TOMORROW starts here.
Federation and Remote Access for Unified Communications Leveraging Collaboration Edge

BRKUCC-2666

Darren Henwood
Consulting Systems Engineer
Making Collaboration as Easy & Effective Outside the Network as it is Inside with Jabber

- Search corporate directory
- Access visual voicemail
- Share content
- Make voice calls
- Make video calls
- IM and Presence

WebEx
Make Jabber Mobile Users as Productive on the Road

- Jabber moves between networks
- Uses TLS technology
- Security Choice: No VPN required
  - Secure only Jabber application
  - Personal data is not connected to the network
- Automatic Service Discover
Cisco Jabber Remote Access Options

- Layer 3 VPN Solution
- Secures the entire device and its contents
- AnyConnect allows users access to any permitted applications & data

- New Complementary Offering
- Session-based firewall traversal
- Allows access to collaboration applications ONLY
- Personal data not routed through enterprise network
Branding Terminology Decode

**Collaboration Edge**
Umbrella term describing Cisco’s entire collaboration architecture for edge
... features and services that help bridge islands to enable any to any collaboration…
...collaborate with anyone anywhere, on any device….

**Cisco VCS**
Existing product line option providing advanced video and TelePresence applications
Includes **VCS Control** and **VCS Expressway**

**Cisco Expressway**
New product line option for CUCM customers, providing firewall traversal & video interworking
Includes **Expressway Core** and **Expressway Edge**

**Mobile and Remote Access**
Feature available on **both** VCS and Expressway product lines with X8.1 s/w
Delivers VPN-less access to Jabber and Fixed Endpoints
Expressway X8.1 Product Line Options

- Specialised video applications for video-only customer base and advanced video requirements
- No changes to existing licensing model

- Solution designed for and sold exclusively with CUCM 9.1 and above
- No additional cost for server software licenses for CUCM 9.1+ customers
# VCS and Cisco Expressway Feature Comparison

<table>
<thead>
<tr>
<th>Feature Comparison</th>
<th>Cisco Expressway Series</th>
<th>Cisco VCS Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile and Remote Access</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Business to Business Video</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Advanced Features (Extension Mobility, voicemail, shared line, Call forward all, G729 support, ad-hoc conferencing, etc)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Business to Consumer / Public to Enterprise Access with Jabber Guest</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video Interworking (IPv4 to IPv6, H.323-SIP, MS H.264 SVC-AVC, Standards-based 3rd Party Video endpoints)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video / TelePresence Device Registration &amp; Provisioning</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Video Session Management &amp; Call Control</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>WebEx Enabled TelePresence</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
Expressway - Mobile & Remote Access
What can a Jabber Client do with Expressway?

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

Inside firewall (Intranet) | DMZ | Outside firewall (Public Internet)
# Solution Components Software Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Min Software Version</th>
<th>Projected Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Expressway or Cisco VCS</td>
<td>X8.1</td>
<td>Available</td>
</tr>
<tr>
<td>Cisco Expressway or Cisco VCS</td>
<td>X8.1.1 (MR)</td>
<td>Q1CY14</td>
</tr>
<tr>
<td>CUCM</td>
<td>9.1(2) SU1</td>
<td>Available</td>
</tr>
<tr>
<td>CUCM IM&amp;P</td>
<td>9.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unity Connection</td>
<td>8.6(1)</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Windows</td>
<td>9.7</td>
<td>Q1CY14</td>
</tr>
<tr>
<td>Jabber for iOS</td>
<td>9.6.1</td>
<td>Q1CY14</td>
</tr>
<tr>
<td>Jabber for MAC</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>Jabber for Android</td>
<td>9.6</td>
<td>Q1CY14</td>
</tr>
<tr>
<td>EX/MX/SX/C Series TelePresence Endpoints</td>
<td>TC7.0.1</td>
<td>Available</td>
</tr>
</tbody>
</table>
1. **Expressway E** is the traversal server installed in DMZ. **Expressway C** is the traversal client installed inside the enterprise network.

2. **Expressway C** initiates traversal connections outbound through the firewall to specific ports on **Expressway E** with secure login credentials.

3. Once the connection has been established, **Expressway C** sends keep-alive packets to **Expressway E** to maintain the connection.

4. When **Expressway E** receives an incoming call, it issues an incoming call request to **Expressway C**.

5. **Expressway C** then routes the call to CUCM to reach the called user or endpoint.

6. The call is established and media traverses the firewall securely over an existing traversal connection.
The X8.1 release delivers 3 key capabilities enabling the Expressway Mobile and Remote Access feature:

- XCP Router for XMPP traffic
- HTTPS Reverse proxy
- Proxy SIP registrations to CUCM

(details on new firewall port requirements covered later)
Mobile and Remote Access

- Enable Mobile and Remote Access on Expressway C & E

- Disabled by default in Jabber 9.6 (Windows and iOS)

- Enabled by `jabber-config` key

  <Policies>
  
  <RemoteAccess>ON</RemoteAccess>

  </Policies>

- Mobile and Remote Access can be enabled for groups of users
Service Discovery

• **Edge Detection** determines whether Jabber is inside or outside the corporate firewall
  o Based on SRV records returned from DNS
  o `_cisco-uds` -> inside the company firewall
    Do not transform traffic and route to appropriate service
  o `_collab-edge` -> outside corporate firewall
    Transform all traffic and route through Expressway-E

• **Service discovery** is used to obtain login service
  o Based on highest priority SRV record returned

• **Jabber Common Framework** registers normally
Expressway & Jabber Service Discovery

Inside firewall (Intranet)

DMZ

Outside firewall (Public Internet)

