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 ............................................................................................................................. 32
  SIP Trunk Security Profile Configuration for Expressway-C ............................................................... 33
  Trunk to Expressway-C Gateway .......................................................................................................... 35
  Trunk to Expressway-C for MRA with Expressway-E ......................................................................... 39
  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 .................................................................................................... 48
  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
Presence Settings Configuration.................................................................................................................. 123
Security Settings Configuration.................................................................................................................. 124
Static Route to Front End Configuration.................................................................................................. 125
Skype for Business Server Configuration................................................................................................. 126
  Add Expressway-C to Skype for Business Topology............................................................................... 126
  Configure Encryption Level..................................................................................................................... 128
  Trusted Application Server – IM&P Nodes ............................................................................................... 129
  Update Skype for Business Certificates .................................................................................................. 131
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 X8.8 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
- 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 work 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 X8.8.1
- Jabber Client for Windows Version 11.6.0 Build 35037
- Skype for Business Android Client (6.0.0.8)
• 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_00_admin-guide-cucm-imp_1151/CUCM_BK_A09578D7_00_admin-guide-for-cucm-1105_chapter_01110.pdf

Expressway:

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

![Active Directory Users and Computers](image-url)

*Figure 1: Active Directory Users and Computers*
Figure 2: Active Directory User-1
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.

Figure 4: Certificate Authority- Create New Certificate Template-1
Figure 5: Certificate Authority - Create New Certificate Template-2
Figure 6: Certificate Authority - Create New Certificate Template-3
Figure 7: Certificate Authority - Create New Certificate Template-4
Figure 8: Certificate Authority - Create New Certificate Template - 5
Figure 9: Certificate Authority - Create New Certificate Template-6
Figure 10: Certificate Authority - Create New Certificate Template-7
Figure 11: Certificate Authority- Create New Certificate Template-8
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

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

---

Request a Certificate

Select the certificate type:
- User Certificate

Or, submit an advanced certificate request.

---

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.

---
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

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:

Certificate Template:

ServerandWebClient

Additional Attributes:

Figure 16: Certificate Authority-Certificate Request-4
Download a root certificate from 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 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:

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
Cisco UCM Configuration

Loading certificates on Cisco UCM


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](image)

**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
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 Submit a certificate request in the Certificate Authority for creating a certificate request and downloading the certificate.

Upload root certificate to Cisco UCM
Follow the instructions in Download a root certificate from CA 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
After upload is done, click on the certificate you uploaded and it should look similar to the one below.
In similar, upload the root certificate to tomcat-trust
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’

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

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

Figure 25: Cisco UCM Upload Server Certificate to CallManager-2
Look for the following oids in the certificate file Data to confirm that the certificate has both client and server authentication

![Certificate File Data](image)

**Upload tomcat Certificate**

![Upload Certificate/Certificate chain](image)

**Figure 26: Cisco UCM Upload Server Certificate to tomcat-trust**
Calling Search Space

Navigation: Call Routing->Class of Control->Calling Search Space
SIP Trunk Security Profile Configuration for Expressway-C


1. 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
8. 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.
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
   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
### Figure 28: Cisco UCM Trunk to Expressway-C-1

<table>
<thead>
<tr>
<th>Device Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>SIP Trunk</td>
</tr>
<tr>
<td>Device Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>Trunk Service Type</td>
<td>None (Default)</td>
</tr>
<tr>
<td>Device Name</td>
<td>ExpressC</td>
</tr>
<tr>
<td>Description</td>
<td>Trunk to Expressway C</td>
</tr>
<tr>
<td>Device Pool</td>
<td>DP_Richardson</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Call Classification</td>
<td>OnNet</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>MRCG_Richardson</td>
</tr>
<tr>
<td>Location</td>
<td>Hub_Richardson</td>
</tr>
<tr>
<td>AAR Group</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Tunneled Protocol</td>
<td>None</td>
</tr>
<tr>
<td>QSIG Variant</td>
<td>No Changes</td>
</tr>
<tr>
<td>ASN.1 ROSE OIDs Encoding</td>
<td>No Changes</td>
</tr>
<tr>
<td>Packet Capture Mode</td>
<td>None</td>
</tr>
<tr>
<td>Packet Capture Duration</td>
<td>0</td>
</tr>
<tr>
<td>Media Termination Point Required</td>
<td></td>
</tr>
<tr>
<td>Retry Video Call as Audio</td>
<td></td>
</tr>
<tr>
<td>Pass Replacement Support</td>
<td></td>
</tr>
<tr>
<td>Transmit UTF-8 for Calling Party Name</td>
<td></td>
</tr>
<tr>
<td>Transmit UTF-8 Names in QSIG APDU</td>
<td></td>
</tr>
<tr>
<td>Unattended Port</td>
<td></td>
</tr>
<tr>
<td>SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.</td>
<td></td>
</tr>
</tbody>
</table>
**Figure 29: Cisco UCM Trunk to Expressway-C-2**
**Outbound Calls**

- Connected Party Transformation CSS: <None>
- Use Device Pool Connected Party Transformation CSS

**Caller Information**

- Caller ID DN
- Caller Name
- Maintain Original Caller ID DN and Caller Name in Identity Headers

**SIP Information**

- Destination Address is a SNIP
- Destination Address: [Text]
- Destination Address IPv6: [Text]
- Destination Port: 5061
- Status: 401
- Status Reason: Unauthorized
- Duration: 00:00:12

- HTTP Preferred Originating Codec: [Text]
- BLF Presence Group: [Text]
- SIP Trunk Security Profile: [Text]
- Locking Out-of-Dial Refer: [Text]
- Out-of-Dial Call Search Space: <None>
- SUBSCRIBE Call Search Space: <None>
- SIP Profile: [Text]
- DTMF Signaling Method: [Text]

- Normalization Script
  - Normalization Script: [Text]

- Enable Trace
  - Parameter Name: [Text]
  - Parameter Value: [Text]

