**Application Note** 

# Audio/Video, Desktop Sharing Services on Cisco Unified Communications Manager Release 11.5 and Microsoft Skype for Business Server

# Table of Contents

Introduction	5
Network Topology	6
System Components	6
Hardware Requirements	6
Software Requirements	6
Features	7
Caveats	7
Infrastructure Configuration	8
Cisco Certificates	8
Active Directory Root Certificate Configuration	9
User Configuration	9
Create a Certificate Template in the Certificate Authority	12
Submit a certificate request in the Certificate Authority	21
Download a root certificate from CA	23
Cisco UCM Configuration	25
Loading certificates on Cisco UCM	25
Calling Search Space	
SIP Trunk Security Profile Configuration for Expressway-C	
Trunk to Expressway-C Gateway	35
Trunk to Expressway-C for MRA with Expressway-E	
Trunk to IM and Presence Server	41
SIP Route Pattern	45
Media Resource Group Configuration	46
Media Resource Group List Configuration	47
Add MRGL to Device or Device Pool	
Cisco UCM LDAP Configuration	50
LDAP-Synced users	52
User Management Configuration – Settings to Associate Services	53
Cisco Jabber User Configuration	56
End Point configurations	63
Expressway-C Configuration	81

© 2016 Cisco Systems, Inc. All rights reserved.

Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 2 of 145

System Configuration	81
Microsoft Lync B2BUA configuration (Skype for Business B2BUA)	86
Microsoft Lync (Skype for Business) B2BUA trusted hosts	87
Loading server and trust certificates	87
Call Routing	91
Call Flows	92
Zone and Search Rule Configuration for Audio/Video Integration	93
Zones Configurations	94
Search Rules	97
Configuring Secure Traversal Zone Connection for Unified Communications	100
Installing Expressway Security Certificates	100
Expressway-C Traversal Zone Configuration	101
Expressway-E Traversal Zone Configuration	102
Expressway-C Traversal Zone Search Rules	103
Expressway-E Traversal Zone Search Rules	104
Configuring External (Unknown) IP Address Routing	105
Discover Unified Communication Servers and Services	107
Trust the Certificates Presented to the Expressway-C	107
Discover Unified CM Servers	107
Discover IM and Presence Service Nodes	108
Automatically Generated Zones and Search Rules	109
IM&P Configuration	110
Loading Server and Trust Certificates	110
IM&P Trusted CA Certificate	110
IM&P Server Certificate	113
Application Listeners	115
TLS Contexts	117
Proxy Configuration Settings	118
Incoming ACL Configuration	119
TLS Peer Subject Configuration	121
TLS Peer Subject Configuration for Expressway-C	121
TLS Peer Subject Configuration for Skype for Business Server	122
Presence Gateway Configuration	122
© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 3 of 145	

Presence Settings Configuration	
Security Settings Configuration	
Static Route to Front End Configuration	
Skype for Business Server Configuration	
Add Expressway-C to Skype for Business Topology	126
Configure Encryption Level	
Trusted Application Server – IM&P Nodes	
Update Skype for Business Certificates	131
Test ResultsError! Bo	ookmark not defined.

# Introduction

This document describes the steps and configurations necessary for integrating Cisco Unified Communications Manager (Cisco UCM) release 11.5, Cisco Expressway-C and E release X8.9 and Microsoft Skype for Business (6.0.9319.0) to interoperate in a single domain. Endpoints are configured on both Cisco UCM and Skype for Business Server. The goal of this integration is to enable end users on Cisco CUCM and Skype for Business to make end to end Audio/Video (AV) calls, ad hoc conference calls and share desktop.

## Key Points:

- This testing has been performed with IPv4 using TLS for signaling between Cisco UCM, Microsoft Skype for Business Server, Cisco Expressway-C & Cisco Expressway-E
- Though the solution has been tested with signaling enabled for TLS, it is not mandatory to use TLS and can be deployed with TCP
- Basic Audio/video calls and desktop sharing between Cisco and skype clients works successfully.

## The following items were tested:

### AV:

- Basic outbound and inbound calling between Skype for Business, Cisco UCM and Jabber users with complete audio and video
- Ad hoc conference
- Desktop Share
- Call hold and resume
- Call transfer
- Call forward
- Call park
- Voicemail deposit/retrieval

# **Network Topology**



# System Components

## Hardware Requirements

The following hardware was tested

- Cisco UCS-C240-M3S VMWare Host running ESXi 5.5
- Microsoft Windows Server 2012 running Hyper-V
- Cisco End Points DX70, DX80

## **Software Requirements**

The following software was tested:

- Cisco Unified Communications Manager version 11.5.1.11900-26
- Microsoft Skype for Business Server version 6.0.9319.0
- Cisco Expressway-C version X8.9
- Jabber Client for Windows Version 11.6.0 Build 35037
- Skype for Business Android Client (6.0.0.8)

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 6 of 145

- Skype for Business iOS Client (6.7.0.216)
- Skype for Business Windows Mobile Client (6.3.1558.0)

# Features

This section lists supported and unsupported features. Deviance from the configuration presented in this guide is not supported by Cisco. Please see the Limitations section below for more information.

### Features Supported:

### AV:

- Basic outbound and inbound calling between Skype for Business, Cisco UCM and Jabber users
- Call hold and resume
- Conference

### Features Not Supported or Not Tested:

AV:

• Call transfer using Android mobile clients for Skype for Business is not supported

# Caveats

These are the known limitations, caveats, or integration issues:

- Basic audio only calls from Cisco users towards iOS clients fail.
- Call transfer from Skype for Business mobile clients to Cisco users are failing.
- Call hold/resume on endpoint fails (call drops) for a call from Skype for Business mobile client to cisco end point and cisco endpoint initiates the hold/resume.
- Call hold on Cisco endpoint fails with one way audio for a call from cisco endpoint to Skype for Business mobile client and cisco end point initiates the hold/resume.
- Call hold on Cisco end point fails with no audio (video is fine) for a video call from cisco endpoint to Skype for Business mobile client and cisco end point initiates the hold/resume.

# Infrastructure Configuration

# **Cisco Certificates**

Certificates secure client and server identities. After root certificates are installed, certificates get added to the root trust stores to secure connections between users and hosts, including devices and application users.

For best practices on installing certificates in CUCM, Expressway servers, please refer to the documentations at

### CUCM:

http://www.cisco.com/c/en/us/td/docs/voice\_ip\_comm/cucm/admin/11\_5\_1/CUCM\_BK\_A09578D7\_0 0\_admin-guide-cucm-imp\_1151/CUCM\_BK\_A09578D7\_00\_admin-guide-for-cucm-1105\_chapter\_01110.pdf

### Expressway:

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/productsinstallation-and-configuration-guides-list.html

Note: The below configuration uses TLS with port 5061 between Skype for Business Server and Expressway-C; Expressway-C and Cisco UCM; Cisco UCM and Expressway-C. TLS is not a mandate to configure the supported features, if you are using TCP please use the default TCP port 5060.

# Active Directory Root Certificate Configuration

# User Configuration

- 1. In Active Directory, open Active Directory Users and Computers
- 2. Right click on Users, navigate to New->User
- 3. Enter the details of users as shown in the screen shot below

File       Action       View       Help         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Queries         Image: Sevent Queries       Image: Sevent Queries       Image: Sevent Querie	2 🖬 % 📽	Туре	Descriptio <u>^</u>
Image: Source of the second	1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Туре 🔺	Descriptio 🔨
Active Directory Users and Com ▷ Saved Queries △   Builtin ▷ Computers ▷ Domain Controllers ▷ ProreignSecurityPrincipal: ▷ Managed Service Accour ▷ Microsoft Exchange Secu		Туре	Descriptio A
RTC Accounts			
Delegate Control Find			
New 🕨	Computer		
All Tasks	Contact		
View 🕨	Group		
Refresh Export List	InetOrgPerson msExchDynamicDistributionList		=
Properties	MSMO Queue Alias		
Help	Printer		
💄 User Ti	User		~
< III > <	Shared Folder		>

Figure 1: Active Directory Users and Computers

		testuser	1 Prope	rties		?	x
Published Ce	rtificates	Member Of	Password	d Replica	tion [	Dial-in	Object
Security	Security En		Sess	ions	Re	mote co	ontrol
Remote D	esktop Se	rvices Profile	C	+MC	At	tribute E	Editor
General	Address	Account	Profile	Teleph	ones	Orga	nization
8	testuser1						
First name:		testuser1		Initial	s:		
Last name:							
Display nam	ie:	testuser1					
Description:							
Office:							
Telephone r	number:					Other	
E-mail:		testuser1@te	kvizionlabs	.com			
Web page:						Other	
	O	< (	Cancel	Ар	ply		Help

Figure 2: Active Directory User-1

	testuser	I Prope	rties		?	x
Published Certificates	Member Of	Password	d Replica	tion I	Dial <del>i</del> n	Object
Security Er	Security Environment		Sessions Remote control		ontrol	
Remote Desktop Se	ervices Profile	C	DM+	At	tribute E	ditor
General Address	Account	Profile	Teleph	ones	Orgar	nization
User logon name:						
testuser1		@tekvi;	zionlabs.c	om		~
User logon name (pre-	Windows 2000	)):				
TEKVIZIONLABS		testuser	1			
Logon Hours	Log On To	)				
Unlock account						
User must chan User cannot chan Password never	ge password at ange password • expires using reversible	e encryptic	n			^ ~ ~
Account expires	Wednesday, N	ovember 3	30, 2016			-
0	к с	ancel	App	ply		Help

Figure 3: Active Directory User-2

# Create a Certificate Template in the Certificate Authority

The default certificate templates are not provisioned with required client and server authentication, and have only server authentication enabled. So, a custom template with both client and server authentication is required. The following captures illustrate the steps required to create a client server authentication certificate template to be used during the certificate generation.

🧔 certsrv - [Cer	tification Authority (Lo	cal)\lynclabsp-DC-CA\Certificate Templates]	_ <b>D</b> X
File Action View Help			
🗢 🏟 🙎 🙆 🗟			
<ul> <li>Certification Authority (Local)</li> <li>Iynclabsp-DC-CA</li> <li>Revoked Certificates</li> <li>Issued Certificates</li> <li>Pending Requests</li> <li>Failed Requests</li> <li>Certificate Templater</li> </ul>	Name	Intended Purpose	
Manage			
New	•		
View	•		
Refresh Export L	ist		
Help			
Starts Certificate Templates snapin			

Figure 4: Certificate Authority- Create New Certificate Template-1

<b>.</b>	Certifica	te Templates Console		_ 🗆 X
File Action View Help				
Certificate Templates (dc.lynclal	Template Display Name	Schema Versio	n Verŝi. ⁄	Actions
	Authenticated Session	1	3.1	Certificate Template
	🚇 Basic EFS	1	3.1	
	🚇 Code Signing	1	3.1	More Actions
	🚇 Trust List Signing	1	3.1	Web Server
	🖳 User	1	3.1	Mars Astions
	Representation Administrator	1	4.1	
	Reference CEP Encryption	1	4.1	
	🚇 Domain Controller	1	4.1	
	🚇 Enrollment Agent	1	4.1	
	🚇 Exchange Enrollment Agent	(Offline requ 1	4.1	
	Router (Offline request)	1	4.1	
	Reference User Signature Only	1	4.1	
	🗵 Web Server 📃 📃	1	4.1	
	🖳 Computer	Duplicate Template	5.1	
	🖳 Enrollment Agent (Cor	All Tasks	5.1	
	Root Certification Aut		5.1	
	🚇 Subordinate Certificati	Properties	5.1	
	🗷 EFS Recovery Agent	Help	6.1	
	Rechange Signature Only	1	6.1	
	🗟 Smartcard Logon	1	6.1	
	Exchange User	1	7.1	
< III >	<		>	
Using this template as a base, creates	a template that supports Window	vs Server 2003 Enterprise CAs		

Figure 5: Certificate Authority- Create New Certificate Template-2

Superseded Te Compatibility emplate display r ServerandWebCli emplate name: ServerandWebCli alidity period: 2 years 2 years	emplates General aame: ent	Requ	val period:	ng	Security Cryptography
Compatibility emplate display r ServerandWebCli emplate name: ServerandWebCli alidity period: 2 years 2 years	General ame: ent	Requ	val period:	ng	Cryptography
emplate display r ServerandWebCli emplate name: ServerandWebCli alidity period: 2 years 2 years	ent	Rene	wal period:		
emplate name: ServerandWebCli alidity period: 2 years	ent	Rene	wal period		
emplate name: ServerandWebCli alidity period: 2 years ] Publish certifica	ent	Rener	wal period		
Directory	ate in Active [ matically reen	Directory proll if a du	plicate ce	v	exists in Active

Figure 6: Certificate Authority- Create New Certificate Template-3

Subject Name	e Se	rver	Issuance	Requirements
Compatibility	General	Reque	st Handling	Cryptography
Superseded	Templates	Б	tensions	Security
Application Reduced Basic Constr Certificate To Issuance Po	Policies aints emplate Informat licies	tion		Edit
Description of Ap Server Authentio	plication Policie sation	es:		~
				~

Figure 7: Certificate Authority- Create New Certificate Template-4

Constant of Figure	cation [	Policies Exte	ension 🏓
An application pused.	oolicy defir	nes how a certi	ficate can be
Application poli	cies:		
Server Authen	tication		
		1920	
Add		Edit	Remove

Figure 8: Certificate Authority- Create New Certificate Template-5

Add Application Policy	×
An application policy (called enhanced key usage in Windows 2000 lefines how a certificate can be used. Select the application policy or valid signatures of certificates issued by this template.	)) required
Any Purpose Certificate Request Agent	^
Client Authentication Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Signing Domain Name System (DNS) Server Trust Early Launch Antimalware Driver Embedded Windows System Component Verification Encrypting File System	=
Ne	w
ОК Са	ncel

Figure 9: Certificate Authority- Create New Certificate Template-6

🛱 certsrv - [C	ertification	n Authority (Local)\lynclabsp-DC-CA\Certificate Templates]
File Action View Help		
🧇 🔿 🖄 🙆 👔		
Certification Authority (Local)  Certification Authority (Local)  Inclabsp-DC-CA  Revoked Certificates  Issued Certificates  Pending Requests  Failed Requests  Certificate Tomplates	Name	Intended Purpose
Manage		Catificate Template to Issue
View	•	Certificate rempiate to issue
Refresh Export List		
Help		
Enable additional Certificate Templ	ates on this (	Certification Authority

Figure 10: Certificate Authority- Create New Certificate Template-7

lect one Certificate Template to enable te: If a certificate template that was recommation about this template has been r of the certificate templates in the organ or more information, see <u>Certificate</u>	on this Certification Authonty. ently created does not appear on this list, you may need to wait unti eplicated to all domain controllers. iization may not be available to your CA. <u>Template Concepts.</u>	1
Name	Intended Purpose	~
Key Recovery Agent	Key Recovery Agent	
OCSP Response Signing	OCSP Signing	
RAS and IAS Server	Client Authentication, Server Authentication	
Router (Offline request)	Client Authentication	
ServerandWebClient	Server Authentication, Client Authentication	
Smartcard Logon	Client Authentication, Smart Card Logon	-
Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
Trust List Signing	Microsoft Trust List Signing	=
User Signature Only	Secure Email, Client Authentication	
Workstation Authentication	Client Authentication	~

Figure 11: Certificate Authority- Create New Certificate Template-8

certsrv - [Ce	rtification Authority (Local)\lyr	clabsp-DC-CA\Certificate Templates]	X
File Action View Help			
🗢 🔿 🙋 🙆 📓			
Certification Authority (Local)	Name	Intended Purpose	
<ul> <li>✓ Jynclabsp-DC-CA</li> <li>Revoked Certificates</li> <li>Issued Certificates</li> <li>Pending Requests</li> <li>Failed Requests</li> <li>Certificate Templates</li> </ul>	ServerandWebClient	Server Authentication, Client Authentic	

Figure 12: Certificate Authority- Create New Certificate Template-9

### Submit a certificate request in the Certificate Authority

Below is the process for creating a certificate request in the Certificate Authority

1. Navigate to https://<IP Address of CA>/certsrv

Microsoft Active Directory Certificate Services - lynclabsp-DC-CA

#### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Figure 13: Certificate Authority-Certificate Request-1

Microsoft Active Directory Certificate Services -- lynclabsp-DC-CA Home

Request a Certificate

Select the certificate type:

**User Certificate** 

Or, submit an advanced certificate request.

Figure 14: Certificate Authority-Certificate Request-2

Microsoft Active Directory Certificate Services - lynclabsp-DC-CA

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Figure 15: Certificate Authority-Certificate Request-3

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 21 of 145

Home

Home

- 2. Copy the Generated CSR in to the text field shown below
- 3. Select the Certificate Template 'ServerandWebClient', this is the template we have created in Create a Certificate Template in the Certificate Authority
- 4. Click submit and download the certificate

Microsoft Active Directory Certificate Services -- Iynclabsp-DC-CA

#### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):			$\sim$
	<		>
Certificate Templa	ate:		
Certificate Templa	ate: ServerandWebClient	~	
Certificate Templa	ate: ServerandWebClient	~	
Certificate Templa	ate: ServerandWebClient tes:	~	2

Figure 16: Certificate Authority-Certificate Request-4

Home

#### Download a root certificate from CA

#### Microsoft Active Directory Certificate Services -- lynclabsp-DC-CA

Home

#### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory</u> <u>Certificate Services Documentation</u>.

#### Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Figure 17: Certificate Authority-Download CA certificate-1

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [tekvizionlabs-DC01-CA]	*
	÷

Encoding method:

DER
 Base 64

Install CA certificate Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL

Figure 18: Certificate Authority-Download CA certificate-2

Home

# Cisco UCM Configuration

## Loading certificates on Cisco UCM

Navigation: Cisco Unified OS Administration/Security->Certificate Management

Cisco UCM should trust Expressway-C

#### Cisco UCM Server Certificate

Cisco UCM by default has a self-signed certificate installed. This should be replaced with a certificate generated from a trusted certificate authority.

Generate a CSR				
Certificate List				
Generate Self-sig	gned 🛯 🖆 Upload Certificate/Certif	icate chain 🔋 Gener	ate CSR	
Status 31 records fou	ind			
Certificate List	(1 - 31 of 31)		R	ows per Page 50 🗸
Find Certificate List	where Certificate 🗸 beg	ins with 🗸	Find Clear F	ilter 🔂 😑
Certificate ▲	Common Name	Туре	Distribution	

Figure 19: Cisco UCM Generate CSR-1

- 1. Set Certificate Purpose: CallManager
- 2. Set Distribution: This will be the node to which you are generating a certificate
- 3. Set Common Name: This will be the node to which you are generating a certificate
- 4. Set Parent Domain: This will be the domain of the UCM node

Generate Certificate Si	igning Request
🛐 Generate 🖳 Close	
- <b>Status</b> Warning: Generatin	g a new CSR for a specific certificate type will overwrite the existing CSR for that type
-Generate Certificate Si	igning Request
Certificate Purpose**	CallManager
Distribution*	clus30pub.tekvizionlabs.com
Common Name*	clus30pub.tekvizionlabs.com
Subject Alternate Nam	nes (SANs)
Parent Domain	tekvizionlabs.com
Key Type**	RSA
Key Length*	2048
Hash Algorithm*	SHA256
Generate Close	

#### Figure 20: Cisco UCM Generate CSR-2

Once the CSR is created, open the CSR, copy the content of the CSR and follow the steps shown in <u>Submit</u> <u>a certificate request in the Certificate Authority</u> for creating a certificate request and downloading the certificate

#### Upload root certificate to Cisco UCM

Follow the instructions in <u>Download a root certificate from CA</u> to download the root certificate authority that issued the Expressway-C certificate

- 1. Click Upload Certificate/Certificate Chain
- 2. Select Certificate Purpose: Call Manager-trust

Upload 🖳 Close	runcate chain	
itatus		
i) Warning: Uploadin	g a cluster-wide certificate will distribu	te it to all servers in this cluster
Warning: Uploadin Upload Certificate/Ce	g a cluster-wide certificate will distribu	

Figure 21: Cisco UCM Upload root certificate to Call Manager-trust

After upload is done, click on the certificate you uploaded and it should look similar to the one below.

