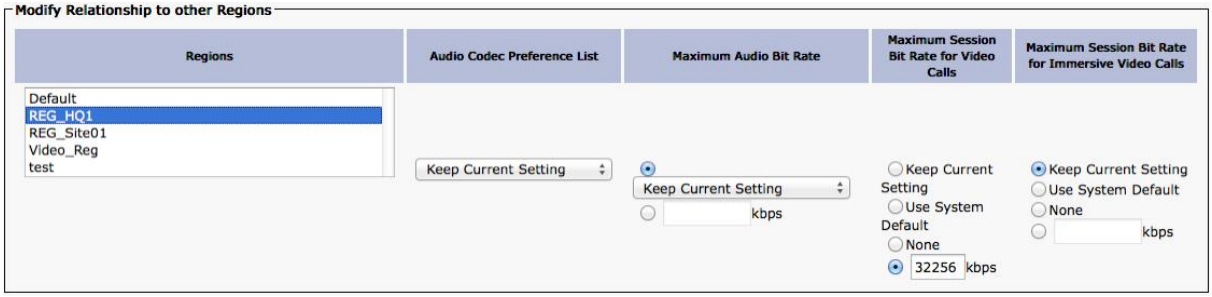


Step 3. Click **Save**.

Step 4. Under Regions, select **REG_HQ1**.

Step 5. Enter the following:

- Maximum Session Bit Rate for Video Calls—32256

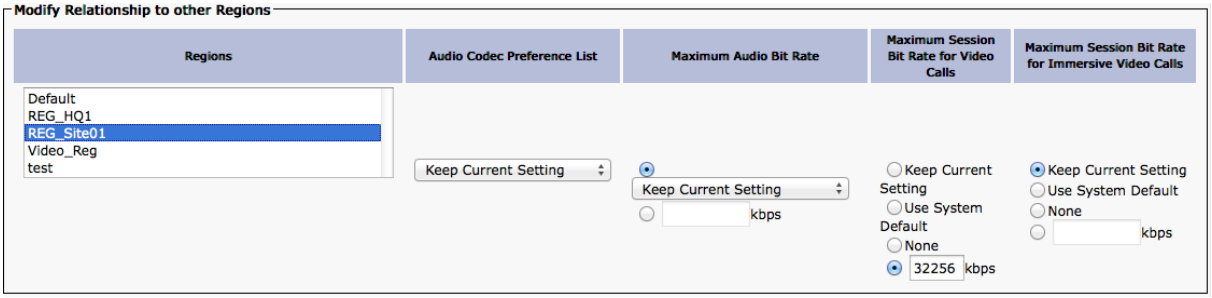


Step 6. Click **Save**.

Step 7. Under Regions, select **REG_Site01**.

Step 8. Enter the following:

- Maximum Session Bit Rate for Video Calls—**32256**



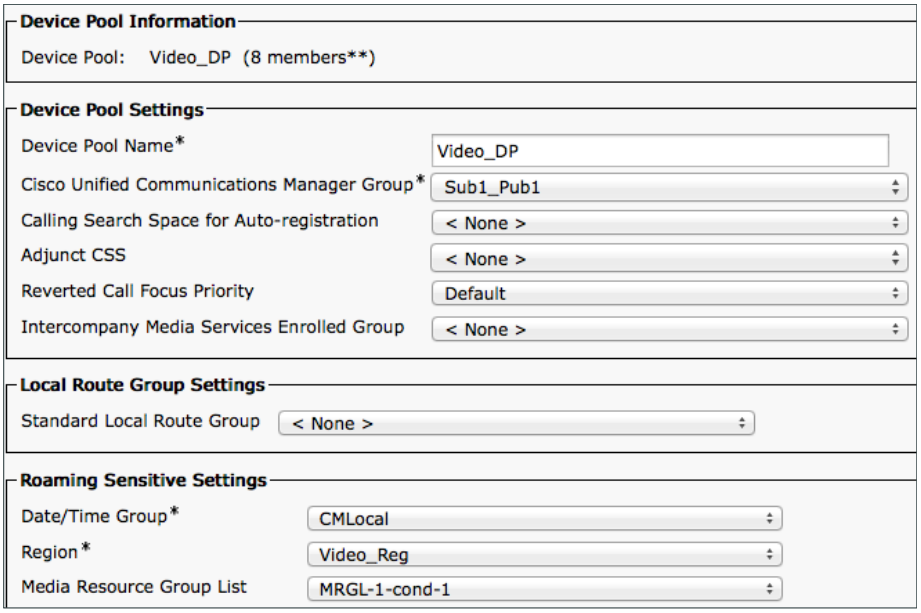
Step 9. Click **Save**.

Procedure 2 Configure device pool in CUCM for video and add the video region

Step 1. Navigate to **System > Device Pool** and click **Add New**.

Step 2. Enter the following into the relevant fields, leaving the other fields at their default values:

- Device Pool Name–**Video_DP**
- Date/Time Group–**CMLocal**
- Region–**Video_Reg**



Step 3. Click **Save**.

Procedure 3 Select the above device pool for all video endpoints

Step 1. Navigate to **Device > Phone**, click **Find**, and select the video endpoint.

Step 2. In Device Pool, select **Video_DP**

Step 3. Click **Save**.

Step 4. Click **Apply Config**.

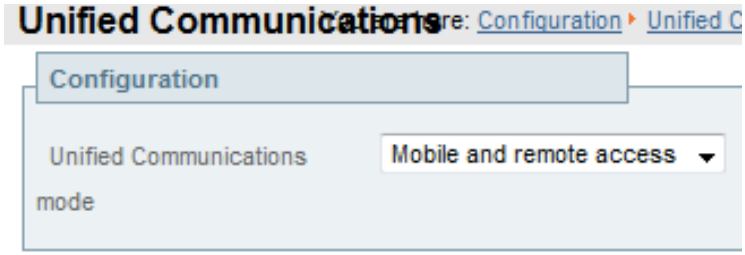
Deploy Mobile and Remote Access

PROCESS

1. Configure Expressway-C for Mobile and Remote Access
2. Discover Unified CM and IM&P server on Expressway-C
3. Configure Expressway-E for Unified CM
4. Configure server certificates and CA certificates on the Expressway-C
5. Configure server certificates and CA certificates on the Expressway-E
6. Configure Unified Communications traversal zone on Expressway-C
7. Configure credentials on Expressway-E
8. Configure traversal server zone on Expressway-E

Procedure 1 Configure Expressway-C for Mobile and Remote access

Step 1. Navigate to **Configuration > Unified Communications > Configuration** and set **Mobile and Remote Access** to **On**.

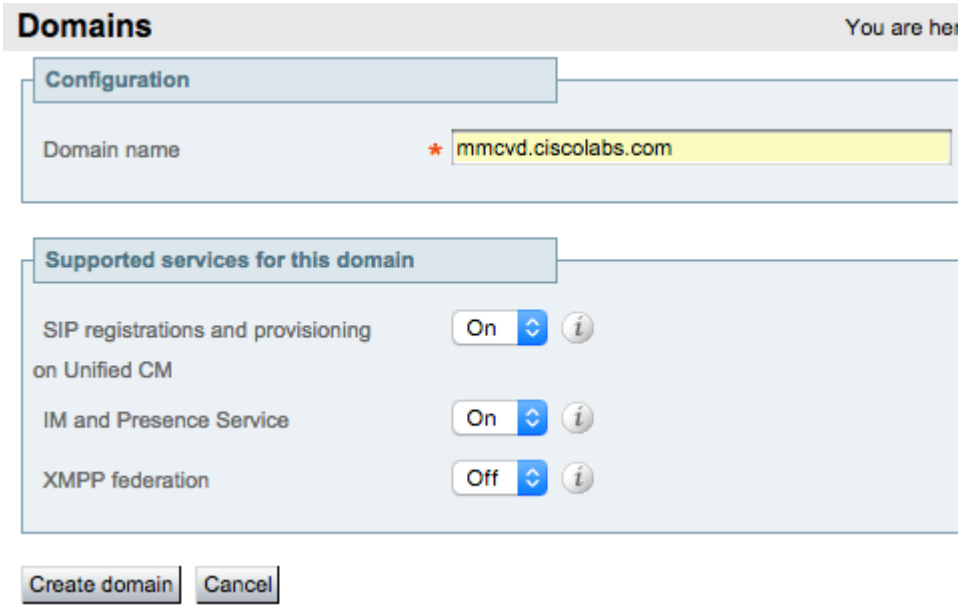


Step 2. Click **Save**.

Step 3. Navigate to **Configuration > Domains** and click **New**.

Step 4. Enter the following values in the relevant fields:

- Domain name—**mmcvd.cisco.com**
- SIP registrations and provisioning on Unified CM—**On**
- IM and Presence services on Unified CM—**On**



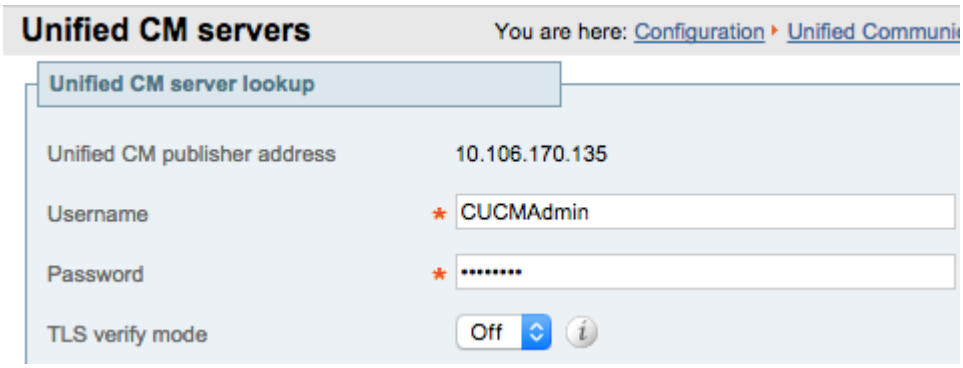
Step 5. Click **Create Domain**.

Procedure 2 Discover Unified CM and IM&P server on Expressway-C

Step 1. Navigate to **Configuration > Unified Communications > Unified CM Servers**, and then click **New**.