**Recording Information**

- This trunk connects to a recording-allowed gateway
- This trunk connects to other clusters with recording-allowed gateways

**Geolocation Configuration**

- Geolocation: <None>
- Geolocation Filter: <None>
- Send Geolocation Information: [Text]

---

*Figure 30: Cisco UCM Trunk to Expressway-C-3*
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
   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
Figure 31: UCM Trunk to Expressway-C for MRA1
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
### Device Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SIP Trunk Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>Trunk Service Type</td>
<td>None (Default)</td>
</tr>
<tr>
<td>Device Name</td>
<td>IM_Presence_Trunk</td>
</tr>
</tbody>
</table>

**Description**
- SIP IM Presence Trunk

**Device Pool**
- Default

**Common Device Configuration**
- < None >

**Cell Classification**
- Use System Default

**Media Resource Group List**
- < None >

**Location**
- Hub_Name

**AAR Group**
- < None >

**Tunnelled Protocol**
- None

**QSIG Variant**
- No Changes

**ASR1 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 ADDU
- [ ] Unattended Port
- [ ] SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
- [ ] Consider Traffic on This Trunk Secure
- [ ] Route Class Signaling Enabled
- [ ] Use Trusted Relay Point
- [ ] PSTN Access
- [ ] Run On All Active Unified CM Nodes

---

**Figure 33: Cisco UCM Trunk to IM&P-1**
### Intercompany Media Engine (IME)

| E.164 Transformation Profile | <None> |

### MLPP and Confidential Access Level Information

<table>
<thead>
<tr>
<th>MLPP Domain</th>
<th>&lt;None&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential Access Mode</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Confidential Access Level</td>
<td>&lt;None&gt;</td>
</tr>
</tbody>
</table>

### Call Routing Information

- Remote Party Id
- Asserted-Identity
- Asserted-Type: Default
- SIP Privacy: Default

### Inbound Calls

<table>
<thead>
<tr>
<th>Significant Digits</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Line ID Presentation</td>
<td>Default</td>
</tr>
<tr>
<td>Connected Name Presentation</td>
<td>Default</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>AAR Calling Search Space</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Prefix DN</td>
<td></td>
</tr>
</tbody>
</table>

- Redirecting Diversion Header Delivery - Inbound

### Incoming Calling Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

<table>
<thead>
<tr>
<th>Number Type</th>
<th>Prefix</th>
<th>Strip Digits</th>
<th>Calling Search Space</th>
<th>Use Device Pool CSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Number</td>
<td>Default</td>
<td>0</td>
<td>&lt;None&gt;</td>
<td>✓</td>
</tr>
</tbody>
</table>

### Incoming Called Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

<table>
<thead>
<tr>
<th>Number Type</th>
<th>Prefix</th>
<th>Strip Digits</th>
<th>Calling Search Space</th>
<th>Use Device Pool CSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Number</td>
<td>Default</td>
<td>0</td>
<td>&lt;None&gt;</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Figure 34: Cisco UCM Trunk to IM&P-2**
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 Configuration](image)

*Figure 36: Cisco UCM SIP Route Pattern*
### Media Resource Group Configuration

**Navigation:** Media Resources->Media Resource Group

<table>
<thead>
<tr>
<th>Media Resource Group Configuration</th>
<th>Related Links: Back To Find/List Go</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="save" alt="Save" /> <img src="delete" alt="Delete" /> <img src="copy" alt="Copy" /> <img src="add_new" alt="Add New" /></td>
<td></td>
</tr>
</tbody>
</table>

**Status**
- Status: Ready

**Media Resource Group Status**
- Media Resource Group: MRG_Richardson_Bridges (used by 21 devices)

**Media Resource Group Information**
- **Name**: MRG_Richardson_Bridges
- **Description**: Conductor Controlled Bridging Resources

**Devices for this Group**
- **Available Media Resources**: EXTMPF
- **Selected Media Resources**: ANN_2 (ANN), ANN_3 (ANN), ANN_2 (FB), CFB_2 (CFB), CFB_3 (CFB)

- **Use Multi-cast for MOH Audio (if at least one multi-cast MOH resource is available)**

---

**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.

![Figure 38: Media Resource Group List Configuration](image-url)
**Add MRGL to Device or Device Pool**

**Navigation:** System->Device Pool

![Device Pool Configuration](image)

**Figure 39: Device Pool Configuration -1**
**Device Mobility Related Information**

- Device Mobility Calling Search Space: < None >
- AAR Calling Search Space: < None >
- AAR Group: < None >
- Calling Party Transformation CSS: < None >
- Called Party Transformation CSS: < None >

**Geolocation Configuration**

- Geolocation: < None >
- Geolocation Filter: < None >

**Cell Routing Information**

**Incoming Calling Party Settings**

<table>
<thead>
<tr>
<th>Number Type</th>
<th>Prefix</th>
<th>Strip Digits</th>
<th>Calling Search Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Number</td>
<td>Default</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>International Number</td>
<td>Default</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Unknown Number</td>
<td>Default</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Subscriber Number</td>
<td>Default</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
</tbody>
</table>

**Incoming Called Party Settings**

<table>
<thead>
<tr>
<th>Number Type</th>
<th>Prefix</th>
<th>Strip Digits</th>
<th>Calling Search Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Number</td>
<td>Default</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>International Number</td>
<td>Default</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Unknown Number</td>
<td>Default</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Subscriber Number</td>
<td>Default</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
</tbody>
</table>

**Phone Settings**

- Caller ID For Calls From This Phone
  - Calling Party Transformation CSS: < None >

- Connected Party Settings
  - Connected Party Transformation CSS: < None >

- Redirecting Party Settings
  - Redirecting Party Transformation CSS: < None >

Figure 40: Device Pool Configuration -2
Cisco UCM LDAP Configuration

LDAP System Configuration

Navigation: System->LDAP->LDAP System

**LDAP System Configuration**

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please Delete All LDAP Directories Before Making Changes on This Page</td>
</tr>
<tr>
<td>Please Disable LDAP Authentication Before Making Changes on This Page</td>
</tr>
</tbody>
</table>

