Enabling External Collaboration and Federation with Expressway

Kevin Roarty, Technical Marketing Engineer
Cisco Collaboration
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKUCC-2801
Agenda

• Expressway Solution Overview including services, compute platforms, licensing, and scale

• Mobile & Remote Access including infrastructure and endpoint feature updates and deployment guidance

• Federation with Expressway
  • Cisco Jabber IM&P Federation
  • Open Video Federation & Skype for Business Interop
  • Cisco Meeting Server WebRTC

• Q & A

• Demo
Solution Overview
The Collaboration Landscape
Enabling Connection of Any Users to Any Services Through Any Network

Users in Headquarters

Mobile and Remote Workers

Suppliers, Partners, and Customers (B2B)

Public/Consumers

Users in Branch Offices

Private WAN

Public Internet

PSTN and IP PSTN

IM and Presence

Content and Data

Social

Voice

Video
Cisco’s Collaboration Edge Architecture and Portfolio
Delivering the Industry’s Most Comprehensive Any-to-Any Collaboration

Performing:
• Firewall traversal
• Session border control (SBC)
• Gateway services
• Mobile and remote worker access
• Cloud connectivity services
• Branch and cloud telephony survivability

Includes the following Cisco products:
• Cisco Expressway
• Cisco TelePresence® Video Communication Server (VCS)
• Cisco Unified Border Element (CUBE)
• Cisco Unified SIP Proxy (CUSP)
• Cisco time-division multiplexing (TDM) and analog gateways
Product Line Options

VCS

- “VCS Control” No Change
- “VCS Expressway” No Change

- Designed for video-centric customer deployments
- Stand-alone licensing model requiring base server and session licenses
- No recent changes to licensing model

Expressway

- “Expressway-C” Or Core
- “Expressway-E” Or Edge

- Included in Cisco UCL, CUWL, Spark Flex licensing schemes
- $0 server software licenses
- X8.9 includes feature updates to service video-centric customer deployments (w/o CUCM)
Expressway Local Registration Support

• Expressway (X8.9+) is now able to register endpoints directly (without CUCM)
• Registrations are enabled using the same top level licenses as used on CUCM
• Expressway C services all registrations (SIP and H.323)
• Expressway E must proxy SIP registrations to Expressway C
• UCL Enhanced License enables SIP Desktop Endpoints (DX70/80, EX60/90)
• TelePresence Room License enables Cisco room systems and 3rd party endpoints, or any other “system” that registers to Expressway
## Cisco Expressway and VCS Feature Comparison

<table>
<thead>
<tr>
<th>Features / Services</th>
<th>Cisco Expressway</th>
<th>Cisco VCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile and Remote Access</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Business to Business Video (including MSFT Video Federation)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Consumer to Business with Jabber Guest</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Cisco Meeting Server WebRTC (Proxy &amp; TURN)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video Interworking (H.323-SIP, IPv4 to IPv6, MSFT Interop)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video / TelePresence Endpoint Registration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Cisco Spark Hybrid Service Connectors</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>WebEx Collaboration Meeting Room (CMR) Cloud/Hybrid</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>XMPP IM &amp; Presence Federation</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SIP IM &amp; Presence Federation with Skype for Business</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
How Expressway Firewall Traversal Works

1. Expressway-E is the traversal server installed in DMZ. Expressway-C is the traversal client installed inside the enterprise network.

2. Expressway-C connects via the firewall to a specific port on Expressway-E with secure login credentials.

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

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

5. Expressway C then initiates connection through CUCM to the endpoint

6. The call is established and media traverses the firewall securely
Expanded Firewall Traversal Capabilities

• The X8 software delivers 3 key capabilities enabling Expressway use cases beyond just video
• Option to proxy remote SIP registrations to Unified CM
• XCP Router for XMPP traffic
• HTTPS Reverse proxy
Compute Platforms, Licensing & Scale
Expressway X8.8+ Licensing

**Business to Business Calls**
- Firewall Traversal Calls consume 1 x RMS on Expressway E (includes MSFT B2B calls)

**Consumer to Business Calls**
- Jabber Guest Calls consume 1 x RMS on Expressway E

**Interoperability Gateway Calls**
- i.e. intradomain MSFT interop calls, consume 1 x RMS on Expressway C Gateway

**Registered Calls (no RMS required)**
- Calls between endpoints registered to Cisco Call control services
- Calls to Cisco conferencing infrastructure or cloud services
- Cisco Meeting Server WebRTC
Expressway License & Resource Usage

- Calls from MRA endpoints or endpoints registered locally to Expressway are classified as Registered calls.

- Calls to/from WebEx or Spark clouds are classified as CMR Cloud calls.

- “Registered” & “Cloud” calls do not consume Rich Media Session licenses, but do count against the overall system capacity.
Compute Platform Options

Specs Based
Virtual Machine Support

<table>
<thead>
<tr>
<th>OVA Size</th>
<th>vCPU</th>
<th>Reserved RAM</th>
<th>Disk Space</th>
<th>NIC(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 3.2 GHz</td>
<td>8GB</td>
<td>132GB</td>
<td>1Gb</td>
</tr>
</tbody>
</table>

Appliance Support

CE 1100

- New appliance based on UCS C220 M4
- Bare metal – no hypervisor
- Solution for customers with security policies that do not allow VMware in the DMZ

Expressway Appliance SKUs
- EXPWY-C-BDL-K9
- EXPWY-E-BDL-K9

VCS Appliance SKUs
- VCS-C-BDL-K9
- VCS-E-BDL-K9
# Expressway X8 Scalability

<table>
<thead>
<tr>
<th>Platform</th>
<th>Server</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Registrations</td>
<td>Video Calls</td>
</tr>
<tr>
<td>Large OVA, CE1100</td>
<td>2,500</td>
<td>500</td>
</tr>
<tr>
<td>Medium OVA</td>
<td>2,500</td>
<td>100</td>
</tr>
<tr>
<td>Small OVA (BE6000)</td>
<td>2,500</td>
<td>100</td>
</tr>
</tbody>
</table>

New

X8.10 release allows for large scale capacity on Large OVA and CE1100 with only 1Gbps NIC.
Expressway Clustering, 4+2

- Cluster up to 6 Expressways for scale and redundancy
- Clustering latency up to 80ms RTT
- Expressway E and C node types cannot be mixed in the same cluster
- Deploy equal number of peers in Expressway C and E clusters (this applies to most Expressway deployments but is not critical if Expressway is handling local registrations)
- Deploy same OVA sizes or appliances throughout cluster
- Customers can deploy multiple clusters for the same domain
TLS Cipher & Minimum Version control in X8.10

- Prepare for successful PCI compliance audits!
- SIP TLS ciphers configurable from X8.6 (CLI only)
- SIP TLS version configurable from X8.8 (CLI only)
- X8.10 allows control of all TLS server interfaces, now including HTTPS and XMPP
- Allows admin to disable TLS 1.0 and 1.1
- New installs default to TLS 1.2 only
Mobile & Remote Access (MRA)
Mobile and Remote Access
with Cisco Expressway

Collab Services

UCM 9.x/10.x/11.x

Expressway-C

Expressway-E

Internal Network

DMZ

External Network

Internet

Jabber @ work

Jabber @ the café

Jabber @ Home

Jabber @ SFO, DEN or ORD

Fixed Remote Endpoints

Internet

External Network

DMZ

Internal Network

Collab Services

UCM 9.x/10.x/11.x

Expressway-C

Expressway-E
Fixed Endpoint Support
Available Today

- DX650, DX70, DX80
- MX, SX, EX, C Series
- TelePresence Endpoints
- Spark Room 55, Spark Room 70, Spark Room Kit, Spark Room Kit Plus

- 7811, 7821, 7841, 7861
- 8811, 8841, 8845, 8851, 8861, 8865
Jabber allows for a secondary domain to be used for edge service discovery. The “VoiceServicesDomain” can be provided in jabber-config.xml from TFTP or Messenger cloud, or bootstrapped into client via MSI or ciscojabber://URL provisioning.
Split DNS SRV Record Requirements

- **collab-edge** record needs to be available in **public** DNS
- Multiple SRV records (and Expressway-E hosts) should be deployed for clusters
- 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 to be available **only** in **internal** DNS

```
_cisco-uds._tcp.example.com. SRV 10 10 8443 ucm1.example.com.
_cisco-uds._tcp.example.com. SRV 10 10 8443 ucm2.example.com.
```
Protocol Workload Summary

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Security</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP</td>
<td>TLS</td>
<td>Session Establishment – Register, Invite, etc.</td>
</tr>
<tr>
<td>Media</td>
<td>SRTP</td>
<td>Audio, Video, Content Share</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TLS</td>
<td>Logon, Provisioning/Configuration, Contact Search, Visual Voicemail</td>
</tr>
<tr>
<td>XMPP</td>
<td>TLS</td>
<td>Instant Messaging, Presence</td>
</tr>
</tbody>
</table>
Hybrid Deployment - Cloud based IM&P

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

Collaboration Services
Unified CM
Expressway C
Expressway E

Internet

Protocol  Security  Service
SIP  TLS  Session Establishment – Register, Invite, etc.
Media  SRTP  Audio, Video, Content Share
HTTPS  TLS  Logon, Provisioning/Configuration, Contact Search, Visual Voicemail
XMPP  TLS  Instant Messaging, Presence

Unity Connection
Conferencing Resources
UDS Directory Search

• All Jabber clients connecting via Expressway will use UDS for directory search (assuming Unified CM IM&P deployment)

• TelePresence endpoints, DX series, IP Phones also use UDS directory search

• For the best contact search experience, all Enterprise Users should be imported into every Unified CM cluster’s end user table

• Home cluster check box needs to be selected on only one cluster for each user

• Unified CM clusters support 80K end users, and can scale as high as 160K with BU approval
Media Path Summary