Collaboration Services

CUCM

Expressway C

Expressway E

Public DNS

Cisco Jabber Client

DNS SRV lookup _cisco-uds._tcp.example.com

Not Found

DNS SRV lookup _collab-edge._tls.example.com

expwyNYC.example.com

TLS Handshake, trusted certificate verification

HTTPS:

get_edge_config?service_name=_cisco-uds&service_name=_cuplogin

_collab-edge record needs to be available in Public DNS
Split DNS SRV Record Requirements

• **_collab-edge** record needs to be available in Public DNS

• Multiple SRV records (and Expressway E hosts) can be deployed for HA

• A GEO DNS service can be used to provide unique DNS responses by geographic region

```
_collab-edge._tls.example.com. SRV 10 10 8443 expwy1.example.com.
_collab-edge._tls.example.com. SRV 10 10 8443 expwy2.example.com.
```

• **_cisco-uds** record needs be available only on internal DNS (available to Expressway C at a minimum)

```
_cisco-uds._tcp.example.com. SRV 10 10 8443 cucm1.example.com.
_cisco-uds._tcp.example.com. SRV 10 10 8443 cucm2.example.com.
```
Jabber in Edge Mode (Transition)

When is discovery done?

- On start up
- Network change events will trigger SRV lookup which may transition you from external to internal
- When you get transport errors (SIP, XMPP & HTTP) will trigger SRV lookup which may transition you from internal to external
  - Only doing SRV lookup when there is network activity happening anyway and this saves battery life on mobile platforms
- During the transition period you will remain logged into the Jabber client, but you will get disconnected temporarily from the IM&P server, your presence will appear as offline, and once connected via Edge you will get reconnected to IM&P automatically and become online again.
Mobile and Remote Access – Directory Integration

- LDAP traffic does not traverse the Collaboration Edge
- When in “edge” mode, UDS directory service provides directory integration for Jabber. UDS service runs on CUCM by default (Cisco Tomcat Service)
- When inside the firewall, Jabber will connect to a LDAP server to provide directory integration
  - Jabber for Mac, Android and iOS, support Basic Directory Integration (BDI). BDI uses a common username and password to connect to a LDAP server for directory integration. BDI configuration is specified in the jabber-config.xml file.
- WebEx Messenger provides directory integration for Jabber/Cloud integrations
Mobile and Remote Access

- LDAP directory integration to be used in on-premise mode
- UDS integration to be used in edge mode [for on-premise deployments]
- WebEx Messenger directory search to be used for cloud-based deployments
Contact Search Considerations (on-premise IM&P)

- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to CUCM
- User Data Services (UDS) is a CUCM RESTful API allowing for contact search, among other things
- All Jabber clients connecting via Expressway will use UDS for contact search
- **Jabber clients deployed on-premise** will use **LDAP** for directory search
- Jabber clients will automatically use UDS for directory search when connecting via Expressway
- The entire corporate directory needs to be sync'd on every CUCM cluster for best contact search experience
Mobile and Remote Access

- Directory integration configured in jabber-config.xml (except for cloud mode)

```xml
<Directory>
  <!-- EDI Settings -->
  <SearchBase1>OU=Employees,OU=AllUsers,DC=example,DC=com</SearchBase1>
  <PhotoURISubstitutionEnabled>True</PhotoURISubstitutionEnabled>
  <PhotoURISubstitutionToken>sAMAccountName</PhotoURISubstitutionToken>
  <PhotoURIWithToken>http://photos.example.com/photo/sAMAccountName.jpg</PhotoURIWithToken>

  <!-- BDI Settings -->
  <BDIPrimaryServerName>ds.example.com</BDIPrimaryServerName>
  <BDIConnectionUsername>readonly@example.com</BDIConnectionUsername>
  <BDIConnectionPassword>readonly</BDIConnectionPassword>
  <BDISearchBase1>OU=Employees,OU=AllUsers,DC=example,DC=com</BDISearchBase1>
  <BDIPhotoURISubstitutionEnabled>True</BDIPhotoURISubstitutionEnabled>
  <BDIPhotoURISubstitutionToken>sAMAccountName</BDIPhotoURISubstitutionToken>
  <BDIPhotoURIWithToken>http://photos.example.com/photo/sAMAccountName.jpg</BDIPhotoURIWithToken>
  <EnableLocalAddressBookSearch>true</EnableLocalAddressBookSearch>

  <!-- UDS Settings for Edge users only -->
  <UDSPhotoURIWithToken>http://photos.example.com/photo/%%uid%%.jpg</UDSPhotoURIWithToken>
</Directory>
```
Contact Search Considerations (Cloud based IM&P)

- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to CUCM
- Corporate directory is also exported to WebEx Messenger cloud
- All Jabber clients will use WebEx Messenger cloud as a contact source for contact search
Global Deployment Topology & Geo DNS

DNS SRV lookup _collab-edge._tls.example.com

Expressway edge access
SME global aggregation
UCM regional clusters

US
Europe
Asia

US SME
EU SME
Asia SME

SJC
RTP
PAR
AMS
LON
TKY
BGL
HKG

expwy.us.example.com
expwy.uk.example.com
expwy.jp.example.com
Design and Deployment Considerations
Protocol Workload Summary

Collaboration Services

Inside firewall (Intranet)

DMZ

Outside firewall (Public Internet)

Internet

Protocol

SIP

Media

HTTPS

XMPP

Security

TLS

SRTP

TLS

Security

Service

TLS

Session Establishment – Register, Invite, etc. via CUCM

SRTP

Audio, Video, Content Share, Advanced Control

TLS

Logon, Provisioning/Configuration, Contact Search, Visual Voicemail

TLS

Instant Messaging, Presence

Unified CM IM&P

Conference Resources

Other UC Infrastructure & Resources

Cisco Public
Jabber in Edge Mode

All communication from the client to Expressway Edge is secured using TLS (even if CSF device has not been CAPF enrolled)
Hybrid Deployment - Cloud Based IM&P