**LDAP System Information**

- Enable Synchronizing from LDAP Server
- LDAP Server Type: Microsoft Active Directory
- LDAP Attribute for User ID: sAMAccountName

![Figure 41: LDAP System Configuration](image)

**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: Reenter 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
Figure 42: Cisco UCM LDAP Directory
LDAP Authentication

![Figure 43: Cisco UCM LDAP Authentication](image)

**LDAP-Synced users**

*Navigation: User Management -> End User*

![Figure 44: LDAP-Synced users](image)
Navigation: User Management->End User

Figure 45: Cisco UCM End User Configuration-1
Figure 46: Cisco UCM End User Configuration-2
Figure 47: Cisco UCM End User Configuration-3
Cisco Jabber User Configuration

Navigation: Device->Phone

![Device Information Table]

**Figure 48: Cisco UCM Jabber Client Configuration-1**
Figure 49: Cisco UCM Jabber Client Configuration-2
**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
Figure 51: Cisco UCM Jabber Client Configuration-4
Figure 52: Cisco UCM Jabber Client Configuration-5
### Cisco UC Jabber Client Configuration - 6

#### Park Monitoring

<table>
<thead>
<tr>
<th>Voice Mail</th>
<th>Destination</th>
<th>Calling Search Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Monitoring Forward No Retrieve Destination External</td>
<td>&lt;None&gt;</td>
<td>A blank value means to call the parker's line.</td>
</tr>
<tr>
<td>Park Monitoring Forward No Retrieve Destination Internal</td>
<td>&lt;None&gt;</td>
<td>A blank value means to call the parker's line.</td>
</tr>
</tbody>
</table>

**Park Monitoring Reversion Timer**: A blank value will use value set in Park Monitoring Reversion Timer service parameter.

#### MLPP Alternate Party And Confidential Access Level Settings

<table>
<thead>
<tr>
<th>Target (Destination)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Calling Search Space</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>MLPP No Answer Ring Duration (seconds)</td>
<td></td>
</tr>
<tr>
<td>Confidential Access Mode</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Confidential Access Level</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Call Control Agent Profile</td>
<td>&lt;None&gt;</td>
</tr>
</tbody>
</table>

#### Line Settings for All Devices

| Hold Reversion Ring Duration (seconds) | Setting the Hold Reversion Ring Duration to zero will disable the feature. |
| Hold Reversion Notification Interval (seconds) | Setting the Hold Reversion Notification Interval to zero will disable the feature. |
| Party Entrance Tone* | Default |

#### Line 1 on Device CFSUSER06

| Display (Caller 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 the caller. |
| ASCII Display (Caller ID) | 2656 |
| External Phone Number Mask |  |
| Recording Option* | Call Recording Disabled |
| Recording Profile | <None> |
Figure 54: Cisco UCM Jabber Client Configuration-7
## End Point configurations

### Cisco Telepresence DX70 Configuration

#### Device Configuration

**Navigation:** Device->Phone->DX70

<table>
<thead>
<tr>
<th><strong>Phone Type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Type:</strong> Cisco DX70</td>
</tr>
<tr>
<td><strong>Device Protocol:</strong> SIP</td>
</tr>
</tbody>
</table>

### Real-time Device 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 ID:** | sipdx70.10-2-5-60 |
| **Download Status:** | None |

### Device Information

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

*Figure 55: DX70 Device Configuration-1*
<table>
<thead>
<tr>
<th>Owner</th>
<th>User</th>
<th>Anonymous (Public/Shared Space)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner User ID</td>
<td>spark2</td>
<td></td>
</tr>
<tr>
<td>Mobility User ID</td>
<td>&lt; None &gt;</td>
<td></td>
</tr>
<tr>
<td>Phone Personalization</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Services Provisioning</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Phone Load Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Trusted Relay Point</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>BLF Audible Alert Setting (Phone Idle)*</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>BLF Audible Alert Setting (Phone Busy)*</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Always Use Prime Line*</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Always Use Prime Line for Voice Message*</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td>&lt; None &gt;</td>
<td></td>
</tr>
<tr>
<td>Feature Control Policy</td>
<td>&lt; None &gt;</td>
<td></td>
</tr>
</tbody>
</table>

- 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: < None >
- 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)

**Protocol Specific Information**

- Packet Capture Mode*: None
- Packet Capture Duration: 0
- BLF Presence Group*: Standard Presence group

*Figure 56: DX70 Device Configuration-2*
<table>
<thead>
<tr>
<th>Device Security Profile*</th>
<th>Secured DX70</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rerouting Calling Search Space</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>SUBSCRIBE Calling Search Space</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>SIP Profile*</td>
<td>Standard SIP Profile For Cisco VCS</td>
</tr>
<tr>
<td>Digest User</td>
<td>&lt; None &gt;</td>
</tr>
</tbody>
</table>

- **Media Termination Point Required**
- **Unattended Port**
- **Require DTMF Reception**

### Certification Authority Proxy Function (CAPF) Information

- **Certificate Operation** | No Pending Operation |
- **Authentication Mode** | By Null String |
- **Authentication String**

[Generate String]

- **Key Order** | RSA Only |
- **RSA Key Size (Bits)** | 2048 |
- **EC Key Size (Bits)**

**Operation Completes By** | 2016 11 10 12 (YYYY:MM:DD:HH)

**Certificate Operation Status:** None

**Note:** Security Profile Contains Additional CAPF Settings.

### External Data Locations Information (Leave blank to use default)

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
</tr>
<tr>
<td>Messages</td>
</tr>
<tr>
<td>Services</td>
</tr>
<tr>
<td>Authentication Server</td>
</tr>
<tr>
<td>Proxy Server</td>
</tr>
<tr>
<td>Idle</td>
</tr>
<tr>
<td>Idle Timer (seconds)</td>
</tr>
<tr>
<td>Secure Authentication URL</td>
</tr>
<tr>
<td>Secure Directory URL</td>
</tr>
<tr>
<td>Secure Idle URL</td>
</tr>
</tbody>
</table>