Media Traversal

- Call between “C” and “A” on-premise
- Expressway provides firewall traversal for signaling & media
- Expressway-C de-multiplexes media and forwards toward “A”
- Media stream always SRTP encrypted between “C” and Expressway-C
- Media stream only SRTP encrypted between “A” and Expressway-C when both endpoints are provisioned with encrypted security profile (requires UCM mixed mode)

Media Relay

- Call between “C” and “B” both off-premises
- Media is relayed via Expressway-C
- All Media streams SRTP encrypted
# Mobile & Remote Access Deployment Options

<table>
<thead>
<tr>
<th>Unified CM 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 Unified CM cluster</td>
</tr>
<tr>
<td>1</td>
<td>2+</td>
<td>2+</td>
<td>Regional Expressway deployments providing remote access to a central Unified CM cluster</td>
</tr>
<tr>
<td>2+</td>
<td>1</td>
<td>1</td>
<td>Single Expressway deployment providing remote access to a multiple Unified CM clusters</td>
</tr>
<tr>
<td>2+</td>
<td>2+</td>
<td>2+</td>
<td>Regional Expressway deployments providing remote access to multiple Unified CM Clusters</td>
</tr>
</tbody>
</table>
Supporting Multiple Unified CM Clusters

Prerequisites

- Cross cluster UDS API calls are used to find a Jabber user’s home cluster
- Establishing an Intercluster Lookup Service (ILS) network between Unified CM clusters is the easiest way to allow Unified CMs to discover one another and get home cluster discovery working
- SIP URI replication over ILS is optional, not a requirement
- Test this yourself within a browser, substitute in UCM addresses and username(s) specific to your deployment

https://UCM/cucm-uds/clusterUser?username=mdude

- Confirm the username lookup results always redirect to the same home UCM cluster, no matter which UCM cluster you send the lookup request to
Designing for Multiple Expressway Clusters

Two approaches for deploying Expressway MRA at scale

Global approach - single domain (example.com) used for collab-edge DNS SRV records

- allows all MRA clients to find any edge
- Requires all Expressway C clusters to be integrated with all CUCM + IM&P clusters
- Geo DNS load balancing can be used to help prioritize local edge resources, see Cisco Preferred Architecture Enterprise CVD for more details

Segmented approach - subdomains (amer.example.com, emea.example.com, apac.example.com) used for collab-edge DNS SRV records

- Allows for better capacity planning and control
- Limits the CUCM + IM&P clusters that Expressway C needs to be integrated with
- Bootstrapping service domain can be more challenging, and less obvious to end users
MRA Client Authentication Options

SAML SSO is an option for Jabber clients providing
• The potential for stronger client authentication, dictated by Identity Provider’s capabilities
• Alignment with the broader enterprise authentication strategy
• Expressway “SSO Exclusive” configuration option removes non-SSO MRA authentication option

Non-SSO authentication (username + password) applies to all other MRA clients including
• TelePresence Endpoints with TC or CE firmware
• 78xx and 88xx Cisco IP Phones
• Jabber clients when SSO is not enabled
• No option today to enforce mutual TLS for MRA client authentication
New OAuth 2.0 Support in X8.10

- OAuth 2.0 is used for token based authorization with existing MRA SSO support
- X8.10 introduces a new OAuth option for Jabber clients that applies to both SSO and non-SSO deployments
- New OAuth support includes both access tokens and a refresh token
- The refresh token reduces user authentication frequency and provides faster reconnect to services

Additional Resources

- New white paper on deploying OAuth
Expressway MRA Access Control Menu

- Authentication Path selection dictates which options are available below.
- New OAuth with Refresh option (does not require SSO).
- Only applies to SAML SSO (implicit OAuth login flow).
- Required for any non-Jabber MRA clients, or Jabber clients without SSO or OAuth with Refresh.

New in X8.10
## Jabber OAuth with Refresh Token Support

### Minimum 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>X8.10.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>11.5(1) SU3</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM IM&amp;P</td>
<td>11.5(1) SU3</td>
<td>Available</td>
</tr>
<tr>
<td>Unity Connection</td>
<td>11.5(1) SU3</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Windows</td>
<td>11.9</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for iPhone and iPad</td>
<td>11.9</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Mac</td>
<td>11.9</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Android</td>
<td>11.9</td>
<td>Available</td>
</tr>
</tbody>
</table>
UCM 12.0 User Based MRA policy

- MRA End User Policy in UCM 12.0(1) - User Profile Configuration
  - Allows admin to selectively disable MRA for user or groups of users
  - Policy can also be used to restrict MRA users from voice/video calling services
  - Requires 100% Jabber 12.0+ client population
  - Expressway Access Control should be set to only allow “Authorize by OAuth token with Refresh”
Edge Server Authentication

- Edge 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
- Cisco Endpoints will rely on a trusted CA list included in firmware
- No CTL option or requirement for Edge Server certificate authentication
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

X509v3 Extended Key Usage:
- TLS Web Client Authentication
- TLS Web Server Authentication

• Public CA signed certificates allow Jabber clients and endpoints to validate the server certificate without a CTL
• No requirement to include Expressway certs in CTL
• Wildcard certificates not supported
• Don’t upload stacked certificates, separate signed server cert from CA chain
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
  - SIP: TCP 7001
  - Traversal Media: UDP 2776 to 2777 (or 36000 to 36011 for large VM/appliance)
  - XMPP: TCP 7400
  - HTTPS (tunneled over SSH between C and E): TCP 2222

- External firewall needs to allow the following inbound connections to Expressway
  - SIP: TCP 5061
  - HTTPS: TCP 8443
  - XMPP: TCP 5222
  - Media: UDP 36002 to 59999
High Level MRA Deployment Guidance

Start on solid ground
- Jabber service discovery needs to work on-prem
- Start on-prem and then add edge access
- Verify end user home cluster discovery in multi Unified CM cluster deployments

Don’t forget about DNS
- Understand split DNS SRV requirements, get DNS change requests in the queue
- A common DNS domain simplifies matters, but is not required

Review TCP and UDP port requirements with firewall team, and minimize UDP ports open to Expressway-E from internet if required

Verify Expressway CA signed certs
- Confirm SANs returned in CA signed cert match what was requested in the CSR
- Verify cert includes both TLS Web Server & Client Authentication Extended Key Usage
## Initial Jabber & TelePresence MRA Support

### Minimum 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>X8.1.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>9.1(2) SU4</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM 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>Available</td>
</tr>
<tr>
<td>Jabber for iPhone and iPad</td>
<td>9.6.1</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Mac</td>
<td>9.6</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Android</td>
<td>9.6</td>
<td>Available</td>
</tr>
<tr>
<td>EX/MX/SX/C Series TelePresence Endpoints</td>
<td>TC 7.1</td>
<td>Available</td>
</tr>
<tr>
<td>DX70 &amp; DX80</td>
<td>CE 8.2</td>
<td>Available</td>
</tr>
<tr>
<td>Spark Room Kits</td>
<td>CE 9.0</td>
<td>Available</td>
</tr>
</tbody>
</table>
IP Phone Feature Set
7800/8800 Series + Expressway

- Access to corporate directory (UDS)
- Encrypted signaling and media (UCM mixed mode not required)
- Call Forward, Transfer, Ad-hoc & Meetme Conferencing, MWI
- Call Park, Call pickup, iDivert, Call Back, Mobile Connect, Extension Mobility
- Device management including configuration, firmware upgrades, reset/restart/applyConfig
- Multiple line appearances
- Shared line features including Remote in Use, Hold/Resume, Privacy, Barge/cBarge, Merge
MRA Advanced Line Support for IP Phones
Enabling Shared Lines & Multiple Line support

- SIP Path headers setting needs to be enabled to allow advanced line support
- CUCM 11.5(1)SU3 is recommended before enabling SIP Path Headers on Expressway C

- This setting maps to the following auto-generated zone setting
  xConfiguration Zones Zone 3 Neighbor SIP RFC3327 Enabled: "Yes"
# IP Phone MRA Support

## Minimum 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>X8.7</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>10.5(2) SU2</td>
<td>Available</td>
</tr>
<tr>
<td>7811, 7821, 7841, 7861 IP Phones</td>
<td>11.0</td>
<td>Available</td>
</tr>
<tr>
<td>8811, 8841, 8845, 8851, 8861, 8865 IP Phones</td>
<td>11.0</td>
<td>Available</td>
</tr>
<tr>
<td>DX650, DX70, DX80 Collaboration Endpoints</td>
<td>10.2(4) SR</td>
<td>Available</td>
</tr>
</tbody>
</table>

**Software requirements for multiple lines and shared line features**

<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>X8.9.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>11.5(1) SU3</td>
<td>Available</td>
</tr>
<tr>
<td>7811, 7821, 7841, 7861 IP Phones</td>
<td>11.5 SR1</td>
<td>Available</td>
</tr>
<tr>
<td>8811, 8841, 8845, 8851, 8861, 8865 IP Phones</td>
<td>11.5 SR1</td>
<td>Available</td>
</tr>
</tbody>
</table>
MRA Built-in Bridge (BiB) Recording
Now in Feature Preview with X8.10.2+

![Diagram of network components including UCM, Expressway-C, Expressway-E, Recording Server, PSTN, and SIP signaling]
MRA Built-in Bridge (BiB) Recording

- Allows customers to extend their existing voice recording solution to devices connecting via Expressway Mobile & Remote Access
- This has been in field trial with customers and call recording vendors for the past several months
- What we’ve learned so far includes…
- Voice recording over MRA works as expected for Jabber and IP Phones!
- Some recording servers use UCM’s CTI interface for selective recording, and to correlate users with recordings – CTI monitoring support is not supported with Jabber iOS and Android devices yet
- All Jabber clients lack support for injecting & mixing of notification tones
Forward Proxy for Apple Push Notification

Expressway provides an optional proxy for Jabber iOS APNs

- Voice Push (HTTPS)
- IM/Chat Push (HTTPS)
Expressway Forward Proxy for Apple Push Notification

Design Considerations

• Expressway-C Forward Proxy listens on TCP 8445 (non-configurable)
• Forward Proxy requires an Expressway C & E pair
• Configure UCM with a proxy address that includes either
  A. Expressway-C FQDN
  B. Expressway-C Cluster FQDN (allows for failover and forward proxy usage across Expressway cluster)
• UCM will verify the FQDN (or IP address) configured as the proxy address is included in the Expressway-C certificate
• Expressway-C CA cert needs to be include in UCM’s Tomcat-trust
• Cisco Cloud Service CA certs only need to be trusted on UCM (Tomcat-trust)
Expressway Forward Proxy for Apple Push Notification

Security Considerations

• Expressway is NOT providing an open forward proxy!!!