Inside firewall (Intranet)  DMZ  Outside firewall (Public Internet)

Collaboration Services
Unified CM  Expressway C  Expressway E

Conference Resources
Other UC Infrastructure & Resources

Protocol
SIP
Media
HTTPS
XMPP

Security
TLS
SRTP
TLS
TLS

Service
Session Establishment – Register, Invite, etc. via CUCM
Audio, Video, Content Share, Advanced Control
Logon, Provisioning/Configuration, Contact Search, Visual Voicemail
Instant Messaging, Presence
CUCM provides call control for both mobile and on-premise endpoints

**Media Traversal**

“C” calls “A” on-premise
Expressway solution provides firewall traversal for media
Expressway C de-multiplexes media and forwards towards “A”

**Media Relay**

“C” calls “B” off-premise
Media is relayed via Expressway C

**Optimised Media (roadmap ICE)**

“B” calls “D” off-premise
Both “B” and “D” are ICE enabled
STUN binding success
Media flows are optimised between endpoints
Expressway Clustering, 4+2

- Cluster Expressways for scale and redundancy
- Expressway Clusters support up to 6 peers
- Expressway E and C node types cannot be mixed in the same cluster
- Deploy equal number of peers in Expressway C and E clusters
- Deploy same OVA sizes throughout cluster
- Expressway remote access is limited to one customer domain per cluster
- However customers can deploy multiple clusters for the same customer domain
# Mobile & Remote Access Deployment Options

<table>
<thead>
<tr>
<th>CUCM Clusters</th>
<th>Expressway C Clusters</th>
<th>Expressway E Clusters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Single Expressway deployment providing remote access to a central CUCM cluster</td>
</tr>
<tr>
<td>1</td>
<td>2+</td>
<td>2+</td>
<td>Regional Expressway deployments providing remote access to a central CUCM cluster</td>
</tr>
<tr>
<td>2+</td>
<td>1</td>
<td>1</td>
<td>Single Expressway deployment providing remote access to a multiple CUCM clusters</td>
</tr>
<tr>
<td>2+</td>
<td>2+</td>
<td>2+</td>
<td>Regional Expressway deployments providing remote access to multiple CUCM Clusters</td>
</tr>
</tbody>
</table>
Unsupported: Unbalanced Expressway Deployments

- This model is still supported for traditional VCS Expressway deployments
- But this is **not supported for the new mobile and remote access** functionality introduced in X8.1
- Expressway X8.1 remote access requires a Expressway C cluster for each Expressway E cluster
- **Only one “Mobile & Remote Access” enabled Traversal zone per cluster**
Unsupported: Expressway Chained Traversal

- Chained traversal is often used in environments with heightened security policies.
- This option is still supported for traditional VCS deployments, or Expressway deployments that do not require the remote and mobile access feature.
- Not supported for the new mobile and remote access functionality introduced in X8.1.
- Only one “Mobile & Remote Access” enabled Traversal zone per cluster.
Existing VCS Customers

• Customers with VCS-C and VCS-E can add Mobile and Remote Access to an existing deployment
• Simply add a parallel traversal zone on existing VCSs to support mobile and remote access
• Ideal for mid-market customers, POCs, or pilot programs
• Concurrent session scale is the primary reason for adding Expressways dedicated to Mobile & Remote access
  o Will the number of remote Jabber users making calls over Expressway crush my existing TelePresence deployment?
• The difference in security posture between B2B video and remote access solutions is another consideration
  o Does it makes sense for the customer to combine these solutions on the same VMs?
Parallel Deployments of VCS & Expressway

- _collab-edge SRV records don’t conflict with existing VCS SRV record usage

B2B Video SIP & H.323 (inbound & outbound)
Cisco Jabber Video for TelePresence Registration
Cisco TelePresence Endpoints (TC) Registration to VCS
WebEx Enabled TelePresence (outbound)

Add _collab-edge SRV to Public DNS
AnyConnect & Expressway Coexistence

- Customers that have deployed AnyConnect can also deploy Expressway Mobile & Remote Access feature
- For the best end user experience, prevent all Jabber traffic from using the AnyConnect tunnel
  - Active calls going through Expressway will be dropped if AnyConnect tunnel is established mid-call
- Expressway can provide Jabber client access to on-premise collaboration services even with an active AnyConnect tunnel established
- Requirements to keep Jabber traffic going through Expressway
  - AnyConnect split tunnel providing connectivity to internal enterprise network only (not including Expressway E)
  - Deny access (ASA DNS inspection) to the internal DNS SRV records (_cisco-uds & _cuplogin) to AnyConnect clients
Expressway Configuration Summary

- Enable Mobile & Remote Access feature, Configuration > Unified Communications
- Provide IM&P Publisher address and supply admin credentials for each IM&P cluster (not required for hybrid deployments)
- Provide CUCM Publisher address and supply admin credentials for each CUCM cluster
  - Expressway C connects to each Publisher and discovers all cluster nodes
  - Neighbour Zone auto-generated for each CUCM node
  - Search Rules auto-generated for each CUCM node
- Add the customer domain and select services
- Generate certificate signing requests and procure CA signed certs
- Configure Traversal Zone with Mobile & Remote Access feature enabled
# Unified Communications Configuration

- Expressway C

## Unified Communications

<table>
<thead>
<tr>
<th>Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile and remote access</td>
<td>On</td>
</tr>
<tr>
<td>Jabber Guest support</td>
<td>On</td>
</tr>
</tbody>
</table>