*Figure 57: DX70 Device Configuration-3*
<table>
<thead>
<tr>
<th>Secure Idle URL</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Information URL</td>
<td></td>
</tr>
<tr>
<td>Secure Messages URL</td>
<td></td>
</tr>
<tr>
<td>Secure Services URL</td>
<td></td>
</tr>
</tbody>
</table>

**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 >
- **Confidential Access Mode**: < None >
- **Confidential Access Level**: < None >

**Product Specific Configuration Layout**

<table>
<thead>
<tr>
<th>Room Name (from Exchange(R))</th>
<th>Parameter Value</th>
<th>Override Common Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Access*</td>
<td>Enabled</td>
<td>✓</td>
</tr>
<tr>
<td>SSH Access*</td>
<td>Disabled</td>
<td>✓</td>
</tr>
<tr>
<td>Default Call Protocol*</td>
<td>SIP</td>
<td>✓</td>
</tr>
<tr>
<td>Quality Improvement Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multipoint Mode*</td>
<td>Use Media Resource Group List</td>
<td>✓</td>
</tr>
<tr>
<td>Telnet Access*</td>
<td>On</td>
<td>✓</td>
</tr>
<tr>
<td>Microphone Unmute On Disconnect*</td>
<td>On</td>
<td>✓</td>
</tr>
<tr>
<td>Call Logging Mode*</td>
<td>On</td>
<td>✓</td>
</tr>
<tr>
<td>OSD Encryption Indicator*</td>
<td>Auto</td>
<td>✓</td>
</tr>
<tr>
<td>Alternate phone book server type*</td>
<td>UDS</td>
<td>✓</td>
</tr>
<tr>
<td>Alternate phone book server address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 58: DX70 Device Configuration-4*
### Figure 59: DX70 Device Configuration

<table>
<thead>
<tr>
<th>Default Volume</th>
<th>Max Total Downstream Rate</th>
<th>Max Total Upstream Rate</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>10000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CTMS Settings**
- CTMS Multiparty Conferencing: On
- CTMS Encryption Mode: Off

**Far End Camera Control Settings**
- Far End Camera Control: On
- Far End Camera Control Signaling Capability: On

**Facility Service Settings**
- Facility Service Type: Helpdesk
- Facility Service Name: 
- Facility Service Number: 
- Facility Service Call Type: Video

**Standby Settings**
- Standby Mode: On
- Standby Delay: 10
- Standby Action: Privacy Position

**Serial Port Settings**
- Serial Port: On
- Serial Port Login Required: On

**Admin username and password**
- Admin Username: admin
- Admin Password: ***************

### Figure 60: DX70 Device Configuration

**Dial Plan**
- Site Access Code: 
- Inter Site Access Code: 
- Off-Net Access Code: 
- National Dialing Digits: 
- International Dialing Digits: 

**Directory Number**
- Country Code: 
- Area Code: 
- Local Number: 

**Osd**
- Todays Bookings: Off
Line Configuration

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

<table>
<thead>
<tr>
<th>Directory Number Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number*</td>
</tr>
<tr>
<td>Route Partition</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Alerting Name</td>
</tr>
<tr>
<td>ASCII Alerting Name</td>
</tr>
<tr>
<td>External Call Control Profile</td>
</tr>
<tr>
<td>Allow Control of Device from CTI</td>
</tr>
<tr>
<td>Associated Devices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Directory Number Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Mail Profile</td>
</tr>
<tr>
<td>Calling Search Space</td>
</tr>
<tr>
<td>BLF Presence Group*</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
</tr>
<tr>
<td>Auto Answer*</td>
</tr>
<tr>
<td>Reject Anonymous Calls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enterprise Alternate Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Enterprise Alternate Number</td>
</tr>
</tbody>
</table>

Figure 61: DX70 Line [1] Configuration-1
### Directory URIs

<table>
<thead>
<tr>
<th>Primary</th>
<th>URI</th>
<th>Partition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="mailto:spark2@tekvizzolabs.com">spark2@tekvizzolabs.com</a></td>
<td>Directory URI</td>
</tr>
</tbody>
</table>

### PSTN Failover for Enterprise Alternate Number, +E.164 Alternate Number, and URI Dialing

**Advertised Failover Number**: < None >

### AAR Settings

<table>
<thead>
<tr>
<th>Voice Mail</th>
<th>AAR Destination Mask</th>
<th>AAR Group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt; None &gt;</td>
<td>&lt; None &gt;</td>
</tr>
</tbody>
</table>

**Select AAR**

- Voice Mail
- AAR Destination Mask
- AAR Group

### Call Forward and Call Pickup Settings

<table>
<thead>
<tr>
<th>Voice Mail</th>
<th>Destination</th>
<th>Calling Search Space</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Use System Default</td>
</tr>
<tr>
<td>Forward All</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Forward</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Internal</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Busy</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
</tbody>
</table>

**Select Forward All**

- Voice Mail
- Destination
- Calling Search Space

Figure 62: DX70 Line [1] Configuration-2
### Figure 63: DX70 Line [1] Configuration-3

<table>
<thead>
<tr>
<th>Park Monitoring</th>
<th>Voice Mail</th>
<th>Destination</th>
<th>Calling Search Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Monitoring</td>
<td>□ or</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Forward No</td>
<td></td>
<td></td>
<td>A blank value means to call the parker’s line.</td>
</tr>
<tr>
<td>Retrieve</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Park Monitoring</td>
<td>□ or</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Forward No</td>
<td></td>
<td></td>
<td>A blank value means to call the parker’s line.</td>
</tr>
<tr>
<td>Retrieve</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Park Monitoring Reversion Timer</td>
<td></td>
<td></td>
<td>Default</td>
</tr>
<tr>
<td>Voice Mail</td>
<td>□ or</td>
<td></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Destination</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calling Search Space</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLPP Alternate Party And Confidential Access Level Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target (Destination)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLPP Calling Search Space</td>
<td>&lt; None &gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLPP No Answer Ring Duration (seconds)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential Access Mode</td>
<td>&lt; None &gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential Access Level</td>
<td>&lt; None &gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Control Agent Profile</td>
<td>&lt; None &gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Line Settings for All Devices

| Hold Reversion Ring Duration (seconds) | Setting the Hold Reversion Ring Duration to zero will disable the feature |
| Hold Reversion Notification Interval (seconds) | Setting the Hold Reversion Notification Interval to zero will disable the feature |
| Party Entrance Tone | Default |