Step 2. Enter the following values in the relevant fields:

- Unified CM publisher address– **10.106.170.135**
- Username–**CUCMAdmin**
- Password–**[Password]**
- TLS verify mode–**Off**[1]



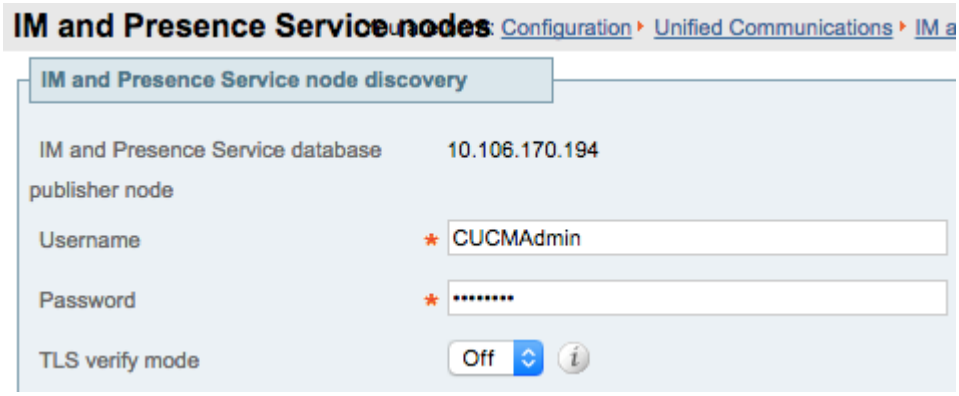
Step 3. Click **Add Address**.

Next, you configure the IM&P server for remote access.

Step 4. Navigate to **Configuration > Unified Communications > IM and Presence servers**, and then click **New**.

Step 5. Enter the following values in the relevant fields:

- IM and Presence publisher address—**10.106.170.194**
- Username—**CUCMAdmin**
- Password—**[Password]**
- TLS verify mode—**Off**[1]

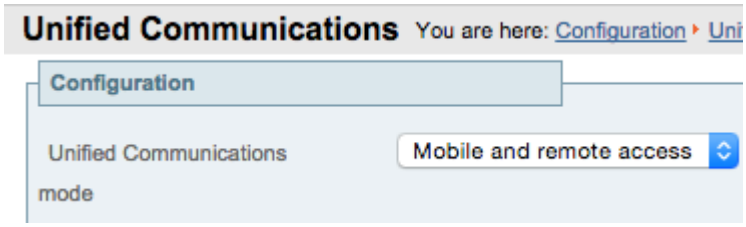


Step 6. Click **Add Address.**

	Tech Tip
[1]The TLS verify mode can be turned on if we provide in the address field FQDN names of CUCM and CUCM IM&P respectively. In addition, the tomcat certificates of the both servers needs to be trusted by the Expressway-C	

Procedure 3 Configure Expressway-E for Mobile and Remote access

Step 1. Navigate to **Configuration > Unified Communications > Configuration**, and then set **Mobile and remote access** to **On**.

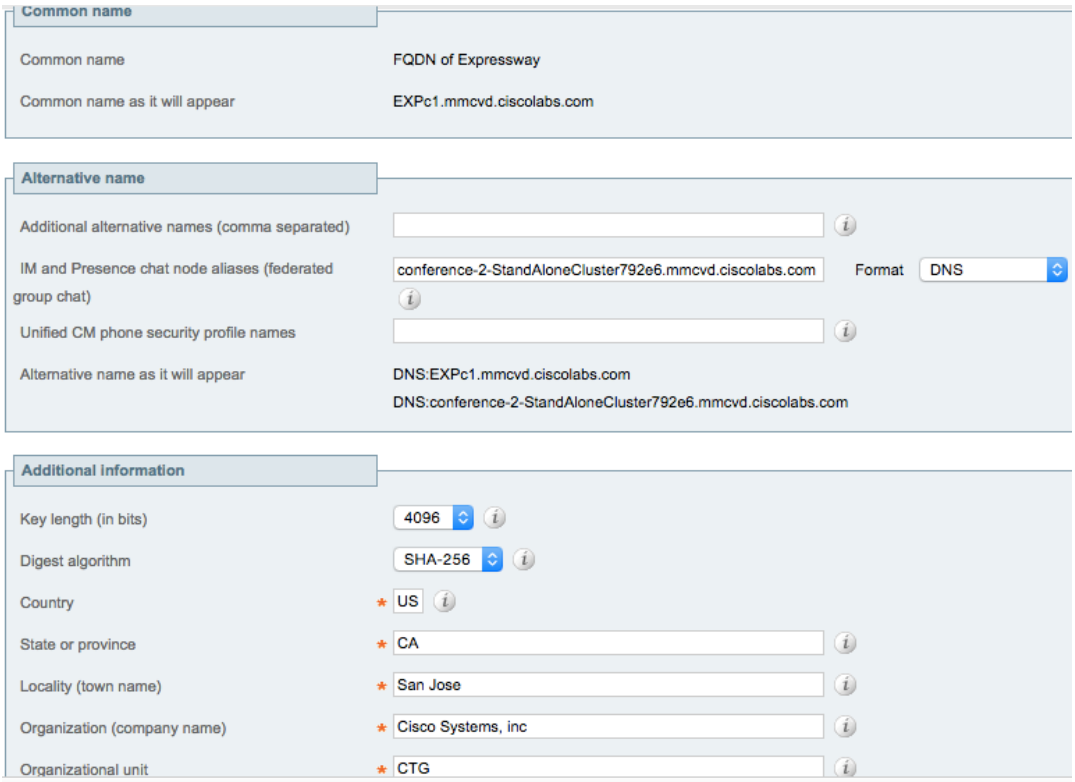


Step 2. Click **Save**.

Procedure 4 Configure server certificates and CA certificates on the Expressway-C

Step 1. To generate a CSR, navigate to **Maintenance > Security certificates > Server certificate, fill the below fields and leave rest at their defaults.** Next, click **Generate CSR.**

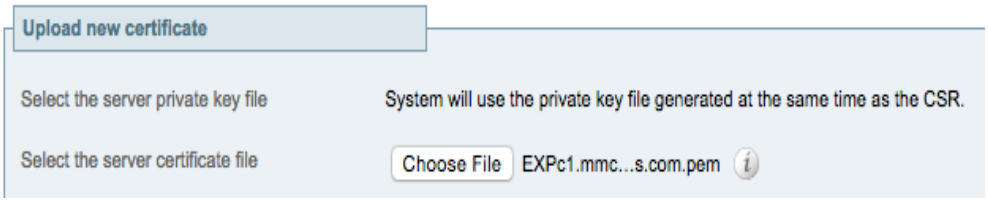
- Additional Information
  - Key length (in bits)-**4096**
  - Digest Algorthm -**SHA256**
  - Country- **US**
  - State or province - **California**
  - Locality (town name)-**San jose**
  - Organization (Company name)- **Cisco**
  - Organizational unit- **CTG**



Step 2. Then Click **Generate CSR**. Once the certificate is generated, download the .PEM file, rename the file to the .cer format if required and get it signed by your private CA.

Step 3. Next, obtain your private root Certificate Authority (CA) certificates and public root CA certificates uesd to sign your Expressway-C and Expressway-E respectively. These needs to be uploaded on to the Expressway-C, navigate to **Maintenance > Security certificates > Trusted CA certificate Choose the private root CA certificate file and click Append CA certificate**

Step 4. Next, navigate to **Maintenance** > **Security Certificates** > **Server certificate**. Click on the choose file and select the signed certificate to be uploaded in step 2. Then click the Upload New Certificate to upload the new server certificate.



Procedure 5	Configure server certificates and CA certificates on the Expressway-E

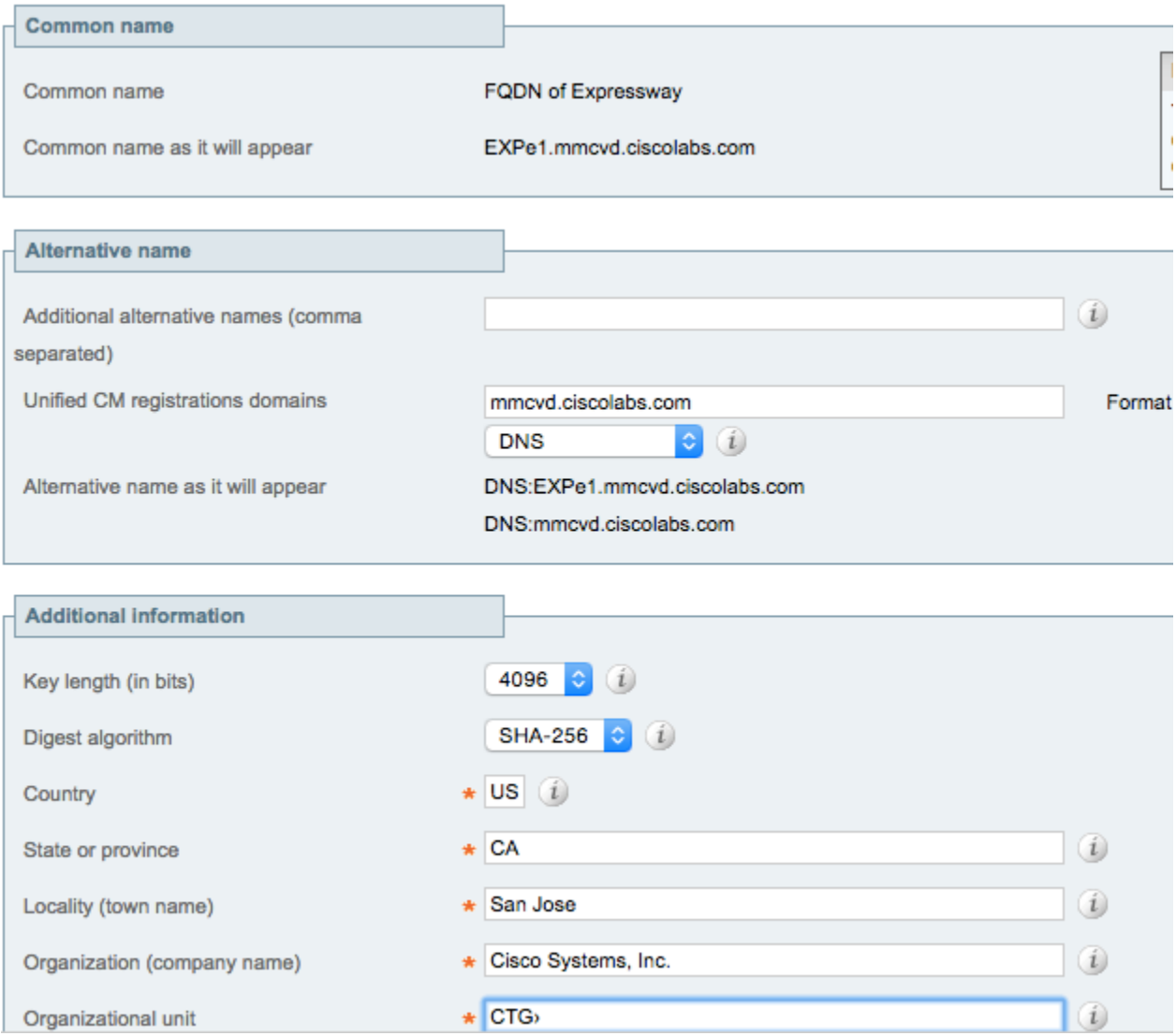
Remote and mobile clients must verify (by validating the server certificate) the identity of the Expressway-E to which they are connecting. To do this, in their list of trusted CAs, the clients must have the certificate authority that was used to sign the Expressway-E's server certificate.