## IM and Presence servers and Unified CM servers

<table>
<thead>
<tr>
<th>IM and Presence servers</th>
<th>discover IM and Presence servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM servers</td>
<td>Configure Unified CM servers</td>
</tr>
</tbody>
</table>

## Advanced

<table>
<thead>
<tr>
<th>HTTP server allow list</th>
<th>Configure HTTP server allow list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jabber Guest servers</td>
<td>Configure Jabber Guest servers</td>
</tr>
<tr>
<td>Advanced settings</td>
<td>Show advanced settings</td>
</tr>
</tbody>
</table>
Unified Communications Configuration

- Expressway C

Cisco Expressway-E

Status  System  Configuration  Applications  Users  Maintenance

Unified Communications

You are here: Configuration → Unified Communications → Configuration

Configuration

- Mobile and remote access: On
- Jabber Guest support: On

Save
Note: No domain configuration required on Expressway E
# Expressway E Traversal Server Zone

## Edit zone

<table>
<thead>
<tr>
<th>Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Traversal Server MRA</td>
</tr>
<tr>
<td>Type</td>
<td>Traversal server</td>
</tr>
<tr>
<td>Hop count</td>
<td>Max: 25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connection credentials</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>traversal</td>
</tr>
<tr>
<td>Password</td>
<td>Add/Edit local authentication database</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H.323</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Off</td>
</tr>
<tr>
<td>Protocol</td>
<td>Assent</td>
</tr>
<tr>
<td>H.460.19 demultiplexing mode</td>
<td>Off</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>On</td>
</tr>
<tr>
<td>Port</td>
<td>7001</td>
</tr>
<tr>
<td>Transport</td>
<td>TLS</td>
</tr>
<tr>
<td>Mobile and remote access</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS verify mode</td>
<td>On</td>
</tr>
<tr>
<td>TLS verify subject name</td>
<td>cluster.collabedge.ucsdemolab.com</td>
</tr>
<tr>
<td>Media encryption mode</td>
<td>Force encrypted</td>
</tr>
<tr>
<td>ICE support</td>
<td>On</td>
</tr>
<tr>
<td>Poison mode</td>
<td>Off</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication policy</td>
<td>Do not check credentials</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UDP / TCP probes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP retry interval</td>
<td>Max: 2</td>
</tr>
<tr>
<td>UDP retry count</td>
<td>Max: 5</td>
</tr>
<tr>
<td>UDP keep alive interval</td>
<td>Max: 20</td>
</tr>
<tr>
<td>TCP retry interval</td>
<td>Max: 2</td>
</tr>
<tr>
<td>TCP retry count</td>
<td>Max: 5</td>
</tr>
<tr>
<td>TCP keep alive interval</td>
<td>Max: 20</td>
</tr>
</tbody>
</table>
Expressway C Unified Communications Status

- Status > Unified Communications

<table>
<thead>
<tr>
<th>Unified Communications (last updated: 03:06:32 EST)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications status</td>
</tr>
<tr>
<td>Jabber Guest support</td>
</tr>
<tr>
<td>Unified Communications services</td>
</tr>
<tr>
<td>IM and Presence servers</td>
</tr>
<tr>
<td>Unified CM servers</td>
</tr>
<tr>
<td>Current provisioned sessions</td>
</tr>
<tr>
<td>Total provisioning requests since last restart</td>
</tr>
<tr>
<td>Total provisioned sessions since last restart</td>
</tr>
<tr>
<td>Unified CM calls</td>
</tr>
</tbody>
</table>

**Domains**

<table>
<thead>
<tr>
<th>Name</th>
<th>Services</th>
<th>Associated zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>ce.ucdemolab.com</td>
<td>Unified CM registrations, IM and Presence</td>
<td>Traversal Client MPA</td>
</tr>
<tr>
<td>ucdemolab.com</td>
<td>Unified CM registrations, IM and Presence, Jabber Guest</td>
<td>Traversal Client MPA</td>
</tr>
</tbody>
</table>

**Zones**

<table>
<thead>
<tr>
<th>Name</th>
<th>SIP status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traversal Client MPA</td>
<td>Active</td>
</tr>
</tbody>
</table>

**Advanced status information**

- View provisioning sessions
- View sip tunnel status
Allowed Reverse Proxy Traffic

- Expressway E server will be listening on TCP 8443 for HTTPS traffic
- Basic mobile & remote access configuration allows inbound authenticated HTTPS requests to the following destinations on the enterprise network
  - All discovered CUCM nodes TCP 6970 (TFTP file requests) & TCP 8443 (UDS API)
  - All discovered IM&P nodes TCP 7400 (XCP Router) & TCP 8443 (SOAP API)
- HTTPS traffic to any additional hosts need to be added to the Exp-C allow list
- Provides a mechanism to support Visual Voice Mail access, contact photo retrieval, Jabber custom tabs, etc.
Supported Services with Collab Edge

- Instant Messaging and Presence – Cloud & On Premise
- Softphone Voice and Video Calls – CUCM 9.0 +
- Conferencing – Audio and Video
- Video Desktop Share – BFCP
- WebEx Desktop Share
- Visual Voicemail – Using HTTP Whitelisting on Expressway-C
- Installer Update - Using HTTP Whitelisting on Expressway-C
- Custom HTML Tabs - Using HTTP Whitelisting on Expressway-C
- Directory Search [UDS] – Dictated by Edge Detection Service
- Directory Photo Resolution - Using HTTP Whitelisting on Expressway-C
Mobile and Remote Access - Voicemail

- Jabber connects to Unity Connection over a REST interface to gather voicemail data to display in the visual voicemail tab
  - This is a HTTP connection and will not be allowed through the collaboration edge architecture by default.