### Line 1 on Device SEP0050680B4CE9

| Display (Caller 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 |

© 2016 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com
Page 70 of 145
Figure 64: DX70 Line [1] Configuration-4
Cisco DX80 Configuration

Device Configuration

**Navigation:** Device->Phone->DX80

<table>
<thead>
<tr>
<th>Device Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device is Active</strong></td>
<td>✔</td>
</tr>
<tr>
<td><strong>Device is trusted</strong></td>
<td>✔</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
<td>7426ACEF053D</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>SEP7426ACEF053D</td>
</tr>
<tr>
<td><strong>Device Pool</strong></td>
<td>DP_Richardson</td>
</tr>
<tr>
<td><strong>Common Device Configuration</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Phone Button Template</strong></td>
<td>Standard Cisco TelePresence DX80</td>
</tr>
<tr>
<td><strong>Common Phone Profile</strong></td>
<td>Standard Common Phone Profile</td>
</tr>
<tr>
<td><strong>Calling Search Space</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>AAR Calling Search Space</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Media Resource Group List</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>User Hold MOH Audio Source</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Network Hold MOH Audio Source</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Hub_None</td>
</tr>
<tr>
<td><strong>AAR Group</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>User Locale</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Network Locale</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>Default</td>
</tr>
<tr>
<td><strong>Device Mobility Mode</strong></td>
<td>Default</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>User</td>
</tr>
<tr>
<td><strong>Owner User ID</strong></td>
<td>spark3</td>
</tr>
<tr>
<td><strong>Mobility User ID</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Phone Load Name</strong></td>
<td>sipdx80.ce821.rel.loads</td>
</tr>
<tr>
<td><strong>Use Trusted Relay Point</strong></td>
<td>Default</td>
</tr>
<tr>
<td><strong>Always Use Prime Line</strong></td>
<td>Default</td>
</tr>
<tr>
<td><strong>Always Use Prime Line for Voice Message</strong></td>
<td>Default</td>
</tr>
<tr>
<td><strong>Geolocation</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Retry Video Call as Audio</strong></td>
<td>✔</td>
</tr>
<tr>
<td><strong>Ignore Presentation Indicators</strong></td>
<td>✔</td>
</tr>
</tbody>
</table>

*Figure 65: DX80 Device Configuration-1*
Figure 66: DX80 Device Configuration-2
Figure 67: DX80 Device Configuration-3

### External Data Locations Information

- **Information**
- **Directory**
- **Messages**
- **Services**
- **Authentication Server**
- **Proxy Server**
- **Idle**
- **Idle Timer (seconds)**
- **Secure Authentication URL**
- **Secure Directory URL**
- **Secure Idle URL**
- **Secure Information URL**
- **Secure Messages URL**
- **Secure Services URL**

### Extension Information

- **Enable Extension Mobility**
- **Log Out Profile**
- **Log in Time**
- **Log out Time**

### MLPP and Confidential Access Level Information

- **MLPP Domain**
- **MLPP Indication**
- **MLPP Preemption**
- **Confidential Access Mode**
- **Confidential Access Level**

© 2016 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com
Page 74 of 145
Figure 68: DX80 Device Configuration-4
<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Port</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>PC Voice VLAN Access</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>PC Port Remote Configuration</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Switch Port Remote Configuration</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Detect Unified CM Connection Failure</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>Gratuitous ARP</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP): Switch Port</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP): PC Port</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP): PC Port</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>LLDP Asset ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LLDP Power Priority</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Power Negotiation</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Automatic Port Synchronization</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>802.1x Authentication</td>
<td>User Controlled</td>
<td></td>
</tr>
<tr>
<td>Always On VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Store VPN Password on Device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow User-Defined VPN Profiles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Require Screen Lock</td>
<td>User Controlled</td>
<td></td>
</tr>
<tr>
<td>Maximum Screen Lock Timeout</td>
<td>600</td>
<td></td>
</tr>
<tr>
<td>Enforce Screen Lock During Display-On Time Lock Device During Audio Call</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Kerberos Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kerberos Realm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Load Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer Firmware Sharing</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Log Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Log Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Profile</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Web Access</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

Figure 69: DX80 Device Configuration-5
<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Access*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Android Debug Bridge (ADB)*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Multi-User*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Allow Applications from Unknown Sources*</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Allow Applications from Google Play</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Cisco UCM App Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Image</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company Photo Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voicemail Server (Primary)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voicemail Server (Backup)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence and Chat Server (Primary)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence and Chat Server Type*</td>
<td>Cisco WebEx Connect</td>
<td></td>
</tr>
<tr>
<td>Presence and Chat Single Sign-On (SSO) Domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-User URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email address for customer support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer support upload URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Credentials Persistent for Expressway Sign in*</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

*These features are marked with an asterisk (*) and may vary depending on the specific model of the DX80 device.
Line Configuration

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

<table>
<thead>
<tr>
<th>Directory Number Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number*</td>
</tr>
<tr>
<td>Route Partition</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Alerting Name</td>
</tr>
<tr>
<td>ASCII Alerting Name</td>
</tr>
<tr>
<td>External Call Control Profile</td>
</tr>
<tr>
<td>Allow Control of Device from CTI</td>
</tr>
<tr>
<td>Associated Devices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Directory Number Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Mail Profile</td>
</tr>
<tr>
<td>Calling Search Space</td>
</tr>
<tr>
<td>BLF Presence Group*</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
</tr>
<tr>
<td>Auto Answer*</td>
</tr>
<tr>
<td>Reject Anonymous Calls</td>
</tr>
</tbody>
</table>