• Mutual TLS authentication is required - Client certificates must be signed by a (Expressway-C) trusted CA

• HTTP Proxy destinations are hardcoded, and the list cannot be extended by admin
# Jabber iOS APNs Support

## Minimum Software Requirements

### IM/Chat APNs support

<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Expressway (or Cisco VCS)</td>
<td>X8.9.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM &amp; IM&amp;P</td>
<td>11.5(1) SU2</td>
<td>Available</td>
</tr>
<tr>
<td>Cisco Jabber for iPhone and iPad</td>
<td>11.8 MR</td>
<td>Available</td>
</tr>
</tbody>
</table>

### Voice APNs support

<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Expressway (or Cisco VCS)</td>
<td>X8.10.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>11.5(1) SU3</td>
<td>Available</td>
</tr>
<tr>
<td>Cisco Jabber for iPhone and iPad</td>
<td>11.9</td>
<td>Available</td>
</tr>
</tbody>
</table>

### Expressway Forward Proxy APNs support

<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Expressway (or Cisco VCS)</td>
<td>X8.10.2</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM &amp; IM&amp;P</td>
<td>11.5(1) SU4 12.5(1)</td>
<td>Targeting Feb 2018 Targeting 2H CY18</td>
</tr>
</tbody>
</table>

Jabber iOS customers should plan to migrate to APNs before June 2018.
Cisco Jabber IM&P Federation
Jabber IM&P Federation with Expressway
Now extending to organizations using Microsoft

- Internal Network
- DMZ
- External Network
- Internet
- Microsoft ® Office 365
- Organizations with Skype™ for Business on premises
- WebEx Messenger Cloud
- Organizations with Cisco Collab
- Standards based XMPP service
- XMPP
- SIP
IM&P Interdomain Federation with Skype for Business

Overview

• Expressway provides an alternative to the Cisco ASA TLS Proxy for interdomain SIP federation

• Expressway alone can be used for SIP IM&P only interdomain federation with organizations using Skype for Business (additional requirements for audio and video calling)

• SIP IM&P federation requires a named federated domain entry on IM&P server, in contrast to the open federation capabilities when using XMPP

• No RMS licenses required for SIP IM&P only sessions

• Including federated contact in buddy list will allow for the best presence experience
IM&P Interdomain Federation with Skype for Business

Design Considerations

• Publish _sipfederationtls._tcp.example.com DNS SRV record(s) in public DNS to make your Expressway E(s) known to business partners

• Expressway E should have a public CA signed cert, and will need to trust root CA certificates used by federated domains

• Trusted TLS peer relationship, including a neighbor zone to IM&P on Expressway C is required

• Expressway search rules are required to handle chat invites and presence subscriptions

• Each federated domain needs to be administratively defined on IM&P server, including a next hop destination matching Expressway C

• Configuration details in chapter 8 of the IM&P Interdomain Federation Guide Release 11.5(1)SU2 and the Expressway guide
## SIP IM&P Microsoft Federation Support

Minimum 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>X8.9.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>11.5(1)SU2</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM IM&amp;P</td>
<td>11.5(1)SU2</td>
<td>Available</td>
</tr>
</tbody>
</table>
Open Video Federation + Skype for Business Video Interop
Open Video Federation
Enabling business to cloud or B2B video

Cisco Collaboration Cloud
Organizations with Cisco Collab
Standards based SIP/H.323 Video

Internal Network
DMZ
External Network

UCM
Expressway-C
Expressway-E
Open Video Federation

Easy as a phone call or sending an email

- Enables Business to Business Video Calling, inbound and/or outbound
- No requirement for predefined peering relationship
- Provides Business to Cloud Video Calling, i.e. WebEx CMR cloud
- Multivendor interoperability through industry standards (SIP, H.323)
- Dial Plan and Call Policy Rules dictate how open video federation truly is
Expanded Open Video Federation
CMS allows for video interoperability with organizations using Microsoft

- Organizations with Skype™ for Business on premises
- Cisco Collaboration Cloud
- Organizations with Cisco Collab
- Standards based SIP/H.323 Video

Diagram:
- Internal Network
- DMZ
- Expressway-C
- Expressway-E
- Cisco Meeting Server
- Internet
Federated Video Interop with Skype for Business

Overview

- Expressway provides a fully supported alternative to the Cisco Meeting Server SIP Edge component for interdomain SIP video federation
- Cisco Meeting Server allows video interoperability with both Office 365 (cloud) and organizations with on-premises Skype for Business infrastructure
- BFCP ↔ RDP bidirectional content share
- Allows Jabber clients to escalate chat session to A/V calls (requires IM&P)
- Open video federation model is possible, in contrast to IM&P named federation requirements
- Compatible with CUCM, Expressway, and VCS based call control
- RMS license + Cisco Meeting Server licensing required for audio/video/content call with federated Skype for Business contacts
Federated Video Interop with Skype for Business

Design Considerations

• Publish _sipfederationtls._tcp.example.com DNS SRV record(s) in public DNS to make your Expressway E(s) known to business partners

• Expressway E should have a public CA signed cert and will need to trust root CA certificates used by federated domains

• Expressway C dial plan will route inbound point to point MS SIP audio/video calls through CMS in gateway mode and then route to CUCM or local endpoints

• Expressway C dial plan routes outbound video calls to Expressway E first, and if no SIP or H.323 SRV records are found by the DNS zone, Expressway C will try routing the call through CMS and then route to Expressway E where the DNS zone will look for _sipfederationtls SRV records

• Configuration details outlined in the Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure (Expressway X8.9.2) guide
Skype for Business Video Federation Support
Minimum 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>X8.9</td>
<td>Available</td>
</tr>
<tr>
<td>Cisco Meeting Server</td>
<td>2.1.2</td>
<td>Available</td>
</tr>
</tbody>
</table>


Cisco Meeting Server
WebRTC via Expressway
WebRTC Access to Cisco Meeting Server Spaces
Expressway + CMS WebRTC

Overview

- Expressway E&C pair provides firewall traversal for WebRTC clients, including https reverse proxy & TURN server
- Does not replace Web Bridge! The CMS Web Bridge, Call Bridge, XMPP, and database components are all required
- Allows for guest access to Cisco Meeting Server spaces, end user access (with login) too
- No RMS license required for CMS WebRTC calls
- Bidirectional content (chrome extension required when sharing from WebRTC side)
Expressway WebRTC Proxy

DNS & Certificate Considerations

• Choose meaningful FQDN for WebRTC access and configure this FQDN as “guest account client URI” on both CMS and Expressway, and in CMS as the Web Bridge URI

• Split DNS A records allows easy internal & external WebRTC access
  • Externally the FQDN name resolves to Expressway E public IP address
  • Internally FQDN name resolves to CMS (Web Bridge)

• Include the FQDN in Expressway E and CMS Web Bridge certificate as SAN
Expressway WebRTC Proxy

Opening HTTPS port and protecting admin web interfaces

- External firewall needs to allow TCP 443 and 80 from internet (TCP 80 is optional, and only used to redirect end users to TCP 443)

- Move the Expressway web admin listening port off TCP 443 to TCP 7443, 445, or 9000

- External firewall should block Expressway E web admin TCP port from internet

- CMS web admin should also be configured to listen on non-standard HTTPS port, i.e. TCP 7443 (webadmin listen a 7443)

- Admins: don’t forget to update your web admin browser bookmark(s) to include the non-standard HTTPS port!
TURN Server Configuration
Dual NIC + Static NAT Expressway E

- Add Expressway E TURN server details to CMS via API, do not add via CMS web gui
- Optionally define TURN server with IP address (CMS resolves TURN server DNS A record before sending to clients)
- Expressway E TURN server not required, CMS TURN server is an option

Expressway E LAN2 Static NAT
# Expressway CMS WebRTC Proxy

## Minimum 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>X8.9.2</td>
<td>Available</td>
</tr>
<tr>
<td>Cisco Meeting Server</td>
<td>2.1.4</td>
<td>Available</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>28</td>
<td>Available</td>
</tr>
<tr>
<td>Mozilla Firefox (beta)</td>
<td>25.0.1</td>
<td>Available</td>
</tr>
</tbody>
</table>
Closing Thoughts
Key Takeaways

- Expressway X8.10 includes feature updates to support video-centric customer deployments (w/o CUCM)
- Cisco VCS customers should plan migration to Expressway
- Expressway MRA feature support continues to grow
- Plan your upgrade to UCM 11.5(1)SU3 and Expressway X8.10 to take advantage of new OAuth with Refresh login flows
- Expressway + Cisco Meeting Server supports B2B video interop with organizations using Skype for Business today
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKUCC-2801
Please complete your Online Session Evaluations after each session.

Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt.