Certificate Details for	tekvizionlabs-DC01-CA, CallManager-trust
🗙 Delete 🔋 Downloa	d .PEM File Download .DER File
Chalum	
Status	
Status: Ready	
-Certificate Settings —	
File Name	tekvizionlabs-DC01-CA.pem
Certificate Purpose	CallManager-trust
Certificate Type	trust-certs
Certificate Group	product-cm
Description(friendly nam	ne) Signed Certificate
[ Version: V3 Serial Number: 68310 SignatureAlgorithm: S Issuer Name: CN=tek Validity From: Mon Fe To: Sun Feb 1 Subject Name: CN=te Key: RSA (1.2.840.11 Key value: 3082010a0282010100a 6494581e7e9fd25ddeb cb60e909ee904de9aac 165e6f8d00eee19850b	Alactric
ct4705c337436dd7b44f	1028d2494335tt226t4290a27905a69c2c6c728b3ca7t9b5e8e7391b50dd17f
Delete Download .	'EM File   Download .DER File

Figure 22: Cisco UCM root certificate example

In similar, upload the root certificate to tomcat-trust

Upload Certificate/Certifica	te chain
Upload 🖳 Close	
Status Warning: Uploading a clus Upload Certificate/Certifica	ster-wide certificate will distribute it to all servers in this cluster
Certificate Purpose*	tomcat-trust
Description(friendly name) Upload File	Choose File root_cert_teknlabs.cer.cer
Upload Close	

Figure 23: Cisco UCM Upload root certificate to tomcat-trust

Upload Server Certificate

5. After the certificate download is complete click on 'Upload Certificate/Certificate chain'

Certificate List				
Generate Self-sign	Upload Certificate/Certifi	cate chain 🔋 Genera	ate CSR	
Status 31 records found	1			
Certificate List (1	- 31 of 31)			Rows per Page 50 🗸
Find Certificate List w	here Certificate 🗸 begi	ns with 🗸	Find Clea	r Filter 🛛 🕂 👄
Certificate ▲	Common Name	Туре	Distribution	

Figure 24: Cisco UCM Upload Server Certificate to CallManager-Trust-1

- 6. Set Certificate Purpose: Call Manager
- 7. Browse and upload the file

Upload Certificate/Ce	rtificate chain		
🐴 Upload 🖳 Close			
-Status Warning: Uploadir -Upload Certificate/Co	g a cluster-wide certificate will distribute i rtificate chain	t to all servers in this	cluster
Certificate Purpose*	CallManager	~	
Description(friendly name)	CA Signed Certificate		
Upload File			Browse
Upload Close			

Figure 25: Cisco UCM Upload Server Certificate to CallManager-2

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 30 of 145 Look for the following oids in the certificate file Data to confirm that the certificate has both client and server authentication

- Certificate File Data	
caa3a493ac7b4d9712402758cdcabb29cd261401a7fe12d6bbbc00c0a050e90203	
010001	~
Extensions: 9 present	
[	
Extension: ExtKeyUsageSyntax (OID.2.5.29.37)	
Critical: false	
Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2,	
Ĩ	
Extension: KeyUsage (OID.2.5.29.15)	
Critical: true	
Usages: digitalSignature, keyEncipherment,	
1	
	<u> </u>
Evtension: SubjectAltName (OID 2 5 29 17)	*
Extension. Subject (Manie (OID.2.5.25.17)	

#### Upload tomcat Certificate

Upload Certificate/Certificate chain					
Upload 🖳 Close					
Status Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster					
Certificate Purpose*	tomcat				
Description(friendly name)					
Upload File	C:\Users\sjonnada	\Downloads\CUCM_Cert_Server.cer	Browse		
Upload Close					

Figure 26: Cisco UCM Upload Server Certificate to tomcat-trust

# Calling Search Space

### Navigation: Call Routing->Class of Control->Calling Search Space

Calling Sea	rch Space Configuration	Related Links: Back To Find/List	✔ Go
Save	🗙 Delete 📋 Copy 🕂 Add New		
Status — Status	: Ready		
Calling Se Name*	arch Space Information		
Description	Calling Search Space for Directory URI lookup		
- Route Part Available Pa	titions for this Calling Search Space rtitions** Global Learned E164 Numbers Global Learned E164 Patterns Global Learned Enterprise Numbers Global Learned Enterprise Patterns		
Selected Pa	rtitions Directory URI	X	
Save D	elete Copy Add New		

# SIP Trunk Security Profile Configuration for Expressway-C

#### Navigation: System -> Security -> SIP Trunk Security Profile

- Set Name: Enter a name for the security profile. When you save the new profile, the name displays in the SIP Trunk Security Profile drop-down list box in the Trunk Configuration window.
- 2. Set **Description**: Enter a description relevant to your security profile
- 3. Set Device Security Mode: Encrypted
- 4. Set Incoming Transport Type: TLS
- 5. Set Outgoing Transport Type: TLS
- 6. Set **X.509 Subject Name:** Enter the subject name of the X.509 certificate for the SIP trunk device, which is the subject name of Expressway-C here.
- 7. Set Incoming Port: 5061
- Confirm Accept unsolicited notification: is checked
   If you want Cisco Unified Communications Manager to accept incoming non-INVITE, unsolicited notification messages that come via the SIP trunk, check this check box.
- 9. Confirm Accept replaces header: is checked

If you want Cisco Unified Communications Manager to accept new SIP dialogs, which have replaced existing SIP dialogs, check this check box

SIP Trunk Security Profile Configuration						
🔚 Save 🗶 Delete 📋 Copy 😋 Reset 🥒 Apply Config 🕂 Add New						
Status						
Status						
(1) Status: Ready						
SIP Trunk Security Profile Informati	on					
Name*	Expressway Secure SIP Trunk Profile					
Description	Expressway Secure SIP Trunk Profile					
Device Security Mode	Encrypted <b>v</b>					
Incoming Transport Type*	TLS					
Outgoing Transport Type	TLS					
Enable Digest Authentication						
Nonce Validity Time (mins)*	600					
K.509 Subject Name	expressc2.tekvizionlabs.com					
Incoming Port*	5061					
Enable Application level authorization	1					
Accept presence subscription						
Accept out-of-dialog refer**						
Cept unsolicited notification						
🗹 Accept replaces header						
Transmit security status						
Allow charging header SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter					
Save Delete Copy Reset A	Apply Config Add New					

Figure 27: Cisco UCM Security Profile for Expressway-C Trunk

## Trunk to Expressway-C Gateway

To configure Expressway-C, please refer to section Expressway-C Configuration

#### Navigation: Device -> Trunk

#### **Device Information**

- 1. Set Trunk Type: SIP Trunk
- 2. Set Device Protocol: SIP
- 3. Set Trunk Service Type: None
- 4. Set **Device Name**: Enter a name for the trunk
- 5. Set **Description:** Enter a description relevant to your trunk
- Set Device Pool: Select the Device Pool you configured under System -> Device Pool For trunks, device pools specify a list of Cisco Unified Communications Managers that the trunk uses to distribute the call load dynamically
- 7. Set Media Resource Group List: Select the Media Resource Group List you configured under Media Resources -> Media Resource Group List
- 8. Confirm **SRTP Allowed:** is checked
- 9. Set **Consider Traffic on This Trunk Secure**: When using both SRTP and TLS
- 10. Set Calling Search Space: CSS Directory URI

#### **SIP Information**

- 11. Set the **Destination Address**: Enter the FQDN of the Expressway-C to which you are establishing a trunk.
- 12. Set **SIP trunk Security Profile**: Select the security profile you created under System -> Security -> SIP Security Profile
- 13. Set **SIP Profile**: Select the SIP Profile you created under Device -> Device Settings -> SIP Profile
- 14. Set Normalization Script: Select the existing normalization script vcs-interop

Trunk Configuration		Related Links: Back To Find/List	~
🔚 Save 🗶 Delete 👇 Reset 🕂 Ad	Id New		
- SIP Trunk Status			
Service Status: Full Service	lave 0 hour 7 minutes		
Duration: Time In Full Service: 15 c	lays 0 nour 7 minutes		
– Device Information ––––––			
Product:	SIP Trunk		
Device Protocol:	SIP Nana (Dafault)		
Device Name*	ExpressC		
Description	Trunk to Expressway C		
Device Pool*	DP Richardson	$\sim$	
Common Device Configuration	< None >	$\sim$	
Call Classification*	OnNet	$\checkmark$	
Media Resource Group List	MRGL_Richardson	~	
Location*	Hub_None	~	
AAR Group	< None >	~	
Tunneled Protocol*	None	~	
QSIG Variant*	No Changes	~	
ASN.1 ROSE OID Encoding*	No Changes	~	
Packet Capture Mode*	None	~	
Packet Capture Duration	0		
Media Termination Point Required			
Retry Video Call as Audio			
Path Replacement Support			
Transmit UTF-8 for Calling Party Name			
Transmit UTF-8 Names in QSIG APDU			
Unattended Port			
SRTP Allowed - When this flag is checke do so will expose keys and other informatic	d, Encrypted TLS needs to be configured in th	e network to provide end to end security. Failure	to
Consider Traffic on This Trunk Secure*	When using both sRTP and TLS	×	
Route Class Signaling Enabled*	Default	~	
Use Trusted Relay Point*	Default	~	
PSTN Access			
Run On All Active Unified CM Nodes			

Figure 28: Cisco UCM Trunk to Expressway-C-1
Intercompany Mo 164 Transformat	ion Profile < No	:) one >			~		
ILPP and Confide	ential Access Le	vel Informa	ation				
ILPP Domain	< None	>			~		
onfidential Acces	s Mode < None	>			~		
onfidential Acces	s Level < None	>			~		
Call Routing Info	rmation ———						
Remote-Party-	Id						
Asserted-Ident	ity						
sserted-Type*	efault			~			
IP Privacy*	Default V						
Inbound Calls —							
Significant Digits	ĸ	All			~		
Connected Line I	D Presentation*	Default			~		
Connected Name Presentation*							
Calling Search Sp	ace	CSS Direct	ory URI		$\sim$		
AAR Calling Sear	h Space	< None >			~		
Prefix DN							
Redirecting Di	version Header	Delivery - Ir	nbound				
– Incoming Callin	ng Party Setting	s ———					
If the adminis	trator sets the p	refix to Def	ault this indicates (	call proces	sing will use prefix at the next lev	el setting (De	evicePool/Service
Parameter). O	thermse, the var		Clear Prefix Sett	ings	Default Prefix Settings		prenx assigned.
Number Type	e P	refix	Strip Digits		Calling Search Space		Use Device Pool CSS
Incoming Num	ber Default		0	< None	>	~	•
- Incoming Calle	d Party Setting	5		_			
If the adminis	trator sets the p	refix to Def	ault this indicates	call proces	sing will use prefix at the next lev	el setting (De	evicePool/Service
Parameter). O	therwise, the val	lue configur	ed is used as the	prefix unle	ss the field is empty in which case	e there is no	prefix assigned.
			Clear Prefix Sett	ings	Default Prefix Settings		
The second se	e P	refix	Strip Digits		Calling Search Space		Use Device Pool CSS
Number Type							122 15
Number Type Incoming Num	ber Default		0	< None	>	$\sim$	✓

Figure 29: Cisco UCM Trunk to Expressway-C-2

Connected Party Settings	- Norse -					
Willes Device Real Connected Party To	< None >		•			
Se Device Pool Connected Party In	ansiormation CSS					
- Outbound Collin						
Called Party Transformation CSS	< None >		~			
Villee Device Dool Called Party Transfer	mation CES					
Calling Party Transformation CSS	< None >		~			
			•			
L Use Device Pool Calling Party Transfo Calling Party Selection*	rmation CSS					
Calling Line ID Presentation*	Originator		*			
Calling have Presentation	Default		~			
Calling wante Presentation	Default		~			
	Deliver DN only in	connected party	~			
Redirecting Diversion Header Delivery	y - Outbound					
Redirecting Party Transformation CSS	< None >		~			
Use Device Pool Redirecting Party Tra	ansformation CSS					
Caller Information						
Caller ID DN						
Caller Name						
Maintain Original Caller ID DN and C	Caller Name in Identii	ty Headers				
	caller Marrie III 10enu	ty neduers				
- SIP Information						
Destination						
Destination Address is an SRV						
Destination Address	8	Destination Address I	Du6	Destination Port	Status Status Reaso	Duration
	1.		FV0	Descination Fort		
1* expressc2.lynclabsp.local			PVU	5061	up	Time Up: 0 day 0 hour 22 minutes
1* expressc2.lynclabsp.local MTP Preferred Originating Codec*	711ulaw		~	5061	up	Time Up: 0 day 0 hour 22 minutes 🕒
1* expressc2.lynclabsp.local MTP Preferred Originating Codec* BLF Presence Group*	711ulaw Standard Presence	group		5061	up	Time Up: 0 day 0 hour 22 minutes 主
1* expressc2.lynclabsp.local MTP Preferred Originating Codec* BLF Presence Group* SIP Trunk Security Profile*	711ulaw Standard Presence Expressway Secure	group SIP Trunk Profile		5061	up	Time Up: 0 day 0 hour 22 minutes 庄
1*         expressc2.lynclabsp.local           MTP Preferred Originating Codec*           BLF Presence Group*           SIP Trunk Security Profile*           Rerouting Calling Search Space	711ulaw Standard Presence Expressway Secure < None >	group SIP Trunk Profile	× × ×	5061	up	Time Up: 0 day 0 hour 22 minutes 庄
expressc2.lynclabsp.local     MTP Preferred Originating Codec*     BLF Presence Group*     SIP Trunk Security Profile*     Rerouting Calling Search Space     Out-Of-Dialog Refer Calling Search Space	711ulaw Standard Presence Expressway Secure < None > < None >	group SIP Trunk Profile		5061	up	Time Up: 0 day 0 hour 22 minutes 庄
1* expressc2.lynclabsp.local MTP Preferred Originating Codec* BLF Presence Group* SIP Trunk Security Profile* Rerouting Calling Search Space Out-Of-Dialog Refer Calling Search Space SUBSCRIBE Calling Search Space	711ulaw Standard Presence Expressway Secure < None > < None >	group SIP Trunk Profile		5061	up I	Time Up: 0 day 0 hour 22 minutes 庄
1* expresse2.lynclabsp.local MTP Preferred Originating Codec* BLF Presence Group* SIP Trunk Security Profile* Rerouting Calling Search Space Out-Of-Dialog Refer Calling Search Space SUBSCRIBE Calling Search Space SIP Profile*	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profil	group SIP Trunk Profile Por Cisco VCS		Details	up	Time Up: 0 day 0 hour 22 minutes 庄
expressc2.lynclabsp.local  MTP Preferred Originating Codec*  BLF Presence Group*  SIP Trunk Security Profile*  Rerouting Calling Search Space Out-Of-Dialog Refer Calling Search Space  SUBSCRIBE Calling Search Space  SIP Profile*  DTMF Signaling Method*	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile Por Cisco VCS	V V V V V	Details	up I	Time Up: 0 day 0 hour 22 minutes 庄
1*         expressc2.lynclabsp.local           MTP Preferred Originating Codec*           BLF Presence Group*           SIP Trunk Security Profile*           Rerouting Calling Search Space           Out-Of-Dialog Refer Calling Search Space           SUBSCRIBE Calling Search Space           SIP Profile*           DTMF Signaling Method*	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile Pror Cisco VCS	V V V V V iew	Details	up	Time Up: 0 day 0 hour 22 minutes 庄
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile e For Cisco VCS	V V V V V V V	Details	up	Time Up: 0 day 0 hour 22 minutes 庄
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Normalization Script	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile 2 For Cisco VCS	V V V V V V V	Details	up	Time Up: 0 day 0 hour 22 minutes 庄
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Normalization Script         ucs-interop         Enable Trace	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile e For Cisco VCS	V V V V V V	Details	up	Time Up: 0 day 0 hour 22 minutes 庄
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Normalization Script         Prameter Name         1	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile e For Cisco VCS	V V V V V iew	Details	up	Time Up: 0 day 0 hour 22 minutes 庄
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Vcs-interop         Enable Trace         1	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile e For Cisco VCS	V V V V V iew	Details	up	Time Up: 0 day 0 hour 22 minutes 庄
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Vcs-interop         Enable Trace         Parameter Name         1	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile e For Cisco VCS Parameter Value	V V V V V iew	Details	up	Time Up: 0 day 0 hour 22 minutes 庄
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Vcs-interop         Enable Trace         Parameter Name         1         Image: Supplementation	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile e For Cisco VCS	V V V V V iew	Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Ves-interop         Enable Trace         Parameter Name         1         © None         Q This trunk connects to a recording-end	711ulaw Standard Presence Expressway Secure < None > < None > Standard SIP Profile RFC 2833	group SIP Trunk Profile e For Cisco VCS Parameter Value	V V V V V iew	Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Normalization Script         Parameter Name         1         Image: Search Space         Image: Script Search Space         Image: Search Space         SIP Profile*         Image: Search Space	711ulaw Standard Presence Expressway Secure < None > < None > < Standard SIP Profile RFC 2833 abled gateway with recording-enable	group SIP Trunk Profile  For Cisco VCS  Parameter Value  ed nateways		Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Vcs-interop         Enable Trace         Parameter Name         1         Image: Structure Content Structure         Image: Structure Content Structure         Image: Structure	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profile RFC 2833 Nabled gateway with recording-enable	group SIP Trunk Profile Por Cisco VCS Parameter Value ed gateways		Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Vocs-interop         Enable Trace         Parameter Name         1         Image: Structure Content Structure         Image: Other Content Structure	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profile RFC 2833 Abled gateway with recording-enable	group SIP Trunk Profile		Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Normalization Script         Normalization Script         Parameter Name         1         Image: Construct Structure         Image: Constructure         Recording Information         Image: Constructure         Image: Constremon	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profile RFC 2833 Abled gateway with recording-enable	group SIP Trunk Profile Parameter Value Parameter Value		Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Normalization Script         Normalization Script         SIP Profile*         OTMF Signaling Method*         Recording Information <ul> <li>None</li> <li>This trunk connects to a recording-en</li> <li>This trunk connects to other clusters</li> </ul> Geolocation Configuration         Geolocation Filter	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profile RFC 2833 Abled gateway with recording-enable	group SIP Trunk Profile Parameter Value Parameter Value		Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Normalization Script         Normalization Script         Parameter Name         1         © None         O This trunk connects to a recording-en         O This trunk connects to other clusters         Geolocation Configuration         Geolocation Filter         Sand Geologation Lifetomation	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profile RFC 2833 Abled gateway with recording-enable	group SIP Trunk Profile Per Cisco VCS Parameter Value ed gateways		Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SUBSCRIBE Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Normalization Script         Vcs-interop         Enable Trace         Parameter Name         1         Onne         O This trunk connects to a recording-en         O This trunk connects to other clusters         Geolocation Configuration         Geolocation Filter         Send Geolocation Information	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profile RFC 2833 abled gateway with recording-enable	group SIP Trunk Profile  For Cisco VCS  Parameter Value  ed gateways		Details	up	Time Up: 0 day 0 hour 22 minutes
1*       expressc2.lynclabsp.local         MTP Preferred Originating Codec*         BLF Presence Group*         SIP Trunk Security Profile*         Rerouting Calling Search Space         Out-Of-Dialog Refer Calling Search Space         SIP Profile*         DTMF Signaling Method*         Normalization Script         Ves-interop         Enable Trace         Parameter Name         1         Struct Configuration         @ None         O This trunk connects to a recording-end         O This trunk connects to other clusters         Geolocation Configuration         Geolocation Filter < None >         Geolocation Filter < None >         Searel Delete Reset Add New	711ulaw Standard Presence Expressway Secure < None > < None > < None > Standard SIP Profile RFC 2833 abled gateway with recording-enable	group SIP Trunk Profile  For Cisco VCS  Parameter Value  ed gateways  V V V		Details		Time Up: 0 day 0 hour 22 minutes

Figure 30: Cisco UCM Trunk to Expressway-C-3

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 38 of 145

# Trunk to Expressway-C for MRA with Expressway-E

To configure Expressway-C, please refer to section Expressway-C Configuration

## Navigation: Device -> Trunk

## **Device Information**

- 1. Set Trunk Type: SIP Trunk
- 2. Set Device Protocol: SIP
- 3. Set Trunk Service Type: None
- 4. Set **Device Name**: Enter a name for the trunk
- 5. Set **Description:** Enter a description relevant to your trunk
- Set Device Pool: Select the Device Pool you configured under System -> Device Pool For trunks, device pools specify a list of Cisco Unified Communications Managers that the trunk uses to distribute the call load dynamically
- 7. Set Media Resource Group List: Select the Media Resource Group List you configured under Media Resources -> Media Resource Group List
- 8. Confirm SRTP Allowed: is checked
- 9. Set Consider Traffic on This Trunk Secure: When using both SRTP and TLS
- 10. Set Calling Search Space: CSS Directory URI SIP Information
- 11. Set the **Destination Address**: Enter the FQDN of the Expressway-C to which you are establishing a trunk.
- 12. Set **SIP trunk Security Profile**: Select the security profile you created under System -> Security -> SIP Security Profile
- 13. Set **SIP Profile**: Select the SIP Profile you created under Device -> Device Settings -> SIP Profile
- 14. Set Normalization Script: Select the existing normalization script vcs-interop

Trunk Configuration		Related Links: Back To Find/List 🔻 G
🕞 Save 🗙 Delete 🏻 🖕 Reset 🕂 Add New		
Duration: Time In Full Service: 9 days 19 hours 4 minute	s	
Device Information		
Product:	SIP Trunk	
Device Protocol:	SIP	
Trunk Service Type	None(Default)	
Device Name*	ExpresswayC Core	
Description	Trunk to Expressway Core	
Device Pool*	DP_Richardson 🔻	
Common Device Configuration	< None > T	
Call Classification *	OnNet 🔻	
Media Resource Group List	< None > T	
Location*	Hub_None 🔻	
AAR Group	< None >	
Tunneled Protocol*	None	
QSIG Variant*	No Changes	
ASN.1 ROSE OID Encoding*	No Changes	
Packet Capture Mode*	None	
Packet Capture Duration	0	
Media Termination Point Required		
Retry Video Call as Audio		
Path Replacement Support		
Transmit UTF-8 for Calling Party Name		
Transmit UTF-8 Names in QSIG APDU		
Unattended Port		
SRTP Allowed - When this flag is checked, Encrypted TLS neither information	eds to be configured in the network to provide end to end	l security. Failure to do so will expose keys and

Figure 31: UCM Trunk to Expressway-C for MRA1

-SIP Information				
Destination				
Destination Address is an SRV				
Destination Add	ress Dest	ination Address IPv6	Destination Port	Status
1* expresswayC.tekvizionlabs.com			5061	up
MTP Preferred Originating Codec*	711ulaw	Ŧ		
BLF Presence Group*	Standard Presence group	T		
SIP Trunk Security Profile*	Expressway Secure SIP Trunk Profile for mra	Y		
Rerouting Calling Search Space	< None >	T		
Out-Of-Dialog Refer Calling Search Space	< None >	T		
SUBSCRIBE Calling Search Space	CSS Directory URI	T		
SIP Profile*	Standard SIP Profile For Cisco VCS_copy	▼ <u>/iew Details</u>		
DTMF Signaling Method	RFC 2833	<b>T</b>		
-Normalization Script				
Normalization Script vos-interop	<b></b>			
Enable Trace	_			
Parameter Nam	e P;	arameter Value		
1				

Figure 32: UCM Trunk to Expressway-C for MRA2

# Trunk to IM and Presence Server

Navigation: Device -> Trunk

## **Device Information**

- 1. Set Trunk Type: SIP Trunk
- 2. Set **Device Protocol**: SIP
- 3. Set Trunk Service Type: None
- 4. Set **Device Name**: Enter a name for the trunk
- 5. Set **Description:** Enter a description relevant to your trunk
- 6. Set **Device Pool**: Default

For trunks, device pools specify a list of Cisco Unified Communications Managers that the trunk uses to distribute the call load dynamically