Figure 71: DX80 Line [1] 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 78 of 145
Figure 72: DX80 Line [1] Configuration-2
**MLPF Alternate Party And Confidential Access Level Settings**

- **Target (Destination)**
- **MLPF Calling Search Space**
- **MLPF No Answer Ring Duration (seconds)**
- **Confidential Access Mode**
- **Confidential Access Level**
- **Call Control Agent Profile**

**Line Settings for All Devices**

- **Hold Reversion Ring Duration (seconds)**
- **Hold Reversion Notification Interval (seconds)**
- **Party Entrance Tone**

**Line 1 on Device SEP7426ACEF053D**

- **Display (Caller ID)**
- **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)**

**Multiple Call/Call Waiting Settings on Device SEP7426ACEF053D**

- **Note:** The range to select the Max Number of calls is: 1-4
- **Maximum Number of Calls**
- **Busy Trigger**

**Forwarded Call Information Display on Device SEP7426ACEF053D**

**Users Associated with Line**

<table>
<thead>
<tr>
<th>Full Name</th>
<th>User ID</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>threeSpark</td>
<td>spark3</td>
<td></td>
</tr>
</tbody>
</table>

© 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

---

**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.

![Expressway Option Keys](image-url)
DNS Configuration

Navigation: System-> DNS

Figure 77: Expressway-C-DNS Configuration
### NTP Configuration

**Navigation: System->Time**

![NTP Configuration](image)

*Figure 78: Expressway-C-NTP Configuration*
**TLS in SIP Configuration**

**Navigation:** Configuration -> Protocols -> SIP

![SIP Configuration](image)

**Figure 79: Expressway-C-SIP Configuration**
Microsoft Lync B2BUA configuration (Skype for Business B2BUA)


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

Figure 80: Expressway-C-Microsoft Lync (Skype for Business B2BUA) B2BUA Configuration
Microsoft Lync (Skype for Business) B2BUA trusted hosts
Expressway and Skype for Business Front End server should be added to the trusted host list.


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.
List of SAN entries required for Generating CSR:

- Fqdn of the expressway, expressc2.tekvizionlabs.com here.
- Fqdn of the CUCM, clus30pub.tekvizionlabs.com here.
After the CSR is generated and downloaded, follow the steps described in [Submit a certificate request in the Certificate Authority](#) to create a certificate request in CA.
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 Download a root certificate from CA to download the root certificate from CA.

![Trusted CA certificate](image)

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](image)

Figure 87: Expressway-C-Call routing
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:

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
### Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>CUCM Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Neighbor</td>
</tr>
<tr>
<td>Hop count</td>
<td>15</td>
</tr>
</tbody>
</table>

### H.323

Mode: Off

### SIP

<table>
<thead>
<tr>
<th>Mode</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>5081</td>
</tr>
<tr>
<td>Transport</td>
<td>TLS</td>
</tr>
<tr>
<td>TLS verify mode</td>
<td>Off</td>
</tr>
<tr>
<td>Accept proxied registrations</td>
<td>Allow</td>
</tr>
<tr>
<td>Media encryption mode</td>
<td>Auto</td>
</tr>
<tr>
<td>ICE support</td>
<td>Off</td>
</tr>
<tr>
<td>Multistream mode</td>
<td>On</td>
</tr>
<tr>
<td>Preloaded SIP routes support</td>
<td>Off</td>
</tr>
</tbody>
</table>

### Authentication

Authentication policy: Do not check credentials

SIP authentication trust mode: Off

### Location

<table>
<thead>
<tr>
<th>Peer 1 address</th>
<th>cios30pub.tekzionlabs.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer 2 address</td>
<td>cios30sub1.tekzionlabs.com</td>
</tr>
</tbody>
</table>

Figure 91: Expressway-C Zone Configuration for UCM-1
Figure 92: Expressway-C Zone Configuration for UCM-2
Search Rules

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

<table>
<thead>
<tr>
<th>Priority</th>
<th>Rule name</th>
<th>Protocol</th>
<th>Source</th>
<th>Authentication</th>
<th>Mode</th>
<th>Pattern type</th>
<th>Pattern string</th>
<th>Pattern behavior</th>
<th>On match</th>
<th>Target</th>
<th>Rule</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cisco UCM to Skype for Business - 4 Digit Dialing</td>
<td>SIP</td>
<td>UCM Neighbor</td>
<td>No</td>
<td>Alias pattern match</td>
<td>Regex</td>
<td>@expressc2.tekvizionlabs.com:5061</td>
<td>Replace</td>
<td>Stop</td>
<td>To Microsoft Lync client via RFB/UA</td>
<td>Enabled</td>
<td>View/Edit</td>
</tr>
<tr>
<td>2</td>
<td>Path to Lync User Dialing</td>
<td>SIP</td>
<td>UCM Neighbor</td>
<td>No</td>
<td>Alias pattern match</td>
<td>Regex</td>
<td>@expressc2.tekvizionlabs.com:5061</td>
<td>Replace</td>
<td>Stop</td>
<td>To Microsoft Lync server via B2BUA</td>
<td>Enabled</td>
<td>View/Edit</td>
</tr>
<tr>
<td>50</td>
<td>LocalZoneMatch</td>
<td>Any</td>
<td>Any</td>
<td>No</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Enabled</td>
<td>View/Edit</td>
<td>Clone</td>
</tr>
<tr>
<td>100</td>
<td>Route to IMAP</td>
<td>SIP</td>
<td>SFB Zone</td>
<td>No</td>
<td>Alias pattern match</td>
<td>Regex</td>
<td>@expressc2.tekvizionlabs.com:5061</td>
<td>Replace</td>
<td>Continue</td>
<td>IM</td>
<td>Enabled</td>
<td>View/Edit</td>
</tr>
<tr>
<td>110</td>
<td>SFB Zone Rule</td>
<td>SIP</td>
<td>SFB Zone</td>
<td>No</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Enabled</td>
<td>View/Edit</td>
<td>Clone</td>
</tr>
<tr>
<td>120</td>
<td>B2BUA to UCM</td>
<td>SIP</td>
<td>UCM Neighbor</td>
<td>No</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Enabled</td>
<td>View/Edit</td>
<td>Clone</td>
</tr>
<tr>
<td>130</td>
<td>UCM to Lync User Dialing</td>
<td>SIP</td>
<td>UCM Neighbor</td>
<td>No</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Enabled</td>
<td>View/Edit</td>
<td>Clone</td>
</tr>
<tr>
<td>140</td>
<td>Internal zone search rule</td>
<td>Any</td>
<td>Any</td>
<td>No</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Any alias</td>
<td>Enabled</td>
<td>View/Edit</td>
<td>Clone</td>
</tr>
<tr>
<td>150</td>
<td>External IP address search rule</td>
<td>Any</td>
<td>Any</td>
<td>No</td>
<td>Any IP address</td>
<td>Any IP address</td>
<td>Any IP address</td>
<td>Any IP address</td>
<td>Any IP address</td>
<td>Enabled</td>
<td>View/Edit</td>
<td>Clone</td>
</tr>
</tbody>
</table>