All surveys can be completed via the Cisco Live Mobile App or the Communication Stations.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.cisc live.com/global/on-demand-library/.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
• Related sessions
Demo
Thank you
Appendix

A. Expressway MRA Media Traversal
B. Minimize UDP Ports open to Expressway-E
C. Policy Protected Dial Plan for B2B
D. MRA Resources and Troubleshooting
E. Expressway Server Certificates
F. Expressway MRA with SSO
G. XMPP Federation
H. Jabber Guest
I. Migration, Trade in, Ordering Info
Appendix A
Expressway MRA Media Traversal
Components of Expressway Media Traversal

Proxy default component used for media traversal

B2BUA component used when media encryption policy other than “auto” is applied

Assent protocol is used for multiplexed media on Traversal server zones (Expressway E only)
Traversing Media Port Range

Admin configures port range on Configuration > Traversal Subzone menu on both Expressway C & E, defaults to 36000 – 59999

Allocated media port range is divided and shared
1st half goes to Proxy
2nd half goes to B2BUA
Assent Traversal Media Ports

Expressway E

DMZ Firewall

Expressway C

Proxy

B2BUA

Assent Demultiplexing Ports

Admin configures port range on Configuration > Traversal > Ports menu on Expressway E only

Defaults to UDP 2776-7

Large VMs, CE1100, CE1000 require 12 demux ports, automatically allocated from the beginning of the traversal media port range, typically UDP 36000 – 36011
Mobile & Remote Access Media Paths

- The UDP port details, expressway components, and encryption attributes are best understood in the following categories:
  - Internal – media path between Expressway-C and on-prem resources
  - Traversal zone – media path between Expressway-C and Expressway-E
  - External – media path between Expressway-E and MRA clients
MRA Internal Media

• Includes the UDP media traffic between Expressway-C and on-prem clients, endpoints, gateways, conference bridges, other Expressways, etc.

• Expressway-C establishes unique UDP ports from B2BUA portion of traversal media port range to send and receive media traffic

• Voice and Video streams will only be SRTP encrypted when all conditions are satisfied
  • UCM is in mixed mode with a CTL established
  • The MRA client is configured with an encrypted phone security profile
  • The other end of the call (endpoint, gateway, bridge, etc.) is configured for SRTP
MRA Traversal Zone Media

- Includes the UDP media traffic between Expressway-C & Expressway-E
- Voice and Video streams are always SRTP encrypted
- Expressway-C sources media from B2BUA portion of traversal media port range, always sending to the Assent demultiplexing ports of Expressway-E
- Expressway-E returns media traffic to Expressway-C using the UDP ports established for the opposite flow
- Expressway-E assent demultiplexing ports source UDP media traffic to a destination port within the B2BUA media port range of Expressway-C
MRA External Media

- Includes UDP media traffic over the internet between MRA clients and Expressway-E
- Voice and Video streams are always SRTP encrypted
- The Expressway Proxy component is always used on the Expressway-E
- Media latching is used to handle cases where MRA clients send non-routable IP addresses in SIP SDP (very common over the internet)
- Expressway-E establishes unique UDP ports from the Proxy portion of the traversal media port range for each UDP port requirement in the SDP
- Expressway-E uses the source ip address of media traffic received on the unique UDP port to route media traffic in return
- NAT bindings on the far end allow return media traffic to reach the MRA client
Appendix B
Minimize UDP Ports open to Expressway-E
Minimize UDP Ports Open to Expressway-E

• MRA clients require a different number of UDP ports per call depending on client/endpoint capabilities, configuration, and per call SDP negotiation

• Some video endpoints require >10 unique UDP ports per call, and this may continue to grow

• Jabber in phone only mode, or audio only IP phones will require 2 unique UDP ports per call

• The Expressway docs specify the port requirements, to support max scale (500 simultaneous video calls on large VM) which is 24,000 UDP ports

• Non-large VMs & appliances can be configured with a smaller range

• Expressway-C will always require more media ports than Expressway-E
Mobile & Remote Access Media Traversal

- MRA deployments include predictable UDP media traffic paths
- The B2BUA is always engaged for forced media encryption on the Expressway-C
- The proxy component is always used on the Expressway-E
- Traversal Media Port Range is configured on Configuration > Traversal Subzone menu on both Expressway C & E, defaults to 36000 – 59999
- This media port range is divided and shared
  » 1st half goes to Proxy
  » 2nd half goes to B2BUA
MRA Media Traversal Path

Expressway C
DMZ Firewall
Expressway E
Proxy
B2BUA
Proxy
B2BUA
Enterprise Resources
MRA Media Relay Path
Reduced UDP Port Range For Audio Only MRA

Example 1

- Customer is deploying audio only MRA clients thru Expressway
- Expressways are dedicated to MRA, no B2B video or other services provided
- Standard Expressway VMs are deployed, 300 audio only calls per server is the worst case scenario
- 300 audio only calls equates to 600 unique UDP ports (1 RTP + 1 RTCP per call) that need to be open from the internet to Expressway-E
- **Expressway-E** traversal media port range configured for 1200 ports, 36000 - 37199
  - 36000 - 36599 will be dedicated to the Proxy component (open this range of 600 ports on firewall, for source ANY dest Exp-E)
  - 36600 – 37199 will be dedicated to the B2BUA component (will go unused, no need to open ports)
- Expressway-E Assent traversal port configured with default UDP 2776-7
- **Expressway-C** traversal media port range (default) 36000 - 59999
Reduced UDP Port Range for MRA (Including Video)

Example 2

- Customer is deploying a variety of MRA clients including Jabber, TelePresence codecs, IP phones
- Expressways are dedicated to MRA, no B2B video or other services provided
- Standard Expressway VMs are deployed, 150 video calls per server is the worst case scenario in terms of UDP port requirements
- 150 video calls can be satisfied with 1800 unique UDP ports (assumes no more than 12 UDP ports per call) that need to be open from the internet to Expressway-E
- **Expressway-E** traversal media port range configured for 3600 ports, 36000 - 39599
  - 36000 - 37799 will be dedicated to the Proxy component (open this range of 1800 ports on firewall, for source ANY dest Exp-E)
  - 37800 – 39599 will be dedicated to the B2BUA component (will go unused, no need to open ports)
- Expressway-E Assent traversal port configured with default UDP 2776-7
- **Expressway-C** traversal media port range (default) 36000 - 59999
Reduced UDP Port Range for MRA, Large VM

Example 3

- Customer is deploying a variety of MRA clients including Jabber, TelePresence codecs, IP phones
- Expressways are dedicated to MRA, no B2B video or other services provided
- Large Expressway VMs are deployed, 500 video calls per server is the worst case scenario in terms of UDP port requirements
- 500 video calls can be satisfied with 6000 unique UDP ports (assumes no more than 12 UDP ports per call) that need to be open from the internet to Expressway-E
- **Expressway-E** traversal media port range configured for 12012 ports, 36000 - 48011
  - 36000 – 36011 will be dedicated to Assent demultiplexing
  - 36012 - 42011 will be dedicated to the Proxy component (open this 6000 port range on firewall, source ANY dest Exp-E)
  - 42012 – 48011 will be dedicated to the B2BUA component (these will go unused, no need to open ports)
- **Expressway-C** traversal media port range (default) 36000 - 59999
Appendix C
Policy Protected Dial Plan for B2B
Protect your resources including…

PSTN gateways
conference bridges
voice mail system
from unauthorized access through Expressway
Policy in Layers

Filtering Inbound Unauthenticated Video Federation Traffic

• Filter access to Expressway allowing only required TCP & UDP ports
• Call Policy Rules on Expressway protect against scanners and toll fraud
• SIP Trunk CSS provides fine grain access control to gateways/resources
Example of Unauthorized Access Attempts
Simple Example Expressway-E Dial Plan

- calls to the local domain routed to Expressway-C
- calls to non-local domains, from authenticated sources, routed to the internet
Zone Authentication Policy

- Treat as authenticated
  - All messages are classified as authenticated.
  - Messages with an existing P-Asserted-Identity header are passed on unchanged.
  - Messages without an existing P-Asserted-Identity header have one inserted.

- Do not check credentials
  - Messages are not challenged for authentication.
  - All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.

Non-authenticated traffic can be rejected through use of CPL rules
CPL and Authentication Policy

- One rule rejects unauthenticated calls coming from the Internet (Default Zone)
- Outbound calls will be allowed
- CPLs are more effective in security configuration than search rules because search rules don’t have an option to reject calls
Expressway Routing

Does the alias match a transform?

- Yes: Apply Transform
- No: Does calling or called match a CPL rule?

- Yes: Does the alias match a search rule?
  - Yes: Place Call
  - No: Next lower-priority rule until end of rules or the alias is found

- No: Does the alias match a search rule?
  - Yes: Apply Transform
  - No: Is the alias found?
    - Yes: Place Call
    - No: If “allow”
      - Allow/Reject
    - If “reject”
      - Forbidden
2 Expressway Call Policy Approaches

Allow-based policy:
- Allow calls matching internal dialplan for users and rooms
- Allow multiparty meetings
- Deny all other inbound calls (includes access code to PSTN, Unity calls, etc.)