This design requires secure communications between Expressway-C and Expressway-E, as well as between Expressway-E and endpoints located outside the enterprise.

Step 1. To generate a CSR, navigate to **Maintenance > Security certificates > Server certificate**, fill the below fields leaving other at default. Next, click **Generate CSR**.

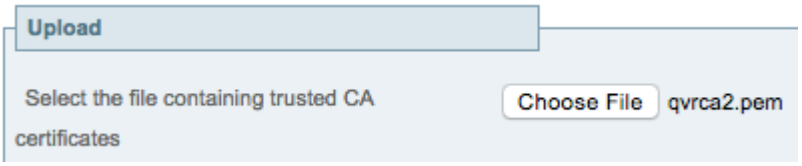
- Under Alternative name
  - Unified CM registrations domains-**mmcvd.cisco.com**

- Additional Information
  - Key length (in bits)-**2046**
  - Digest Algorthm-**SHA256**
  - Country-**US**
  - State or province-**California**
  - Locality (town name)-**San jose**
  - Organization (Company name)- **Cisco**
  - Organizational unit-**CTG**

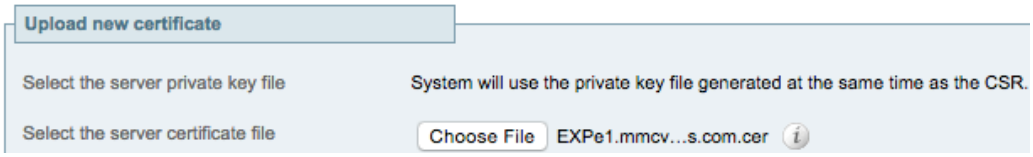


Step 2. Once the certificate request is generated via the Generate CSR, download the .PEM file to be sent for signing to the public CA.

Step 3. Next, obtain your private root Certificate Authority (CA) certificates and public root CA certificates uesd to sign your Expressway-C and Expressway-E respectively. Both needs to be uploaded on to the Expressway-E as well, navigate to **Maintenance > Security certificates > Trusted CA certificate. Choose the private root CA certificate file and click Append CA certificate.**



Step 4. Next, navigate to **Maintenance** > **Security Certificates** > **Server certificate**. Click on the *choose file* and select the server certificate signed by the public CA to be uploaded. Then click on the **Upload New certificate**.



Procedure 6 Configure Unified Communications traversal zone on Expressway-C

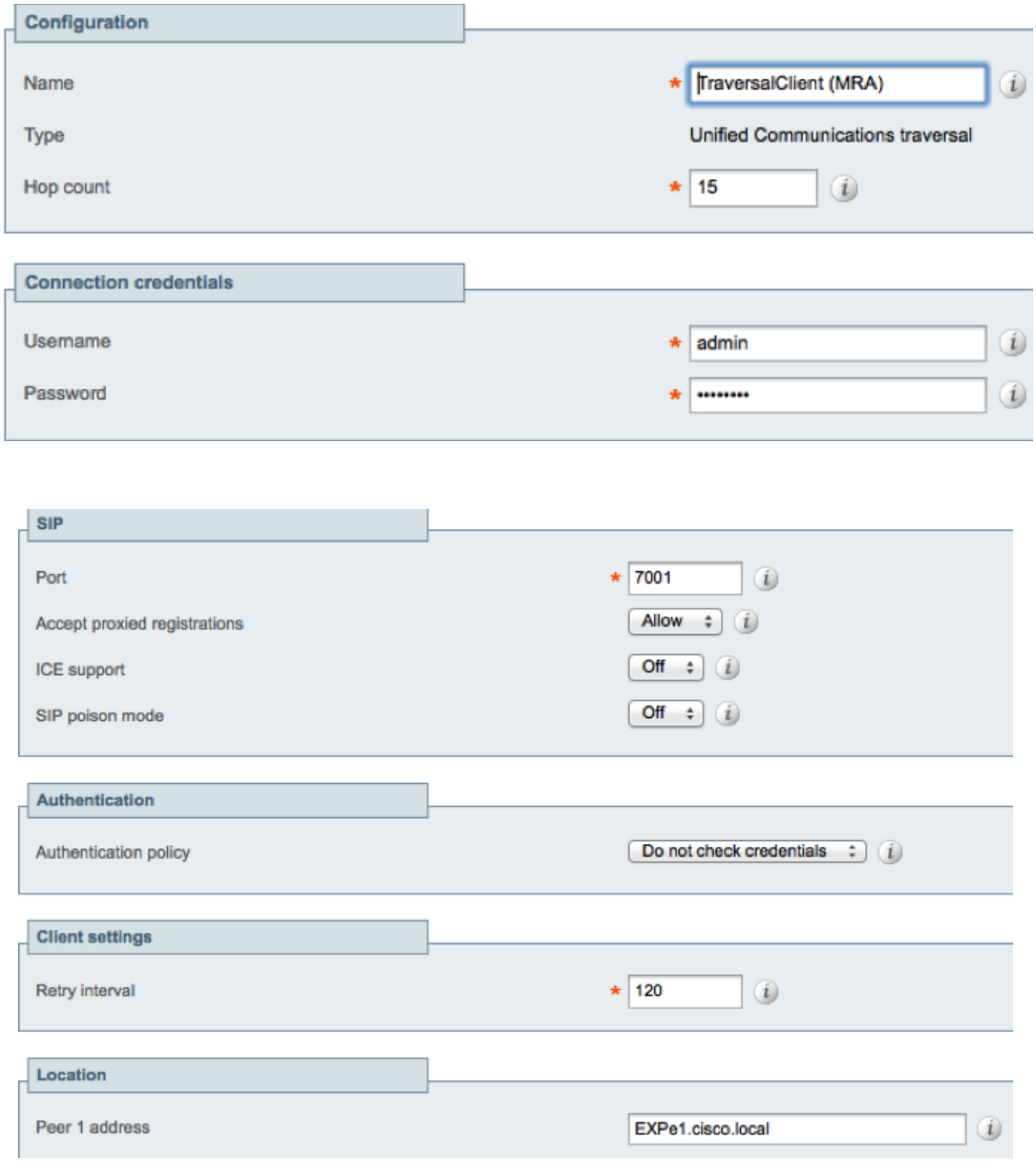
Step 1. Navigate to **Configuration > Zones > Zones** and click **New**.

Step 2. Enter the following into the relevant fields, leaving the other fields at their default values:

- Under Configuration:
  - Name–**TraversalClient (MRA)**
  - Type–**Unified Communications traversal**
- Under Connection credentials:
  - Username–**admin**
  - Password–**[password]**
- Under SIP:
  - Port–**7001**
  - Accept proxied registrations–**Allow**
  - Mobile and remote access–**Yes**
  - ICE support–**Off**
  - Poison mode–**Off**
- Under Location:
  - Peer 1 address–**EXPe1.mmcvd.ciscolabs.com**

Tech Tip

The FQDN in the peer address should resolve to the Expressway-E NAT public IP address to engage NAT reflection. Hence the DNS used by Expressway-C should resolve the Expressway-E hostname to Expressaway-E NAT IP address



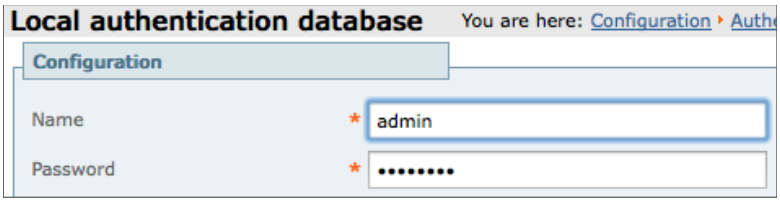
Step 3. Click **Create zone**.

Procedure 7 Configure the credentials on Expressway-E

Step 1. Navigate to **Configuration > Authentication > Local database** and click **New**.

Step 2. Enter the following values in the relevant fields:

- Name–**admin**
- Password–**[password]**



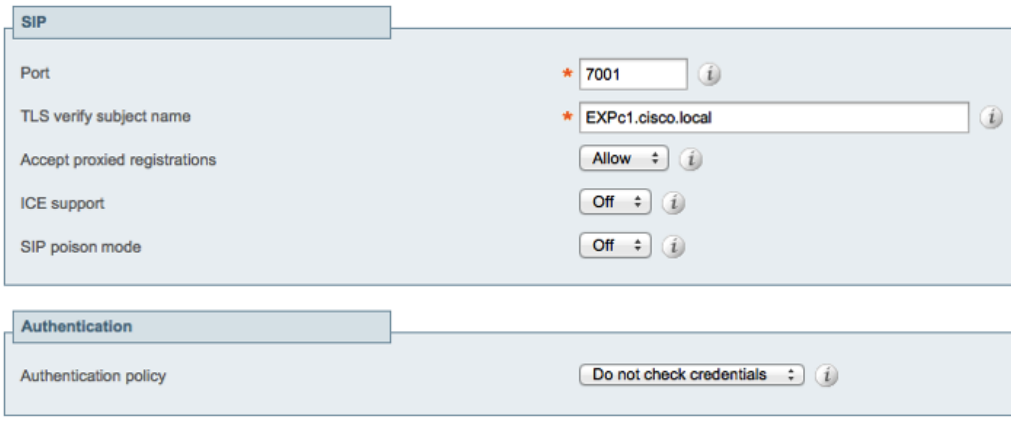
Step 3. Click **Create credential**.