## **SIP Information**

- 7. Set the **Destination Address**: Enter the FQDN of the Cisco IM&P Server to which you are establishing a trunk.
- 8. Set SIP trunk Security Profile: Non-Secure SIP Trunk Profile
- 9. Set SIP Profile: Select the SIP Profile you created under Device -> Device Settings -> SIP Profile

runk Configuration		Related Links: Back To Find/I	List 🗸
📄 Save 💥 Delete 💁 Reset 👍 Add N	ew		
Status			
U Status: Ready			
CID Taugh Status			
Service Status: Full Service			
Duration: Time In Full Service: 0 day 0	hour 9 minutes		
Device Information			
Product:	SIP Trunk		
Device Protocol:	SIP		
Trunk Service Type	None(Default)		
Jevice Name	IM_Presence_Trunk		
Jescription	SIP IM Presence Trunk		
Jevice Pool*	Default	~	
Common Device Configuration	< None >	~	
Call Classification <sup>*</sup>	Use System Default	~	
ledia Resource Group List	< None >	~	
ocation*	Hub_None	~	
AR Group	< None >	~	
unneled Protocol*	None	~	
QSIG Variant <sup>*</sup>	No Changes	~	
SN.1 ROSE OID Encoding*	No Changes	~	
acket Capture Mode*	None	~	
Packet Capture Duration	0		
Media Termination Point Required	( <del>)</del>	i e f	
✓ Retry Video Call as Audio			
Path Replacement Support			
Transmit UTE-8 for Calling Party Name			
Transmit LITE-8 Names in OSIG APDU			
Skip Allowed - When this riag is checked, will expose keys and other information.	Encrypted ILS needs to be configured in the netv	ork to provide end to end security. Fai	iure to a
Consider Traffic on This Trunk Secure <sup>*</sup>	When using both sRTP and TLS	~	
Route Class Signaling Enabled*	Default	~	
Jse Trusted Relay Point <sup>*</sup>	Default	~	
PSTN Access			

Figure 33: Cisco UCM Trunk to IM&P-1

164 Transforma	ation Profile < No	ne >			~		
LPP and Confid	dential Access Le	vel Informat	ion —				
CPP Domain	< None	>			~		
onfidential Acce	ss Mode < None	>			$\sim$		
onfidential Acce	ss Level < None	>			$\checkmark$		
all Routing Inf	ormation ———						
🖞 Remote-Party	-Id						
Asserted-Ider	ntity						
serted-Type*	Default			~			
P Privacy*	Default			~			
Inbound Calls <sup>.</sup>				12			
Significant Digits	*	All			~		
Connected Line	ID Presentation*	Default			~		
Connected Name Presentation*		Default					
Calling Search S	pace	< None >					
- AR Calling Sea	rch Space	< None >					
Profix DN	in opere	< None >					
			0				
Redirecting [	Diversion Header	Delivery - Int	ound				
- Incoming Call	ling Party Setting	s					
Parameter). (	strator sets the p Otherwise, the va	refix to Defa lue configure	d is used as the	call proces prefix unle	sing will use prefix at the next leve ess the field is empty in which case	there is no p	prefix assigned.
			Clear Prefix Set	tings	Default Prefix Settings		
Number Typ	pe P	refix	Strip Digits		Calling Search Space		Use Device Pool CSS
Incoming Nur	mber Default		0	< None	>	~	✓
- Incoming Call	led Party Setting	5					
If the admini Parameter), (	strator sets the p Otherwise, the va	refix to Defa lue configure	d is used as the	call proces prefix unle	sing will use prefix at the next leve ess the field is empty in which case	l setting (De there is no j	prefix assigned.
,.		0	Clear Prefix Set	tings	Default Prefix Settings		
Number Typ	pe P	refix	Strip Digits		Calling Search Space		Use Device Pool CSS

Figure 34: Cisco UCM Trunk to IM&P-2

Outbound Calls		
Called Party Transformation CSS	< None >	T
🖉 Use Device Pool Called Party Transform	nation CSS	
Calling Party Transformation CSS	< None >	T
🖉 Use Device Pool Calling Party Transforr	nation CSS	
Calling Party Selection*	Originator	T
Calling Line ID Presentation*	Default	•
Calling Name Presentation*	Default	T
Calling and Connected Party Info Format $^{st}$	Deliver DN only in connected party	T
Redirecting Diversion Header Delivery	- Outbound	
Redirecting Party Transformation CSS	< None >	T
Use Device Pool Redirecting Party Tran	sformation CSS	
Caller Information		
Caller Name		
Maintain Original Caller ID DN and Ca	ller Name in Identity Headers	
P Information		
N		
Destination Address is an SRV		
Destination Addre	255 Destination	Address IPv6 D

Destination Address		Destination Address IPv6		Destination	
1* clus30pimp.tekvizionlabs.com	1* clus30pimp.tekvizionlabs.com			5060	
MTP Preferred Originating Codec*	711ulaw	Ψ	]		
BLF Presence Group*	Standard Presence gro	up 🔻	]		
SIP Trunk Security Profile*	Non Secure SIP Trunk	Profile 🔻	]		
Rerouting Calling Search Space	< None >	•	]		
Out-Of-Dialog Refer Calling Search Space	< None >	۲	]		
SUBSCRIBE Calling Search Space	< None >	•			
SIP Profile*	SIP Profile IMP	۲	<u>View Details</u>		
DTMF Signaling Method	No Preference	T	<b></b>		

Figure 35: Cisco UCM Trunk to IM&P-3

# SIP Route Pattern

Navigation: Call Routing -> SIP Route Pattern

- 1. Set IPv4 Pattern: Enter the Domain name of the deployment
- 2. Set Description: Enter the description of the SIP Route Pattern
- 3. Set **SIP Trunk**: From the drop-down list select your trunk to Expressway-C

SIP Route Pattern C	onfiguration			
Save 🗙 Delete	Copy 🕂 Add Ne	w		
- Status				
i Status: Ready				
Pattern Definition—				
Pattern Usage	Domain Routing			
IPv4 Pattern*	tekvizionlabs.com			
IPv6 Pattern				
Description	Domain Routing			
Route Partition	< None >	۲		
SIP Trunk/Route List*	ExpressC	۲	(Edit)	
Block Pattern				
┌ Calling Party Transf	ormations			
Use Calling Party's	External Phone Mask			
Calling Party Transform	nation Mask			
Prefix Digits (Outgoing	Calls)			
Calling Line ID Presen	tation* Default		•	
Calling Line Name Pre	sentation* Default		▼	
	·			
Connected Party Tra	nsformations			
Connected Line ID Pre	sentation* Default		¥	
Connected Line Name	Presentation* Default		T	
Save Delete C	opy Add New			

Figure 36: Cisco UCM SIP Route Pattern

# Media Resource Group Configuration

## Navigation: Media Resources->Media Resource Group

Media Resource Group Co	nfiguration	Related Links: Back To Find/List	❤ Go
Save X Delete	Copy 🔂 Add New		
Status i Status: Ready			
Media Resource Group St Media Resource Group: MRG	atus Richardson_Bridges (used by 21 devices)		
Media Resource Group Ir Name* MRG_Richardson Description Conductor Contr	formation _Bridges olled Bridging Resources		
Devices for this Group     Available Media Resources**	ЕХТМТР		
Selected Media Resources*	ANN_2 (ANN) ANN_3 (ANN)	^	
Use Multi-cast for MOH Au	Adhoc_Bridge (CFB) CFB_2 (CFB) CFB_3 (CFB) dio (If at least one multi-cast MOH resource is	available)	
Save Delete Copy	Add New		1

Figure 37: Media Resource Group Configuration

# Media Resource Group List Configuration

## Navigation: Media Resources->Media Resource Group List

Add the above created media resource group to a newly defined media resource group list.

Media Resource Group List Configuration	Related Links: Back To Find/List	✔ Go
🔜 Ssve 🗶 Delete [ Copy 🕂 Add New		
Status Status: Ready		
Media Resource Group List Status Media Resource Group List: MRGL_Richardson (used by 4 devices)		
Media Resource Group List Information Name * MRGL_Richardson		
Media Resource Groups for this List		
Available Media Resource Groups MRG_EXTMTP		
Selected Media Resource Groups MRG_Richardson_Bridges		

Figure 38: Media Resource Group List Configuration

# Add MRGL to Device or Device Pool

## Navigation: System->Device Pool

Device Pool Configuration				Related Links: Back To Find/List	Ƴ Go
🔚 Save 🗙 Delete 📄 Cop	y 🎦 Rese	t 🖉 Apply Config 🕂 Add New			
- Status					^
(1) Status: Ready					
— Device Pool Information — Device Pool: DP_Richardson (8	members**)				
— Device Pool Settings ———					
Device Pool Name*		DP_Richardson			
Cisco Unified Communications Ma	nager Group*	Default	~		
Calling Search Space for Auto-reg	istration	< None >	~		
Adjunct CSS		< None >	~		
Reverted Call Focus Priority		Default	~		
Intercompany Media Services Enro	olled Group	< None >	~		
Local Route Group Settings -     Standard Local Route Group	None >	<b>v</b>			
- Pooming Consitive Cottings -					
Date/Time Group*	CMLocal	$\checkmark$	1		
Region*	Default	$\sim$	1		
Media Resource Group List	MRGL_Richa	rdson 🗸	1		
Location	Richardson	~			
Network Locale	< None >	~			
SRST Reference*	Disable	~			
Connection Monitor Duration***					
Single Button Barge*	Default				
Join Across Lines*	Default	~			
Physical Location	< None >	~			
Device Mobility Group	< None >	~			
Wireless LAN Profile Group	< None >	✓ 1	View Details		

Figure 39: Device Pool Configuration -1

vice Mobility Calling Search S R Calling Search Space R Group ling Party Transformation CS	space < None >			
R Calling Search Space R Group Illing Party Transformation CS			<u> </u>	
R Group Iling Party Transformation CS	< None >		~	
lling Party Transformation CS	< None >		×	
	S < None >		$\checkmark$	
lled Party Transformation CSS	S < None >		×	
eolocation Configuration -				
olocation < None >		~		
olocation Filter < None >		~		
all Routing Information —				
ncoming Calling Party Set	ttinas ———			
If the administrator sets the	prefix to Default this indicate	es call processing will use p	prefix at the next level setting (DevicePool/Service Parameter). Other	erwise,
the value configured is used	as the prefix unless the field	is empty in which case the	ere is no prefix assigned.	
Number Type	Prefix	Strip Digits	Calling Search Space	
National Number	Default		< None > V	
International Number	Default		< None >	
Unknown Number	Default		< None >	
Subscriber Number	Default		< None >	
If the administrator sets the the value configured is used	as the prefix unless the field	is empty in which case the	srefix at the next level setting (DevicePool/Service Parameter). Othere is no prefix assigned.	erwise,
	Cle	ar Prefix Settings	Default Prefix Settings	
Number Type	Prefix	Strip Digits	Calling Search Space	
	Default	0	< None >	
International Number	Default	0	< None >	
International Mamber				
Unknown Number	Default	0	< None > V	
Unknown Number Subscriber Number	Default Default	0	< None > V	

Figure 40: Device Pool Configuration -2

# Cisco UCM LDAP Configuration

LDAP System Configuration

## Navigation: System->LDAP->LDAP System

LDAP System Configurat	tion				
Status Please Delete All LDAN Please Disable LDAP A	P Directories Before Authentication Befo	e Making Changes o re Making Changes	on This Page s on This Page		
LDAP System Information	on ————				
🗹 Enable Synchronizing fr	rom LDAP Server				
LDAP Server Type	Microsoft Active Di	rectory		~	
LDAP Attribute for User ID	sAMAccountName			<b>~</b>	

Figure 41: LDAP System Configuration

### LDAP Directory

Navigation: System->LDAP->LDAP Directory

- 1. Set LDAP Configuration Name: Enter a unique name for the LDAP directory
- 2. Set LDAP Manager Distinguished Name: Enter the user ID of the LDAP Manager, who has administrator access rights
- 3. Set LDAP Password: Enter a password for the LDAP Manager
- 4. Set Confirm Password: Renter the password you provided in LDAP Password field
- 5. Set **LDAP User Search Base:** Enter the location where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup.
- 6. LDAP Server Information:
  - a. Set **Host Name or IP Address for Server:** Enter the host name or IP address of the server where the data for this LDAP directory resides.
  - b. Set **LDAP Port:** Enter the port number on which the corporate directory receives the LDAP requests.
  - c. Confirm Use SSL: is checked
- 7. Click save
- 8. To sync users from the LDAP Directory directly into Communications Manager, you must activate the **Cisco DirSync service**
- 9. Before performing full sync, make sure 'Email' field for users are configured in Active Directory Users and Computers as shown in Figure 2: Active Directory User

DAP Directory			Related Links: Back to LDAP D	Directory Find/List
🚽 Save 🗙 Delete	🗋 Copy 🏠 Perfo	rm Full Sync Now 🕂 Add New		
DAP Directory Inforn	nation-			
DAP Configuration Nam	e* Directory			
DAP Manager Distinguis	thed Name* administrat	ter®teluvizienlahe com		
AP Password*	administrati	conducer vizioniabs.com		
onfirm Deceword*	••••••			
AD Licer Search Pace*	com licore	de=talwizianlahe_de=com		
AP Custom Filter for U	Jsers < None >	T		
/nchronize*	Users (	Only Users and Groups		
AP Custom Filter for (	Groups <pre>&lt; None &gt;</pre>	Ψ		
OAP Directory Synch	ronization Schedule –			
orform Sync Just Once				
arform a Re-sync Every	* 7	DAY 🔻		
ext Re-sync Time (YYY	Y-MM-DD hh:mm)* 201	6-11-03 00:00		
tandard User Fields 1	To Be Synchronized —			
isco Unified Communicat	tions Manager User Field	s LDAP Attribute	Cisco Unified Communications Manager User Fields	LDAP Attribut
ser ID		sAMAccountName	First Name	givenName
iddle Name		middleName 🔻	Last Name	sn
anager ID		manager	Department	department
hone Number		telephoneNumber 🔻	Mail ID	mail
tle		title	Home Number	homephone
lobile Number		mobile	Pager Number	pager
irectory URI		msRTCSIP-primaryuseraddress 🔻	Display Name	displayName
ote: Custom User Field Custom	Names must be same User Field Name	across all synchronization agreements. LDAP Attribute		
roup Information	1 Defeult Here Beels			
ccess Control Groups	1-Default User Kank			
		Add to Acc	ass Control Crown	
		Remove fr	om Access Control Group	
		-		
ature Group Template	Default Feature Group	Template 🔻		
	Warning: The selected f	eature Group Template does not have a Unive	ersal Line Template configured. The new line features below	/ will not be active.
Apply mask to synce Mask	telephone numbers to	create a new line for inserted users		
Assign new line from	the need list if one was	not created based on a synced LDAD tolophor	ne number	
Order DN Pool S	tart DND	not created based on a synced CDAP telephon		
21170015				
Add DM Deal				
Add DN POOL				
DAP Server Informat	ion —			
Uset Name on TD	Address for Server*		LDAP Port* Use TLS	
Host Name of 1P /	to on the sector of the sector			

Figure 42: Cisco UCM LDAP Directory

## LDAP Authentication

LDAP Authentication		
Save		
Status Status: Ready		
LDAP Authentication for End User	s Users administrator@tekvizionlabs.com 	
LDAP Server Information Ho DC01.tekvizionlabs.com Add Another Redundant LDAP Ser	ost Name or IP Address for Server*	LDAP Port <sup>*</sup> Use TLS 636
Save		

Figure 43: Cisco UCM LDAP Authentication

# LDAP-Synced users

Navigation: User Management-> End User

Find a	nd List Users							
d A	dd New Se	lect All Clear All	Delete Sele	cted				
Statur	records found							
User	(1 - 5 of 5)						Rows p	er Page 50 🔻
Find U	ser where First	name	▼ contains	▼ spark		Find Clear Filter 🕂 🛥		
	User ID 📥	Meeting Number	First Name	Last Name	Department	Directory URI	User Status	User Rank
	spark1	2601	spark	one		spark1@tekvizionlabs.com	Enabled LDAP Synchronized User	1
	spark2	2602	spark	two		spark2@tekvizionlabs.com	Enabled LDAP Synchronized User	1
	<u>spark5</u>		Spark	five		spark5@tekvizionlabs.com	Enabled LDAP Synchronized User	1
	<u>spark4</u>	2603	Spark	four		spark4@tekvizionlabs.com	Enabled LDAP Synchronized User	1
	<u>spark3</u>	2659	Spark	three		spark3@tekvizionlabs.com	Enabled LDAP Synchronized User	1
Add	New Select A	ll Clear All Dele	te Selected					

Figure 44: LDAP-Synced users

# User Management Configuration – Settings to Associate Services

Cisco UCM End User Configuration

User Information	
Licer Status	Evabled LDAR Synchronized Upor
User ID*	Enabled LDAF Synchronized Oser
Self-Service User ID	900K1
	2001
PIN	Edit Credential
Confirm PIN	
Last name*	one
Middle name	
First name	spark
Display name	spark one
Title	
Directory URI	spark1@tekvizionlabs.com
Telephone Number	
Home Number	
Mobile Number	
Pager Number	
Mail ID	spark1@tekvizionlabs.com
Manager User ID	
Department	
User Locale	< None > T
Associated PC	
Digest Credentials	
Confirm Digest Credentials	
User Profile	Standard (Factory Default) User Profile
User Rank*	I-Default liser Pank
Convert User Account—	
Convert LDAP Synchron	nized User to Local User
Service Settings	
Home Cluster	
Enable User for U	nified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)
Include mee	ting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)
UC Service Profile	Service_Profile View Details

## Navigation: User Management->End User

Figure 45: Cisco UCM End User Configuration-1

Device Information			
Controlled CFSUSER06			
Devices		Device Asso	ociation
		Line A	ppearance Association for Presen
Available			
Profiles			
	**		
CTI			
Device		♥	
Profiles		*	
Extension Mobility			
Available Profiles			
	<b>*</b> *		
Controlled Profiles			
			<b>₩</b>
			^
Default Profile	Not Selected	~	
BLF Presence Group*	Standard Presence group	~	
SUBSCRIBE Calling Search Space	< None >	~	
Allow Control of Device from C	-11		
Enable Extension Mobility Cros	s Cluster		
Directory Number Associatio	ns		
Primary Extension 2656	~		
— Mobility Information ———			
Enable Mobility			

Enable Mobile Voice Access

Figure 46: Cisco UCM End User Configuration-2

Mobility Information ————				
Enable Mobility				
Enable Mobile Voice Access				
Maximum Wait Time for Desk Pickup*	10000			]
Remote Destination Limit*	4			7
Remote Destination Profiles				_
				View Details
	I			view betains
Mutilevel Precedence and Preem	ption Authorization –			
MLPP User Identification Number				
MLPP Password				
Confirm MLPP Password				
MLPP Precedence Authorization Level	Default		~	
Associated CAPF Profiles				
			View Details	
D				
Groups Admin-3rd Party API				
Application Client Users	^		A of bbA	ccess Control Group
Standard Audit Users Standard CAR Admin Users	~		Remov	e from Access Control Group
Standard CCM Admin Users		View		·
Roles Standard AXL API Access		7		
Standard Admin Rep Tool Adr Standard Audit Log Administr	nin 🔨			
Standard CCM Admin Users	~			
Details		View		
Conference Now Information —				
Enable End User to Host Conference	e Now			
Attendees Access Code				
Save Delete Add New				

Figure 47: Cisco UCM End User Configuration-3

# Cisco Jabber User Configuration

## Navigation: Device->Phone

Device Information		
Device is Active		
M Device is trusted		
Device Name*	CSFUSER06	
Description	Cisco Jabber for 2656	
Device Pool*	DP_Richardson 🔻	<u>View Details</u>
Common Device Configuration	CiscoJabber 🔹	View Details
Phone Button Template*	Standard Client Services Framework	]
Common Phone Profile*	Standard Common Phone Profile	View Details
Calling Search Space	CSS Directory URI	]
AAR Calling Search Space	< None > T	]
Media Resource Group List	< None > T	]
User Hold MOH Audio Source	1-SampleAudioSource 🔻	]
Network Hold MOH Audio Source	1-SampleAudioSource 🔻	]
Location*	Hub_None T	]
AAR Group	< None > T	]
User Locale	< None > T	]
Network Locale	< None > T	]
Built In Bridge*	Default 🔻	]
Device Mobility Mode*	Default 🔻	View Current Device Mobility Settings
Owner	User Anonymous (Public/Shared Space)	_
Owner User ID *	spark4 🔻	
Mobility User ID	< None > T	]
Primary Phone	CSFUSER06	]
Use Trusted Relay Point*	Default 🔻	]
Always Use Prime Line*	Default 🔻	]
Always Use Prime Line for Voice Message*	Default 🔻	]
Geolocation	< None > ¥	]
Ignore Presentation Indicators (internal	calls only)	

Figure 48: Cisco UCM Jabber Client Configuration-1

~	Allow	Control	of	Device	from	CTI	
---	-------	---------	----	--------	------	-----	--

☑ Logged Into Hunt Group

✓ Remote Device

Require off-premise location

#### - Number Presentation Transformation -

Calling Party Transformation CSS	< None >	~
Use Device Pool Calling Party	Fransformation CSS (Caller ID F	For Calls From This Phone)

Calling Party Transformation CSS < None >

Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)

Packet Capture Mode*	None	~	
Packet Capture Duration	0	4	-
BLF Presence Group*	Standard Presence group	~	
SIP Dial Rules	< None >	~	
MTP Preferred Originating Codec*	711ulaw	~	
Device Security Profile*	jabber-secured	~	
Rerouting Calling Search Space	< None >	~	
SUBSCRIBE Calling Search Space	< None >	~	
SIP Profile*	Standard SIP Profile-for phone devices	~	View Details
Digest User	< None >	~	
Media Termination Point Requir	ed		
Unattended Port			
Require DTMF Reception			

V

#### - Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	No Pending Operation	~
Authentication Mode*	By Authentication String	$\sim$
Authentication String	4004563915	
Generate String		
Key Order*	RSA Only	$\checkmark$
RSA Key Size (Bits)*	2048	¥
EC Key Size (Bits)		$\sim$
Operation Completes By	2016 1 13 12 (YYYY:MM:DD:HH	)
Certificate Operation Statu Note: Security Profile Cont	is: Upgrade Success tains Addition CAPF Settings.	