Deny-based policy:
- Deny calls to PSTN
- Deny calls to Unity
- Deny calls to instant meetings on Conductor
- Allow everything else matching the internal domain
- Deny all other inbound calls
CPL Rules Example #1
Deny-based policy approach

- Destination has to match the internal dial plan. A simple rule matches the domain portion only. *@ent-pa\.com

Calls from external to external destinations are forbidden
- Simple policy rule protects against scanners sending traffic to @ipAddress
- Calls to Unity, PSTN gateways, Conductor instant meetings are allowed
- This example is a good starting point, further restrictions can be added
CPL Rules Example #2

Deny-based policy approach

- Builds on the existing call policy rules in example #1
- Adds a rule blocking PSTN gateway access from unauthenticated callers

More rules can easily be added to protect other resources
CPL Rules Example #3
Deny-based policy approach

• Allow call to Directory URI and Personal CMR (i.e. user1@ent-pa.com and user1.cmr@ent-pa.com)
  Regex: ^[a-z].*@ent-pa\.com

• Allow calls to scheduled conferences (80991XXX)
  Regex: 80991\d{3}@ent-pa\.com

• Allow calls to personal CMR (80044XXX, 80051XXX, 80065XXX)
  Regex: 80044\d{3}@ent-pa\.com
     80051\d{3}@ent-pa\.com
     80065\d{3}@ent-pa\.com

• Reject everything else
CPL Rules Example #3
Deny-based policy approach

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Rearrange</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthenticated User</td>
<td>^[a-z].*@ent-pa.com</td>
<td>Allow</td>
<td>↓</td>
<td>View/Edit</td>
</tr>
<tr>
<td>Unauthenticated User</td>
<td>80091\d\d\d@ent-pa\com</td>
<td>Allow</td>
<td>↑↓</td>
<td>View/Edit</td>
</tr>
<tr>
<td>Unauthenticated User</td>
<td>80044\d\d\d@ent-pa\com</td>
<td>Allow</td>
<td>↑↓</td>
<td>View/Edit</td>
</tr>
<tr>
<td>Unauthenticated User</td>
<td>80051\d\d\d@ent-pa\com</td>
<td>Allow</td>
<td>↑↓</td>
<td>View/Edit</td>
</tr>
<tr>
<td>Unauthenticated User</td>
<td>80065\d\d\d@ent-pa\com</td>
<td>Allow</td>
<td>↑↓</td>
<td>View/Edit</td>
</tr>
<tr>
<td>Unauthenticated User</td>
<td>^</td>
<td>Reject</td>
<td>↑</td>
<td>View/Edit</td>
</tr>
</tbody>
</table>

- Unauthenticated callers can only access pre-defined number ranges for conference bridges, end user URIs, and personal CMR URIs
- All other destinations are rejected
Differentiated Policy for Inbound Calls

• Neighbor Zones can be established on Expressway-E for specific business partners, allowing for both inbound and outbound calling

• Allows inbound calls from hosts defined in neighbor zone(s) to avoid the default zone, and instead receive differentiated treatment

• Trusted neighbor zones can use Treat as Authenticated policy, allowing inbound calls to bypass CPL rules established for unauthenticated inbound traffic

• Use TLS and TLS verify on neighbor zone config

• This approach can be used to provide broader access to enterprise dialplan and resources on inbound calls from trusted partners
UCM Calling Search Space

Block access at UCM level

- UCM’s SIP trunk calling search space controls access to all dial plan resources
- Inbound trunk CSS will have access to Directory URI, Scheduled meetings, personal CMR and permanent conferences partitions
- UCM has a more granular approach, not based on numeric ranges alone
Monitor Search History

- Monitor the Expressway Status > Search History on a regular basis
- Expressway GUI allows sorting by status and filtering

<table>
<thead>
<tr>
<th>Start time</th>
<th>Search type</th>
<th>Source</th>
<th>Destination</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-10-02 23:41:40</td>
<td>H823 (Setup)</td>
<td>192.168.216.121.61720</td>
<td>135566</td>
<td>Forbidden</td>
<td>View</td>
</tr>
<tr>
<td>2016-10-24 10:52:17</td>
<td>H823 (Setup)</td>
<td>192.168.216.121.61720</td>
<td>135566</td>
<td>Forbidden</td>
<td>View</td>
</tr>
<tr>
<td>2016-08-21 17:17:20</td>
<td>H823 (Setup)</td>
<td>192.168.216.121.61720</td>
<td>135566</td>
<td>Forbidden</td>
<td>View</td>
</tr>
<tr>
<td>2016-08-17 17:36:25</td>
<td>H823 (Setup)</td>
<td>192.168.216.121.61720</td>
<td>135566</td>
<td>Forbidden</td>
<td>View</td>
</tr>
<tr>
<td>2016-08-13 18:12:52</td>
<td>H823 (Setup)</td>
<td>192.168.216.121.61720</td>
<td>135566</td>
<td>Forbidden</td>
<td>View</td>
</tr>
<tr>
<td>2016-08-02 22:06:48</td>
<td>H823 (Setup)</td>
<td>192.168.216.121.61720</td>
<td>135566</td>
<td>Forbidden</td>
<td>View</td>
</tr>
<tr>
<td>2016-08-09 04:16:32</td>
<td>H823 (Setup)</td>
<td>192.168.216.121.61720</td>
<td>135566</td>
<td>Forbidden</td>
<td>View</td>
</tr>
<tr>
<td>2016-08-04 00:44:00</td>
<td>H823 (Setup)</td>
<td>192.168.216.121.61720</td>
<td>135566</td>
<td>Forbidden</td>
<td>View</td>
</tr>
</tbody>
</table>

- Confirm CPL rules are rejecting unwanted calls as desired
- Confirm CPL rules are not rejecting legitimate calls
Monitoring Logs and Call Detailed records

- Consider enabling Expressway remote syslog
- Consider enabling Expressway Call Detail Records
- **Continue** monitoring UCM Call Detailed Records on a regular basis
Appendix D
MRA Resources and Troubleshooting
Relevant Deployment Guides

Expressway Configuration Guides

• Start with the “Expressway Mobile & Remote Access Deployment Guide”
• For guidance on traversal connection between C & E, consult the “Expressway Basic Configuration Deployment Guide” to establish
• For assistance with certificates, consult the “Cisco Expressway Certificate Creation and Use Deployment Guide”

Cisco Jabber Planning and Deployment Guides

• Start with the “Planning Guide for Cisco Jabber”
Starting Point for Troubleshooting

Verify Expressway Traversal Connections

• The SIP connection between Expressway C and E needs to be established first
  • If you don’t have an active SIP traversal connection verify DNS, NTP, SSL certificates, and the trusted CA certificates on both C and E, also check firewall for drops

• SIP messaging over the traversal zone from C to E will provide the mobile remote access configuration details established on the C to the E
  • SSH connection from C to E on TCP 2222 will follow
  • XCP connection from C to E on TCP 7400 will follow only if on-prem IM&P servers have been discovered (doesn’t apply to WebEx cloud IM&P)
### Expressway-C Unified Communications Status

Status > Unified Communications Menu

#### Unified Communications

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unified Communications services</td>
<td>Active</td>
</tr>
<tr>
<td>IM and Presence servers</td>
<td>2</td>
</tr>
<tr>
<td>Unified CM servers</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Activity

<table>
<thead>
<tr>
<th>Activity</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Current provisioned sessions</td>
<td>0</td>
</tr>
<tr>
<td>Total provisioning requests since last restart</td>
<td>0</td>
</tr>
<tr>
<td>Total provisioned sessions since last restart</td>
<td>0</td>
</tr>
<tr>
<td>Unified CM calls: Current video</td>
<td>0</td>
</tr>
<tr>
<td>Unified CM calls: Current audio (SIP)</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Domains

<table>
<thead>
<tr>
<th>Name</th>
<th>Services</th>
<th>Associated zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>ucdemolab.com</td>
<td>Unified CM registrations, IM and Presence</td>
<td>ExpresswayE_force_encryption</td>
</tr>
</tbody>
</table>

#### Zones

<table>
<thead>
<tr>
<th>Name</th>
<th>SIP status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExpresswayE_force_encryption</td>
<td>Active</td>
</tr>
</tbody>
</table>

#### Advanced status information

- View provisioning sessions
- View sfh tunnel status

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
When an entry exists on this page, the user has been able to connect through Expressway E &C, and successfully authenticate against UCM. However, it doesn’t indicate the client is functional yet!

<table>
<thead>
<tr>
<th>Username</th>
<th>Device</th>
<th>User agent</th>
<th>Unified CM server</th>
<th>Expire time</th>
</tr>
</thead>
</table>

This is the UCM server used for UDS provisioning and authentication. It does not reflect where the SIP registration will be sent.
Expressway-E DNS

- Note: Expressway-E servers will often have multiple DNS aliases, especially in dual-nic deployments.

- The Expressway-E system hostname and domain (defined under System > DNS) are combined to form the Expressway-E FQDN.

- Expressway-E FQDN is embedded in the edge xml config served to remote clients, and needs to resolve in public DNS.

```xml
<edgeConfig>
  <sipEdgeServer>
    <server>
      <address>expwy1.example.com</address>
      <tlsPort>5061</tlsPort>
    </server>
    <server>
      <address>expwy2.example.com</address>
      <tlsPort>5061</tlsPort>
    </server>
  </sipEdgeServer>
  ...
</edgeConfig>
```
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

Subsequent home cluster discovery 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

X-Auth token

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://<UCM>/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>`
  - `<homeClusterDetails>`
    - `<selfProvisioningSecureMode>true</selfProvisioningSecureMode>`
    - `<adminProvisioning>true</adminProvisioning>`
  </homeClusterDetails>`
  </clusterUser>`
Request Edge Config In Your Browser

- Build an edge config HTTPS request that Jabber will use in the initial request
  - Destination is your Expressway-E = https://exp-e01.ucdemolab.com:8443/
- Base64 encode your service discovery domain
  - base64(ucdemolab.com) = dWNkZW1vbGFiLmNvbQ==
- Include the get_edge_config resource and internal DNS SRV records
  - By default jabber will request both _cisco-uds and _cuplogin (_cuplogin isn’t required!)
  - /get_edge_config?service_name=_cisco-uds&service_name=_cuplogin
- Put it all together in your browser’s address bar
  
  https://exp-e01.ucdemolab.com:8443/dWNkZW1vbGFiLmNvbQ==/get_edge_config?service_name=_cisco-uds

- Authenticate with UCM end user’s username and password when prompted by your browser
serviceConfig details returned here are a result of Expressway-C DNS SRV lookups and user's home cluster information.

One or more _cisco-uds DNS SRV records are required in internal DNS for Jabber.

The tftpServer entry is not based on a DNS SRV record. Tftp server addresses is mapped to the available TFTP servers in the user's home cluster.

Required for IP Phones over MRA.
Up to 4 members of the Expressway-E cluster will be returned as a sipEdgeServer.