Procedure 8 Configure traversal server zone on Expressway-E

Step 1. Navigate to **Configuration > Zones > Zones** and click **New**.

Step 2. Enter the following into the relevant fields, leaving the other fields at their default values:

- Under Configuration section
  - Name–**TraversalServer (MRA)**
  - Type–**Unified Communication Traversal**
- Under Connection credentials
  - Username–**admin**
- Under SIP section
  - Port–**7001**
  - Accept Proxied Registrations–**Allow**
  - TLS verify subject name–**EXPc1.mmcvd.ciscolabs.com**
  - ICE support–**Off**
  - Poison mode–**Off**

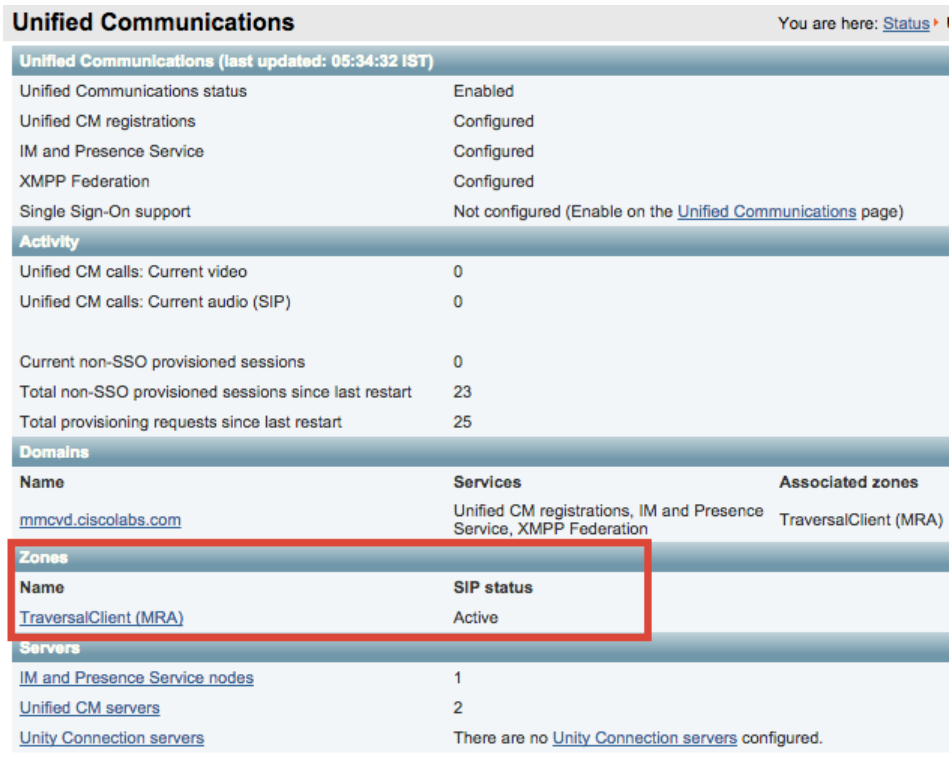


Step 3. Click **Create zone**.

Mobile and remote access is now configured. You can now go to Expressway –C and Expressway –E web interface and check under the **Status** > **Unified Communication status** > to confirm the traversal link is established and all services have been configured

Figure 5. Expressway-C Unified Communication status

Figure 6. Expressway-E Unified Communication status



Unified Communications — You are here: Status

Unified Communications (last updated: 05:34:32 IST)	
Unified Communications status	Enabled
Unified CM registrations	Configured
IM and Presence Service	Configured
XMPP Federation	Configured
Single Sign-On support	Not configured (Enable on the Unified Communications page)
Activity	
Unified CM calls: Current video	0
Unified CM calls: Current audio (SIP)	0
Current non-SSO provisioned sessions	0
Total non-SSO provisioned sessions since last restart	23
Total provisioning requests since last restart	25

Domains

Name	Services	Associated zones
mmcvd.ciscolabs.com	Unified CM registrations, IM and Presence Service, XMPP Federation	TraversalClient (MRA)

Zones

Name	SIP status
TraversalClient (MRA)	Active

Servers

IM and Presence Service nodes	1
Unified CM servers	2
Unity Connection servers	There are no Unity Connection servers configured.

Deploy B2B Collaboration

PROCESS

1. Configure SIP trunk security profile on CUCM for Cisco Expressway-C
2. Configure SIP trunk on CUCM to Expressway-C
3. Configure SIP route pattern on CUCM for B2B
4. Configure firewall
5. Configure neighbor zone on Expressway-C for CUCM
6. Configure traversal client on Expressway-C
7. Configure search rules on Expressway-C
8. Configure transform on Expressway-C
9. Configure traversal server zone on Expressway-E
10. Configure DNS zone on Expressway-E
11. Configure search rules on Expressway-E
12. Configure transform on Expressway-E

Procedure 1 Configure SIP trunk security profile on CUCM for Cisco Expressway-C

For B2B calls to be routed, you must create a SIP trunk between CUCM and Expressway-C.

In this design, the Expressway-C is already configured for mobile and remote access. Port 5060 is used for line-side registrations of endpoints in mobile and remote access scenario. A SIP trunk cannot be formed between Expressway-C and CUCM by using port 5060 because the CUCM cannot accept line-side and trunk-side communication from the same device using the same port.

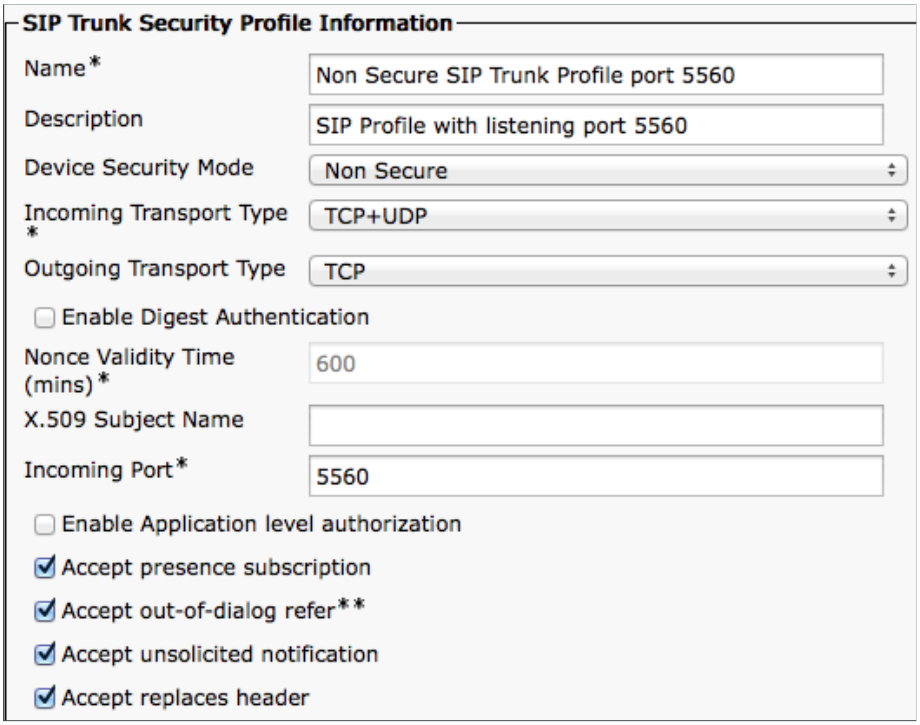
Thus the SIP trunk from Expressway-C to CUCM has to use another SIP port on the CUCM incoming side. This design uses **5560** as the SIP trunk incoming port. You can change the SIP incoming port by creating a new SIP trunk security profile and assigning this profile to the SIP trunk created between CUCM and Expressway-C.

Step 1. Navigate to **System** > **Security** > **SIP Trunk Security Profile** and click Add New.

Step 2. Enter the following values in the relevant fields:

- Name—**Non Secure SIP Trunk Profile port 5560**
- Description—**SIP Profile with listening port 5560**
- Incoming Port—**5560**

- Accept presence subscription—**Selected**
- Accept out-of-dialog refer—**Selected**
- Accept unsolicited notification—**Selected**
- Accept replaces header—**Selected**



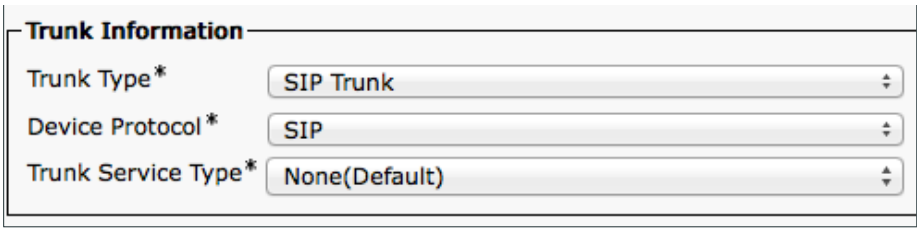
Step 3. Click **Save**.

Procedure 2 Configure SIP trunk on CUCM to Cisco Expressway-C

Step 1. Navigate to **Device > Trunk** and click **Add New**.