- On the Expressway-C, we can create a HTTP whitelist which allows Jabber to send HTTP requests to specified internal hosts.
Mobile and Remote Access

• What should we whitelist?
  o Unity Connection Server for Visual Voicemail
  o Directory photo server if using http server to deliver photos
  o HTML tab host e.g. company intranet html tab
  o HTML tab icon host
  o Jabber update host
CUCM Requirements
Expressway Remote Access from CUCM Perspective

- Remote access provided by Expressway is, for the most part, transparent to CUCM
- Think SIP line integration, versus SIP trunk
- No requirement to build a SIP trunk on CUCM to Expressway C or E
- No requirement to make dial plan changes
- No remote access policy mechanism to limit edge access to certain Jabber users or devices
- Remote Jabber clients or TelePresence Endpoints registering to CUCM through Expressway will appear to CUCM as Expressway-C IP address (opportunity for CUCM Device Mobility feature usage)
Interaction with SIP Trunk

- SIP trunk is **not required** between Expressway C (or VCS-C) and CUCM for Mobile & Remote Access
- However, if CUCM includes a SIP trunk for other integrations, **CUCM will reject any SIP registration attempts from remote Jabber or TP endpoints**, as the register method is not accepted on CUCM SIP trunk interface
- Update CUCM SIP trunk security profile to listen on ports other than TCP 5060 or 5061 (you could use 5560, 5561, etc.)
- Port change allows SIP trunk integration + mobile & remote access
Debugging (Logs)

- Check lossy network connection
  - Search string “RTP STATS”

```
[media::rtp::SessionImpl::logRtpStatsWithLock] - RTP STATS,session_id=6,session_type=audio-main,rx_bytes_recv=3920,rx_pkts_recv=49,rx_pkts_lost=0,rx_curr_loss=0.00%,rx_cum_loss=0.00 %,rx_bitrate=1,rx_jitter=2,rx_fec_pkts_recv=49,rx_fec_pkts_lost=0,rx_fec_curr_loss=0.00%,rx_fec_cum_loss=0.00%,tx_bytes_sent=3920,tx_pkts_sent=49,tx_pkts_recv=9,tx_pkts_lost=0,tx_curr_loss=0.00%,tx_cum_loss=0.00%,tx_bitrate=1,tx_jitter=2,tx_round_trip=113,tx_last_ssrc=7547D352,tx_last_ext_high_seq=4321,tx_received_rb=1,tx_active_sources=1,tx_total_sources=1
```

- Search string “steady_state_adaption”
  - [steady_state_adaption, Sender_side] Network IS CONSISTENTLY LOSSY. New sending bitrate will be hard reduction to 302kbps.
UDS Directory Search

• All Jabber clients connecting via Expressway will use UDS for directory search (assuming CUCM IM&P deployment)
• TelePresence endpoints always use UDS for directory search
• For the best contact search experience, all Enterprise Users should be imported into every CUCM cluster’s end user table
• Home cluster check box needs to be selected on only one cluster for each user

• CUCM clusters support 80K end users, and can scale as high as 160K with BU megacluster approval
Security
Firewall Port Details

• No inbound ports required to be opened on the internal firewall

• Internal firewall needs to allow the following outbound connections from Expressway C to Expressway E
  o SIP: TCP 7001
  o Traversal Media: UDP 36000 to 36011
  o XMPP: TCP 7400
  o HTTPS (tunneled over SSH between C and E): TCP 2222

• External firewall needs to allow the following inbound connections to Expressway
  o SIP: TCP 5061
  o HTTPS: TCP 8443
  o XMPP: TCP 5222
  o Media: UDP 36002 to 59999
  o TURN server control: UDP 3478 – 3483
  o TURN server media: UDP 24000 – 24999

Jabber Guest, not required for Mobile & Remote Access
Media Port Range Expansion

• X8.1 scalability improvements require a media port range expansion
• X8.1 default media Port Range is now UDP 36000 – 59999
• VCS systems upgraded from X7 to X8.1 will need to manually update port range, Configuration > Local Zone > Traversal Subzone

### Traversal Subzone

<table>
<thead>
<tr>
<th>Ports</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Traversal media port start</td>
<td>36000</td>
<td>59999</td>
</tr>
<tr>
<td>Traversal media port end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Traversal Media Port Changes

Important change for existing VCS customers to understand

• X7 release included the ability to configure the Expressway Media demultiplexing RTP port and RTCP port

• Upon upgrading to X8.1 the traversal media ports are automatically migrated to the first 2 ports in the current media port range (details on previous slide)

• Customers will need to coordinate X8.1 upgrade with firewall port change

• New X8.1 installs on the Large OVA will use UDP 36000 – 36011, the expanded port range is required to support scalability improvements
Edge Server Authentication

• No matter which client authentication model is deployed, server authentication is always performed by the remote device
  
  • i.e. remote Jabber clients and remote endpoints will always validate the Expressway E Server Certificate presented in the TLS handshake

• Jabber Clients will rely on the underlying platform trusted CA list

• TelePresence Endpoints will rely on a trusted CA list included in firmware

• No CTL requirement for Edge Server authentication
High Level Deployment Guidance

• Start on solid ground
  o Jabber service discovery needs to work on-premise
  o Start on-premise and then add edge access
  o Verify end user home cluster discovery in multi CUCM cluster deployments

• Don’t forget about DNS
  o Understand split DNS SRV requirements, get DNS change requests in the queue
  o A common DNS domain simplifies matters

• Review TCP and UDP port requirements with firewall team

• Verify Expressway CA signed certs
  o Confirm SANs returned in CA signed cert match what was requested in the CSR
  o Verify cert includes both TLS Web Server & Client Authentication Extended Key Usage
Scalability and Licensing
# New Compute Platforms for X8