Figure 49: Cisco UCM Jabber Client Configuration-2

Extension Information	
Enable Extension Mobility	
Log Out Profile Use Current Device Settings	~
Log in Time < None >	
Log out Time      < None >	
MLPP and Confidential Access Level Information	1
MLPP Domain < None >	~
Confidential Access Mode < None >	~
Confidential Access Level < None >	~
	¥
SND Incoming Call Alert < None >	~
Product Specific Configuration Layout	
Parameter Value	Override Common Settings
Video Calling <sup>*</sup> Enabled	
2	
<ul> <li>Interactive Connectivity Establishment (ICE)</li> </ul>	
ICE	Enabled V
Default Candidate Type	Host V
Server Reflexive Address	Enabled 🗸
Primary TURN Server Host Name or IP Address	
Secondary TURN Server Host Name or IP Address	
TURN Server Transport Type	
TOKN Server Osername	
TURN Server Password	
- Instant Messaing	
File Types to Block in File Transfer	
UBLS to Block in File Transfer	
De la chercher	
Automatically Start in Phone Control*	Enabled
Automatically Control Tethered Desk Phone*	
Extend and Connect Canability*	
Display Contact Photos "	Enabled V
Number Lookups on Directory*	Enabled V
Jabber For Windows Software Update Server URL	
Problem Report Server URL	
Analytics Collection*	Disabled V
Analytics Server URL	
element element	
Cisco Support Field	configurationfile=jabber-config.xml

Figure 50: Cisco UCM Jabber Client Configuration-3

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 58 of 145

Ch-h		
Status		
— Directory Number Informa	ation	
Directory Number*	656	Urgent Priority
Route Partition <	: None > 🗸	-
Description U	ser One	]
Alerting Name	ser One	]
ASCII Alerting Name	ser One	]
External Call Control Profile <	None > 🗸	
✓ Allow Control of Device fro	m CTI	
Associated Devices	FSUSER06	
		Edit Line Appearance
	**	
Dissociate Devices		
- Directory Number Setting		
Voice Mail Profile		
Calling Search Space	< None >	(Choose <none> to use system default)</none>
BLF Presence Group*	Standard Presence group	
User Hold MOH Audio Source	< None >	×
Network Hold MOH Audio Sour	ce < None >	~
Auto Answer*	Auto Answer Off	~
Reject Anonymous Calls		
Futurning Alternation Normal		
Add Enterprise Alternate Num	te Number	
+E.164 Alternate Number	umber	
Add TE.104 Alternate N	under	

Figure 51: Cisco UCM Jabber Client Configuration-4

Directory URIs —							
Primary			URI	Partiti	on	Advertise Globally via ILS	Edit/Remove
	spark4@tel	vizionlabs.co	m	Directory URI			Edit End User
				< None >	•		
Add Row							
- PSTN Failover for Advertised Failover	Enterprise	Alternate N None >	umber, +E.164 Alternate Numbe	r, and URI Dialing			
AAR Settings							
	Voice I	Mail	AAR Destinat	ion Mask	AA	R Group	
AAR (	or				< None >		•
Retain this des forwarding history	stination in th /	ie call					
-Call Forward and	Call Pickup	Settings —					
		Voice Mail	Destinat	ion	Calling 9	Search Space	
Calling Search Sp	ace Activatio	n Policy			Use System Default		¥
Forward All		🗆 or			< None >		•
Secondary Calling	Search Spa	ce for Forwar	d All		< None >		¥
Forward Busy Inte	ernal	🗆 or			< None >		•
Forward Busy Exte	ernal	🗆 or			< None >		•
Forward No Answe	er Internal	🗆 or			< None >		Ŧ
Forward No Answe	er External	🗆 or			< None >		¥
Forward No Cover Internal	age	or or			< None >		T
Forward No Cover External	age	or			< None >		T
Forward on CTI Fa	ailure	🗆 or			< None >		•

Figure 52: Cisco UCM Jabber Client Configuration-5

— Park Monitoring —				
	Voice Mail	Destination		Calling Search Space
Park Monitoring	or			< None > 🗸 A blank
Forward No Retrieve			V	alue means to call the parker's line.
Destination External				
Park Monitoring	or			< None > 🗸 A blank
Forward No Retrieve			v	alue means to call the parker's line.
Destination Internal				
Park Monitoring Rever	sion		A blank	value will use value set in Park Monitoring Reversion Timer
limer	service	parameter		
— MLPP Alternate Par Target (Destination)	rty And Confid	iential Access Level Settings —		
MUDD Calling Search S				
MLPP Calling Search S	pace	< None >		✓
MLPP No Answer Ring	Duration (secor			
Confidential Access M	ode	< None >	· · · · · · · · · · · · · · · · · · ·	✓
Confidential Access Le	evel	< None >	*	×
Call Control Agent Pro	file	< None >		✓
— Line Settings for A Hold Reversion Ring D	II Devices —			
(seconds)	aradon	the feature		Setting the Hold Reversion Ring Duration to zero will disable
Hold Reversion Notific	ation Interval			Setting the Hold Reversion Notification Interval to zero will
(seconds)		disable the feature		
Party Entrance Tone*		Default	~	
Line 1 on Device C	FSUSER06 —			
Display (Caller ID)	2656	6 - Jan	Display text for	a line appearance is intended for displaying text such as a
	caller.	f a directory number for calls. If yo	u specify a number, th	e person receiving a call may not see the proper identity of the
ASCII Display (Caller ID)	2656			
External Phone Number Mask				
Recording Option*	Call Recording	Disabled	$\checkmark$	
Recording Profile	< None >		~	

Figure 53: Cisco UCM Jabber Client Configuration-6

Recording Gatew Media Source*	ay Preferred	T	
Monitoring < Non Calling Search Space	e >	T	
Multiple Call/Call Waitin	g Settings on Device CSFUSER06		
Note:The range to select th	e Max Number of calls is: 1-6		
Maximum Number of Calls	6		
Busy Trigger*	2		(Less than or equal to Max. Calls)
Caller Number Redirected Number Dialed Number	ne		
	Full Name	User ID	Permission
✓ four,Spar	<u>k</u>	spark4	<b>i</b>
Associate	End Users Select All Clear All Delete Select	ted	
Save Delete Reset	Apply Config Add New		

Figure 54: Cisco UCM Jabber Client Configuration-7

# End Point configurations

*Cisco Telepresence DX70 Configuration* Device Configuration

#### Navigation: Device->Phone->DX70

Phone Type —		
Product Type: Device Protoco	Cisco DX70 I: SIP	
Real-time Devic	e Status	
Registration:	Registered with Cisco Unified Communications Manager clus30sub1.tekvizionlabs.com	

 IPv4 Address:
 10.80.20.29

 Active Load ID:
 sipdx70.10-2-5-212

 Inactive Load
 sipdx70.10-2-5-60

 ID:
 Download

 None
 Status:

#### -Device Information-

Device is Active		
MAC Address*	881DFC6123C8	
Description	SEP881DFC6123C8	
Device Pool*	DP_Richardson	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Cisco DX70 SIP	]
Common Phone Profile*	Standard Common Phone Profile	View Details
Calling Search Space	< None > T	]
AAR Calling Search Space	< None > T	]
Media Resource Group List	MRGL_Richardson 🔹	]
User Hold MOH Audio Source	< None > T	]
Network Hold MOH Audio Source	< None > •	]
Location*	Hub_None T	]
AAR Group	< None > T	]
User Locale	< None > T	]
Network Locale	< None > T	]

Figure 55: DX70 Device Configuration-1

Owner	User Anonymous (Public/Shared Space)	
Owner User ID*	spark2	¥
Mobility User ID	< None >	¥
Phone Personalization*	Default	¥
Services Provisioning*	Default	¥
Phone Load Name		
Use Trusted Relay Point*	Default	¥
BLF Audible Alert Setting (Phone Idle)*	Default	¥
BLF Audible Alert Setting (Phone Busy)*	Default	•
Always Use Prime Line*	Default	Ŧ
Always Use Prime Line for Voice Message*	Default	V
Geolocation	< None >	Ŧ
Feature Control Policy	< None >	Ŧ
Ignore Presentation Indicat	ors (internal calls only)	
Allow Control of Device from	n CTI	
🗹 Logged Into Hunt Group		
Remote Device		
Protected Device****		
-Number Presentation Transf	formation	
┌ Caller ID For Calls From Th	is Phone	
Calling Party Transformation	CSS < None >	Ŧ
☑ Use Device Pool Calling Pa	arty Transformation CSS (Caller ID For Calls From Th	is Phone)
Remote Number		
Calling Party Transformation	CSS < None >	T
🕑 Use Device Pool Calling Pa	arty Transformation CSS (Device Mobility Related Inf	ormation)
- Duotocol Coocific Tufermeti		
Protocol Specific Informatio		
Packet Capture Mode	None	*

Packet Capture Mode*	None	<u>'</u>
Packet Capture Duration	0	
BLF Presence Group*	Standard Presence group	

Figure 56: DX70 Device Configuration-2

Device Security Profile*	Secured DX70	
Rerouting Calling Search Space	< None >	]
SUBSCRIBE Calling Search Space	< None >	]
SIP Profile*	Standard SIP Profile For Cisco VCS	View Details
Digest User	<pre>&lt; None &gt;</pre>	]
🔲 Media Termination Point Requir	ed	
Unattended Port		
Require DTMF Reception		
Certification Authority Proxy Fi	Inction (CAPF) Information	

Certificate Operation*	No Pending Operation	¥
Authentication Mode*	By Null String	Ŧ
Authentication String		
Generate String		
Key Order*	RSA Only	Ŧ
RSA Key Size (Bits)*	2048	Ŧ
EC Key Size (Bits)		Ŧ
Operation Completes By	2016 11 10 12 (YYYY:MM:DD:HH)	
Certificate Operation Status: Note: Security Profile Contai	None ns Addition CAPF Settings.	

-External Data Locations	Information (Leave blank to use default)	
Information		
Directory		
Messages		1
Services		1
Authentication Server		
Proxy Server		
Idle		
Idle Timer (seconds)		
Secure Authentication URL		
Secure Directory URL		
Secure Idle URL		
		,

Figure 57: DX70 Device Configuration-3

Secure Idle URL	
Secure Information URL	
Secure Messages URL	
Secure Services URL	

#### - Extension Information

Enable Extension Mobility				
Log Out Profile	Use Current Device Settings			
Log in Time	< None >			
Log out Time	< None >			

#### MLPP and Confidential Access Level Information-

MLPP Domain	< None >	$\checkmark$
Confidential Access Mode	< None >	¥
Confidential Access Level	< None >	$\checkmark$

Product Specific Configuration Layout		
?	Parameter Value	Override Common Settings
Room Name (from Exchange(R))		
Web Access*	Enabled 🗸	
SSH Access*	Disabled 🗸	
Default Call Protocol*	SIP 🗸	
Quality Improvement Server		
Multipoint Mode*	Use Media Resource Group List 🛛 🗸	
Telnet Access*	On 🗸	
Microphone Unmute On Disconnect*	On 🗸	
Call Logging Mode*	On 🗸	
OSD Encryption Indicator*	Auto 🗸	
Alternate phone book server type*	UDS 🗸	
Alternate phone book server address		

Figure 58: DX70 Device Configuration-4

Default Volume	70
Max Total Downstream Rate	10000
Max Total Unstream Rate	10000
System Name	10000
System Name	
CTMS Settings	
CTMS Multiparty Conference	ing* On 🗸
CTMS Encryption Mode*	Off 🗸
- Cash Cashal Cash	
Far End Camera Control Set	angs
Far End Camera Control Siz	naling Canability* O-
rai cilo camera control sig	
Facility Service Settings	
Facility Service Type*	Helpdesk 🗸
Facility Service Name	
Facility Service Number	
Facility Service Call Type*	Video
	•
Standby Settings	
Standby Mode* On	V
Standby Delay 10	
Standby Action* Privacy P	osition 🗸
-Serial Port Settinos	
Serial Port*	On v
Serial Port Login Required*	
Admin username and passw	ord
Admin Username admin	
Admin Password	••••••

### Figure 59: DX70 Device Configuration-5

Dial Plan	
Site Access Code	
Inter Site Access Code	
Off-Net Access Code	
National Dialing Digits	
International Dialing Digits	
Country Code Area Code Local Number	
Osd Todays Bookings <sup>*</sup> Off	✓

Figure 60: DX70 Device Configuration-6

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 67 of 145

# Line Configuration

Directory Num	nber Infori	nation			
Directory Number*	2602			L	Jrgent Priority
Route Partition	< None >		¥		
Description					
Alerting Name					
ASCII Alerting Name					
External Call Control Profile	< None >		¥		
Allow Contr	ol of Device	from CTI			
Associated	SEP881DF0	C6123C8			
Devices				Ed	it Device
				Ed	it Line Appearance
			Ψ.		
		~~			
Dissociate Devices			<b>A</b>		
200000			-		
Directory Num	nber Settin	gs			
Voice Mail Prof	ile	< None >		• ((	Choose <none> to</none>
		use system default)			
Calling Search	Space	CSS Directory URI		•	
BLF Presence (	Group*	Standard Presence group		•	
User Hold MOH Source	Audio	< None >		¥	
Network Hold N Source	10H Audio	< None >		¥	
Auto Answer*		Auto Answer with Speakerphone		¥	
Reject Anor	nymous Call	s			
Enterprise Alt	ternate Nur	nber			
Add Enterprise	e Alternate I	lumber			
Add Enterprise	- Alternate I	ium out			

Navigation: Device->Phone->DX70->Line [1]

Figure 61: DX70 Line [1] Configuration-1

-Directory URI	s ———				
Primary		URI			Partition
	spar	k2@tekvizionlabs.com	Dir	rectory	URI
			<	None >	Υ.
Add Row					
-PSTN Failover Advertised Failo	<b>for Ente</b> ver Numb	erprise Alternate Number, +E.164 Alternate Numbe oer	r, ar	nd URI	Dialing
-AAR Settings -					
Voice Mail		AAR Destination Mask			AAR Group
AAR				< None	e >
or					
Retain this destination in the call forwarding history					
-Call Forward a	and Call I	Pickup Settings			
	Voice Mail	Destination			Calling Search Space
Calling Search	Space A	ctivation Policy			Use System Default
Forward All					< None >
	or				
Secondary Ca	lling Sear	ch Space for Forward All			< None >
Forward Busy Internal	or				< None >
Forward Busy	or				< None >

Figure 62: DX70 Line [1] Configuration-2

Forward Unregistered Internal	✓ or			< None >	~
Forward Unregistered External	🗸 or			< None >	~
No Answer Ring Duration (se	conds) 20				
Call Pickup Group	< No	ne >	~		

— Park Monitoring ———			
Voice Mail	Destination		Calling Search Space
Park Monitoring or Forward No Retrieve Destination External		< No value	ne > 🗸 A blank means to call the parker's line.
Park Monitoring or Forward No Retrieve Destination Internal		< No value	means to call the parker's line.
Park Monitoring Reversion	ervice parameter	A blank val	ue will use value set in Park Monitoring Reversion Timer
	6		
Target (Destination)	Confidential Access Level Setting	js —	]
MLPP Calling Search Space	< None >	~	-
MLPP No Answer Ring Duration	n (seconds)		]
Confidential Access Mode	< None >	~	
Confidential Access Level	< None >	~	
Call Control Agent Profile	< None >	~	
— Line Settings for All Device Hold Reversion Ring Duration	es		
(seconds)	the feature	S(	etting the Hold Reversion Ring Duration to zero will disable
Hold Reversion Notification Int (seconds)	erval disable the feature	S	etting the Hold Reversion Notification Interval to zero will
Party Entrance Tone*	Default	~	
- Line 1 on Dovice CED00E0	60084650		
Display (Caller	00004029	Display text for a l	ine appearance is intended for displaying text such as a

ID) Display text for a line appearance is intended for displaying text such as a name instead of a directory number for calls. If you specify a number, the person receiving a call may not see the proper identity of

Figure 63: DX70 Line [1] Configuration-3

_ Multiple (	Call/Call Waiting Settings on De	vice SEP881DFC6123C8				
Note:The calls is: 1-	Note:The range to select the Max Number of calls is: 1-200					
Maximum	Maximum Number of Calls* 4					
Busy Trigg	er*	2 (L				
		than or equal to Max. Calls)				
Forwarde	d Call Information Display on D	evice SEP881DFC6123C8				
Caller	Name					
Caller	Number					
Redire	cted Number					
Dialed	Number					
Users As	sociated with Line					
	Full Name	User ID	Permission			
	🗹 <u>two,spark</u> spark2 🛈					
Associate End Users Select All Clear All Delete Selected						
Save Delete Reset Apply Config Add New						

Figure 64: DX70 Line [1] Configuration-4

*Cisco DX80 Configuration* Device Configuration

### Navigation: Device->Phone->DX80

Device Information			
🗹 Device is Active			
V Device is trusted			
MAC Address*	7426ACEF053D		
Description	SEP7426ACEF053D		
Device Pool*	DP_Richardson	•	View
	Details		
Common Device Configuration	< None >	۲	<u>View</u>
Dhana Buttan Tamplata*	Details		1
	Standard Cisco TelePresence DX80	-	]
Common Phone Profile"	Standard Common Phone Profile	•	View
Calling Search Space	< None >	•	]
AAR Calling Search Space	< None >	•	ĺ
Media Resource Group List	< None >	•	ĺ
User Hold MOH Audio Source	< None >	•	ĺ
Network Hold MOH Audio Source	< None >	•	j
Location*	Hub_None	۲	]
AAR Group	< None >	•	]
User Locale	< None >	•	]
Network Locale	< None >	•	]
Privacy*	Default	۲	
Device Mobility Mode*	Default	۲	View
	Current Device Mobility Settings		
Owner	🖲 User 🔍 Anonymous (Public/Shared Space)		
Owner User ID*	spark3	۲	]
Mobility User ID	< None >	۲	)
Phone Load Name	sipdx80.ce821.rel.loads		
Use Trusted Relay Point*	Default	•	]
Always Use Prime Line*	Default	•	]
Always Use Prime Line for Voice Message*	Default	۲	]
Geolocation	< None >	۲	]
Retry Video Call as Audio			
Ignore Presentation Indicat	ors (internal calls only)		

Figure 65: DX80 Device Configuration-1

© 2016 Cisco Systems, Inc. All rights reserved.

Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 72 of 145
Ignore Presentation Indicators (internal calls only)

Allow Control of Device from CTI

☑ Logged Into Hunt Group

Remote Device

Protected Device\*\*\*\*

#### - Number Presentation Transformation -

- Caller ID For Calls From This Phone Calling Party Transformation CSS <a>[< None ></a>

☑ Use Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)

- Remote Number -

Calling Party Transformation CSS < None >

Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)

Packet Capture Mode*	None	~
Packet Capture Duration	0	
BLF Presence Group*	Standard Presence group	~
SIP Dial Rules	< None >	~
MTP Preferred Originating Codec*	711ulaw	$\sim$
Device Security Profile*	DX80 secured	~
Rerouting Calling Search Space	< None >	~
SUBSCRIBE Calling Search Space	< None >	~
GIP Profile*	Standard SIP Profile For TelePresence	Conferencin View De
Digest User	< None >	~
Media Termination Point Requir	ed	
Unattended Port		
Require DTMF Reception		

 $\checkmark$ 

~

<ul> <li>Certificate Operation*</li> </ul>	Proxy Function (CAPF) Information	n
Certificate Operation	No Pending Operation	•
Authentication Mode*	By Null String	~
Authentication String		
Generate String		
Key Order*	RSA Only	~

Figure 66: DX80 Device Configuration-2

RSA Key Size (Bits)*	2048	~	
EC Key Size (Bits)		~	
Operation Completes By	2016 2 7 12 (YYYY:MM:DD	нн)	
Certificate Operation Statu Note: Security Profile Con	is: None tains Addition CAPF Settings.		
– External Data Location	IS Information (Leave blank to use defau	lt)	
Messages	10		
Messages			
Services			
Authentication Server			
Proxy Server	l		
Idle			
Idle Timer (seconds)			
Secure Authentication URL			
Secure Directory URL			
Secure Idle URL			
Secure Information URL			
Secure Messages URL			
Secure Services URL			
	2		
– Extension Information	1 <del></del>		
Enable Extension Mobil	ity		
Log Out Profile Use Cu	rrent Device Settings V		
Log in Time < None >			
Log out Time < None >			
– MLPP and Confidential	Access Level Information		
MLPP Domain	< None >	✓	
MLPP Indication*	Default		
MLPP Preemption*	Default	<u> </u>	
Confidential Access Mode	< None >	✓	
Confidential Access Level	< None >	$\checkmark$	

Figure 67: DX80 Device Configuration-3

– Do Not Disturb ——				
🗌 Do Not Disturb				
DND Option*	Use Common Phone Profile	Setting 🗸		
DND Incoming Call Alert	< None >	✓		
- Secure Shell Informa Secure Shell User	ation —			
Secure Shell Password				
– Product Specific Con	figuration Layout ———	-		
		Parameter Value		Override Common Settings
Disable Speakerphor	ne			
Disable Speakerphor	ne and Headset			
Disable USB				
SDIO*		Disabled	~	
Bluetooth*		Enabled	~	
Allow Bluetooth Contacts	s Import*	Enabled	~	
Allow Bluetooth Mobile H	landsfree Mode*	Enabled	~	
Days Display Not Active		Sunday	~	
		Monday Tuesday	~	
Display On Time		07:30		
Display On Duration		10:30		
Display On When Incomi	ing Call*	Enabled	~	
Essble Audible Alert			1	
EnergyWise Domain				
EnergyWise Endpoint Se	curity Secret			
Allow EnergyWise Ov     Recording Tone*	rriaes	Disabled		
Recording Tone Local Vo	olume*		•	
Recording Tone Persote	Volume*	100		
Recording Tone Remote	volume	50		
Cookle widebood or d	-*			
Enable Wideband Codec	S	Use System Default	~	
Video Calling*		Enabled	~	
Device UI Profile*		Simple	~	
Wifi*		Enabled	$\sim$	