Step 2. Enter the following:

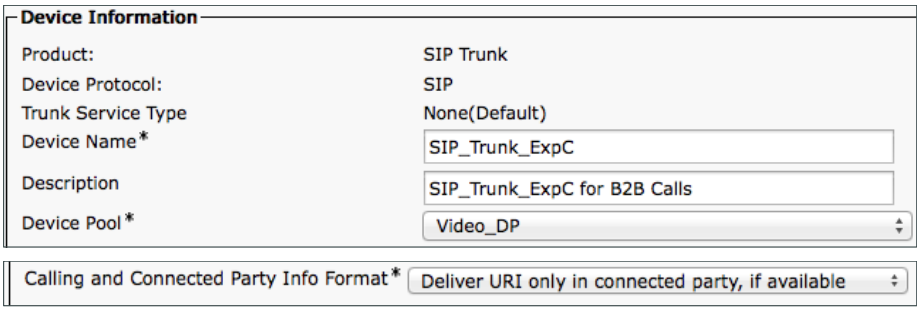
- Trunk Type—**SIP Trunk**
- Device Protocol—**SIP**
- Trunk Service Type—**None (Default)**

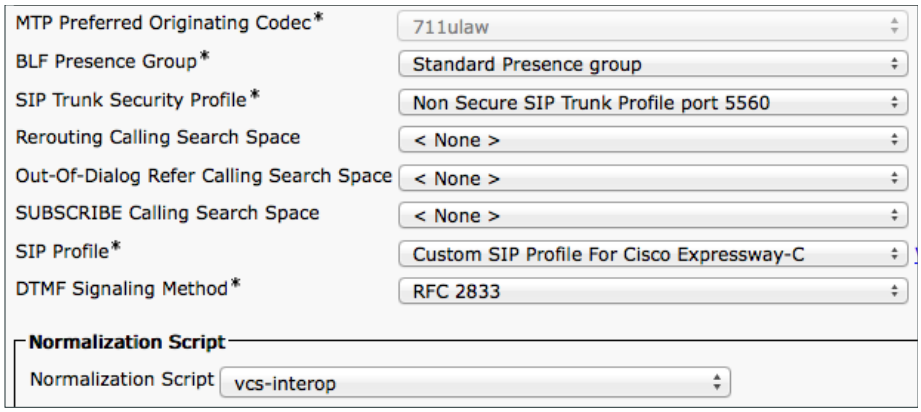


Step 3. Click **Next**.

Step 4. Enter the following into the relevant fields. Leave the other fields at their default values.

- Device Name–**SIP_Trunk_ExpC**
- Description–**SIP_Trunk_ExpC for B2B Calls**
- Device Pool–**Video_DP**
- Calling and Connected Party Info Format–**Deliver URI only in connected party, if available**
- Destination Address–**[Expressway-C IPv4 address]**
- Destination port-**5060**
- SIP Trunk Security Profile–**Non Secure SIP Trunk Profile port 5560**
- SIP Profile–**Standard SIP profile for VCS**
- DTMF Signaling Method–**RFC 2833**
- Normalization Script–**vcs-interop**





Step 5. Click **Save**.

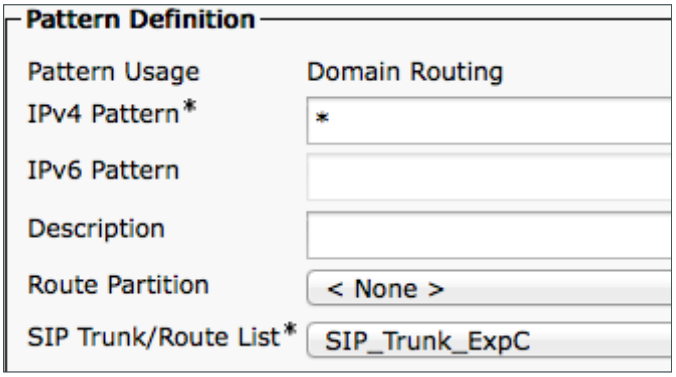
Procedure 3 Configure SIP route pattern on CUCM for B2B

The following SIP route pattern is configured to route all B2B calls towards the Expressway-C, which doesn't match any existing route patterns.

Step 1. Navigate to **Call Routing > SIP Route Pattern** and click **Add New**.

Step 2. Enter the following into the relevant fields, leaving the other fields at their default values:

- Pattern Usage—**Domain Routing**
- IPv4 Pattern—*****
- SIP Trunk/Route List—**SIP_Trunk_ExpC**



Step 3. Click **Save**.

Procedure 4 Configure firewall

The firewall must be configured to allow traffic on following ports between your inside network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located) and between the DMZ and the public Internet as per the easy access configuration firewall port requirements

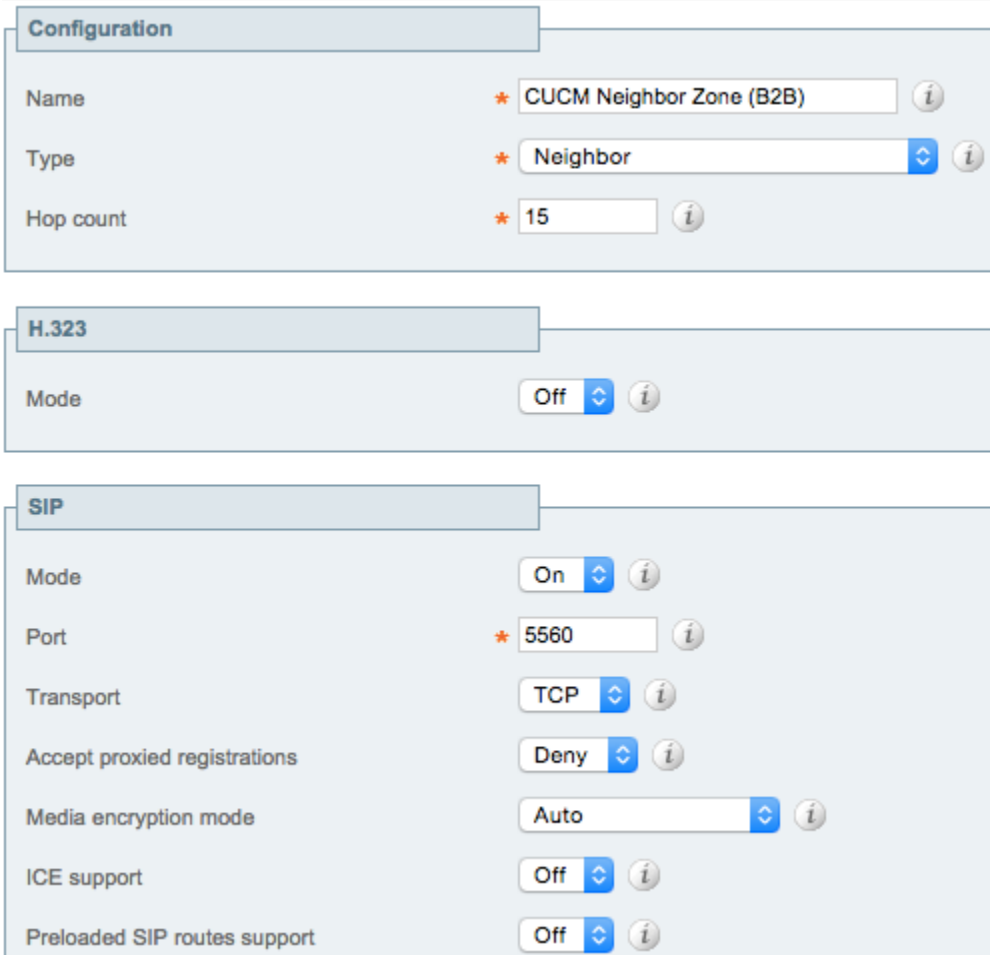
Procedure 5 Configure neighbor zone on Expressway-C for CUCM

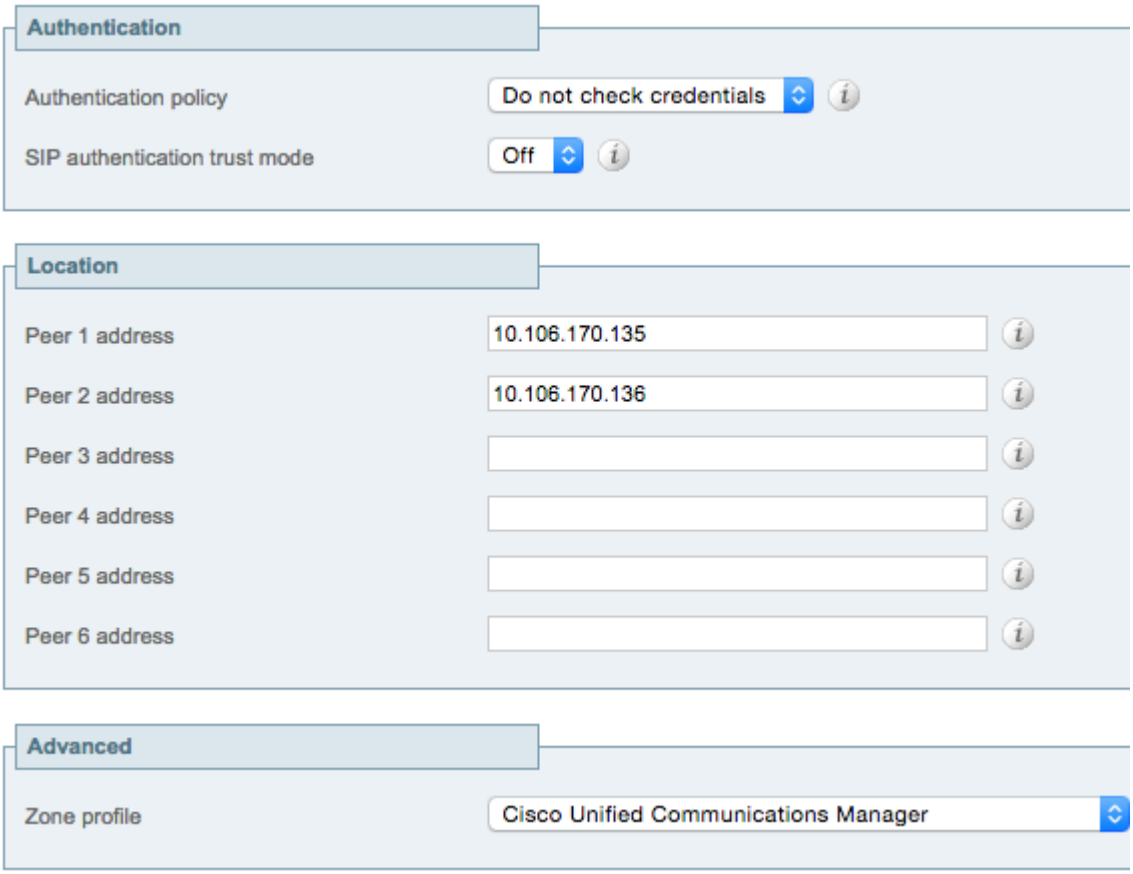
Step 1. Navigate to **Configuration > Zones > Zones** and click **New**.