One sipRequest “route string” is provided to clients for each Expressway-C in the cluster (up to 4).
Up to 4 members of the Expressway-E cluster will be returned as a xmppEdgeServer

Up to 4 members of the Expressway-E cluster will be returned as a httpEdgeServer
The userUdsServer entry will include a UCM server that belongs to the end user's home cluster. This may be a different cluster than where the _cisco-uds SRV record points.
Cisco Jabber Client Initialization

Jabber provisioning & registration sequence

• Jabber service discovery DNS SRV lookups are followed by several HTTPS requests

• Jabber will then establish an XMPP connection and authenticate (PLAIN SASL) after receiving a one time password over the HTTPS connection

• The Jabber client is not functional without an XMPP connection (unless using phone only mode)

• The Jabber SIP registration is one of the last steps

• Jabber will also establish an HTTPS connection for visual voicemail if that service is provisioned on Unity Connection, provided the Unity Connection server has been added to the allow list on Expressway C
Cisco Jabber Client Initialization

Sampling of initial Jabber HTTPS requests

GET /dWNkZW1vbGFiLmNvbQ/get_edge_config?service_name=_cisco-uds

GET /dWNkZW1vbGFiLmNvbS9odHRwYi51Y2RlbW9sYWluY29tLzg0NDM/cucm-uds/clusterUser?username=mdude

GET /dWNkZW1vbGFiLmNvbS9odHRwYi51Y2RlbW9sYWluY29tLzg0NDM/cucm-uds/servers

GET /dWNkZW1vbGFiLmNvbS9odHRwYi51Y2RlbW9sYWluY29tLzg0NDM/cucm-uds/user/mdude

GET /dWNkZW1vbGFiLmNvbS9odHRwYi51Y2RlbW9sYWluY29tLzg0NDM/cucm-uds/user/mdude/devices

GET /dWNkZW1vbGFiLmNvbS9odHRwYi51Y2RlbW9sYWluY29tLzg0NDM/cucm-uds/user/mdude/global-settings.xml

GET /dWNkZW1vbGFiLmNvbS9odHRwYi51Y2RlbW9sYWluY29tLzg0NDM/cucm-uds/user/mdude/jabber-config.xml

POST /dWNkZW1vbGFiLmNvbS9odHRwYi51Y2RlbW9sYWluY29tLzg0NDM/EPASSoap/service/v80
Cisco Jabber Client Initialization

Base64 decoded HTTPS requests

GET /base64(ucdemolab.com)/get_edge_config?service_name=_cisco-uds
GET /base64(ucdemolab.com/https/cucm-pub.ucdemolab.com/8443)/cucm-uds/clusterUser?username=mdude
GET /base64(ucdemolab.com/https/cucm-pub.ucdemolab.com/8443)/cucm-uds/servers
GET /base64(ucdemolab.com/https/cucm-sub2.ucdemolab.com/8443)/cucm-uds/user/mdude
GET /base64(ucdemolab.com/https/cucm-pub.ucdemolab.com/8443)/cucm-uds/user/mdude/devices
GET /base64(ucdemolab.com/http/cucm-pub.ucdemolab.com/6970)/SP3d2e8a13-21da-2a19-fb54-c36848840d66.cnf.xml
GET /base64(ucdemolab.com/http/cucm-pub.ucdemolab.com/6970)/global-settings.xml
GET /base64(ucdemolab.com/http/cucm-pub.ucdemolab.com/6970)/jabber-config.xml
POST /base64(ucdemolab.com/https/imp1.ucdemolab.com/8443)/EPASSoap/service/v80
HTTPS in the Network Log

• Monitor the HTTPS requests in the Network Log from the GUI
• Under the Status > Logs > Network Log, start by filtering on “trafficserver”

• Most recent logs are at the top
• Default INFO level logging is usually sufficient
• You can use this on both Expressway E & C
Diagnostic Logging

Maintenance > Diagnostics > Diagnostic logging Menu

- Use the diagnostic logging feature when you want to capture network and event logs in the same file and download for analysis

- Optionally include tcpdump to download and analyze in Wireshark
Expressway Mobile & Remote Access

from Unified CM perspective

- Remote access provided by Expressway is, for the most part, transparent to Unified CM
- MRA Integration is established on Expressway-C
- Think SIP line integration rather than SIP trunk integration
- No requirement to provision a SIP trunk on Unified CM for Expressway-C
- 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 endpoints registering to Unified CM through Expressway will appear to Unified CM as Expressway-C IP address
Interaction with SIP trunk

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

SIP 405 will be returned to SIP Register request if there is SIP trunk port conflict
Parallel Traversal Zones

- One **Traversal Zone** used for Open Video Federation
- Provides SIP, and optionally H.323
- Media Encryption Mode = Auto or Best Effort

- **Unified Communications Traversal Zone** used for Mobile & Remote Access, Jabber Guest, XMPP Federation
- Provides SIP, XMPP, HTTP
- Media Encryption Mode = Forced
MRA Client Authentication (non-SSO)

1 of 2

- MRA clients/devices need to be associated with an end user in the Unified CM database
- This association allows the Unified CM end user’s credentials to be used for client authentication when connecting through Expressway
- The end user’s device establishes an initial HTTP TLS session with the Expressway-E server, and the Expressway-E challenges all unauthenticated requests
- The Expressway-E server relays authentication attempts to the Expressway-C
- Expressway-C utilizes the Unified CM UDS API to locate an end user’s home cluster, and subsequently authenticate users against Unified CM
- Unified CM authentication can be based on the local database or optionally configured to authenticate end users against an LDAP directory
MRA Client Authentication (non-SSO)

2 of 2

- Upon successful authentication, the Expressway-C relays an X-Auth token to the remote client through the Expressway-E
- X-Auth token can be used for subsequent authentication purposes up until the expiration time, default of 8 hours
- SIP digest authentication is used for client authentication for clients connecting to Expressway-E on TCP 5061, the X-auth token is reused as for digest authentication
- The client authentication for XMPP connections is based on the PLAIN SASL standard, RFC 4616
- In practice the Cisco client first connects on TCP 8443 to Expressway-E and requests a one-time password or token from the IM&P server over the secured HTTPS connection
- Once the token is acquired, the client establishes a new TLS connection to TCP 5222 and supplies the token in the XMPP Plain SASL authentication attempt
Enabling MRA “service mode” on 7800/8800 phones

• Service mode introduced to differentiate between UCM, Cloud, and Expressway
• MRA can be enabled on networks serving DHCP option 150

• Enter Service Domain used to lookup collab-edge DNS SRV record, followed by username and password
Enabling Expressway MRA Mode on DX (1 of 2)

- DNS is required
- Reset network settings from Settings App
- If DHCP option 150 is served on local network, uncheck the “enable automatic local telephony service discovery”
Enabling Expressway MRA Mode on DX (2 of 2)

Service domain entry will be used to lookup collab-edge DNS SRV record
Persistent User Credentials

Applies to DX series, 7800 & 8800 phones

- New product specific option introduced on UCM device configuration page
- Enabled via device pack COP file

- Defaults to Disabled, requiring the user to re-enter password on a re-occurring basis
- When Enabled, the endpoint will cache the end user credentials (encrypted on device) and the user will **not** be prompted to authenticate again
Problem Report Tool (PRT)

• End users can send Problem Reports (PRT) through Expressway

• Deploy web server for collecting PRTs on internal network

• Sample PRT HTTP post script
  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/dx/series/rel-notes/1023/DX00_BK_RB889E3E_00_release-notes-dx-series-1023.html#DX00_RF_PF35EC13_00

• Assign PRT URL under common phone profile or at the device level

  Email address for customer support
  Customer support upload URL
  http://prtserver.ucdemolab.com/prt_upload.php

• Add the PRT web server FQDN to the Expressway-C HTTP server allow list
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 though Expressway may be dropped if AnyConnect tunnel is established mid-call

• Requirements to keep Jabber traffic going through Expressway
  1. AnyConnect split tunnel providing connectivity to internal enterprise network only (not including Expressway-E)
  2. Deny access (ASA DNS inspection) to the internal DNS SRV records (_cisco-uds & _cuplogin) to AnyConnect clients

Contact Search Considerations (Cloud Based IM&P)

- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to Unified CM
- Corporate directory is also exported to WebEx Messenger cloud
- All Jabber clients will use WebEx Messenger cloud as a contact source for contact search
Contact Search Considerations (On-premise IM&P)

- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to Unified CM
- User Data Services (UDS) is a Unified CM RESTful API allowing for contact search, among other things
- Jabber clients can use LDAP (EDI/BDI) or UDS for directory search when on-prem or connected via VPN
- All Jabber clients will automatically use UDS for directory search when connecting via Expressway
- Sync entire corporate directory to every Unified CM cluster for best contact search experience
UDS to LDAP Proxy - Contact Search
(on-premise IM&P)

- UCM 11.5 option to forward all UDS directory searches to LDAP v3 compliant server
- Allows Organizations to scale beyond 160,000 user limit
- New UCM 11.5 menu LDAP> LDAP Search
- Provides same attributes as classic UDS operation
- Requires Jabber 11.7
Appendix E
Expressway Server Certificates
Subject Alternative Name (SAN) Requirements

Expressway-E Server Certificate

• The domain(s) used to discover the collab-edge service record are required to be included as a DNS SAN in all Expressway-E server certificates

• Service discovery domain in this case is **ucdemolab.com**

  DNS X509v3 Subject Alternative Name: DNS:ucdemolab.com

• This domain is used for SRV lookups, extracted from here

• Or in some environments this will be Jabber’s VoiceServicesDomain (not exposed to end user)

• This is a security measure that allows clients to verify connections to edge servers authoritative for their domain (RFC 6125)
Expressway-E Certificate Requirements

DX, 78XX, 88XX specific requirements

• Trust model based on broadly trusted Public Certificate Authorities

• Endpoint firmware includes trusted public root CA certificates

• No option to import and trust other root CA certificates on these endpoints

• Expressway-E certificate needs to be signed by trusted public CA chain

• Latest Certificate Authority trust list posted on cisco.com

DX650, DX70, DX80

8811, 8841, 8845, 8851, 8861, 8865

7811, 7821, 7841, 7861
Unified CM Mixed Mode & Expressway-C SANs

1 of 2

• Expressway-C Server Certificate Generation CSR page has the option to include Unified CM phone security profile names as additional SANs

  DNS X509v3 Subject Alternative Name: DNS:secure-udt.ucdemolab.com

• This is only required in deployments that include encrypted phone security profiles (requires Unified CM to be in mixed mode with CTL deployed)

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

• Unified CM needs to find a match between the Expressway certificate’s CN or SAN and the phone security profile name to authorize the TLS registration on TCP 5061
Unified CM Mixed Mode & Expressway-C SANs

2 of 2

- A single phone security profile of type *Universal Device Template* can be associated with multiple device types in UCM.