## Specs Based Virtual Machine Support

<table>
<thead>
<tr>
<th>OVA Size</th>
<th>vCPU</th>
<th>Reserved RAM</th>
<th>Disk Space</th>
<th>vNIC(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>2 x 1.8 GHz</td>
<td>4GB</td>
<td>132GB</td>
<td>1Gb</td>
</tr>
<tr>
<td>Medium</td>
<td>2 x 2.4 GHz</td>
<td>6GB</td>
<td>132GB</td>
<td>1Gb</td>
</tr>
<tr>
<td>Large</td>
<td>8 x 3.3 GHz</td>
<td>8GB</td>
<td>132GB</td>
<td>10Gb</td>
</tr>
</tbody>
</table>

## Appliance Support

- **Existing VCS Appliance**
- **New Offering**

- New appliances based on UCS C220 M3
- Bare metal – no hypervisor
- Fixed configurations for high and low end deployment
- Solution for customers with security policies that do not allow VMware in the DMZ
- CE500 Single components, 1Gbps interfaces
- CE1000 Redundant components, 1 or 10Gbps
## Expressway X8.1 Scalability

<table>
<thead>
<tr>
<th>Platform</th>
<th>Proxied Registrations</th>
<th>Video Calls</th>
<th>Audio Only Calls</th>
<th>Proxied Registrations</th>
<th>Video Calls</th>
<th>Audio Only Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large OVA</td>
<td>5,000</td>
<td>500</td>
<td>1,000</td>
<td>20,000</td>
<td>2,000</td>
<td>4,000</td>
</tr>
<tr>
<td>Medium OVA</td>
<td>2,500</td>
<td>100</td>
<td>200</td>
<td>10,000</td>
<td>400</td>
<td>800</td>
</tr>
<tr>
<td>Small OVA (BE6K)</td>
<td>2,500</td>
<td>100</td>
<td>200</td>
<td>2,500</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>VCS Appliance</td>
<td>2,500</td>
<td>100</td>
<td>200</td>
<td>10,000</td>
<td>400</td>
<td>800</td>
</tr>
</tbody>
</table>

Note: Expressway C&E or VCS-C can be clustered across multiple BE6000s for redundancy purposes, but with no additional scale benefit
Cisco Expressway Licensing

CUCM 9.1.2 or higher

Expressway C

Expressway E

Internet

Fixed and Mobile Users at no additional cost

- Mobile and Fixed Endpoint registration
- IM & Presence
- Video and Audio Media Sessions
- Includes Virtual Edition Expressway Server Software
  - No Cost with CUCM 9.1.2 or later

Business to Business, Jabber Guest, 3rd party interworking – Concurrent Sessions

- Business to Business Video and Audio Media Sessions
- Includes Virtual Edition Expressway Server Software
- Expressway Rich Media Session licenses available a la carte
Expressway Rich Media Session Licenses

- Rich Media Session is the only session license type sold with Expressway (simple!)
- Rich Media Session licenses are consumed for either traversal or non-traversal call types
- A traversal call will require a Rich Media Sessions license on both the Expressway E and Expressway C
- Mobile and Remote Access Feature has no requirements for Rich Media Sessions licenses
- Rich Media Sessions should be purchased for Expressways deployed for
  - B2B Video
  - Jabber Guest
  - 3rd party video interworking
# Expressway License Keys

<table>
<thead>
<tr>
<th>License Description</th>
<th>PID</th>
<th>Expressway C (EXPWY-VE-C-K9)</th>
<th>Expressway E (EXPWY-VE-E-K9)</th>
</tr>
</thead>
<tbody>
<tr>
<td>X8 Release Key</td>
<td>LIC-SW-EXP-K9</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Expressway Series</td>
<td>LIC-EXP-SERIES</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>H323-SIP interworking Gateway</td>
<td>LIC-EXP-GW</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Traversal Server Feature Set</td>
<td>LIC-EXP-E</td>
<td>N/A</td>
<td>Included</td>
</tr>
<tr>
<td>Advanced Networking Option</td>
<td>LIC-EXP-AN</td>
<td>N/A</td>
<td>Included</td>
</tr>
<tr>
<td>TURN Relay Option</td>
<td>LIC-EXP-TURN</td>
<td>N/A</td>
<td>Included</td>
</tr>
<tr>
<td>Expressway Rich Media Session</td>
<td>LIC-EXP-RMS</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Microsoft Interoperability Option</td>
<td>LIC-EXP-MSFT</td>
<td>Optional</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Expressway: Unified CM Calls

- Calls from endpoints using the Mobile and Remote Access feature are classified as **Unified CM calls**.

- Unified CM calls do not consume Rich Media Sessions (Expressway) or Traversal Licenses (VCS).

- But Unified CM Calls do count against the overall system capacity.

<table>
<thead>
<tr>
<th>Resource usage (last updated: 21:08:20 PST)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM calls</td>
<td>Current video</td>
</tr>
<tr>
<td></td>
<td>Current audio (SIP)</td>
</tr>
<tr>
<td></td>
<td>Peak video</td>
</tr>
<tr>
<td></td>
<td>Peak audio (SIP)</td>
</tr>
<tr>
<td>Rich media session traversal calls</td>
<td>Current video</td>
</tr>
<tr>
<td></td>
<td>Current audio (SIP)</td>
</tr>
<tr>
<td></td>
<td>Peak video</td>
</tr>
<tr>
<td></td>
<td>Peak audio (SIP)</td>
</tr>
<tr>
<td>Rich media session non-traversal calls</td>
<td>Current</td>
</tr>
<tr>
<td></td>
<td>Peak</td>
</tr>
<tr>
<td>Monitored resource usage</td>
<td>Current</td>
</tr>
<tr>
<td>Rich media sessions</td>
<td>License usage current</td>
</tr>
<tr>
<td></td>
<td>License usage peak</td>
</tr>
</tbody>
</table>
Flexible Call Licensing