Step 2. Enter the following into the relevant fields:

- Name—**CUCM Neighbor Zone (B2B)**

- Type–**Neighbor**
- H.323 Mode–**Off**
- SIP Mode–**On**
- Port–**5560**
- Transport–**TCP**
- Peer 1 Address–**10.106.170.135**
- Peer 2 Address–**10.106.170.135**
- Zone Profile–**Cisco Unified Communications Manager**





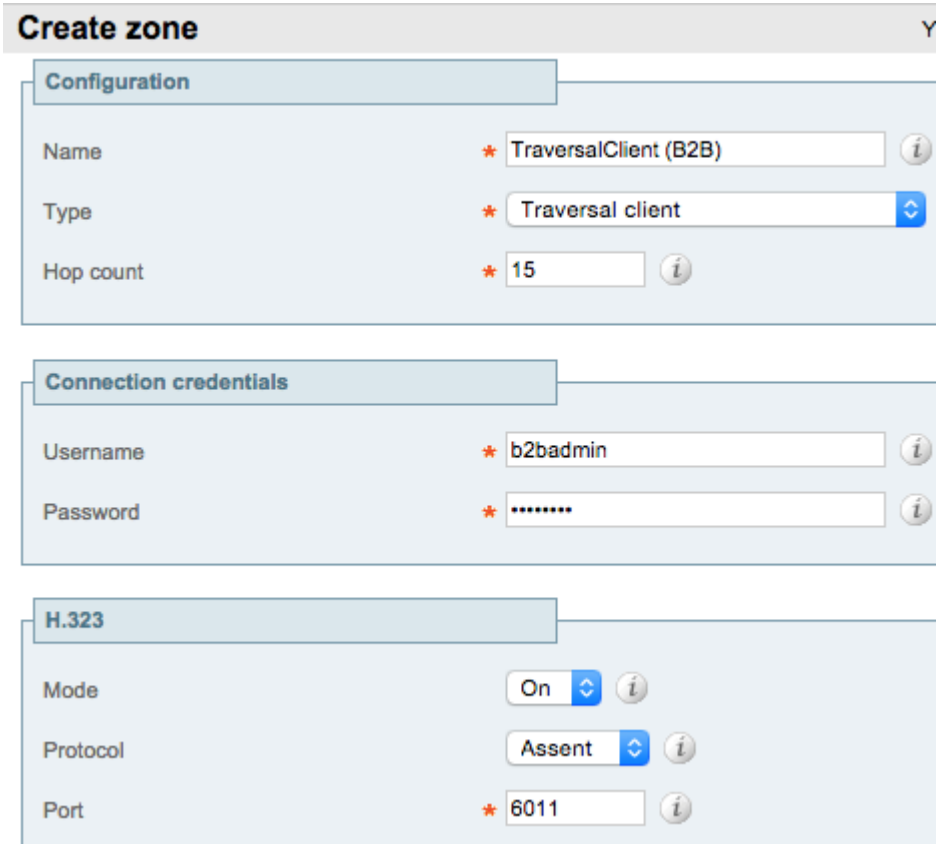
Step 3. Click **Create Zone**.

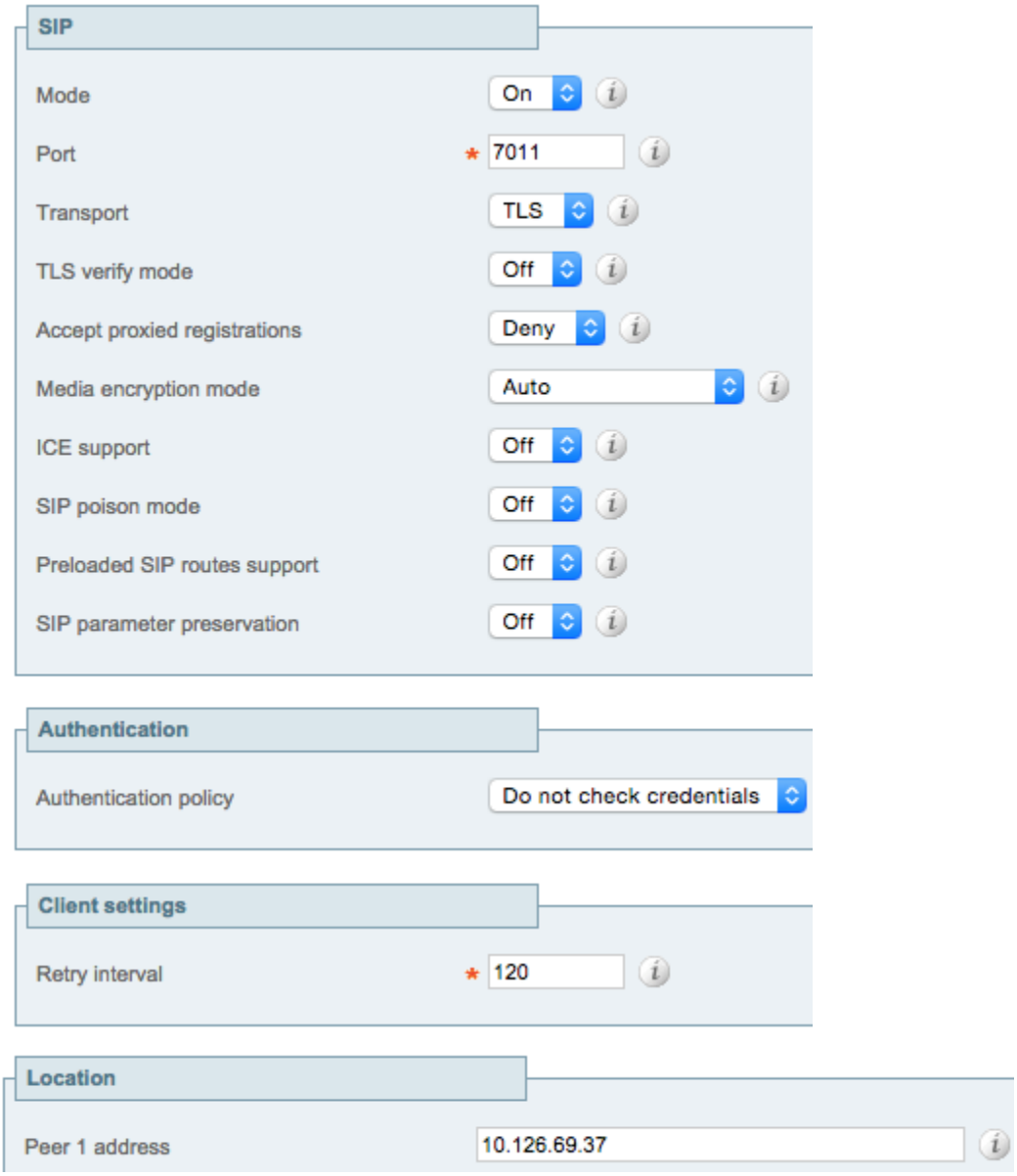
Procedure 6 Configure traversal client zone on Expressway-C

Step 1. Navigate to **Configuration > Zones > Zones**, and then click **New**.

Step 2. Enter the following into the relevant fields, leaving the other fields at their default values:

- Name–**TraversalClient (B2B)**
- Type–**Traversal Client**
- Username–**b2badmin**
- Password–**[Password]**
- H.323 Port–**6011**
- SIP Port–**7011**
- Transport–**TLS**
- Peer 1 Address–**10.126.69.37**


Create zone
Configuration
Name
TraversalClient (B2B)
Type
Traversal client
Hop count
15
Connection credentials
Username
b2badmin
Password
H.323
Mode
On
Protocol
Assent
Port
6011



Step 3. Click **Create Zone**.

Procedure 7 Configure search rules on Expressway-C

Step 1. Navigate to **Configuration > Dial Plan > Search Rules**, and click **New**.

Step 2. Enter the following into the relevant fields, leaving the other fields at their default values:

- Rule Name—Outbound **B2B**

- Description—Outbound **B2B calls**
- Priority—**101**
- Mode—**Alias Pattern Match**
- Pattern type—**Regex**
- Pattern String**-(?!.*@mmcvd.ciscolabs.com.*$)(.*)**
- Pattern Behavior—**Leave**
- On Successful Match—**Stop**
- Target—**TraversalClient (B2B)**
- State—**Enabled**

Step 3. Click **Create Search Rule**.

Step 4. Click **New**.

Step 5. Enter the following into the relevant fields, leaving other fields at their default values:

- Rule Name—Inbound **B2B**
- Description—Inbound **B2B**
- Priority—**100**
- Mode—**Alias Pattern Match**
- Pattern type—**Regex**
- Pattern String**—(.*)(@mmcvd.ciscolabs.com).***
- Pattern Behavior—**Replace**
- Replace String**—\1\2**
- On Successful Match—**Stop**
- Target—**CUCM Neighbor Zone (B2B)**
- State—**Enabled**

Step 6. Click **Create Search Rule**.

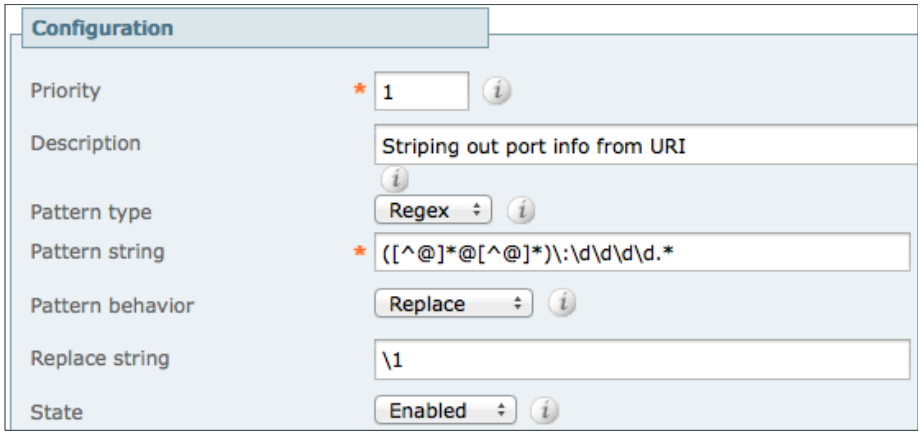
Procedure 8 Configure transform on Expressway-C

Step 1. Navigate to **Configuration > Dial Plan > Transforms** and click **New**.