- Optionally name the profile to match an existing name in Expressway-C certificate.

- This approach is not as obvious as dedicating a SAN for security profile names, but minimizes Expressway-C certificate SANs and allows you to add encrypted MRA endpoints without having to update the Expressway-C certificate.

![Phone Security Profile Information](image)

- **Phone Security Profile Information**
  - **Product Type:** Universal Device Template
  - **Device Protocol:**
    - **Name:** expwyc.ucdemolab.com
    - **Description:** used for encrypted MRA endpoints
    - **Nonce Validity Time:** 600
    - **Device Security Mode:** Encrypted
    - **Transport Type:** TLS
  - Enable Digest Authentication: No
  - TFTP Encrypted Config: No

- **Phone Security Profile CAPF Information**
  - **Authentication Mode:** By Null String
  - **Key Order:** RSA Only
  - **RSA Key Size (Bits):** 2048
  - **EC Key Size (Bits):** None

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.
Optional SANs for XMPP Federation

Applies to on-prem IM&P customers only

• The Expressway Server Certificate Generate CSR page will also insert “IM&P chat node aliases” as SANs

• These specific SANS will allow for **TLS XMPP federation**

  X509v3 Subject Alternative Name: conference-1-ucdemolabIMP1.ucdemolab.com

• There will be 1 chat node alias per deployed Unified CM IM&P server

• Expressway XMPP federation is an optional deployment that builds largely on the same configuration used for Mobile & Remote Access
### Expressway-C Certificate Signing Request

#### Generate CSR

<table>
<thead>
<tr>
<th>Common name</th>
<th>FQDN of Expressway cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name</td>
<td>cluster.collabedge1c.ucdemolab.com</td>
</tr>
</tbody>
</table>

**Only required when using encrypted devices with UCM in mixed mode**

<table>
<thead>
<tr>
<th>Alternative name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN of Expressway cluster plus FQDNs of all peers in the cluster</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IM and Presence chat node aliases (federated group chat)</th>
<th>FQDN of Expressway cluster plus FQDNs of all peers in the cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure-ucd.ucdemolab.com</td>
<td>conference-1-ucdemolabIMP1.ucdemolab.com, conference-2-ucdemolabIMP1.ucdemolab.com</td>
</tr>
</tbody>
</table>

**Only required for XMPP federation**
Expressway-E Certificate Signing Request

Include the Unified Communications domain configured on the Expressway-C

Use DNS SAN format

Copy Chat Node Aliases from the Expressway-C CSR (XMPP federation)
Expressway Trusted CA Certificates

- X8 software does **not** include the default trusted CA certificate list
- VCS customers upgrading from X7 or prior should consider purging this list
- Don’t upload more than one certificate with the same Common Name
## Expressway Trusted CA Certificates

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Expressway-C Trusted CA</th>
<th>Expressway-E Trusted CA</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 MTLS 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 MTLS connections</td>
</tr>
<tr>
<td>Unified CM Tomcat certificates or CA cert 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>Unified CM CallManager CA cert chain</td>
<td>✔</td>
<td>✗</td>
<td>Only required when Unified CM is in mixed mode for end to end TLS. CallManager and Tomcat certs need to be signed in this case so Expressway-C can validate the same common name on multiple certificates</td>
</tr>
<tr>
<td>Unified CM IM&amp;P Tomcat certificates or CA cert 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>
</tbody>
</table>
Appendix F
Expressway MRA with SSO
(Implicit Grant Flow)
Why Single Sign-On?

- Security & Compliance: align with the broader enterprise authentication strategy
- Simplify end user login
- Simplify user provisioning and deprovisioning for admin
- Integral to a common identity architecture - providing users with a single identity across cloud and on-prem services
- Mobile devices drive need for externally reachable identity and access management systems
- Potential for stronger client authentication
What’s Involved with SSO and Edge?

• Security Assertion Markup Language (SAML) v2 – open standards based protocols for user authentication
• Identity Provider (IdP) – Responsible for User Authentication
• OAuth - open standards based protocol for token based authorization
• Tokens & Cookies
• Export & import metadata to form trust relationships between IdP, Expressway, Unified CM, Unity Connection
Jabber + Expressway SSO Solution

SAML Solution Network Elements

Collaboration Services
- Unified CM
- Unified CM IM&P
- Unity Connection

Identity Provider

Service Provider

Directory

Internal Network

DMZ

External Network

Identity Infrastructure

LDAP

UCM

EXPWY-C

EXPWY-E

DNS

Browser

Jabber 10.6

Identity Provider

Proxy

IdP

IdP Proxy

SAML Request

SAML Assertion

Domain Name System

MORE DETAILS IN APPENDIX

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
## Jabber + Expressway SSO Support

### Minimum 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>X8.5.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>10.5(2)</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM IM&amp;P</td>
<td>10.5(2)</td>
<td>Available</td>
</tr>
<tr>
<td>Unity Connection</td>
<td>10.5(2)</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Windows</td>
<td>10.6</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for iPhone and iPad</td>
<td>10.6</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Mac</td>
<td>10.6</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Android</td>
<td>10.6</td>
<td>Available</td>
</tr>
</tbody>
</table>

Your SAML v2.0 IdP must be reachable from internet
Cisco has tested the most popular IdPs →
Jabber iOS SSO Authentication Enhancement

- Allowing Safari browser enables iOS client certificate–based SSO
- Requires Apple iOS 9+, SSO, UCM 11.5, Expressway X8.9, Jabber 11.8, and a client certificate enrollment mechanism
- Authentication method remains between client and IdP
Mobile and Remote Access X8.9 Enhancement

- Embedded Safari for Jabber iOS
- If “Allow Jabber iOS clients to use embedded Safari browser" is set to “Yes” on the Expressway-E, then the get_edge_sso response will contain <allowEmbeddedSafari>true</allowEmbeddedSafari>

- Admins are recommended to use the same setting on the Expressway as the CUCM, otherwise the users will get an inconsistent experience

HTTPS: GET /get_edge_sso
HTTPMSG:
HTTP/1.1 200 OK
<?xml version='1.0' encoding='UTF-8'?>
<SSOResult version="1.0">
  <Response>
    <SingleSignOn>
      <Status enabled="true"/>
      <Token reuse="false"/>
      <allowEmbeddedSafari>true</allowEmbeddedSafari>
    </SingleSignOn>
  </Response>
</SSOResult>
Cookies and Access Token

• IDP Cookie: Set by the IDP in the Browser when Assertion is provided. This could be of type “Session” or “Permanent”. This is the core of the Single Sign On Experience.

• SP Session Cookie: this is set by SP (CUCM) on the Browser when the Resource access is granted.

• Access Token: the OAuth Access token is provided when the browser is redirected to the target Resource.

• Cookies and OAuth Access Token depends on Timers that are set by Admins
SSO Edge Transitions

**EDGE to ON-PREM → Seamless reconnection**

- Tokens issued through Expressway are valid for direct connections to Unified CM and Unity Connection

**ON-PREM to EDGE →** Jabber will need to re-authenticate, which may be transparent to the user depending upon IdP cookie expiration

- Tokens issued directly by Unified CM and Unity Connection will not be valid for connections through Expressway
- If the IdP cookie has expired, the user will be prompted via the standard re-establish SSO session pop-up
Single Sign On Cookie/Token Flowchart (Implicit Grant Flow)

Resource Request → Valid SP Cookie

Valid SP Cookie

NO → Authentication Process

YES → Access Token Expired

Access Token Expired

YES → Set IDP Cookie

NO → Valid IDP Cookie

Valid IDP Cookie

YES → Set SP Cookie and New Access Token

NO → NO → NO → NO → Resource
New Expressway SSO APIs

Jabber Edge SSO support Jabber introduces two new APIs on Expressway

• “get_edge_sso” API enables Jabber to query the Expressways for SSO support
  Requires username to locate home cluster and check for SSO status

• The “authorize” API enables Jabber to request for OAuth tokens to be used for SSO
The Browser is the "OAuth Client". The Browser accesses some resources on the Service via a GET request to `/authorize`.

302 Found Location: https://ad01.eft.cisco.com/adfs/ls

GET https://ad01.eft.cisco.com/adfs/ls/?SAMLRequest=...

200 Ok [Login Form]

POST [Credentials]

200 Ok {Action=POST value=Assertion} Set-Cookie=Idp_Cookie

The IdP returns the SAML assertion to the browser in a hidden form in a 200 OK message. The hidden form instructs the browser to POST the SAML assertion to the Assertion Consumer Service (ACS) of the SP.
The Expressways reuse the Assertion to get and access_token for the end user. The Expressway-C generates the **SAML Bearer Grant API**

**POST /samlsp Assertion**

The Assertion contains a Subject for the Authz service. The Service calls the **SAML Bearer Grant API on the Authz**. It POSTs the Assertion as a parameter to the API endpoint.