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 which the search process that this rule is applied, 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
Figure 94: Expressway-C Search rule CISCO UCM to Skype for Business - 4 Digit Dialing

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

![Configuration](image)

**Expressway-C Traversal Zone Search Rules**

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

---

© 2016 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com
Page 103 of 145
**Expressway-E Traversal Zone Search Rules**

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

   - **Rule name**: External IP address search rule
   - **Description**: Route external IP address
   - **Priority**: 100
   - **Protocol**: Any
   - **Source**: Any
   - **Request must be authenticated**: No
   - **Mode**: Any IP address
   - **On successful match**: Continue
   - **Target**: Traversals
   - **State**: Enabled

![Figure 104: Expressway-C External IP address search rule](image)

---

**Figure 102: Expressway-C Dial Plan Configuration**

**Figure 103: Expressway-E Dial Plan Configuration**
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.
2. 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.
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](image)

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.
- 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.

![IM and Presence Service nodes](image)

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).

1. Repeat the discovery procedure for other IM and Presence Service nodes/clusters, if required.
2. 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 [Download a root certificate from CA](#) 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:
3. Click on the uploaded certificate and it should look similar to the one below
### Certificate Details for tekvizionlabs-DC01-CA, cup-trust

<table>
<thead>
<tr>
<th>Status</th>
<th>Status: Ready</th>
</tr>
</thead>
</table>
| Certificate Settings | 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 |
| Certificate File Data | Version: V3  
Serial Number: 6831D13ACF87EDA34976B8DA8FAE157A  
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)  
**Issuer Name: CN=tekvizionlabs-DC01-CA, DC=tekvizionlabs, DC=com**  
Validity From: Mon Feb 16 08:56:47 CST 2015  
To: Sun Feb 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: 3082010a0282010100a05c7d070856af7a252520211cc62381eeb32800bd0d584fb8b57ba780aa7e0494581e7e9f2d5ddeb19a7322c220cacc870491cb4ae8de95ab5cdd78fe8e7555e954e4a90be29cb609e904de9aacc6b42b6175228fe6b0b7a7e8c96c278ef9c4491121290a8d2b0d7f628c7f165e8f8d0000e19850b45b8ac4f7aaf1e80c0bf62a60582ad754837f47913a3e288c2594c752eb0bb0b0cf4705c337436dd7b44f10282d2494335f226f429a27905a69c2c6c728b3c7f9b5e8e7391b50d17f |

*Figure 108: IM&P-Root Certificate Example*
**IM&P Server Certificate**


**Generate CSR**

1. Click on ‘Generate CSR’

![Figure 109: IM&P Generate CSR-1](image)

2. Set **Certificate Purpose**: Cup
3. Set **Distribution**: Select the IM&P publisher node
4. Set **Key Length**: 2048

![Figure 110: IM&P Generate CSR-2](image)
After the CSR is generated and downloaded, follow the steps described in Submit a certificate request in the Certificate Authority to create a certificate request in CA.

Upload Certificate

5. Once the certificate is downloaded, click on ‘Upload Certificate/Certificate chain’

7. Click on the uploaded certificate and it should look similar to the one below
### Certificate Details for clus30pimp.tekvizionlabs.com, cup

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regenerate</td>
<td>Regenerate</td>
</tr>
<tr>
<td>Generate CSR</td>
<td>Generate CSR</td>
</tr>
<tr>
<td>Download .PEM File</td>
<td>Download .PEM File</td>
</tr>
<tr>
<td>Download .DER File</td>
<td>Download .DER File</td>
</tr>
</tbody>
</table>

#### 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

```
[  
  Version: V3  
  Serial Number: 280000006725EAB83E8467288678000000000072  
  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:  
  3082010a262020100d41614fdfe6e035f6e073bb2a1801221595d921860adf41610e71e6fc0  
  4222b15d3490357af8be7abc37ee5a4e0af833778ceed75c282182f4ec26d8066e7ff335153237401  
  03cc5ac7c0de934a7d6e5d30ce4e68044efafdf13f92c79e6103c81e0d1dc676d5f31571453b393f  
  d5d46b4c7ef2caeeab4da8f50c3c365d113658ab6afeae3bce73a84222873a83871d21e453cd204  
```

---

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

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](image)

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


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

<table>
<thead>
<tr>
<th>Status</th>
<th>Related Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status: Ready</td>
<td>Back To Find/List</td>
</tr>
</tbody>
</table>

**Incoming ACL Information**

Configure an address which will be added to the SIP Proxy list of allowed incoming addresses. Note: any address added to this list will bypass digest authentication. By default, the behavior is to deny all incoming requests.