Figure 68: DX80 Device Configuration-4

PC Port*	Enabled V	
Span to PC Port*	Disabled V	
PC Voice VLAN Access*	Enabled 🗸	
PC Port Remote Configuration*	Disabled V	
Switch Port Remote Configuration*	Disabled V	
Detect Unified CM Connection Failure*	Normal	
Gratuitous ARP*	Disabled V	
Cisco Discovery Protocol (CDP): Switch Port*	Enabled 🗸	
Cisco Discovery Protocol (CDP): PC Port*	Enabled 🗸	
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP- MED): Switch Port*	Enabled V	
Link Layer Discovery Protocol (LLDP): PC Port*	Enabled 🗸	
LLDP Asset ID		
LLDP Power Priority*	Unknown 🗸	
Power Negotiation*	Enabled 🗸	
Automatic Port Synchronization*	Disabled V	
802.1× Authentication*	User Controlled 🗸	
Always On VPN		
Store VPN Password on Device		
Allow User-Defined VPN Profiles		
☑ Allow User-Defined VPN Profiles Require Screen Lock*	User Controlled	
☑ Allow User-Defined VPN Profiles Require Screen Lock* Maximum Screen Lock Timeout*	User Controlled V	
<ul> <li>✓ Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>✓ Enforce Screen Lock During Display-On Time</li> </ul>	User Controlled V	
<ul> <li>✓ Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>✓ Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> </ul>	User Controlled 600 Disabled	
<ul> <li>✓ Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>✓ Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> <li>Kerberos Server</li> </ul>	User Controlled  Controlled	
<ul> <li>Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> <li>Kerberos Server</li> <li>Kerberos Realm</li> </ul>	User Controlled	
<ul> <li>✓ Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>✓ Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> <li>Kerberos Server</li> <li>Kerberos Realm</li> <li>Load Server</li> </ul>	User Controlled	
<ul> <li>✓ Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>✓ Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> <li>Kerberos Server</li> <li>Kerberos Realm</li> <li>Load Server</li> <li>IPv6 Load Server</li> </ul>	User Controlled	
<ul> <li>Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> <li>Kerberos Server</li> <li>Kerberos Realm</li> <li>Load Server</li> <li>IPv6 Load Server</li> <li>Peer Firmware Sharing*</li> </ul>	User Controlled	
<ul> <li>Allow User-Defined VPN Profiles</li> <li>Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>Enforce Screen Lock During Display-On Time</li> <li>Lock Device During Audio Call*</li> <li>Kerberos Server</li> <li>Kerberos Realm</li> <li>Load Server</li> <li>IPv6 Load Server</li> <li>Peer Firmware Sharing*</li> <li>Log Server</li> </ul>	User Controlled	
<ul> <li>✓ Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>✓ Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> <li>Kerberos Server</li> <li>Kerberos Realm</li> <li>Load Server</li> <li>IPv6 Load Server</li> <li>Peer Firmware Sharing*</li> <li>Log Server</li> <li>IPv6 Log Server</li> </ul>	User Controlled	
<ul> <li>✓ Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>✓ Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> <li>Kerberos Server</li> <li>Kerberos Realm</li> <li>Load Server</li> <li>IPv6 Load Server</li> <li>Peer Firmware Sharing*</li> <li>Log Server</li> <li>IPv6 Log Server</li> <li>Log Server</li> <li>Log Profile</li> </ul>	User Controlled	
<ul> <li>✓ Allow User-Defined VPN Profiles Require Screen Lock*</li> <li>Maximum Screen Lock Timeout*</li> <li>✓ Enforce Screen Lock During Display-On Time Lock Device During Audio Call*</li> <li>Kerberos Server</li> <li>Kerberos Realm</li> <li>Load Server</li> <li>IPv6 Load Server</li> <li>Peer Firmware Sharing*</li> <li>Log Server</li> <li>Log Server</li> <li>Log Server</li> <li>Log Profile</li> </ul>	User Controlled	

Figure 69: DX80 Device Configuration-5

SSH Access*	Disabled V	
Android Debug Bridge (ADB)*	Disabled 🗸	
Multi-User*	Disabled 🗸	
Allow Applications from Unknown Sources*	Disabled 🗸	
Allow Applications from Google Play		
Enable Cisco UCM App Client		
Background Image		
Company Photo Directory		
Voicemail Server (Primary)		
Voicemail Server (Backup)		
Presence and Chat Server (Primary)		
Presence and Chat Server Type*	Cisco WebEx Connect 🗸	
Presence and Chat Single Sign-On (SSO) Domain		
Multi-User URL		
Email address for customer support		
Customer support upload URL		
User Credentials Persistent for Expressway Sign in $st$	Disabled V	

Figure 70: DX80 Device Configuration-6

# Line Configuration

Directory N	umber Infor	mation		
Directory	2659			Urgent Priority
Route [	< None >		¥	
Description				
Alerting Name	User Eight			
ASCII Alerting Name	User Eight			
External [ Call Control	< None >		¥	
Profile				
Allow Cor	ntrol of Devic	e from CTI		
Associated Devices	SEP7426ACEF	053D	*	Edit Device
			_	Edit Line Appearance
L			·	
Dissociate		**		
Devices				
L			*	
Directory N	umber Setti	105		
Voice Mail Pr	ofile			Chaose (None)
voice riairri	0.110	to use system default)		(Choose <none></none>
Calling Sear	ch Space	< None >		T
BLF Presence	e Group*	Standard Presence group		Y
User Hold MC Source	OH Audio	1-SampleAudioSource		T
Network Hold Source	d MOH Audio	1-SampleAudioSource		T
Auto Answer	.*	Auto Answer Off		¥
🗌 Reject Ar	nonymous Cal	ls		

Navigation: Device->Phone-> DX80 ->Line [1]

Figure 71: DX80 Line [1] Configuration-1

AAR Settings				
Va	oice Mail	AAR Destination Mask	AAR Group	
AAR 🗌 or			< None >	~
Retain this destination forwarding history	in the call			
Call Forward and Call I	Pickup Settings Voice	Destination	Calling Search S	ipace
Calling Search Space Act	Mail			
Calling Search Space Act			Use System Derault	• •
			<pre>&lt; None &gt;</pre>	~
Secondary Calling Search	n Space for Forward All		< None >	~
Forward Busy Internal	🗌 or 📃		< None >	~
Forward Busy External	🗌 or 📃		< None >	~
Forward No Answer Internal	🗌 or		< None >	~
Forward No Answer External	🗌 or		< None >	~
Forward No Coverage Internal	🗌 or		< None >	~
Forward No Coverage External	🗌 or		< None >	~
Forward on CTI Failure	🗌 or 🛛		< None >	~
Forward Unregistered Internal	🗌 or 🛛 🚺		< None >	~
Forward Unregistered External	🗌 or		< None >	~
o Answer Ring Duration (	seconds) 300		7	
all Pickup Group	< None >	~	]	
Park Monitoring ———			200	
V	oice Iail	Destination	Calling Search Space	
Park Monitoring Forward No	] or		< None > value means to call the parker's line.	✓ A blank

< NOTE >							
value means t	o call	the	parker's	line.			

Figure 72: DX80 Line [1] Configuration-2

Destination External

Park Monitoring	or			< None >	A blank
Retrieve Destination Internal			X	value means to call the par	ker's line.
ark Monitoring Reversion			A blank	value will use value set in	Park Monitoring Reversion Timer
imer	service pa	arameter			
MLPP Alternate Party A	and Confide	ntial Access Level Sett	ings —		
arget (Destination)					
1LPP Calling Search Space	•	< None >		~	
ILPP No Answer Ring Dura	ition (seconds	s)			
Confidential Access Mode		< None >		~	
Confidential Access Level		< None >		~	
Call Control Agent Profile		< None >		~	
Line Settings for All De old Reversion Ring Durati	vices —				
seconds)	1	the feature		Setting the Hold Reversi	on Ring Duration to zero will disable
Iold Reversion Notification	Interval [			Setting the Hold Reversi	on Notification Interval to zero will
seconds)	1	disable the feature			
arty Entrance Tone*		Default	~		
ASCII Display (Caller ID)	name instea of the caller	ad of a directory number f r.	or calls. If you specify a num	ber, the person receiving a	a call may not see the proper identit
ASCII Display (Caller ID) Line Text Label External Phone	name instea of the caller	ad of a directory number f	or calls. If you specify a num	ber, the person receiving a	a call may not see the proper identit
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Ladicator Boliny *	name instea of the caller	ad of a directory number f n Policy	or calls. If you specify a num	ber, the person receiving a	a call may not see the proper identit
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator	name instea of the caller Use System	ad of a directory number f	v	ber, the person receiving a	a call may not see the proper identit
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone	Iname instea of the caller Use System Default	ad of a directory number f  n Policy n Default	v	ber, the person receiving a	a call may not see the proper identit
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)*	Iname instead of the caller	ad of a directory number f  n Policy n Default	v	ber, the person receiving a	a call may not see the proper identit
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active)	Use System	ad of a directory number f  n Policy n Default n Default	Compared to the second se	this line when any line on t	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active) Call Pickup Group Audio Alert Setting (Phone Idle)	Iname instead of the caller Use System Use System Use System Use System	ad of a directory number f  n Policy n Default n Default n Default	Compared to the second se	this line when any line on t	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active) Call Pickup Group Audio Alert Setting (Phone Idle)	Iname instead of the caller Use System Default Use System Use System	ad of a directory number f	Constant of the constant	this line when any line on t	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active) Call Pickup Group Audio Alert Setting (Phone Idle)	Iname instead of the caller Use System Default Use System Use System Use System	ad of a directory number f	Control of the second	this line when any line on t uration-3	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active) Call Pickup Group Audio Alert Setting (Phone Idle)	Default Use System Use System Use System Use System Use System Use System	ad of a directory number f	Cor calls. If you specify a num  Cor calls. If you specify a num  Applies to  Cor calls. If you specify a num  Cor calls. If you sp	this line when any line on t	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active) Call Pickup Group Audio Alert Setting (Phone Idle) fultiple Call/Call Waiting lote:The range to select th faximum Number of Calls*	Ame instead of the caller Use System Use System Use System Use System Use System Use System Settings or e Max Number	ad of a directory number f	Control of the second	this line when any line on t	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Idle)* Call Pickup Group Audio Alert Setting (Phone Idle) Iultiple Call/Call Waiting Iote:The range to select th Iaximum Number of Calls*	Use System	ad of a directory number f	Image: constraint of the second se	this line when any line on t	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active) Call Pickup Group Audio Alert Setting (Phone Idle) Nultiple Call/Call Waiting Iote:The range to select th Iaximum Number of Calls* Ious Trigger*	Ame instead of the caller of the caller Use System Use System Use System Use System Use System Gettings of Max Number American Strategy Settings of Max Number Settings of Settings of Setings of Setings of Setings of Settings of Settings of S	n Default n Default Figure 7 n Default for the september of calls is: 1-4 4 4 0 Default 4	Control calls. If you specify a num  Control ca	this line when any line on t	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active) Call Pickup Group Audio Alert Setting (Phone Idle) Nultiple Call/Call Waiting Iote: The range to select th Iaximum Number of Calls* Busy Trigger*	Iname instead of the caller Iname instead of the caller Iname instead Use System Use System Use System Use System Use System Use System Iname instead Settings of Max Number ion Display of	ad of a directory number f n Default n Default Figure 7. n Default Figure 7. n Device SEP7426ACEF0 er of calls is: 1-4 4 4 4 on Device SEP7426ACEF1	Costable Control of C	this line when any line on t	the phone has a call in progress.
ASCII Display (Caller ID) Line Text Label External Phone Number Mask Visual Message Waiting Indicator Policy* Audible Message Waiting Indicator Policy* Ring Setting (Phone Idle)* Ring Setting (Phone Active) Call Pickup Group Audio Alert Setting (Phone Idle) Nultiple Call/Call Waiting Iote:The range to select th Iaximum Number of Calls* usy Trigger*	ame instea of the caller use System Default Use System Use System Use System Settings of e Max Number of bion Display of	ad of a directory number f	Costable Control of C	this line when any line on t	the phone has a call in progress.

Reun	ecteu	Num

🔲 Dialed Number

#### Users Associated with Line

	Full Name		User ID	Per	mission	
	three,Spark	sp	ark3	í		
	Associate End Users Select All	Clear All Delete Selected				

Save Delete Reset Apply Config Add New

Figure 74: DX80 Line [1] Configuration-4

© 2016 Cisco Systems, Inc. All rights reserved.

Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

# Expressway-C Configuration

# System Configuration

IP Configuration

### Navigation: System->IP Address

(j)

Save

Status		
Protocol	IPv4	
IPv4 gateway	10.80.20.1	
LAN 1	IPv4 address	10.80.20.6
	IPv4 subnet mask	255.255.255.0

Figure 75: Expressway-C-IP Address Configuration

### Option Keys

#### Navigation: Maintenance->Option keys

Note: AV integration between Skype for Business and UCM via Expressway requires the option keys as shown below.

Ensure the required licenses for the highlighted options are installed and available if video integration is performed.

Status System Configuration Applic	ations Users Maintenance		? •
Option keys		Ye	ou are here: <u>Maintenance</u> ⊁ Option keys
Key 👻	Description	Status	Validity period
116341C00-1-F60D1E7F	Microsoft Interoperability	Active	Unlimited
116341E00-1-01D2F5B1	Expressway Series	Active	Unlimited
116341W50-1-7C16DE39	50 Traversal Calls	Active	Unlimited
Delete Select all Unselect all			
System information	·		
Serial number	01616DF6		
Active options	50 Rich Media Sessions, 0 Room Systems, 0 D FindMe, Device Provisioning, Microsoft Interope	)esktop Systems, Encry erability, Expressway Se	ption, Interworking, ries.
Software option	]		
Add option key		)	
Add option			
Release key	·		
Release key			
Set release key			
Current licenses			
Traversal calls 50			

Figure 76: Expressway-C-Options

## DNS Configuration

### Navigation: System-> DNS

DNS			You are here: <u>System</u> + f
DNS settings		]	
System host	† expressc2	i	
Domain name	tekvizionlabs.com	i	
DNS requests	t Use the ephemeral port range	ge 🔻 i	
port range			
Default DNS ser	vers	]	
Address 1	† 10.85.0.12	(j)	
Address 2	†	i	
Address 3	†	i	
Address 4	†	i	
Address 5	†		
Per-domain DNS	servers	]	
Address 1	10.85.0.12	i	Domain names: tekvizionlabs.com
		1	
Address 2		(i)	Domain names:
Address 3	t	(i)	Domain names:
Address 4	•		
Address 4		U	Lomain names:
Address 5	t	(j	Domain names:
		1	
Save Flush DNS	cache		

Figure 77: Expressway-C-DNS Configuration

## NTP Configuration

### Navigation: System->Time

ITP server 1	Address 10.10.10.5	Authentication
	Disabled 🗸 👔	
ITP server 2	† Address	(1) Authentication
	Disabled 🗸 🕡	
VTP server 3	† Address	Authentication
	Disabled 🗸 🕧	
VTP server 4	† Address	Authentication
	Disabled 🗸 🕧	
ITP server 5	† Address	Authentication
	Disabled 🗸 👔	

Figure 78: Expressway-C-NTP Configuration

### TLS in SIP Configuration

# Navigation: Configuration->Protocols->SIP

IP	You	are here: Configuration Protocols S
Configuration		1
SIP mode	On V ()	
UDP mode	On V (1)	
UDP port	* 5060	
TCP mode	On 🗸 👔	
TCP port	* 5060	
TLS mode	On 🗸 👔	
TLS port	* 5061	
Mutual TLS mode	Off V	
Mutual TLS port	* 5062	
TCP outbound port start	* 25000	
TCP outbound port end	* 29999 ()	
TLS handshake timeout (seconds)	* 5	
Certificate revocation checking		
Certificate revocation checking mode	On V ()	
Use OCSP	Yes V	
Use CRLs	Yes V Di Manage CRLs	
Allow CRL downloads from CDPs	Yes 🗸 🧃	
Fallback behavior	Treat as revoked V	
Advanced		
SDP max size	* 32768	
SIP TCP connect timeout	* 10 (i)	

Figure 79: Expressway-C-SIP Configuration

## Microsoft Lync B2BUA configuration (Skype for Business B2BUA)

Navigation: Applications->B2BUA->Microsoft Interoperability->Configuration

- 1. Set Microsoft Interoperability: Enabled
- 2. Set **destination address:** Enter the IP address or FQDN of the server to which the B2BUA sends the signaling messages, Skype for Business Server here.
- 3. Set destination port: 5061
- 4. Set signaling transport: TLS

Microsoft Interoperability		You are here: <u>Applications</u> > <u>B2BUA</u> > <u>Microsoft interoperability</u> > Configurat
Microsoft interoperability	Enabled 🔻 👔	
Destination address	fe01.tekvizionlabs.com	Configure trusted hosts
Listening port	* 5061	
Signaling transport	TLS V	
Remote Desktop Protocol		
Enable RDP transcoding for this B2BUA	Yes 🔻 🕕	
External transcoders		
Enable external transcoders for this B2BUA	No V	
SIP broker		
Enable broker for inbound SIP	No V (j)	
TURN		
Offer TURN services	Yes	i
Advanced		
Advanced settings	Show advanced settings	

#### Save

B2BUA service	
Status	Connected
Expressway	
URI	<sip:localservice.localdomain:5061;transport=tls;lr></sip:localservice.localdomain:5061;transport=tls;lr>
Mode	Standard
Status	Alive
Microsoft server	
URI	<sip:fe01.tekvizionlabs.com:5061;transport=tls;lr;ds></sip:fe01.tekvizionlabs.com:5061;transport=tls;lr;ds>
Mode	Microsoft
Status	Alive

Figure 80: Expressway-C-Microsoft Lync (Skype for Business B2BUA) B2BUA Configuration

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 86 of 145

## Microsoft Lync (Skype for Business) B2BUA trusted hosts

Expressway and Skype for Business Front End server should be added to the trusted host list.

Trusted hosts	You are here: <u>Applications</u> + <u>B2BUA</u> + <u>Microsoft interoperability</u> + <u>Trusted hosts</u> + Edit
Configuration	
Name	expressc2.tekvizionlabs.com
IP address	10.80.20.6
Туре	Microsoft infrastructure 🔻 👔
Save Delete Cancel	

Navigation: Applications->B2BUA->Microsoft Lync->B2BUA trusted hosts

Figure 81: Expressway-C-Microsoft Lync (Skype for Business) B2BUA trusted hosts-1

Trusted hosts	You are here: <u>Applications</u> • <u>B2BUA</u> • <u>Microsoft interoperability</u> • <u>Trusted hosts</u> • Edit
Configuration	
Name	fe01.tekvizionlabs.com
IP address	10.85.0.20
Туре	Microsoft infrastructure 🔻
Save Delete Cancel	

Figure 82: Expressway-C-Microsoft Lync (Skype for Business) B2BUA trusted hosts-2

### Loading server and trust certificates

#### Expressway-C Server Certificate

#### Navigation: Maintenance->Security Certificates->Server certificate

This is used to manage the Expressway-C's server certificate. This certificate is used to identify the Expressway-C server when it communicates with systems using TLS encryption.

	You are here: Maintenance Security certificates Server certi
Server certificate data	
Server certificate	Show (decoded) Show (PEM file)
Currently loaded certificate expires	May 28 2016
eset to default server certificate	
Certificate signing request (CSR)	
Certificate request	There is no certificate signing request in progress
Certificate request	There is no certificate signing request in progress
Certificate request	There is no certificate signing request in progress
Certificate request Generate CSR Upload new certificate Select the server private key file	There is no certificate signing request in progress

Figure 83: Expressway-C-Generate CSR-1

List of SAN entries required for Generating CSR:

- Fqdn of the expressway, expressc2.tekvizionlabs.com here.
- Fqdn of the CUCM, clus30pub.tekvizionlabs.com here.

Generate CSR	You are here: <u>Maintenance</u> > <u>Security certificates</u> > Generate CSR
Common name	
Common name	FQDN of Expressway cluster 🔻 🦚
Common name as it will	expressc2.tekvizionlabs.com
appear	
Alternative name	
Subject alternative names	FQDN of Expressway cluster plus FQDNs of all peers in the cluster <b>*</b>
Additional alternative names	expressc2.tekvizionlabs.com,clus30pub.tekvizionlabs.com
(comma separated)	
Alternative name as it will	DNS:expressc2.tekvizionlabs.com
appear	DNS:clus30pub.tekvizionlabs.com
Additional information	
Key length (in bits)	2048 V (1)
Country	* US (1)
State or province	* Texas
Locality (town name)	* Richardson
Organization (company name)	* Tekvizion
Organizational unit	* Labs
Email address	
Generate CSR	



After the CSR is generated and downloaded, follow the steps described in <u>Submit a certificate request in</u> <u>the Certificate Authority</u> to create a certificate request in CA.

You are here: Maintenance  Security certificates  Server certificate
cate Signing Request saved.
Show (decoded) Show (PEM file)
May 28 2016

#### Reset to default server certificate

Certificate signing request (CSR)	
Certificate request	Show (decoded) Show (PEM file) Download
Generated on	Jul 25 2014
scard CSR	
Upload new certificate	
Upload new certificate Select the server private key file	System will use the private key file generated at the same time as the CSR.

Upload server certificate data

Figure 85: Expressway-C-Server Certificate Upload

### Expressway-C Trusted CA Certificate

### Navigation: Maintenance->Security Certificates->Trusted CA certificate

This allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway-C. When a TLS connection to Expressway-C mandates certificate verification, the certificate presented to the Expressway-C 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.

Follow the steps described in <u>Download a root certificate from CA</u> to download the root certificate from CA.

Trusted CA certificate			You are here: Maintenance > Security certificates > Trusted CA certificates					
Туре	Issuer	-			Subject	Expiration date	Validity *View	
Show all (decoded	) Show all (PEM file)	Delete	Select all	Unselect all				
Upload			]					
Select the file cor	ntaining trusted CA	ĺ.			Browse			

Figure 86 Expressway-C-Trusted Certificate Upload

# Call Routing

### Navigation: Configuration->Call routing

- 1. Set Call Signaling optimization: On
- 2. Set Call loop detection mode: On

Call routing		You are here: Configuration • Call routing
Configuration		
Call signaling optimization	On 🗸 (j)	
Call loop detection mode	On 🗸 🥼	

Save

Figure 87: Expressway-C-Call routing

© 2016 Cisco Systems, Inc. All rights reserved.

Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

# **Call Flows**

### CISCO UCM -> Skype for Business Internal

The Audio/Video signaling flow from Cisco UCM (including PSTN calls) to Skype for Business are as follows:

- 1. The CISCO UCM routes it to the Expressway-C.
- 2. Expressway-C routes the Cisco UCM call to the Skype for Business Front End.
- 3. The resulting signaling path:
  - a. Audio/Video signaling: session is established between the CISCO UCM and the B2BUA on the Expressway-C and Expressway-C to Skype for Business Front End.

### Skype for Business->CISCO UCM Internal

The Audio/Video (AV) signaling flows are as follows:

- 1. A Skype for Business user starts a call.
- 2. The Skype for Business Front End routes it to the Expressway-C.
- 3. Expressway-C routes the SIP AV invite to CUCM and thereby it is sent to the CUCM endpoint.
- 4. The resulting signaling path:
  - a. Audio/Video signaling: session is established between the Skype for Business Front End and the B2BUA on the Expressway-C.

### CISCO UCM -> Skype for Business External

The Audio/Video signaling flow from Cisco UCM (including PSTN calls) to Skype for Business are as follows:

- 1. The Expressway-E routes the call to Expressway-C and the expressway-C routes the call towards CISCO UCM and the CUCM routes it to the Expressway-C.
- 2. Expressway-C routes the Cisco UCM call to the Skype for Business Front End.
- 3. The resulting signaling path:
  - a. Audio/Video Media: Expressway- E and Microsoft Edge server anchors the media between Cisco and Skype for Business external clients



# Zone and Search Rule Configuration for Audio/Video Integration

Figure 88: Audio/Video Call flow Skype for Business to UCM



Figure 89: Audio/Video Call flow UCM to Skype for Business

### **Zones Configurations**

Figure 90 captures all configured Zones in Expressway-C:

Zon	es						Y	ou are here: C
	Name 🔻	Туре	Calls	Bandwidth used	H323 status	SIP status	Search rule status	Actions
	DefaultZone	Default zone	0	0 kbps	On	On		View/Edit
	CUCM Neighbor	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 1	View/Edit
	Directory to B2BUA	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 1	View/Edit
	SFB Zone	Neighbor	0	0 kbps	Off	Active	No search rules configured	View/Edit
	To Microsoft Lync server via B2BUA	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 3	View

New Delete Select all Unselect all

Figure 90: Summary of all Zones configured in Expressway-C

### Zone Configuration for CISCO UCM

Navigation: Configuration->Zones->Zones

- 1. Set Name: Enter a name for this zone
- 2. Set Type: Neighbor
- 3. Set Mode: On
- 4. Set Port: 5061
- 5. Set Transport: TLS
- 6. Set TLS verify mode: Off
- 7. Set Authentication policy: Treat as authenticated
- 8. Set SIP authentication trust mode: Off
- 9. Set the Peers: Enter the IP address or FQDN of the neighbor, Cisco UCM here

© 2016 Cisco Systems, Inc. All rights reserved.

Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

Configuration	
Name	* CUCM Neighbor
Туре	Neighbor
Hop count	* 15
H.323	
Mode	Off • ()
SIP	
Mode	
Port	* 5061
Transport	TLS T
TLS verify mode	Off • ()
Accept proxied registrations	Allow 🔻 👔
Media encryption mode	Auto 🔹 🚺
ICE support	Off • (i)
Multistream mode	On T
Preloaded SIP routes support	Off •
Authentication	
Authentication policy	Do not check credentials 🔻 🧃
SIP authentication trust mode	Off • ()
Location	
Peer 1 address	elus30pub.tekvizionlabs.com
Peer 2 address	SIP: Reachable: 10.80.20.2:5061 clus30sub1.tekvizionlabs.com
	on . Readiable. 10.00.20.3.0001

Figure 91: Expressway-C Zone Configuration for UCM-1

Peer 3 address	
Peer 4 address	
Peer 5 address	
Peer 6 address	

	Advanced	
	Zone profile	Custom V (i)
	Monitor peer status	Yes V
	Call signaling routed mode	Always V
	Automatically respond to H.323 searches	
	Automatically respond to SIP searches	
	Send empty INVITE for interworked calls	On V (1)
	SIP parameter preservation	
	SIP poison mode	
	SIP encryption mode	Auto V
	SIP REFER mode	Forward V
	SIP multipart MIME strip mode	
	SIP UPDATE strip mode	
	Interworking SIP search strategy	Options V
	SIP UDP/BFCP filter mode	
	SIP UDP/IX filter mode	
	SIP record route address type	
	SIP Proxy-Require header strip list	
L		

#### Save Cancel Delete

Active
0
0 kbps
0 kbps
1

Figure 92: Expressway-C Zone Configuration for UCM-2

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 96 of 145

### Search Rules

Figure 93 shows a summary of all the defined Search rules.

	Priority v	Rule name	Protocol	Source	Authentication required	Mode	Pattern type	Pattern string	Pattern behavior	On match	Target	State	Actions	
	<u>25</u>	<u>CUCM to Lync - 4</u> Digit Dialing	SIP	CUCM Neighbor	No	Alias pattern match	Regex	(2…)@te kvizionla bs.com:5 061	Replace	Continue	<u>To Microsoft</u> Lync server via B2BUA	Enabled	<u>View/Edit</u>   <u>Clone</u>	*
	<u>30</u>	<u>PSTN to Lync 10</u> Digit Dialing	SIP	CUCM Neighbor	No	Alias pattern match	Suffix	@expres sc2.tekvi zionlabs. com:506 1	Replace	Stop	<u>To Microsoft</u> Lync server via B2BUA	✓ Enabled	<u>View/Edit</u>   <u>Clone</u>	
	<u>50</u>	LocalZoneMatch	Any	Any	No	Any alias				Continue	LocalZone	✓ Enabled	<u>View/Edit</u>   <u>Clone</u>	
	<u>100</u>	Route to IM&P	SIP	SFB Zone	No	Alias pattern match	Regex	CUP_(.*)	Replace	Continue	IMP	Enabled	<u>View/Edit</u>   <u>Clone</u>	
	<u>110</u>	SFB Zone Rule	SIP	SFB Zone	No	Any alias				Stop	Directory to B2BUA	✓ Enabled	<u>View/Edit</u>   <u>Clone</u>	
	<u>130</u>	CUCM to Lync - UserID Dialing	SIP	CUCM Neighbor	No	Any alias				Continue	<u>To Microsoft</u> Lync server via B2BUA	Enabled	<u>View/Edit</u>   <u>Clone</u>	
	<u>140</u>	B2BUA to CUCM	SIP	Any	No	Any alias				Stop	CUCM Neighbor	✓ Enabled	<u>View/Edit</u>   <u>Clone</u>	
	<u>160</u>	Traversal zone search rule	Any	Any	No	Any alias				Continue	Traversalzone	✓ Enabled	<u>View/Edit</u>   <u>Clone</u>	
	<u>170</u>	External IP address search rule	Any	Any	No	Any IP address				Continue	Traversalzone	✓ Enabled	<u>View/Edit</u>   <u>Clone</u>	-
Nev	v Delete	Enable Disable	Select all	Unselect all					Search ru	les are appli	ed in priority order, v	with 1 being	the highest pri	iority

Figure 93: Summary of Expressway-C Search Rules

#### Search Rule CISCO UCM to Skype for Business - 4 Digit Dialing

#### Navigation: Configuration->Dial Plan-> Search rules

- 1. Set Rule name: Enter a name for this search rule
- 2. Set **Priority:** This represents the order in the search process that this rule is applied, when compared to the priority of the other search rules.
- 3. Set **Protocol:** SIP
- 4. Set Source name: Enter the zone to which this rule applies
- 5. Set Mode: Alias pattern match
- 6. Set **Pattern type:** Regex
- 7. Set Pattern string: (2...)@expressc2.tekvizionlabs.com:5061
- 8. Set Pattern behavior: Replace
- 9. Set Replace string: +1972852\1@tekvizionlabs.com;user=phone
- 10. Set On successful match: Continue
- 11. Set Target: Select the zone to query if the alias matches the search rule, to B2BUA here
- 12. Set State: Enabled

Edit search rule	You are here: Configuration > Dial plan > Search rules > Edit search rule
Configuration	]
Rule name	M DUCM to Lync - 4 Digit Dialing
Description	Calls from CUCM to Lync using 4digit@domain ()
Priority	* 25 ()
Protocol	SIP 🔻 👔
Source	Named 🔻 🕡
Source name	* CUCM Neighbor
Request must be authenticated	No 🔻 🚯
Mode	Alias pattern match 🔻
Pattern type	Regex 🔻 🚺
Pattern string	* (2)@tekvizionlabs.com:5061
Pattern behavior	Replace 🔻 👔
Replace string	+1972852\1@tekvizionlabs.com;user=phone
On successful match	Continue 🔻 🕧
Target	* To Microsoft Lync server via B2BUA 🔹 i
State	Enabled

Save Delete Cancel



Search Rule CISCO UCM to Skype for Business - UserID Dialing

Navigation: Configuration->Dial Plan-> Search rules

- 1. Set Rule name: Enter a name for this search rule
- 2. Set **Priority**: This represents the order in the search process that this rule is applied, when compared to the priority of the other search rules.
- 3. Set **Protocol:** SIP
- 4. Set Source: Named
- 5. Set Source name: CUCM\_ Neighbor
- 6. Set Target: To Microsoft Lync server via B2BUA (Skype for Business server)
- 7. Set State: Enabled

Edit search rule	You are here: Configuration > Dial plan > Search rules > Edit search
Configuration	
Rule name	CUCM to Lync - UserID Dialing
Description	URI Dialing from CUCM to Lync Using userid
Priority	• 130 👔
Protocol	SIP V (1)
Source	Named V
Source name	CUCM Neighbor
Request must be authenticated	No V
Mode	Any alias V (i)
On successful match	Continue V
Target	To Microsoft Lync server via B2BUA 🔍 👔
State	Enabled V

Figure 95: Expressway-C Search rule for URI based dialing from CISCO UCM to Skype for Business

### Search Rule B2BUA to CISCO UCM

Navigation: Configuration->Dial Plan-> Search rules

- 1. Set **Rule name:** Enter a name for this search rule
- 2. Set **Priority:** This represents the order in the search process that this rule is applied, when compared to the priority of the other search rules.
- 3. Set Protocol: SIP
- 4. Set Source: Any
- 5. Set **Mode:** Any alias
- 6. Set On successful match: Stop
- 7. Set Target: CUCM\_ Neighbor
- 8. Set State: Enabled

dit search rule	You are here: Configuration > Dial plan > Se	arch rules • Edit search r
Configuration		
Rule name	* B2BUA to CUCM	
Description	Any call from B2BUA to CUCM	
Priority	<b>★ 140</b> (1)	
Protocol	SIP V	
Source	Any v	
Request must be authenticated	No v 1	
Mode	Any alias 🗸 👔	
On successful match	Stop v	
Target	* CUCM Neighbor V	
State	Enabled v	

Figure 96: Expressway-C Search rule for B2BUA to CUCM

# Configuring Secure Traversal Zone Connection for Unified Communications

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E. This involves:

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

### Installing Expressway Security Certificates

Expressway-C and Expressway-E should have the trusted and signed CA certificate. Refer to Loading server and trusted certificates in the expressway-C section for certificate request and upload.

Note: When you generate a CSR in the expressway-c, you must include the phone security profile names under the Unified CM Phone Security profile names in the Alternative names section as shown below, this will help you to register jabber as an external User:

Generat	te CSR	,	You are here: <u>Maintenance</u> •	Security certificates	Generate CSR
Commo	n name				
Common	name	FQDN of Expressway			
Common	name as it will appear	expresswayC.tekvizionlabs.com			
Alternati	ive name				
Additional	l alternative names (comma			(i)	
separated	)				
IM and Pr	resence chat node aliases			Format	
(federated	group chat)	DNS 🔻 👔		_	
Unified Cl	M phone security profile names	jabber-secured		1	
Alternativ	e name as it will appear	DNS:expresswayC.tekvizionlabs.com			
		DNS:jabber-secured			

Figure 97:Expressway-C certificate request

### Expressway-C Traversal Zone Configuration

There should be a Unified Communications traversal zone between Expressway-C and Expressway-E for the MRA services.

### Navigation: Configuration->Zones->Zones

- 1. Set Name: Enter a name for this zone
- 2. Set Type: Unified Communications traversal
- 3. Username: username for this traversal zone to communicate with EXP-E
- 4. Password: Password
- 5. Set SIP Mode: On
- 6. Set **Port:** 7003
- 7. Authentication policy: Do not check credentials
- 8. Set Peer 1 address: Enter the FQDN of the Expressway-E

Edit zone		You are here: Configuration	Zones V Zones V Edit zone
Name *	Traversalzone (1)		
Туре	Unified Communications traversal		
Hop count *	15 (1)		
Connection credentials			
Username *	traversaluser		
Password *	· · · · · · · · · · · · · · · · · · ·		
SIP			
Port *	7003		
Accept proxied registrations	Allow		
ICE support	Off V		
Multistream mode	On V (i)		
SIP poison mode	Off V (i)		
Preloaded SIP routes support	Off <b>v</b>		
SIP parameter preservation	Off V (i)		
Authentication			
Authentication policy	Do not check credentials <b>v</b>		
Client settings			
Retry interval *	120 (1)		
Peer 1 address	expresswayE.tekvizionlabs.com SIP: Reachable: 10.80.20.12:7003	<u>í</u>	

Figure 98: Expressway-C Traversal zone for Expressway-E

# Expressway-E Traversal Zone Configuration

Navigation: Configuration->Zones->Zones

- 1. Set Name: Enter a name for this zone
- 2. Set Type: Unified Communications traversal
- 3. Username: username for this traversal zone to communicate with EXP-E
- 4. Password: Password

© 2016 Cisco Systems, Inc. All rights reserved.

Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 102 of 145

- 5. Set Port: 7003
- 6. TLS Verify subject name: FQDN of Expressway-C
- 7. Authentication policy: Do not check credentials

Name * Traversalzone   Type Unified Communications traversal   Hop count * 15   Connection credentials   Connection credentials   Username * traversaluser   Password Add/Edit local authentication database   SIP   Port * 7003   TLS verify subject name * expresswayC.tek/vizionlabs.com   Accept provied registrations Alow v   Alow v 4   On v 4   SIP poison mode On v   Off v 6   SIP poison mode Off v   Off v 6   SIP parameter preservation Off v   Multistream mode Off v   Off v 6   SIP parameter preservation Off v   Muthentication Off v   Authentication Do not check credentials v	Configuration	
Type Unified Communications traversal   Hop count + 15   Ø     Connection credentials   Username + traversaluser   Ø   Add/Edit local authentication database     SIP   Port + 7003   Its verify subject name + expresswayC.tekvizioniabs.com   Accept proxied registrations   Alow ♥   Ø   ICE support   Off ♥   Ø   ISIP poison mode   Off ♥   Ø   Øff ♥   Øff ♥	Name	* Traversalzone
Hop count * 15   Connection credentials   Username   * traversaluser   @   Password   Add/Edit local authentication database     SIP   Port   * 7003   ILS verify subject name   * expresswayC.tekvizionlabs.com   Accept proxied registrations   Allow • @   ICE support   Off • @   Mutistream mode   On • @   SIP poison mode   Off • @   Preloaded SIP routes support   Off • @   SIP parameter preservation   Off • @   Authentication policy	Туре	Unified Communications traversal
Connection credentials   Username * traversaluser   Password Add/Edit local authentication database     SIP   Port * 7003   Port * 7003   ILS verify subject name * expresswayC.tek v/zionlabs.com   Accept proxied registrations Allow • i   Accept proxied registrations Allow • i   ICE support Off • i   Multistream mode On • i   SIP poison mode Off • i   Preloaded SIP routes support Off • i   Off • i I   Authentication policy Do not check credentials • i	Hop count	* 15 (i)
Username * traversaluser   Password Add/Edit local authentication database     SIP   Port * 7003   ILS verify subject name * expresswayC.tekvizionlabs.com   Accept proxied registrations Allow • i   ICE support Off • i   Multistream mode On • i   SIP poison mode Off • i   Preloaded SIP routes support Off • i   SIP parameter preservation Off • i   Authentication policy Do not check credentials • i	Connection credentials	
Password Add/Edit local authentication database     SIP     Port * 7003 • •     Port * 7003 • •     TLS verify subject name * • expresswayC tekvizionlabs.com     Accept proxied registrations Allow • •     Accept proxied registrations Allow • •     Accept proxied registrations Allow • •     Allow • • •     Accept proxied registrations Allow • •     Allow • • •     Authentication     Authentication policy Do not check credentials • •	Username	* traversaluser
SIP         Port       * 7003         TLS verify subject name       * expresswayC.tekvizionlabs.com         Accept proxied registrations       Allow V         Accept proxied registrations       Allow V         ICE support       Off V         Multistream mode       On V         SIP poison mode       Off V         Preloaded SIP routes support       Off V         SIP parameter preservation       Off V         Authentication policy       Do not check credentials V	Password	Add/Edit local authentication database
SIP   Port   TLS verify subject name   * expresswayC.tekvizionlabs.com   Accept proxied registrations   Allow ♥ i   ICE support   Off ♥ i   Multistream mode   On ♥ i   SIP poison mode   Off ♥ i   Preloaded SIP routes support   Off ♥ i   SIP parameter preservation   Off ♥ i   Authentication   Authentication policy   Do not check credentials ♥ i		
Port * 7003   TLS verify subject name * expresswayC.tekvizionlabs.com   Accept proxied registrations Allow ♥ i   Accept proxied registrations Allow ♥ i   ICE support Off ♥ i   Muttistream mode On ♥ i   SIP poison mode Off ♥ i   Preloaded SIP routes support Off ♥ i   SIP parameter preservation Off ♥ i   Authentication Do not check credentials ♥ i	SIP	
TLS verify subject name * expresswayC.tekvizionlabs.com   Accept proxied registrations Allow ▼    ICE support Off ▼    Multistream mode On ▼    SIP poison mode Off ▼    Preloaded SIP routes support Off ▼    Off ▼     SIP parameter preservation Off ▼	Port	* 7003
Accept proxied registrations       Allow ▼ i         ICE support       Off ▼ i         Multistream mode       On ▼ i         SIP poison mode       Off ▼ i         Preloaded SIP routes support       Off ▼ i         SIP parameter preservation       Off ▼ i         Authentication policy       Do not check credentials ▼ i	TLS verify subject name	* expresswayC.tekvizionlabs.com
ICE support       Off ▼ i         Multistream mode       On ▼ i         SIP poison mode       Off ▼ i         Preloaded SIP routes support       Off ▼ i         SIP parameter preservation       Off ▼ i         Authentication policy       Do not check credentials ▼ i	Accept proxied registrations	Allow
Multistream mode       On <ul> <li>i</li> <li>SIP poison mode</li> <li>Off              <ul></ul></li></ul>	ICE support	Off 🔻 👔
SIP poison mode Off     Preloaded SIP routes support Off     Off   i   SIP parameter preservation Off       Authentication policy Do not check credentials	Multistream mode	On ▼ (1)
Preloaded SIP routes support       Off ▼ i         SIP parameter preservation       Off ▼ i         Authentication	SIP poison mode	Off <b>v</b>
SIP parameter preservation          Off • i         Authentication         Authentication policy             Do not check credentials • i	Preloaded SIP routes support	Off <b>v</b>
Authentication Do not check credentials V (i)	SIP parameter preservation	Off <b>T</b>
Authentication policy Do not check credentials		
Authentication policy Do not check credentials  (i)	Authentication	
	Authentication policy	Do not check credentials  (i)

Figure 99: Expressway-E Traversal zone for Expressway-C

# Expressway-C Traversal Zone Search Rules

- 1. Go to Configuration > Dial plan > Search rules.
- 2. Click New.
- 3. Configure the fields as follows

I	Edit search rule		You are here: Configuration > Dial plan > Search rules > Edit search rule
	- Configuration		
	Rule name	*[	Traversal zone search rule
	Description		search traversal zone EXPe
	Priority	*	100 1
	Protocol	0	Any 🔻 👔
	Source	[	Any 🔻 👔
	Request must be authenticated	[	No 🔻 👔
	Mode	[	Any alias
	On successful match	[	Continue 🔻 🧃
	Target	*[	Traversalzone •
	State	[	Enabled V (i)
	Save Delete Cancel		

Figure 100: Expressway-C Traversal Zone Search rule for Expressway-E

# Expressway-E Traversal Zone Search Rules

- 1. Go to Configuration > Dial plan > Search rules.
- 2. Click New.
- 3. Configure the fields as follows

E	Edit search rule		You are here: Configuration > Dial plan > Search rules > Edit search rule
[	Configuration		
	Rule name	* ]	Traversal zone search rule
	Description	5	search traversal zone EXPc (i)
	Priority	* [1	100 (1)
	Protocol		Any 🔻 🛈
	Source		Any 🔻 👔
	Request must be authenticated		No 🔻 (i)
	Mode		Any alias 🔹 👔
	On successful match		Continue 🔻 👔
	Target	*[	Traversalzone
	State		Enabled <b>T</b>
	Save Delete Cancel		

Figure 101: Expressway-E Traversal Zone Search rule for Expressway-C

# Configuring External (Unknown) IP Address Routing

The following configuration defines how an Expressway routes calls (and other requests) to external IP addresses. An external IP address is an IP address which is not 'known' to the Expressway and therefore assumed to be a publicly routable address.

Known IP addresses are addresses defined in a subzone (using a subzone membership subnet rule).