Step 2. Enter the following into the relevant fields:

- Priority—**1**

- Description–**Striping out port info from URI**
- Pattern type–**Regex**
- Pattern string–**([^@]*@[^@]*)\:\d\d\d\d.***
- Pattern behavior–**Replace**
- Replace string–**\1**
- State–**Enabled**



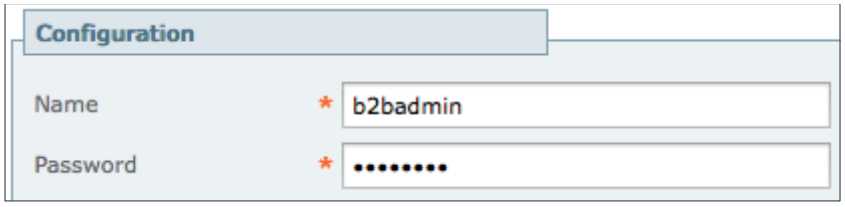
Step 3. Click **Create Transform**.

Procedure 9 Configure traversal server zone on Expressway-E

Step 1. Navigate to **Configuration > Authentication > Devices > Local Database** and click **New**.

Step 2. Enter the following into the relevant fields:

- Name–**b2badmin**
- Password–**[Password]**



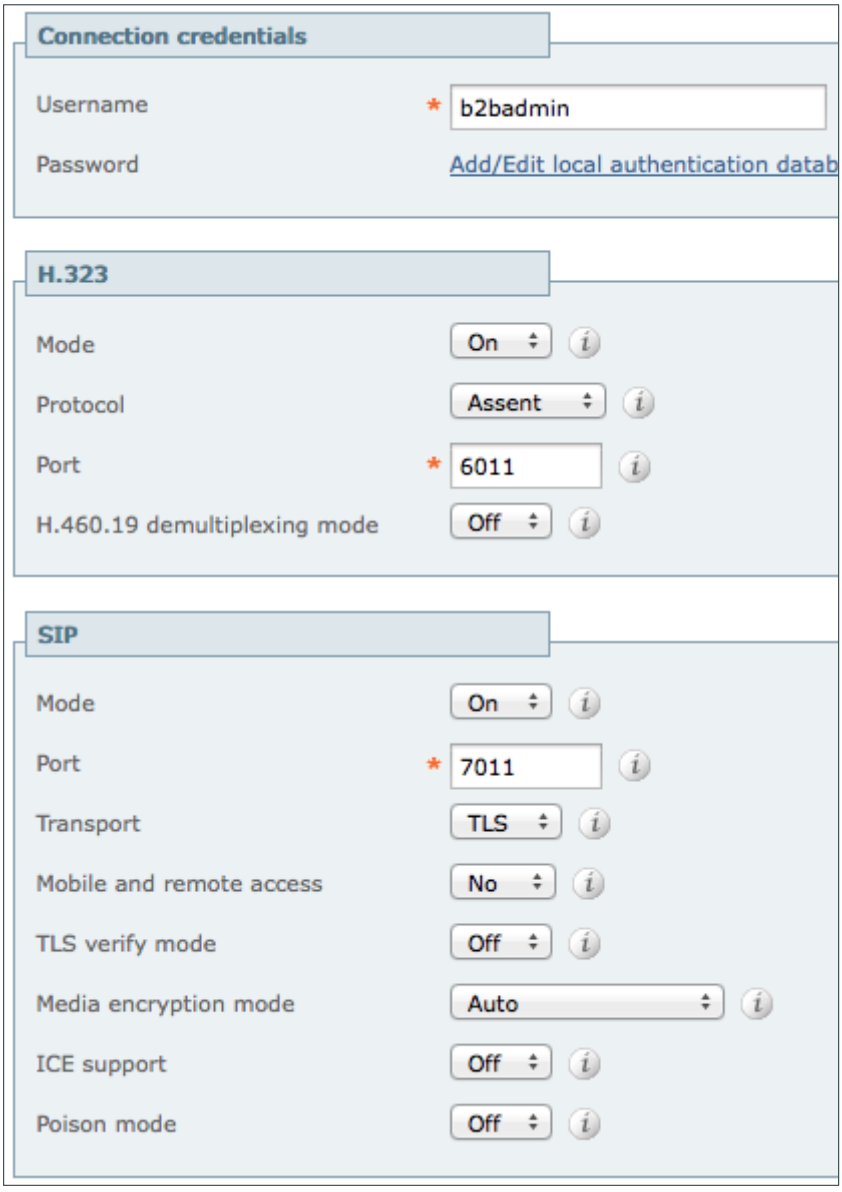
Step 3. Click **Create credential**.

Step 4. Navigate to **Configuration > Zones > Zones** and click **New**.

Step 5. Enter the following into the relevant fields, leaving other fields at their default values:

- Name–**TraversalServer (B2B)**
- Type–**Traversal Server**

- Username—**b2badmin**
- H.323 Port—**6011**
- SIP Port—**7011**
- Mobile and remote access—**No**
- Transport—**TLS**



Step 6. Click **Create Zone**.

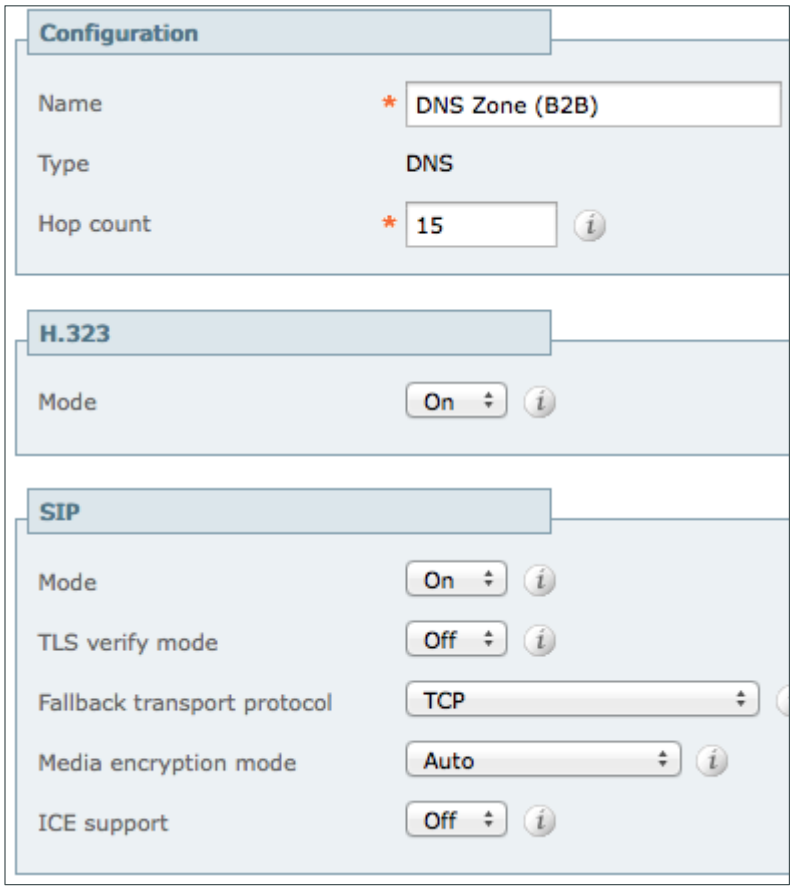
Procedure 10 Configure DNS zone on Expressway-E

For a B2B call, the Expressway-E doesn't need to have established peering relationships with remote domains. Rather, the Expressway-E routes calls to remote domains via information discovered in public DNS. Using DNS enables open video federation.

Step 1. Navigate to **Configuration > Zones > Zones** and click **New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Name—**DNS Zone (B2B)**
- Type—**DNS**
- H.323 Mode—**On**
- SIP Mode—**On**
- Fallback Transport Protocol—**TCP**



Step 3. Click **Create Zone**.

Procedure 11 Configure search rules on Expressway-E

Step 1. Navigate to **Configuration > Dial Plan > Search Rules**, and click **New**.

Step 2. Enter the following into the relevant fields, leaving other fields at their default values:

- Rule Name– Outbound **B2B_**
- Description**Outbound B2B calls**
- Priority–**101**
- Mode–**Alias Pattern Match**
- Pattern type–**Regex**
- Pattern String**–(?!.*@mmcvd.ciscolabs.com$).***
- Pattern Behavior–**Leave**
- On Successful Match–**Stop**
- Target–**DNS Zone (B2B)**
- State–**Enabled**

Step 3. Click Create Search Rule.

Step 4. Click New.

Step 5. Enter the following into the relevant fields, leaving other fields at their default values:

- Rule Name– Inbound **B2B_**
- Description–Inbound **B2B calls to mmcvd.ciscolabs.com**
- Priority–**100**
- Mode–**Alias Pattern Match**
- Pattern type–**Regex**
- Pattern String**–(.*)(@mmcvd.ciscolabs.com).***
- Pattern Behavior–**Replace**
- Replace String–**\1\2**
- On Successful Match–**Stop**
- Target–**TraversalServer (B2B)**
- State–**Enabled**

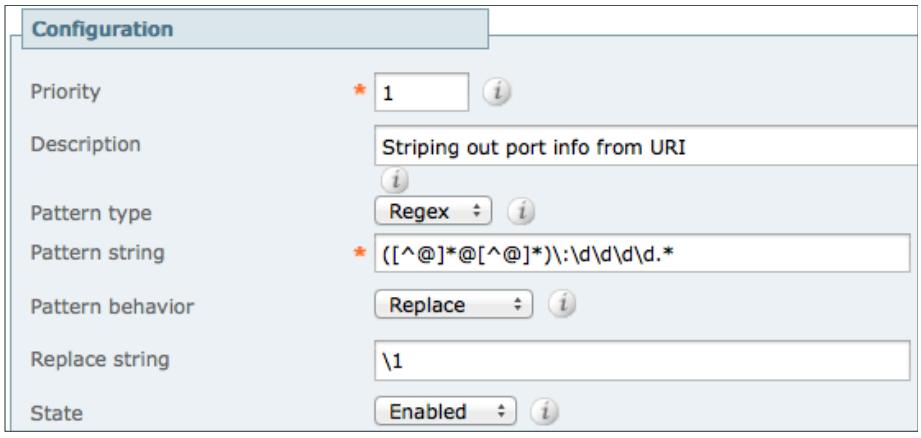
Step 6. Click **Create Search Rule**.