- X8.1 introduces audio-only classification for SIP traversal or Unified CM calls
- Calls with only one m= line in the SDP will be classified as Audio calls
- 1 Expressway Rich Media Session license allows either 1 video call or 2 audio-only SIP calls
- 1 VCS Traversal license allows either 1 video call or 2 audio-only SIP calls
- Example:
  - 100 VCS Traversal licenses allows for
  - 90 video and 20 audio-only simultaneous calls

```
Session-Expires: 1800
Allow-Events: dialog Recv-Info: x-cisco-conference
Content-Type: application/sdp
Content-Length: 237
v=0
o=tandberg 7 3 IN IP4 182.16.1.115
s=-
c=IN IP4 182.16.1.115
b=AS:64
t=0 0
m=audio 2336 RTP/AVP 8 0 101
b=TIAS:64000
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```
Direct Peering Model – B2B Communications

The relationship (trunk) between the companies is configured using the domain of the peer, i.e. calls to *@peerdomain.com will be routed over the trunk to the peer VCS Expressway.

Dialing Joe.Shmoe@peerdomain.com will route across the trunk

Enterprise A
Exp-C
Exp-E
Enterprise B
VCS-C
VCS-E
VCS-C
DNS
Internet
SIP
H.323
SIP and H.323
Media
Dual Profile
Enterprise C
Exp-C
Exp-E
## Expressway Series Roadmap

### X7.2 (Shipping)

**Edge Features:**
- SRTP-to-RTP Conversion
- Enhanced certificate management
- Access Control Lists
- Controlled TLS
- Scale (AES-NI support)

**Available Now Remote and Mobile Collaboration:**
- Simple, secure, scalable collaboration
- Connect remotely with Jabber and TC endpoints
- Register directly to CUCM 9.1.2 (or better)
- Voice, Video, IM&P, Directory, Visual Voicemail outside the network without a VPN
- AVC-SVC gateway: Lync 2013 Interop

### 1HCY14 (to be committed)

**Remote and Mobile Collaboration:**
- Additional endpoint support: DX Series
- Enhanced Mobility Support incl. DVO
- Single Sign-On Support
- Media Path Optimisation (ICE)
- Inter-domain XMPP Federation
- Inter-company AVC-SVC gateway

### 2HCY14 (under investigation)

**Remote and Mobile Collaboration:**
- Streamlined provisioning, management, and alarm handling
- Granular Policy Control
- RDP interop

---

© 2013 Cisco and/or its affiliates. All rights reserved.
Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com
Unsupported Features

• CTI phone control
• CAPF client certificate provisioning
• Jabber file transfer (supported only in hybrid IM&P deployment)
• Jabber Mobile features include DVO-R, GSM handoff, session persistency
• TC Endpoint OBTP
• TC Endpoint management (SNMP, SSH/HTTP access)
• Media Path Optimisation (ICE)
Cisco recommends Enhanced Directory Integration for deployments of Jabber for Windows

Recommendation is in order to ensure scalability of the solution for our Enterprise customers.

Existing Jabber 9.2 UDS deployments will continue to receive TAC support
  • Jabber 9.6 will only use UDS in edge mode

9.2 UDS deployments should not exceed 200 users per cluster.

Additional UDS capacity will be available in upcoming Jabber and CUCM releases
  • Batch API
  • Distributed Caching Refresh
Directory Search in 9.6/9.7

- LDAP directory integration to be used in on premise mode
- UDS integration to be used in edge mode [for on-premise deployments]
- WebEx Messenger directory search to be used in cloud mode
HTML Tabs White List

- HTML Tabs are supported through Collaboration Edge
- Create whitelist on Expressway-C
  - Specify host
What to Whitelist?

- Visual Voicemail
- Directory Photo Host
- Jabber Update Server
- HTML Tabs
- HTML Tab Icons
- Webmail
Reverse Proxy Usage

Initial get_edge_config and internal SRV record request (decrypted)

GET /dWNkZW1vbGFiLmNvbQ/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin HTTP/1.1
Authorization: Basic bWR1ZGU6Ghpc3Bhc3N3ZHdpbGxiZXJlc2V0
Host: collabedge1e.ucdemolab.com:8443
Accept: */*
User-Agent: Jabber-Win-472

Base64 encoded credentials

Base64 decode = ucdemolab.com

Initial get_edge_config and internal SRV record request (decrypted)

GET /dWNkZW1vbGFiLmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0NDM/cucm-uds/clusterUser?username=mdude HTTP/1.1
Host: collabedge1e.ucdemolab.com:8443
Accept: */*
Cookie: X-Auth=7f501814-e61f-483a-8620-ed0b5d3792db
User-Agent: Jabber-Win-472

Base64 decode = ucdemolab.com/https/cucm-pub.ucdemolab.com/8443

Subsequent home cluster discovery request (decrypted)

Not a general purpose reverse proxy, intended for Cisco clients only!
Home Cluster Discovery

- Expressway C will use the following UDS API to determine a user’s home cluster
  https://<CUCM>/cucm-uds/clusterUser?username=<USERNAME>

  - `<result version="10.0.1" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/user/mjackson" found="true"/>
    - `<homeCluster>cucm2-1.eft.cisco.com</homeCluster>`
  - `</clusterUser>`

- `<clusterUser version="10.0.1" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/clusterUser?username=mjackson">`
  - `<result found="true" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/user/mjackson" version="10.0.1">`
    - `<homeCluster serversUri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/servers">cucm2-1.eft.cisco.com</homeCluster>`
    - `<selfProvisioningSecureMode>true</selfProvisioningSecureMode>
    - `<adminProvisionMode>false</adminProvisionMode>`
  - `</clusterUser>`
Expressway Server Certificates
Expressway Server Certificates

- Expressway E Server certificates should be signed by 3rd party Public CA
- Expressway C server certificates can be signed by 3rd party Public CA or Enterprise CA