The SAML Assertion contains end user information. The Assertion also has a Subject field for the Authz. The Authz checks these, and the digital signature on the Assertion and returns the access_token.

**POST /authorise_proxy**

The SAML Assertion contains a Subject for the Authz service. The Service calls the **SAML Bearer Grant API on the Authz**. It POSTs the Assertion as a parameter to the API endpoint.

**200OK [access_token]**

**Set-Cookie= SP_Cookie**

**Simplified Call-Flow**

**POST /token/authorise_proxy**
Authorization: Basic 3(service-autz secret)
Host: CUCM
Content-Type: application/x-www-form-urlencoded
grant_type:urn:left:params:oauth:grant-type:saml2-bearer
&assertion=xxx &scope=resource
Once Expressway has authorized the user, it caches the OAuth token, generates the SIP token – not for unity- and gives it to Jabber.

200 OK [OAuth Token + Sip Token + User name + Timers]

Jabber Signs (OAuth, Identity)

Simplified Call-Flow
Edge SSO Tokens

- Jabber receives three tokens via two different calls to the Expressway authorize API

- In the first request to Expressway Jabber retrieves the **CUCM OAuth Token** which is used to authenticate all HTTP (including UDS) and XMPP traffic traversing the edge.

- This same request also provides Jabber with a **Expressways SIP Token** which is required for SIP traffic to traverse the edge. This token can have longer lifetime than the CUCM token.

- In the subsequent request to Expressway Jabber retrieves the **Unity OAuth Token** for use by Voicemail HTTP traffic. (/authorize with service=base64(domain/protocol/address/port)
Edge SSO Timers (Implicit Grant Flow)

A) IdP Session timeout
   • Configured on the IdP (e.g. ADFS2, OpenAM, Ping, etc.)
   • Default depends on IDP
   • Typically expect 8 – 10 hours

B) OAuth Token expiry
   • Configured on CUCM/Unity - Default 60 minutes

C) SIP Token Extra TTL
   • Configured on EXP-C (or VCS-C)
   • Value is added onto OAuth Token expiry to get SIP Token Expiry
   • Default 0 - Max 48 hours

D) SIP REGISTER expiry refresh
   Configurable on CUCM (various settings depending on device type)

   For mobile device types, register expires typically = 10 to 12 minutes

   With 12 minute register expiry, sip stack attempts to refresh register 10 minutes after last successful one

   For all other devices (including CSF) register expires = 2 minutes –
   SIP stack attempts to refresh register 1 minute 55 seconds after last successful one
Appendix G
XMPP Federation
XMPP Federation Solution Overview
Extending the reach of your organization's Jabber deployment
Expressway XMPP Federation

Design Considerations

- An Expressway XMPP Federation deployment can easily co-reside on a Expressway C & E pair deployed for MRA

- A dedicated Expressway C & E pair could also be deployed specifically for federation

- Only one Expressway cluster pair should be deployed for XMPP federation

- xmpp-server DNS server record(s) are required for public federation, but not strictly required (static routes can be used)

- Contact card details are not provided to federated contacts

- SIP Federation can still be used on IM&P when Expressway is deployed for external XMPP federation
Enabling XMPP Federation on Expressway

Configuration Steps

Prerequisites

- UCM IM&P “XMPP Federation Node Status” must be turned off
- Relies on Expressway “Unified Communications” Traversal Zone

Open TCP 5269 inbound on external firewall to Expressway-E from ANY

Publish _xmpp-server._tcp SRV record for your domain in public DNS

Expressway-C: Configure Domain(s) enabled for XMPP Federation

Expressway-E

- Enable XMPP Federation
- Optionally configure static routes or DNS lookup for Federation
- Configure XMPP Parameters (Dialback secret, TLS settings and Allow/Deny List)

Restart XCP Router Services on UCM IM&P Server(s)
XMPP Federation Policy

• Expressway provides options for either Public or Private federation

• Security mode of **TLS optional** is the most flexible for public xmpp federation

• Dialback secret provides proof of possession (RFC3920) for xmpp servers to prevent address spoofing

• TLS Required and Client-side certificates not compatible with WebEx Messenger

• Optional privacy mode allows for list of domains either allowed or blocked
XMPP Federation Support
Minimum 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>X8.2</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>9.1(2)</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM IM&amp;P</td>
<td>9.1(1)</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Windows</td>
<td>9.7</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for iPhone and iPad</td>
<td>9.6.1</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Mac</td>
<td>9.6</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Android</td>
<td>9.6</td>
<td>Available</td>
</tr>
</tbody>
</table>

Federate with WebEx Messenger cloud or any standards based XMPP server
Appendix H
Consumer to Business Video with Jabber Guest
Jabber Guest Consumer to Business Video
Extending the reach of your organization's video deployment
Why Jabber Guest?

• Enhance customer interactions with click to call video links embedded in email and on your website

• Make experts easy to find and consult with on video

• HR Interviews: Video Recruiting and Interviews

• Jabber Guest 11 introduces guest content share

• Voice, video and content streams SRTP encrypted over the internet

• Ideal for customers that haven’t transitioned to, or invested in Cisco Meeting Server

• Jabber Guest api available for link creation and management
Jabber Guest 11 (Random String) Link Config

Details
- **Link:** https://jabberguest.udemolab.com/call/tcsvibf9y5a4
- **Enabled:** Yes
- **Destination:** kroarty.pmr
- **Creator:** linkadmin
- **Display name:** Kevin's Personal Meeting Room
- **Caller name:** Jabber Guest 11
- **Caller SIP alias:**

Options:
- **State:**
  - Always Active
  - Active Between
- **Start:** 02/01/2017 11:59 PM
- **End:** 02/22/2017 11:59 PM
- **Auto call:**
  - Disable
  - Enable
- **Seconds:** 3
- **Guest video policy:**
  - send and receive, can start/stop sending during call (default)
  - cannot send or receive throughout call
  - receive only, cannot start sending during call
  - receive only initially, can start/stop sending during call

Cisco Jabber Guest: main_11.0.0.36 © 2009-2016 Cisco Systems, Inc. All rights reserved.
Jabber Guest

Design Considerations

- Jabber Guest cannot co-reside on an Expressway C & E pair deployed for MRA
- Jabber Guest requires one rich media session license per call (Expressway E)
- Include Jabber Guest link domain name in Expressway E certificate as SAN
- External firewall required to map inbound TCP 443 to TCP 9443 of Expressway E (allowing for links without needing to include TCP port numbers)

- Expressway E network design trade offs
  - Dual NIC Expressway E deployments allow for assent media traversal between C & E, but requires TCP 5061 open between Expressway-E and Jabber Guest
  - Single NIC Expressway E deployments do not allow for assent media traversal and require UDP ports open between E & C, but no requirement for TCP 5061 between Expressway E and Jabber Guest Server
# Jabber Guest Support

## Minimum 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>X8.2</td>
<td>Available</td>
</tr>
<tr>
<td>Unified CM</td>
<td>8.6(2)</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber Guest</td>
<td>10.5</td>
<td>Available</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>10</td>
<td>Available</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>18</td>
<td>Available</td>
</tr>
<tr>
<td>Apple Safari</td>
<td>5</td>
<td>Available</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>8</td>
<td>Available</td>
</tr>
<tr>
<td>iOS (mobile app)</td>
<td>7</td>
<td>Available</td>
</tr>
<tr>
<td>Android (mobile app)</td>
<td>5</td>
<td>Available</td>
</tr>
</tbody>
</table>
Appendix I
Migration, Trade in, Ordering Info
Why Migrate from VCS to Expressway Series?

- More Cost Effective
- Functionally same as VCS*
- Easy to understand Licensing
- Predictable licensing and support costs
- Spark Flex Plan available

- Will not require CUCM
- Same Admin Experience
- Minimal or no config changes needed
- Easy upgrade to CUWL Meetings to get PMP+
- Easy transfer to CUCM unlocks UC features

Simple migration process
## Ordering SKUs

<table>
<thead>
<tr>
<th></th>
<th>Top Level SKU</th>
<th>Valid Option SKUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Registration (UCL)</td>
<td>R-UCL-UCM-LIC-K9</td>
<td>LIC-CUCM-11X-ENH-A&lt;br&gt;LIC-CUCM-10X-ENH-A</td>
</tr>
<tr>
<td>TelePresence Room (UCL)</td>
<td>R-UCL-UCM-LIC-K9</td>
<td>LIC-TP-11X-ROOM&lt;br&gt;LIC-TP-10X-ROOM</td>
</tr>
<tr>
<td>Desktop Registration (BE6K)</td>
<td>R-CBE6K-K9</td>
<td>BE6K-START-UCL35&lt;br&gt;BE6K-UCL-ENH</td>
</tr>
<tr>
<td>TelePresence Room (BE6K)</td>
<td>R-CBE6K-K9</td>
<td>BE6K-UCL-TP-RM</td>
</tr>
<tr>
<td>Desktop Registration plus PMP (CUWL)</td>
<td>CUWL-11X-K9</td>
<td>NEW-UWL-11X-PRO</td>
</tr>
<tr>
<td>Desktop Registration plus PMP (BE6K)</td>
<td>R-CBE6K-K9</td>
<td>BE6K-START-PRO35&lt;br&gt;BE6K-UWL-PRO</td>
</tr>
</tbody>
</table>

Full ordering information may be found in the [Expressway and VCS Ordering Guide](#).
Promotions and Discounts

Refresh Collaboration Portal

Refresh Collab Promo Series

Trade in of old VCS appliances will secure additional discount on new CE1100 VCS appliance

Instructions for TMP Program
VCS Appliance to Virtual Server Migration

• Price of this migration is now $0
• SWSS is required on new VM
• Migration SKU’s remain the same
  • R-VMVCS-C-M-K9 to migrate VCS Control
  • R-VMVCS-E-M-K9 to migrate VCS Expressway
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKUCC-2801
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you