Procedure 12 Configure transform on Expressway-E

Step 1. Navigate to **Configuration > Dial Plan > Transforms** and click **New**.

Step 2. Enter the following into the relevant fields:

- Priority—**1**
- Description—**Striping out port info from URI**
- Pattern type—**Regex**
- Pattern string—**([^@]*@[^@]*)\:\d\d\d\d.***
- Pattern behavior—**Replace**
- Replace string—**\1**
- State—**Enabled**



Step 3. Click **Create Transform**.

Section 2: Deploy Cisco Unified Border Element (CUBE)

Easy Access Configuration Sheet

The following tables provide you with a place to capture all the information you may need during the configuration of CUBE-related services. Each table comprises the information items needed, references the example values used in this CVD, and provides a column into which you may enter your own particular site specific values in an easy-reference format.

Table 15. CUBE Network configuration

Item	CVD Configuration	Site-Specific details
HQ CUBE - LAN Interface	10.106.170.5	
HQ CUBE - WAN Interface	10.126.69.45	
SP SBC IP address (public)	10.106.170.145	
Branch CUBE - LAN interface	10.106.170.113	
Branch CUBE- WAN interface	10.126.69.46	
SP SBC IP Address (public)	10.126.69.35	
HQ Pub CUCM IP address	10.106.170.135	

Install and Configure CUBE

PROCESS

1. Enabling and configuring CUBE application on the HQ IOS router
2. Creating Route patterns on CUCM to route IP PSTN calls to the HQ CUBE
3. Creating SIP trunk between CUCM and HQ CUBE
4. Enabling the CUBE application on the branch IOS router

Procedure 1 Enabling and configuring CUBE application on the HQ IOS router

Step 1. Telnet/ssh into the IOS router.

Step 2. Enter into the global configuration mode and run the below commands to enable CUBE application:

```
Voice service voip
Mode border-element license capacity 200
Allow-connections sip to sip
```

Step 3. Configure other global settings to meet Service Provider requirement as below:

```
Voice service voip
  Sip
  Early-offer forced
  Header-passing
  Error-passthru
```

Step 4. Enable the topology hiding on the CUBE

```
Voice service voip
   address-hiding
```

Step 5. Configure IOS dial-peers on the HQ CUBE for call routing

```
voice class uri 1 sip
host ipv4:10.106.170.135

voice class uri 2 sip
host ipv4:10.106.170.145

voice class e164-pattern-map 1
  e164 9011T
  e164 91[2-9]..[2-9].....
  e164 9[2-9].....
  e164 [2-9].....

dial-peer voice 100 voip
description ***CUCM to HQ CUBE***
incoming uri via 1
session protocol sipv2
codec g711ulaw
dtmf-relay rtp-nte

dial-peer voice 101 voip
description ***HQ CUBE to CUCM***
destination-pattern [2-9].....
session protocol sipv2
```

```
session target ipv4:10.106.170.135
codec g711ulaw
dtmf-relay rtp-nte

dial-peer voice 102 voip
description ***Service provider to HQ CUBE***
incoming uri via 2
session protocol sipv2
codec g711ulaw
dtmf-relay rtp-nte

dial-peer voice 155 voip
 description ***HQ CUBE to Service Provider***
 translation-profile outgoing digitstrip
 session protocol sipv2
 session target ipv4:10.106.170.145
 destination e164-pattern-map 1
 codec g711ulaw
 dtmf-relay rtp-nte
```

Step 6. Configure the voice translation rules to strip of the access code 9

```
voice translation-rule 100
rule 1 /^9\(.*\)/ /\1/
```

Step 7. Configure voice translation profile to associate translation rule created in **step 6**

```
voice translation-profile digitstrip
translate called 100
```

Procedure 2	Creating Route patterns on CUCM to route IP PSTN calls to the HQ CUBE

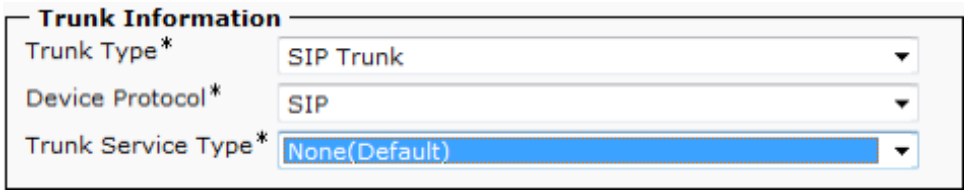
For creating route pattern on CUCM please refer to the document Unified Communication for BE6K technology design guide.

Procedure 3 Creating SIP trunk between CUCM and HQ CUBE

Step 1. After logging into the web administration of the CUCM navigate to the **Device->Trunk** Menu and then click **Add New**

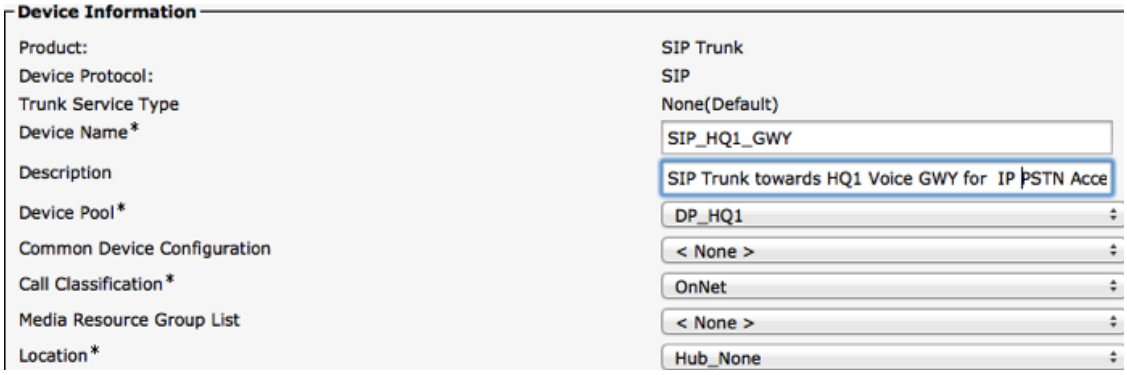
Step 2. On the trunk configuration page enter the following details

- Trunk Type–**SIP Trunk**
- Device protocol–**SIP**
- Trunk Service type–**Default**



Step 3. On the next page, in the Device information section, enter the following details

- Device Name–**SIP_HQ1_GWY**
- Description–**SIP trunk to CUBE**
- Devicepool–**DP_HQ1**
- Call Classification–**OnNet**
- Location–**Hub_None**



Step 4. Next, in the **SIP information section**, enter the following values and then click **Save**

- Destination Address 1–**10.106.170.5**
- Destination port–**5060**
- Sip Trunk Security Profile–**Non - secure SIP Trunk Profile**
- SIP Profile–**Standard SIP profile**

Step 5. In the message window click **OK**

Step 6. On the **Trunk Configuration** page, click **Reset**

Step 7. On **Device Reset** page, click Reset and then click **close**

Procedure 4 Enabling the CUBE application on the branch IOS router

Reader Tip

In branch router where CUBE is enabled, recommendation is to have a dedicated MPLS circuit to the local service provider. Hence, in which case IP addressing scheme might change if we choose to connect to a different service provider. So it might be required to use a second interface on branch router to establish the IP PSTN link.

Step 1. telnet/ssh into the branch IOS gateway

```
telnet 10.106.170.113 / ssh 10.106.170.113
```

Step 2. Enter into the global configuration mode to enable the **CUBE** application

```
Voice service voip
Mode border-element license capacity 50
Allow-connections sip to sip
```

Step 3. Enable address hiding on the CUBE

```
Voice service voip
Address-hiding
```

Step 4. Configure the **IOS dial-peers on the branch CUBE**

```
voice class uri 2 sip
host ipv4:10.126.69.35

voice class e164-pattern-map 1
  e164 9011T
  e164 91[2-9]..[2-9]......
  e164 9[2-9]......
  e164 [2-9]......

dial-peer voice 2102 voip
```

```
description ***Service Provider to Branch CUBE***
incoming uri via 2
session protocol sipv2
codec g711ulaw
dtmf-relay rtp-nte

 dial-peer voice 2155 voip
 description ***Branch CUBE to Service provider***
 translation-profile outgoing digitstrip
 session protocol sipv2
 session target ipv4:10.126.69.35
 destination e164-pattern-map 1
 codec g711ulaw
 dtmf-relay rtp-nte
```

Reader Tip

The dial plan configuration shown here aligns with the UC CVD. CUCC was used to configure dial plans on the CUCM which by default configures North American Numbering Plan (NANP). However, you can modify your dial plans to meet your specific needs.

Tech Tip

There can be SIP trunking to more than one service provider either for load balancing or as alternate routing option. For SRST configuration please refer the Unified Communications using the BE6K tehcnology design guide:
http://www.cisco.com/c/en/us/solutions/enterprise/validated-designs-collaboration/index.html

Tech Tip

The branch might also consider to have a back up E1/T1 PSTN in case of WAN failure or access to emergency services.

Appendix A: Product List

Component	Product Description	Part Numbers	Software
Call Control	Cisco Business Edition 6000 with up to 1000 users	BE6K-SW-11.0	11.5(1)
Cisco Collaboration Edge	Cisco Expressway-C	EXPWY-VE-C-K9	X8.8
	Cisco Expressway-E	EXPWY-VE-E-K9	X8.8
Soft Client	Cisco Jabber for Windows	JAB-DSK-K9	11.6
	Cisco Jabber for IOS		11.6
Hard Endpoints	TC Endpoints		CE8.2.1
	DX series		CE8.2.1
	8800/7800 series		11.6
CUBE	Cisco Unified Border Element		15.6.3(T)

Feedback

Please send comments and suggestions about this guide to collab-mm-cvd@external.cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Cisco 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)