- Expressway server certificates need to allow for both client & server authentication
  - Public CA signed certificates allow Jabber clients and endpoints to validate the server certificate without a CTL
  - Jabber clients with a CTL will not use the CTL to validate Expressway certificate - no requirement to include Expressway certs in CTL
- No support for wildcard certificates
- Don’t upload stacked certificates, separate signed server cert from CA chain
Expressway Certs and Clustering

- Set a cluster name (System > Clustering) even when starting with a single node
- Generate server certificate CSR with Common Name set to “FQDN of VCS Cluster”

<table>
<thead>
<tr>
<th>Status</th>
<th>System</th>
<th>Configuration</th>
<th>Applications</th>
<th>Users</th>
<th>Maintenance</th>
</tr>
</thead>
</table>

Generate CSR

- Common name
  - Common name
  - Common name as it will appear

- FQDN of VCS cluster
  - cluster.collabedge1.ucdemolab.com

- Build Expressway E Traversal Server zone with the “TLS verify subject name” set to “Cluster FQDN”

- TLS verify mode
  - On
- TLS verify subject name
  - cluster.collabedge1.ucdemolab.com
Expressway Certificate Signing Request (CSR)

Maintenance > Security Certificates > Server Certificate

Click Generate CSR to load this page ---->
Cert Subject Alternative Name (SAN) Requirements

- Customer’s primary domain required to be included as a DNS SAN in all Expressway E server certificates
- Primary domain as in example.com or cisco.com or
- This domain is used for SRV lookups and extracted from here
- This is a security measure that allows clients to verify connections to edge servers authoritative for their domain (RFC 6125)
- Similar usage exists with CUCM IM&P XMPP certificates

DNS X509v3 Subject Alternative Name: DNS:ucdemolab.com
CUCM Mixed Mode & Expressway SANs

- Expressway C Server Certificate Generation CSR page will also include the option to include CUCM security profile names as additional SANs

  DNS X509v3 Subject Alternative Name: DNS:secure.ex90.ucdemolab.com

- This is **only required in deployments that include encrypted security profiles** (requires CUCM to be in mixed mode with CTL deployed)

- The Expressway C server certificate will be presented to CUCM during the TLS handshake on behalf of remote endpoints with encrypted security profiles

- UCM needs to find a match between the Expressway certificate’s CN or SAN and the phone security profile name to authorise the TLS registration on TCP 5061

- CUCM phone security profile names cannot be shared across device types
Optional SANs for Future Usage

- The Expressway Server Certificate Generate CSR page will also insert "chat node aliases" as SANs.
- These specific SANS will allow for TLS XMPP federation.

There will be 1 chat node alias per deployed CUCM IM&P server.

Expressway XMPP federation is still a roadmap feature, but this inclusion will potentially save customers from having to get new certificates signed in the future when deploying XMPP federation.
Expressway Trusted CA Certificates

- Trusted CA certificates can now be viewed in either a decoded human-readable format, or in base64 encoded PEM format
- X8.1 release will **not** include the default trusted CA certificate list
- VCS customers upgrading from X7 or prior should consider purging this list

<table>
<thead>
<tr>
<th>Trusted CA certificate</th>
<th>Type</th>
<th>Issuer</th>
<th>Subject</th>
<th>Expiration date</th>
<th>Validity</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>O=Cisco Systems, CN=DST Root CA X3</td>
<td>Matches Issuer</td>
<td>Oct 22 2015</td>
<td>Valid</td>
<td>View (decoded)</td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td>O=Cisco, OU=CTG-TME, CN=硬件实验室</td>
<td>Matches Issuer</td>
<td>Jul 18 2016</td>
<td>Valid</td>
<td>View (decoded)</td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td>O=Digital Signature Trust Co., CN=DST Root CA X3</td>
<td>Matches Issuer</td>
<td>Sep 30 2021</td>
<td>Valid</td>
<td>View (decoded)</td>
<td></td>
</tr>
</tbody>
</table>

**Upload**

Select the file containing trusted CA certificates

**Append CA certificate** | **Reset to default CA certificate**

© 2014 Cisco and/or its affiliates. All rights reserved.
# Expressway Trusted CA Certificates

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Expressway C</th>
<th>Expressway E</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public CA cert chain used to sign Expressway E certificate</td>
<td>✔️</td>
<td>✔️</td>
<td>Required to establish Traversal Zone connections</td>
</tr>
<tr>
<td>Public or Enterprise CA cert chain used to sign Expressway C certificate</td>
<td>✔️</td>
<td>✔️</td>
<td>Required to establish Traversal Zone connections</td>
</tr>
<tr>
<td>CUCM Tomcat certificates or CA chain</td>
<td>✔️</td>
<td>✗</td>
<td>Only required when Expressway C configured to use TLS Verify mode on Unified CM discovery</td>
</tr>
<tr>
<td>CUCM CallManager certificates or CA chain</td>
<td>✔️</td>
<td>✗</td>
<td>Only required when CUCM is in mixed mode for end to end TLS</td>
</tr>
<tr>
<td>CUCM IM&amp;P Tomcat certificates or CA chain</td>
<td>✔️</td>
<td>✗</td>
<td>Only required when Expressway C configured to use TLS Verify mode on IM&amp;P discovery</td>
</tr>
<tr>
<td>CUCM CAPF certificate(s)</td>
<td>✗</td>
<td>✔️</td>
<td>Only required when remote endpoints authenticate with LSC certificate</td>
</tr>
</tbody>
</table>
Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.
- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com