- All requests destined for external IP addresses, originating at the Expressway-C are routed to the Expressway-E using a search rule.
- The Expressway-E then attempts to open a connection directly to the IP address

To configure how the Expressway handles calls to unknown IP addresses:

- 1. Go to Configuration > Dial plan > Configuration.
- 2. Configure the fields as follows:

Expressway-C:

C	ial plan configuration	You are here: Configuration > Dial plan > Configuration
Γ	Configuration	
	Calls to unknown IP addresses	Indirect V
	Fallback alias	
	Save	

Figure 102: Expressway-C Dial Plan Configuration

#### Expressway-E:

Dial plan configuration		You are here: Configuration > Dial plan > Configuration
Configuration		
Calls to unknown IP addresses	Direct V (i)	
Fallback alias		
Save		



To create the search rules to route calls to IP addresses to the Expressway-E:

- 1. On the Expressway-C Go to Configuration > Dial plan > Search rules.
- 2. Click New.
- 3. Configure the fields as follows:

E	Edit search rule		You are here: Configuration > Dial plan > Search rules > Edit search rule
[	Configuration		
	Rule name	*	External IP address search rule
	Description		Route external ip address
	Priority	*	100 (1)
	Protocol		Any 🔻 👔
	Source		Any 🔻 🛈
	Request must be authenticated		No 🔻 🕡
	Mode		Any IP address 🔹 🧃
	On successful match		Continue 🔻 👔
	Target	*	Traversalzone 🔻 👔
	State		Enabled

Save Delete Cancel

Figure 104: Expressway-C External IP address search rule

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 106 of 145

# Discover Unified Communication Servers and Services

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

**Note:** The connections configured in this procedure are static. You must refresh the configuration on the Expressway-C after you reconfigure or upgrade any of the discovered Unified Communications nodes

Go to Configuration > Unified Communications > <UC server type> and click Refresh servers.

# Trust the Certificates Presented to the Expressway-C

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

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

# Discover Unified CM Servers

1. On Expressway-C, go to Configuration > Unified Communications > Unified CM servers. The page lists any Unified CM nodes that have already been discovered

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 107 of 145

- 2. Add the details of a Unified CM publisher node
  - Click New.
  - Enter the Unified CM publisher address.
  - You must enter an FQDN when TLS verify mode is On.
  - Enter the Username and Password of an account that can access this server.
  - Note: These credentials are stored permanently in the Expressway database. The corresponding Unified CM user must have the Standard AXL API Access role.
  - [Recommended] Leave TLS verify mode switched On to ensure Expressway verifies the node's certificates.
  - The Unified CM node presents its tomcat certificate for AXL and UDS queries, and its Call Manager certificate for subsequent SIP traffic. If the Unified CM server is using self-signed certificates, the Expressway-C's trusted CA list must include a copy of the tomcat certificate and the Call Manager certificate from every Unified CM server.
  - Click Add address.
  - Set the TLS Verify mode to on, make sure the expressway-c and cucm certificates were signed by the CA.
  - If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

Unified CM servers			You are here: Configuration > Unified Communications > Unified CM servers > Edit
Γ	Unified CM server lookup		
	Unified CM publisher address	clı	us30pub.tekvizionlabs.com
	Username	* a	dministrator (1)
	Password	* ••	·····
	TLS verify mode	0	)n ▼ (j)

Figure 105: Expressway-C Unified CM Servers

- 3. Repeat the discovery procedure for other Unified CM nodes/clusters, if required.
- 4. Click Refresh servers to refresh all the node details after configuring multiple publisher addresses

### Discover IM and Presence Service Nodes

- 1. On Expressway-C, go to Configuration > Unified Communications > IM and Presence Service nodes.
- 2. The page lists any IM and Presence Service nodes that have already been discovered.
- 3. Add the details of an IM and Presence Service database publisher node:
  - Click New.
  - Enter the address of the IM and Presence Service database publisher node.
  - You must enter an FQDN when TLS verify mode is On.

© 2016 Cisco Systems, Inc. All rights reserved.

Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 108 of 145
- Enter the Username and Password of an account that can access this server.
- Note: These credentials are stored permanently in the Expressway database. The corresponding IM and Presence Service user must have the Standard AXL API Access role.
- [Recommended] Leave TLS verify mode switched On to ensure Expressway verifies the node's tomcat certificate (for XMPP-related communications).
- [Optional] Select which deployment this node/cluster will belong to.
- The Deployment field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.
- Click Add address.
- If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.
- If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

I	M and Presence Service nodes		You are here: Configuration > Unified Communications > IM and Presence Service nodes > Edit
	IM and Presence Service node discovery		]
	IM and Presence Service database publisher node	1	0.80.20.4
	Username	*	administrator (1)
	Password	*	
	TLS verify mode	0	On <b>v</b> (j)

Figure 106: Expressway-C IM and Presence Service nodes

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

- 4. Repeat the discovery procedure for other IM and Presence Service nodes/clusters, if required.
- 5. Click Refresh servers to refresh all the node details after configuring multiple publisher addresses.

## Automatically Generated Zones and Search Rules

Expressway-C automatically generates non-configurable neighbor zones between itself and each discovered Unified CM node. A TCP zone is always created, and a TLS zone is created also if the Unified CM node is configured with a Cluster Security Mode (System > Enterprise Parameters > Security Parameters) of 1 (Mixed) (so that it can support devices provisioned with secure profiles). The TLS zone

is configured with its TLS verify mode set to On if the Unified CM discovery had TLS verify mode enabled. This means that the Expressway-C will verify the CallManager certificate for subsequent SIP communications. Each zone is created with a name in the format 'CEtcp-<node name>' or 'CEtls-<node name>'.

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

## **IM&P** Configuration

## Loading Server and Trust Certificates

IM&P Server should trust Skype for Business Front End Server.

## IM&P Trusted CA Certificate

Follow the steps described in <u>Download a root certificate from CA</u> to download the root certificate from CA

### Upload root Certificate

- 1. Set **Certificate Purpose:** cup-trust
- 2. The services *Cisco SIP Proxy Service, Cisco Presence Engine* must be restarted in order for the changes to take effect:

👌 Upload 🛛 🖳 Close			_	_
tatus				
👔 Warning · Unloadin	a a cluster-wide certi	ficate will distribute	t to all cervers i	n this cluster
i) Warning: Uploadin Jpload Certificate/Ce	g a cluster-wide certi rtificate chain	ficate will distribute	t to all servers i	n this cluster
Warning: Uploadin Upload Certificate/Ce Certificate Purpose*	g a cluster-wide certi	ficate will distribute	t to all servers i	
Warning: Uploadin Jpload Certificate/Ce Certificate Purpose* Description(friendly name)	g a cluster-wide certi ertificate chain cup-trust	ficate will distribute	t to all servers i	]

Figure 107:IM&P-Upload Root Certificate

3. Click on the uploaded certificate and it should look similar to the one below

entificate Details f	ion tological by DC01 CA, our trust
	or tekvizioniabs-DC01-CA, cup-trust
Delete 🧃 Dowi	nload .PEM File Download .DER File
Status	
i Status: Ready	
Certificate Settings	5
File Name	tekvizionlabs-DC01-CA.pem
Certificate Purpose	cup-trust
Certificate Type	trust-certs
Certificate Group	product-cup
Description(friendly	name) Trusted local cluster own-certificate
[ Version: V3 Serial Number: 68	31D134CE87ED434976BBD48E4E1574
SignatureAlgorithn	n: SHA1withRSA (1.2.840.113549.1.1.5)
ssuer Name: CN=	tekvizionlabs-DC01-CA, DC=tekvizionlabs, DC=com
Validity From: Mon To: Sup Fe	Feb 16 08:56:47 CST 2015 h 16 09:06:46 CST 2020
Subject Name: CN	=tekvizionlabs-DC01-CA, DC=tekvizionlabs, DC=com
Key: RSA (1.2.840	.113549.1.1.1)
Key value:	0035c7d070856sf7a252520211cc62381eeb32800bd0d584fb88b57ba780aa7e0
6494581e7e9fd25dd	leb19a7322c220cac870491cb4ae8de95ab5cddd78fe8e7556e954cea490be2d9
cb60e909ee904de9a	aacce6b42b6175228fefc8b7a7e8c96c278ef9c44a91121c9ba48d2bed07f628c7f
165e6f8d00eee1985	0045b8ac4f7aa1e8cd0bf62af058d2a754837f47913a2e888c2594c752ebb60b0
CI4703C3374300070	44102002494955622014290827905809020007200508719056067591D5000171
Delete Downloa	d .PEM File Download .DER File

Figure 108:IM&P-Root Certificate Example

## IM&P Server Certificate

Navigation: Cisco Unified IM and Presence OS Administration/Security->Certificate Management

Generate CSR

1. Click on Gene	rate CSR
Certificate List	
Generate Self-signed	Upload Certificate/Certificate chain 🔃 Generate CSR
Generate Self-signe	d Upload Certificate/Certificate chain Generate CSR Download CSR
	Figure 109. IM&P Generate CSR-1
	right 105. Inter Scherule CSA 1
2. Set Certificate	Purpose: Cup
3. Set <b>Distributic</b>	n: Select the IM&P publisher node
4. Set Key Lengt	n: 2048
Generate Certificate Sig	gning Request
🛐 Generate 🛄 Close	
~9 🛏	
- Status	
Status	
Warning: Generating	g a new CSR for a specific certificate type will overwrite the existing CSR for that type
Generate Certificate Si	gning Request
Certificate Purpose	cup T
Distribution*	clus30pimp.tekvizionlabs.com
Common Name*	clus30pimp.tekvizionlabs.com
Subject Alternate Nam	es (SANs)
Auto-populated Domains	clus30pimp.tekvizionlabs.com
**	201
Key lype	RSA T
Hash Algorithm *	
Hash Algorithm	SHA256

Figure 110:IM&P Generate CSR-2

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 113 of 145 After the CSR is generated and downloaded, follow the steps described in <u>Submit a certificate request in</u> <u>the Certificate Authority</u> to create a certificate request in CA.

Upload Certificate

- 5. Once the certificate is downloaded, click on 'Upload Certificate/Certificate chain'
- 6. Set Certificate Purpose: cup

Certificate List				
Generate Self-signed	Jpload Certificate/Certificate chain	Generate CSR	Download CSR	
Generate Self-signed	Upload Certificate/C	ertificate chain	Generate CSR	Download CSR
	Figure 111: IM&I	P-Upload Certificate-1		
Upload Certificate/Cert	ificate chain			
		_	_	_
Status-				
i Warning: Uploading	a cluster-wide certificate	will distribute it to a	ll servers in this clu	ster
-Unload Cortificate/Cort	lificato chain —			
Certificate Purpose*			~	
Description(friendly name)				
Upload File	C:\Users\sjonnada\Down	loads\cup-cer.cer		Browse
Upload Close				

#### Figure 112:IM&P-Upload Certificate-2

7. Click on the uploaded certificate and it should look similar to the one below

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 114 of 145

Certificate Details for clus30pimp.tekvizionlabs.com, cup					
Regenerate 🛐 Generate CSR 🧃 Download .PEM File 員 Download .DER File					
Status Status: Ready					
Certificate Settings					
Locally Uploaded 08/09/16					
File Name cup.pem					
Certificate Purpose cup					
Certificate Type certs					
Certificate Group product-cup					
Description(friendly name) Certificate Signed by tekvizionlabs-DC01-CA					
Certificate File Data					
<pre>[ Version: V3 Serial Number: 2800000725EA83E84672886780000000072 SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5) Issuer Name: CN=tekvizionlabs-DC01-CA, DC=tekvizionlabs, DC=com Validity From: Thu Sep 08 16:27:55 CDT 2016 To: Sat Sep 08 16:27:55 CDT 2018 Subject Name: CN=clus30pimp.tekvizionlabs.com, OU=Labs, O=tekvizion, L=Richardson, ST=Texas, C=US Key: RSA (1.2.840.113549.1.1.1) Key value: 3082010a0282010100d416141dfdef6e035cfe0e73bbea11801221595d921860adf4f16100e71e6fc0 422b159d3490357afb8be7abc37ea5a4050cf833778cecd75c826182f4ec26d8066e7ff335153237401 83cc5ac75c0dde934aa7d63a5d30ee468844efadff13f92c78b6183c81e0d1dc67dd5f31571453b393f d5d46b4c7ef2acaeab4da8f50c3c36c5dd113568ab6afeae3bcc72a842222873a83871d21e453cd204</pre>					
Regenerate Generate CSR Download .PEM File Download .DER File					

Figure 113: IM&P-Server Certificate Example

# **Application Listeners**

Navigation: System->Application Listeners

Configure the default Cisco SIP Proxy TLS Listeners for Peer and Server Authentication as shown.

Application Listener Configuration							
🔚 Save 🗙 Delete 🗋 Copy 🕂 Add New							
Status Status: Ready							
- 📻 SIP Listener Configuration	SIP Listener Configuration						
Listener Type	SIP						
Name*	Default Cisco SIP Proxy TLS Listener - Peer Auth X						
Port*	5061						
Service Type	Cisco SIP Proxy						
Transport Type *	TLS V						
TLS Context*	Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context						
Save Delete Copy Add New							

Figure 114:Cisco IM&P Application Listener - Peer Auth

Application Listener Configuration							
🔚 Save 🗙 Delete 🗋 Copy 🕂 Add New							
Status Status: Ready							
- 🔜 SIP Listener Configuration	STP Listener Configuration						
Listener Type	SIP						
Name*	Default Cisco SIP Proxy TLS Listener - Server Auth X						
Port*	5062						
Service Type	Cisco SIP Proxy						
Transport Type *	TLS						
TLS Context* Default_Cisco_UP_SIP_Proxy_Auth_TLS_Context							
Save Delete Copy Add New							

Figure 115: Cisco IM&P Application Listener - Server Auth

## **TLS Contexts**

Navigation: System->Security->TLS Context Configuration

Configure the default Cisco SIP Proxy Peer Authentication TLS context to use the appropriate ciphers and subject mapping as shown

TLS Context Configuration	Related Links: Back To Find/List					
🕞 Save 🗙 Delete 🕂 Add	New					
TLS Context Information						
Name*	Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context					
Description	Default TLS context for Cisco SIP Proxy specifying an authorizat					
Authorization Policy*	Peer					
✓ Disable Empty TLS Fragments	]					
TLS Cipher Mapping						
Available TLS Ciphers	Selected TLS Ciphers**					
TLS_ECDHE_ECDSA_WITH_AES_1 TLS_ECDHE_ECDSA_WITH_AES_2 TLS_ECDHE_RSA_WITH_AES_128 TLS_ECDHE_RSA_WITH_AES_256 TLS_WITH_RSA_NULL_SHA	128_GCM_SHA256 TLS_WITH_RSA_AES_256_CBC_SHA 156_GCM_SHA384 _GCM_SHA384 _GCM_SHA384 _GCM_SHA384 _GCM_SHA384 _GCM_SHA384 _GCM_SHA384 					
	Reset To Default					
**Please ensure that clients or servers connecting to an Application Listener using this TLS Context support one or more of the selected ciphers. Failure to do so will result in rejection of the TLS connection.						
TLS Peer Subject Mapping						
Available TLS Peer Subjects	Selected TLS Peer Subjects					
	<pre>fe01.tekvizionlabs.com expressc2.tekvizionlabs.com </pre>					
- Save Delete Add New						

Figure 116: Cisco IM&P TLS Context - SIP Proxy Peer Auth

## **Proxy Configuration Settings**

Navigation: Presence->Routing->Settings.

Configure the Preferred Proxy Listener to Default Cisco SIP Proxy TLS Listener -Peer Auth

Proxy Configuration Settings		
Save		
Status Status: Ready		
Restart Restart All Proxy Services		
General Configuration		
CVP Enable ACL Configuration		
Method/Event Routing Status*	On	$\checkmark$
Preferred Proxy Listener	Default Cisco SIP Proxy TLS Listener - Peer Auth	~
Save		

Figure 117: Proxy Configuration Settings

## **Incoming ACL Configuration**

Navigation: System->Security->Incoming ACL

Configure address patterns that control which incoming servers and domains can access the IM and Presence Service without authentication

Incoming ACL connections Lists:

Skype for business internal clients

Expressway server's

Skype for Business server's

Incoming Access Control	List Configuration		Related Links: Back To Find/List 🗸 Go		
📊 Save X Delete [	🗋 Copy 🛟 Add New				
Status Status: Ready					
Configure an address whi digest authentication. By c	rmation :h will be added to the SIP Proxy list ( lefault, the behavior is to deny all inco	of allowed incoming addresses. Note: oming requests.	: any address added to this list will bypass		
Description	clients				
Address Pattern*	10.64.0.0/16				
- Save Delete Copy	Add New				

Figure 118: Cisco IM&P Incoming ACL-1

Incoming Access Control	List Configuration		Related Links: Back To Find/List 🗸 Go
🔜 Save X Delete [	🗋 Copy 🛟 Add New		
Status Status: Ready			
Configure an address whic digest authentication. By d	mation h will be added to the SIP Proxy list of efault, the behavior is to deny all incom	allowed incoming addresses. Not ning requests.	te: any address added to this list will bypass
Description Address Pattern*	Expressway IP	×	
- Save Delete Copy	Add New	17	

Figure 119: Cisco IM&P Incoming ACL-2

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 119 of 145

ncoming Access Control Li	ist Configuration	Related Links: Back To Find/List 🗸 Go
🔒 Save 🗙 Delete [	🗋 Copy 🐈 Add New	
Status Status: Ready		
Incoming ACL Inform Configure an address which digest authentication. By de	nation will be added to the SIP Proxy list of allowe fault, the behavior is to deny all incoming re	ed incoming addresses. Note: any address added to this list will bypass equests.
Description Address Pattern*	ExpressWay	
Address Pattern*	All	



Incoming Access Control List Configuration		Related Links: Back To Find/List 🔨 Go
🔚 Save 🗶 Delete 📋	Copy 🛟 Add New	
Status Status: Ready		
Configure an address which wi digest authentication. By defau	on Il be added to the SIP Proxy list of allowed incoming addresses. No Ilt, the behavior is to deny all incoming requests.	te: any address added to this list will bypass
Description	ExpressWay_IPAddr	
Address Pattern*	expressc2.tekvizionlabs.com	
- Save Delete Copy Ad	id New	

Figure 121: Cisco IM&P Incoming ACL-4

Incoming Access Control List	Configuration	Related Links: Back To Find/List 🔻 Go
Save 🗶 Delete 🗋	Copy 🕂 Add New	
Status		
i Status: Ready		
- 🏦 Incoming ACL Informati	on	
Configure an address which wi digest authentication. By defau	ill be added to the SIP Proxy list of allowed incoming addresses. Not ult, the behavior is to deny all incoming requests.	e: any address added to this list will bypass
Description	Lync FrontEnd	
Address Pattern*	fe01.tekvizionlabs.com	
- Save Delete Copy Ad	Jd New	



## **TLS Peer Subject Configuration**

Navigation: System->Security->TLS Peer Subject

## TLS Peer Subject Configuration for Expressway-C

1. Set Peer Subject Name: Enter the Certificate Common Name (CN)

TLS Peer Subject Configuration		Related Links: Back To Find/List  Go
🔚 Save 🗙 Delete 🗋 C	opy 📫 Add New	
Status		
i Status: Ready		
TLS Peer Subject Informatio	n	
Peer Subject Name*	expressc2.tekvizionlabs.com	
Description	ExpressWay	
- Save Delete Copy Add New		

Figure 123: Cisco IMP TLS Peer Subject Configuration-1

### TLS Peer Subject Configuration for Skype for Business Server

1. Set Peer Subject Name: Enter the Certificate Common Name (CN)

TLS Peer Subject Configuration		Related Links: Back To Find/List 🔻 Go	
🔚 Save 🗶 Delete 📔 Copy	🔚 Save 🗙 Delete 🗈 Copy 🕂 Add New		
Status Status: Ready			
TLS Peer Subject Information—			
Peer Subject Name*	fe01.tekvizionlabs.com	]	
Description	Lync_FrontEnd	]	
- Save Delete Copy Add New			

Figure 124: Cisco IMP TLS Peer Subject Configuration-2

## Presence Gateway Configuration

Navigation: Presence-> Gateways

Configure a Cisco Unified Communications Manager gateway

- 1. Set **Presence Gateway Type:** Choose the Cisco UCM to allow IM and Presence Service to receive 'On the Phone' availability information
- 2. Set **Description:** Enter a meaningful description that will help you to distinguish between presence gateway instances when you have configured more than one type of gateway
- 3. Set **Presence Gateway:** Enter the IP Address or FQDN of the Cisco Unified Communications Manager node

Presence Gateway Configuration Related Links: Back To Find/List ▼				
🕞 Save 🗙 Delete 🕂 Add New				
Status				
i Status: Ready				
Presence Gateway Settings (Cisco Unified Communications Manager)				
You can configure a Cisco Unified Communications Manager server as a presence gateway. The IM and Presence Service will then trigger the Cisco Unified Communications Manager to publish phone presence information (e.g. phone on/off hook status).				
Presence Gateway Type*	СИСМ	T		
Description*	Presence Gateway			
Presence Gateway*	clus30pub.tekvizionlabs.com			
- Save Delete Add New				

Figure 125: Cisco IM&P Presence Gateway

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 122 of 145

## Presence Settings Configuration

Navigation: Presence->Settings->Standard Configuration

Configure the Presence Settings to manage the global availability sharing capability for all clients that connect to the IM and Presence Service.

- 1. Set Cluster ID: This unique identifier is automatically generated
- Set CUCM IM and Presence Publish Trunk: Select the appropriate IM and Presence Service SIP trunk required for phone availability integration. This is the trunk configured in Cisco UCM for IM and Presence Server at Devices -> Trunk.
- 3. Confirm Enable Partitioned Intra-domain Federation with LCS/OCS/Lync: is checked
- 4. Set Partitioned Intra-domain Routing Mode: Advanced Routing Mode

resence Settings	
Nave Save	
Status Status: Ready	
Presence Settings	
Cluster ID*	StandAloneClusterd41a0
☑ Enable availability sharii	ng
Allow users to view the approval	availability of other users without being prompted for
NOTE: this option must	be turned on for SIP clients to function properly
Enable use of Email Add	ress for Inter-domain Federation
Maximum Contact List Size (ner user)*	200 🛛 No Limit
Maximum Watchers (per user)*	200 No Limit
CUCM IM and Presence Publish Trunk	IM_Presence_Trunk
Enable ad-hoc present Maximum number of ad-hoc	ence subscriptions
subscriptions*	50
Ad-hoc subscription time-to (seconds)*	live 900
- 🖌 Enable Partitioned I	Intradomain Federation with LCS/OCS/Lync
Partitioned Intradomain Rou Mode*	iting Advanced Routing Mode
Save	

*Figure 126: Cisco IM&P Presence Settings* 

# Security Settings Configuration

Navigation: System->Security->Settings

1. Set SIP Intra-cluster Proxy-to-Proxy Transport Protocol: TCP

Security Settings	
Save	
Status Status: Ready	
General Settings	
✓ Enable XMPP Client to IM/P Service Secure M	ode
Enable XMPP Router-to-Router Secure Mode	
Enable Web Client to IM/P Service Secure Mo	de
Enable Wildcards in XMPP Federation Security	Certificates
SIP Intra-cluster Proxy-to-Proxy Transport Protocol	TCP
Save	

Figure 127: Cisco IM&P Security Settings

## Static Route to Front End Configuration

Navigation: Presence->Routing->Static Routes

A static route is a fixed path through the network, unlike a dynamic route path that automatically calculates according to routing protocols and routing update messages

- 1. Set **Destination Pattern:** Enter the pattern of the static route
- 2. Set Next Hop: Enter the IP address or FQDN of the next hop for the static route.
- 3. Set Next Hop Port: 5061
- 4. Set Route Type: Domain
- 5. Set **Protocol Type:** TLS

Static Route Configuration		Related Links:	Back To Find/List 🔻 Go
🕞 Save 🗶 Delete 🗋 Copy 🕂	Add New		
Status			
(i) Status: Ready			
Static Route Information			
Destination Pattern*	.com.tekvizionlabs		
Description	static route to Lync FrontEnd		
Next Hop*	fe01.tekvizionlabs.com		
Next Hop Port*	5061		
Route Type*	Domain <b>v</b>		
Protocol Type	TLS		
Priority *	1		
Weight*	1		
Allow Less-Specific Route*	On <b>v</b>		
In Service*	On 🔻		
Block Route			
- Save Delete Copy Add New -			

Figure 128: Cisco IM&P Static Route

## Skype for Business Server Configuration

Skype for Business Server should trust Expressway.