<table>
<thead>
<tr>
<th>Description</th>
<th>Address Pattern*</th>
</tr>
</thead>
<tbody>
<tr>
<td>clients</td>
<td>10.84.0.0/16</td>
</tr>
</tbody>
</table>

(save, delete, copy, add new)

*Figure 118: Cisco IM&P Incoming ACL-1*

---

**Incoming Access Control List Configuration**

<table>
<thead>
<tr>
<th>Status</th>
<th>Related Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status: Ready</td>
<td>Back To Find/List</td>
</tr>
</tbody>
</table>

**Incoming ACL Information**

Configure an address which will be added to the SIP Proxy list of allowed incoming addresses. Note: any address added to this list will bypass digest authentication. By default, the behavior is to deny all incoming requests.

<table>
<thead>
<tr>
<th>Description</th>
<th>Address Pattern*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expressway IP</td>
<td>10.80.20.0/24</td>
</tr>
</tbody>
</table>

(save, delete, copy, add new)

*Figure 119: Cisco IM&P Incoming ACL-2*
**Incoming Access Control List Configuration**

**Status**
- Status: Ready

**Incoming ACL Information**
Configure an address which will be added to the SIP Proxy list of allowed incoming addresses. Note: any address added to this list will bypass digest authentication. By default, the behavior is to deny all incoming requests.

<table>
<thead>
<tr>
<th>Description</th>
<th>ExpressWay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Pattern</td>
<td>All</td>
</tr>
</tbody>
</table>

**Figure 120: Cisco IM&P Incoming ACL-3**

**Incoming Access Control List Configuration**

**Status**
- Status: Ready

**Incoming ACL Information**
Configure an address which will be added to the SIP Proxy list of allowed incoming addresses. Note: any address added to this list will bypass digest authentication. By default, the behavior is to deny all incoming requests.

<table>
<thead>
<tr>
<th>Description</th>
<th>ExpressWay_IPAddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Pattern</td>
<td>expressc2.tvkisionlabs.com</td>
</tr>
</tbody>
</table>

**Figure 121: Cisco IM&P Incoming ACL-4**
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 for Skype for Business Server**

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

![Figure 124: Cisco IMP TLS Peer Subject Configuration-2](image)

**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

![Figure 125: Cisco IM&P Presence Gateway](image)
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.
2. **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.

![Presence Settings Configuration](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

![Cisco IM&P Security Settings](image)

*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](image)

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 Server. 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.

```powershell
$route=New-CsStaticRoute -TLSRoute -Destination "expressc2.tekvizionlabs.com" -MatchUri "tekvizionlabs.com" -Port 5061 -UseDefaultCertificate $true
Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$route}
```

**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

**Destination** - FQDN of the Expressway-C

**Port** – Listening port (usually 5061 for TLS)

**MatchUri** – Destination domain

- Verify the configured static routes.
**Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty route**

```xml
  <Route>
    <TLS DefaultCertificate/>
    <Transport Port="5061">
      <TLS DefaultCertificate/>
    </Transport>
  </Route>
</Transport>
```

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

**Configure Encryption Level**

Configure Encryption level parameters through the Windows PowerShell® 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**

```powershell
PS C:\Users\administrator.LYNCLABS> 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.

   ```powershell
   New-CsTrustedApplicationPool -Identity clus30pimp.tekvizionlabs.com -Registrar fe01.tekvizionlabs.com -Site CleanDefaultTopology -TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $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.

   ```powershell
   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

   ```powershell
   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

   ```powershell
   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 -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](Figure 132: Skype for Business Deployment Wizard- Request & Assign Certificates-1)
Figure 133: Skype for Business Deployment Wizard- Request & Assign Certificates-2
Figure 134: Skype for Business Deployment Wizard - Request & Assign Certificates-3
Figure 135: Skype for Business Deployment Wizard- Request & Assign Certificates-4
Figure 136: Skype for Business Deployment Wizard- Request & Assign Certificates-5
Certification Authority Account

- Specify alternate credentials for the certification authority.
  - User name:
  - Password:

Figure 137: Skype for Business Deployment Wizard - Request & Assign Certificates-6
Figure 138: Skype for Business Deployment Wizard- Request & Assign Certificates-7
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 Window]

- Select a CA from the list detected in your environment.
- Friendly name: Skype for Business Server 2015 Default certificate 10/31/2016
- Organization: [Blank] Organizational unit: [Blank]
- 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.
  - [ ] All
  - [ ] tekvizionlabs.com

- Subject name: 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

*Figure 140: Skype for Business Deployment Wizard - Request & Assign Certificates*
To generate a request with the following information, click Next.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Use</td>
<td>Server default, Web services internal, Web services external</td>
</tr>
<tr>
<td>Country/Region</td>
<td>US</td>
</tr>
<tr>
<td>State/Province</td>
<td>Texas</td>
</tr>
<tr>
<td>City/Locality</td>
<td>Plano</td>
</tr>
<tr>
<td>Friendly Name</td>
<td>Skype for Business Server 2015</td>
</tr>
<tr>
<td></td>
<td>Default certificate 10/31/2016</td>
</tr>
<tr>
<td>Key Size</td>
<td>2048</td>
</tr>
<tr>
<td>Exportable</td>
<td>False</td>
</tr>
</tbody>
</table>

Figure 141: Skype for Business Deployment Wizard - Request & Assign Certificates-14
Figure 142: Skype for Business Deployment Wizard - Request & Assign Certificates-15
Figure 143: Skype for Business Deployment Wizard- Request & Assign Certificates-16
Figure 144: Skype for Business Deployment Wizard - Request & Assign Certificates-18

Assign the returned certificate to the Skype for Business Server usages on this server.

View Certificate Details
Figure 145: Skype for Business Deployment Wizard - Request & Assign Certificates-19
Figure 146: Skype for Business Deployment Wizard - Request & Assign Certificates-20