## Add Expressway-C to Skype for Business Topology

Intra-domain federation requires the following configuration on Skype for Business.

• Expressway-C as a trusted application server

In general, the steps to create the trusted application servers is similar to Expressway-C whether using Enterprise or Standard Edition Skype for Business Sever. The steps below outline the overall procedure using the Skype for Business Power Shell.

#### *Trusted Application Server – Expressway-C*

*a.* Create the trusted application pool by running the following command. Use Get-CsPool to verify FQDN of the Registrar.

### New-CsTrustedApplicationPool -Identity expressc2.tekvizionlabs.com –Registrar fe01.tekvizionlabs.com –Site CleanDefaultTopology –TreatAsAuthenticated \$true – ThrottleAsServer \$true –RequiresReplication \$false –Outboundonly \$false -ComputerFqdn expressc2.tekvizionlabs.com

Identity – Name of the trusted application pool Registrar – ServiceID or FQDN of registrar service for the pool Site – Name of the site where you want the pool to be created ComputerFQDN – FQDN of the Expressway-C (used only if using Enterprise Edition Skype for Business)

b. The following command is used to add additional computers to the trusted application if using Enterprise pools. This step can be skipped if using Standard Edition Skype for Business.

# *New-CsTrustedApplicationComputer -Identity expressc3.tekvizionlabs.com -Pool expressc2.tekvizionlabs.com*

Identity – FQDN of the new server being added to the trusted application pool (Enterprise Edition Skype for Business)

Pool – FQDN of the trusted application pool

c. Finally, create a new trusted application and add to the above created application pool, using port 5061

*New-CsTrustedApplication -ApplicationId ExpresswaycApplication1 -TrustedApplicationPoolFqdn expressc2.tekvizionlabs.com -Port 65072* 

ApplicationID – Name of the application. Can be any name TrustedApplicationPoolFQDN – FQDN of the trusted application pool Port: Listening port (65072 for TLS)

d. Publish the topology

#### **Enable-CsTopology**

The configuration can be quickly verified as shown below.

PS C:\Users\administra	ator.TEKVIZIONLABS> Get-CsTrustedApplicationComputer -Identity expressc2.tekvizionlabs.com
Identity : expressc2.1 Pool : expressc2.1 Fqdn : expressc2.1	cekvizionlabs.com cekvizionlabs.com cekvizionlabs.com
PS C:\Users\administra	ator.TEKVIZIONLABS> Get-CsTrustedApplicationPool -Identity expressc2.tekvizionlabs.com
Identity Registrar FileStore ThrottleAsServer TreatAsAuthenticated OutboundOnJy RequiresReplication AudioPortStart AudioPortStart AudioPortStart AppSharingPortStart AppSharingPortCount VideoPortStart VideoPortStart VideoPortStart SependentServiceList ServiceId SiteId PoolFqdn Version Role	TrustedApplicationPool:expressc2.tekvizionlabs.com Registrar:FE01.tekvizionlabs.com True True False False 0 0 0 0 0 0 0 0 1-ExternalServer-1 Site:EnterpriseLyncServer expressc2.tekvizionlabs.com 7 TrustedApplicationPool
PS C:\Users\administr≀ cation1	ator.TEKVIZIONLABS> Get-CsTrustedApplication -Identity expressc2.tekvizionlabs.com/expresswaycappl
Identity ComputerGruus ServiceGruu Protocol ApplicationId TrustedApplicationPoo Port	<pre>: expressc2.tekvizionlabs.com/urn:application:expresswaycapplication1 : {expressc2.tekvizionlabs.com sip:expressc2.tekvizionlabs.com@tekvizionlabs.com;gruu;opaque =srvr:expresswaycapplication1:ltZWrc2_n1WLrLLeaa2KeQAA} : sip:expressc2.tekvizionlabs.com@tekvizionlabs.com;gruu;opaque=srvr:expresswaycapplication1 :ltZWrc2_n1WLrLLeaa2KeQAA : Mtls : urn:application:expresswaycapplication1 IFqdn : expressc2.tekvizionlabs.com : 65072</pre>
VideoPortStart VideoPortStart Applications DependentServiceList ServiceId SiteId PoolFqdn Version Role PS C:\Users\administra cation1 Identity ComputerGruus ServiceGruu Protocol ApplicationId TrustedApplicationPoo <sup>*</sup> Port LegacyApplicationName	0 0 {urn:application:expresswaycapplication1} } 1-ExternalServer-1 Site:EnterpriseLyncServer expressc2.tekvizionlabs.com 7 TrustedApplicationPool ator.TEKVIZIONLABS> Get-CsTrustedApplication -Identity expressc2.tekvizionlabs.com/expressway i expressc2.tekvizionlabs.com/urn:application:expresswaycapplication1 : {expressc2.tekvizionlabs.com sip:expressc2.tekvizionlabs.com@tekvizionlabs.com;gruu;o =srvr:expresswaycapplication1:ltZWrc2_n1WLrLLeaa2KeQAA} : sip:expressc2.tekvizionlabs.com@tekvizionlabs.com;gruu;opaque=srvr:expresswaycapplication1 : tZWrc2_n1WLrLLeaa2KeQAA : wtls : urn:application:expresswaycapplication1 IFqdn : expressc2.tekvizionlabs.com

Figure 129: Skype for Business Static Route to Expressway-C

#### Static Route Configuration for federation

In the Skype for Business Management Shell, use the below commands to create a new static route variable on Skype for Business for federation and then add the route variable to the global static routing configuration collection

# \$route=New-CsStaticRoute -TLSRoute -Destination "expressc2.tekvizionlabs.com" -MatchUri "tekvizionlabs.com" -Port 5061 -UseDefaultCertificate \$true

Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=\$route}

Destination - FQDN of the Expressway-C Port – Listening port (usually 5061 for TLS) MatchUri – Destination domain

• Verify the configured static routes.

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 127 of 145

#### Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty route

Transport	: TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefa ultCert:Fodn=expressc2.tekvizionlabs.com:Port=5061
MatchUri	: tekvizionlabs.com
MatchOnlyPhoneUri	: False
Enabled	: True
ReplaceHostInRequestUri	: False
Element	: <route <br="" xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008">MatchUri="tekvizionlabs.com" MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false"&gt; <transport porte"5061"=""> <tls fqdn="expressc2.tekvizionlabs.com"> <usedefaultcert></usedefaultcert> </tls>  </transport></route>

Figure 130: Skype for Business Static Route to Expressway-C

### Configure Encryption Level

Configure Encryption level parameters through the Windows PowerShell<sup>®</sup> command line interface because they are not configurable on Skype for Business Server Control Panel

Media EncryptionLevel must be set to Require Encryption.

Set-CsMediaConfiguration - identity Global - EncryptionLevel RequireEncryption

PS C:\Users\administrator.LYNCLABSP> Get-CsMediaConfiguration		
Identity	: Global	
EnableQoS	: False	
EncryptionLevel	: RequireEncryption	
EnableSiren	: True	
MaxVideoRateAllowed	: VGA600K	
EnableInCallQoS	: False	
InCallQoSIntervalSeconds	: 35	
EnableRtpRtcpMultiplexing	: True	

Figure 131: Skype for Business Server – Media Configuration

### Trusted Application Server – IM&P Nodes

Add IM&P Publisher as Trusted Application Server

*a.* Create the trusted application pool by running the following command. Use Get-CsPool to verify FQDN of the Registrar.

New-CsTrustedApplicationPool -Identity clus30pimp.tekvizionlabs.com –Registrar fe01.tekvizionlabs.com –Site CleanDefaultTopology –TreatAsAuthenticated \$true – ThrottleAsServer \$true –RequiresReplication \$false –Outboundonly \$false -ComputerFqdn clus30pimp.tekvizionlabs.com

Identity – Name of the trusted application pool Registrar – ServiceID or FQDN of registrar service for the pool Site – Name of the site where you want the pool to be created ComputerFQDN – FQDN of the Cisco IM&P publisher (used only if using Enterprise Edition Skype for Business)

b. The following command is used to add additional peers to the trusted application pool.

# New-CsTrustedApplicationComputer -Identity clus30pimp.tekvizionlabs.com -Pool clus30pimp.tekvizionlabs.com

Identity – FQDN of the new server being added to the trusted application pool (Enterprise Edition SFB) Pool – FQDN of the trusted application pool

c. Finally, create a new trusted application and add to the above created application pool, using port 5061

# *New-CsTrustedApplication -ApplicationId impapplication1 -TrustedApplicationPoolFqdn clus30pimp.tekvizionlabs.com -Port 5061*

ApplicationID – Name of the application. Can be any name TrustedApplicationPoolFQDN – FQDN of the trusted application pool Port: Listening port (5061 for TLS)

d. Publish the topology

#### Enable-CsTopology

#### Add IM&P Subscriber as Trusted Application Server

*a.* Create the trusted application pool by running the following command. Use Get-CsPool to verify FQDN of the Registrar.

New-CsTrustedApplicationPool -Identity clus30simp.tekvizionlabs.com –Registrar fe01.tekvizionlabs.com –Site CleanDefaultTopology –TreatAsAuthenticated \$true – ThrottleAsServer \$true –RequiresReplication \$false –Outboundonly \$false -ComputerFqdn clus30simp.tekvizionlabs.com

Identity – Name of the trusted application pool Registrar – ServiceID or FQDN of registrar service for the pool Site – Name of the site where you want the pool to be created ComputerFQDN – FQDN of the Cisco IM&P publisher (used only if using Enterprise Edition Skype for Business)

b. The following command is used to add additional peers to the trusted application pool.

# *New-CsTrustedApplicationComputer -Identity clus30simp.tekvizionlabs.com -Pool clus30simp.tekvizionlabs.com*

Identity – FQDN of the new server being added to the trusted application pool (Enterprise Edition SFB) Pool – FQDN of the trusted application pool

c. Finally, create a new trusted application and add to the above created application pool, using port 5061

#### *New-CsTrustedApplication -ApplicationId impapplication1 -TrustedApplicationPoolFqdn clus30simp.tekvizionlabs.com -Port 5061*

ApplicationID – Name of the application. Can be any name TrustedApplicationPoolFQDN – FQDN of the trusted application pool Port: Listening port (5061 for TLS)

d. Publish the topology

#### Enable-CsTopology

## Update Skype for Business Certificates

Using the Skype for Business Deployment Wizard update the Skype for Business Certificates with both Server and Client Authentication

Skype for Business Server 2015 - Deployment Wizard		x
Install or update member system		
Deploy > Install or update		2
Step 1: Install Local Configuration Store         Installs local configuration store and populates with data from Central Management Store.         Prerequisites >         Help >         Complete         Run Again		~
Step 2: Setup or Remove Skype for Business Server Components Install and activate, or deactivate and uninstall Skype for Business Server Components based on the topology definition.		=
Prerequisites  Help  Run Again		
Step 3: Request, Install or Assign Certificates This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.	]	
Prerequisites  Help  Complete Run Again		
Step 4: Start Services         Manual After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services.         You can start the services in a pool with the Skype for Business Server cmdlets.         To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet.         To start the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.         Prerequisites ▶		~
Back	Exit	

Figure 132: Skype for Business Deployment Wizard- Request & Assign Certificates-1

elect a Skype for Business Se sage tasks.	rver Certifica	Certificate Wiz te Type and then select a task. E	zard xpand the Certificate Type	to perform advanc	ed certificate
Certificate		Friendly Name	Expiration Date	Location	Reques
<ul> <li>Default certificate</li> </ul>	<ul> <li>Image: A set of the set of the</li></ul>	Skype for Business Server 201	9/6/2018 2:29:24 PM	Local	Assian
<ul> <li>OAuthTokenIssuer</li> </ul>	~	Skype for Business Server OA	4/1/2017 1:40:14 PM	Global	
☑ OAuthTokenIssuer	~	Skype for Business Server	4/1/2017 1:40:14 PM	Global	View
Help Refresh	Import Cert	tificate Process Pending Certific	cates		Close

Figure 133: Skype for Business Deployment Wizard- Request & Assign Certificates-2

د د	tificate Request
Certificate Request	
Select a CA from the list detected in your en DC01.tekvizionlabs.com\tekvizionlabs-DC01	ironment. -CA
Friendly name: Skype for Business Server 2015 Default certi	icate 10/31/2016
Organization: Orga	nizational unit:
Country/Region:	
State/Province: City	/Locality:
Select one or more SIP domains for which a salternative names list.	ip. <sipdomain> entry is to be added to the subject</sipdomain>
Subject name: FE01.tekvizionlabs.com	
Subject alternative name:	
FE01.tekvizionlabs.com fe0101.tekvizionlabs.com dialin.tekvizionlabs.com	~
Specify another CA, change the Certificate Te more. Advanced	mplate, configure additional Subject Alternative Names, and
Help	Back Next Cancel

Figure 134: Skype for Business Deployment Wizard- Request & Assign Certificates-3

5	Certificate Request	x			
S	Delayed or Immediate Requests				
Do you certifica	Do you want to prepare a certificate request to be sent later, or do you want to send it now to an online certification authority?				
Send	the request immediately to an online certification authority				
O Prep	are the request now, but send it later (offline certificate request)				
Help	Back Next Cancel				

Figure 135: Skype for Business Deployment Wizard- Request & Assign Certificates-4

Certificate Request	C
Choose a Certification Authority (CA)	
Select a certification authority to process your request. The Certificate Wizard will automatically import the selected CA's certificate chain if necessary.	
<ul> <li>Select a CA from the list detected in your environment.</li> <li>DC01.tekvizionlabs.com\tekvizionlabs-DC01-CA </li> </ul>	
<ul> <li>Specify another certification authority.</li> </ul>	
Help Back Next Cancel	

Figure 136: Skype for Business Deployment Wizard- Request & Assign Certificates-5

ភ	Certificate Req	uest 🛛 🗙	t
S	Certification Authority Account		
Spec	ify alternate credentials for the certification authori name:	ty.	
Pass	word:		
Help		Back Next Cancel	

Figure 137: Skype for Business Deployment Wizard- Request & Assign Certificates-6

7	Certificate Request	x		
S	Specify Alternate Certificate Template			
By def specif	ault a Skype for Business Server certificate request will use the WebServer certificate template. To / a different certificate template, select the following check box.	)		
Us Ce S	e alternate certificate template for the selected certification authority rtificate template name: erverandWebClient			
Note: requir	Note: The custom template must be installed on the certification authority (CA), and must meet the requirements for Skype for Business Server certificates.			
The te	The template name must be specified, which may differ from the template display name.			
For de	tails about custom certificate templates, see the product documentation.			
Не	lp Back Next Cancel			

Figure 138: Skype for Business Deployment Wizard- Request & Assign Certificates-7

ត	Certificate Request	x
S	Name and Security Settings	
Type a na Note: The automati Friendly r	ame for the new certificate. The name should be easy for you to refer to and remember. I friendly name should not be confused with the subject name which will be determined cally based on the certificate's usages on this computer.	
Skype fo	or Business Server 2015 Default certificate 10/31/2016	
Bit length 2048	the certificate's private key as exportable	
Help	Back Next Cancel	

Figure 139: Skype for Business Deployment Wizard- Request & Assign Certificates-8

- 1. Enter the Organization Information
- 2. Enter the Geographical Information
- 3. Select the sip domain

Certificate Request			
Certificate Request			
Select a CA from the list detected in your environment.			
DC01.tekvizionlabs.com\tekvizionlabs-DC01-CA 🔹			
Friendly name:			
Skype for Business Server 2015 Default certificate 10/31/2016			
Organization: Organizational unit:			
Country/Region:			
United States			
State/Province: Texas City/Locality: Plano			
Select one or more SIP domains for which a sip. <sipdomain> entry is to be added to the subject alternative names list.</sipdomain>			
✓ tekvizionlabs.com			
Cubicat across			
FE01.tekvizionlabs.com			
Subject alternative name:			
FE01.tekvizionlabs.com			
fe0101.tekvizionlabs.com			
dialin.tekvizionlabs.com			
Specify another CA, change the Certificate Template, configure additional Subject Alternative Names, and more.			
Advanced			
Holo Deck Next Correl			
Back INext Cancel			

Figure 140: Skype for Business Deployment Wizard- Request & Assign Certificates-9

© 2016 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com Page 139 of 145

ā	Certificate R	equest	X
Certi	ficate Request Summary		
To generate a req	uest with the following information, clie	ck Next.	
Property	Value		^
Certificate Use	Server default,Web services internal,Web services external		=
Country/Region	n US		
State/Province	Texas		
City/Locality	Plano		
Friendly Name	Skype for Business Server 2015 Default certificate 10/31/2016		
Key Size	2048		
Exportable	False		~
Help		Back Next	Cancel

Figure 141: Skype for Business Deployment Wizard- Request & Assign Certificates-14

ភា	Certificate Request	x		
S	Executing Commands			
Creating new log file "C:\Users\administrator.LYNCLABSP\AppData\Local\Temp\2\Request- CSCertificate-[2016_02_26][15_44_38].xml". Create a certificate request based on Skype for Business Server configuration for this computer. Issued thumbprint "D39048D871BFAC991DDF125CF3B875FDB840B48A" for use "Default,WebServicesInternal,WebServicesExternal" by "dc.lynclabsp.local\lynclabsp-DC-CA". No changes were made to the Central Management Store. Creating new log file "C:\Users\administrator.LYNCLABSP\AppData\Local\Temp\2\Request- CSCertificate-[2016_02_26][15_44_38].html". "Request-CSCertificate" processing has completed successfully. Detailed results can be found at "C:\Users\administrator.LYNCLABSP\AppData\Local\Temp\2 \Request-CSCertificate-[2016_02_26][15_44_38].html".				
Task stat	certificate			
Help	Back Next Cancel			

Figure 142: Skype for Business Deployment Wizard- Request & Assign Certificates-15

7	Certificate Request	x
S	Online Certificate Request Status	
A certifi the loca	cate with thumbprint D39048D871BFAC991DDF125CF3BB75FDBB40B48A has been added to I certificate store.	
🖌 Assig	n this certificate to Skype for Business Server certificate usages.	
Note: If y task in th	rou choose not to assign the certificate now, you can assign it at a later time by using the Assig ne Certificates wizard.	In
View Cer	rtificate Details	
Help	Back Finish Cancel	

Figure 143: Skype for Business Deployment Wizard- Request & Assign Certificates-16

ā	Certificate Assignment	X			
S	Certificate Assignment				
Assign the returned certificate to the Skype for Business Server usages on this server.					
View Cert	incate Details				
Help	Back Next Cancel				

Figure 144: Skype for Business Deployment Wizard- Request & Assign Certificates-18

<u>a</u>	Certificate Ass	ignment	X		
Certificate Assignment Summary					
To assign the fol	lowing certificate to the Skype for Busine	ess Server usages listed, click Next.			
Property	Value		^		
Friendly Name	<ul> <li>Skype for Business Server</li> <li>OAuthTokenIssuer 4/2/2015</li> </ul>				
Thumbprint	EA4DA912A319C214759485C0851 55048F8B4CE7F		=		
Certificate Use	Server default,Web services internal,Web services external				
Issue date	4/2/2015 1:40:14 PM				
Expiration date	e 4/1/2017 1:40:14 PM				
Subject Name (SN)	tekvizionlabs.com		~		
Help		Back Next Cance	el 🛛		

Figure 145: Skype for Business Deployment Wizard- Request & Assign Certificates-19
ភ	Certificate Assignment	x
S	Executing Commands	
The following certificate was assigned for the type "Default": Default: D39048D871BFAC991DDF125CF3BB75FDBB40B48A felync.lynclabsp.local 02/25/2018 CN=lynclabsp-DC-CA, DC=lynclabsp, DC=local 230000008B41E614D42649C0040000000008B The following certificate was assigned for the type "WebServicesInternal": WebServicesInternal: D39048D871BFAC991DDF125CF3BB75FDBB40B48A felync.lynclabsp.local 02/25/2018 CN=lynclabsp-DC-CA, DC=lynclabsp, DC=local 23000008B41E614D42649C0040000000008B The following certificate was assigned for the type "WebServicesExternal": WebServicesExternal: D39048D871BFAC991DDF125CF3BB75FDBB40B48A felync.lynclabsp.local 02/25/2018 CN=lynclabsp-DC-CA, DC=lynclabsp, DC=local 23000008B41E614D42649C004000000008B The following certificate was assigned for the type "WebServicesExternal": WebServicesExternal: D39048D871BFAC991DDF125CF3BB75FDBB40B48A felync.lynclabsp.local 02/25/2018 CN=lynclabsp-DC-CA, DC=lynclabsp, DC=local 230000008B41E614D42649C004000000008B		< III >
Task status: Completed.		
Assign C	ertificate  View Log	)
Help	Back Finish Cancel	

Figure 146: Skype for Business Deployment Wizard- Request & Assign Certificates-20