TOMORROW starts here.
Cisco Expressway at the Collaboration Edge Design Session

BRKUCC-2801

Kevin Roarty
Technical Marketing Engineer
Cisco Collaboration
Abstract

Cisco Expressway is an important part of the Collaboration Edge Architecture offering a mobile and remote access alternative to VPN.

The solution allows Jabber clients to securely traverse the enterprise firewall and access collaboration services deployed on the enterprise network.

Remote Jabber clients will have access to voice/video, instant messaging and presence, visual voicemail, and directory look-up services.

This session will include a solution overview including how Jabber clients connect over the edge and register to Unified CM, the evolution of Expressway firewall traversal, options for IM & Presence services, and also how remote TelePresence endpoints can now register to Unified CM through Expressway.

Participants will receive design guidance including deployment options, limitations, best practices, required software versions, and security considerations.
Agenda

• Terminology Introduction
• Solution Overview
• Product Line Options, Licensing, Scalability
• Design and Deployment Considerations
• Unified CM Requirements
• Authentication & Certificates
• Jabber 10.6 Single Sign On
• New Endpoint Support
• Q & A
Terminology Introduction
Introducing Cisco Collaboration Edge Architecture

Industry’s Most Comprehensive Any-to-Any Collaboration Solution

All the capabilities of Cisco Any-to-Any collaboration to-date

- TDM & analog gateways
- ISDN Video gateways
- Session border control
- Firewall traversal
- Standards-based & secure

B2B

Mobile Workers

Teleworkers

TDM or IP PBX

PSTN or IP PSTN

Branch Office

Cloud Services

Analog Devices

3rd Parties

Consumers

TDM & analog gateways
ISDN Video gateways
Session border control
Firewall traversal
Standards-based & secure
Cisco Expressway

A new gateway solving & simplifying business relevant use cases

- For Unified CM & Business Edition environments
- Based on Cisco VCS Technology
- Standards-based interoperability
Product Line Options

- Specialized video applications for video-only customer base and advanced video requirements
  - **Complete set** of X8 SW features
  - No changes to existing licensing model

- Solution designed for and sold exclusively with Unified CM 9.1 and above (including Business Edition)
  - **Subset** of X8 SW features
  - $0 server software licenses
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 Unified CM and Business Edition customers, providing firewall
traversal & video interworking. Includes Expressway Core and Expressway Edge

Mobile and Remote Access (MRA)
Feature available on both VCS and Expressway product lines with X8 software
Delivers VPN-less access to Jabber and Fixed Endpoints
Expressway Mobile & Remote Access Solution Overview
Mobile and Remote Collaboration with Expressway

Inside firewall (Intranet)  DMZ  Outside firewall

Collaboration Services
Unified Expressway C
Expressway E

Expressway

Internet

Fixed Remote Endpoints (TC Series)

Jabber @ work
Jabber @ SFO, LHR or PVG
Jabber @ Home
Jabber @ the café

Simple, Secure Collaboration: It just works...inside and outside the network, no compromises
Easy to use, easy to deploy: Works with most firewall policies
True Hybrid: Supports on-premise and cloud offerings simultaneously
Standards-based Interoperability, Widely Adopted Protocols
Application Driven Security: Allow the application to establish security associations it needs

Simple, Secure Collaboration:
Easy to use, easy to deploy:
True Hybrid:
Standards-based
Application Driven Security:
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
What can a Jabber client do with Expressway?

A fully featured client outside the network

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

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 **Unified CM** to reach the called user or endpoint.

6. The call is established and media traverses the firewall securely over an existing traversal connection.
X8 Firewall Traversal Capabilities Expanded

The X8 software delivers 3 key capabilities enabling the Expressway Mobile and Remote Access feature

• XCP Router for XMPP traffic
• HTTPS Reverse proxy
• Proxy SIP registrations to Unified CM
# Expressway Mobile & Remote Access 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) SU1</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>
</tbody>
</table>
Product Line Options, Licensing, Scalability
Product Line Options

VCS

- "VCS Control" No Change
- "VCS Expressway" No Change

- Specialized video applications for video-only customer base and advanced video requirements
- **Complete set** of X8 SW features
- No changes to existing licensing model

Expressway

- "Expressway-C" Or Core
- "Expressway-E" Or Edge

- Solution designed for and sold exclusively with Unified CM 9.1 and above (including Business Edition)
- **Subset** of X8 SW features
- $0 server software licenses
# 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>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>CMR Cloud/Hybrid</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>XMPP Federation</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
Cisco Expressway Licensing

**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 Unified CM 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: “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.

### Resource usage

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified CM calls</strong></td>
<td></td>
</tr>
<tr>
<td>Current video</td>
<td>0</td>
</tr>
<tr>
<td>Current audio (SIP)</td>
<td>0</td>
</tr>
<tr>
<td>Peak video</td>
<td>4</td>
</tr>
<tr>
<td>Peak audio (SIP)</td>
<td>1</td>
</tr>
</tbody>
</table>

| **Rich media session traversal calls** |       |
| Current video            | 0     |
| Current audio (SIP)      | 0     |
| Peak video               | 0     |
| Peak audio (SIP)         | 0     |

| **Rich media session non-traversal calls** |       |
| Current                             | 0     |
| Peak                                | 0     |

| **Monitored resource usage** |       |
| Current                           | 0     |

<table>
<thead>
<tr>
<th><strong>Rich media sessions</strong></th>
<th>License usage current</th>
<th>License usage peak</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Flexible Call Licensing

• X8 software release 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 Expressway Rich Media Session licenses allows for 90 video and 20 audio-only simultaneous calls
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>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 3.2 GHz</td>
<td>8GB</td>
<td>132GB</td>
<td>10Gb</td>
</tr>
</tbody>
</table>

Appliance Support

- 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
- EXPWY-CE500-BDL-K9
- EXPWY-CE1K-BDL-K9
- VCS option: CTI-CE500-BDL-K9
- VCS option: CTI-CE1K-BDL-K9
# Expressway X8 Scalability

<table>
<thead>
<tr>
<th>Platform</th>
<th>Server</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MRA Registrations</td>
<td>MRA Registrations</td>
</tr>
<tr>
<td>Large OVA, CE1000</td>
<td>2,500</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>Video Calls</td>
<td>Video Calls</td>
</tr>
<tr>
<td></td>
<td>500</td>
<td>2,000</td>
</tr>
<tr>
<td></td>
<td>Audio Only Calls</td>
<td>Audio Only Calls</td>
</tr>
<tr>
<td></td>
<td>1,000</td>
<td>4,000</td>
</tr>
<tr>
<td>Medium OVA, CE500</td>
<td>2,500</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>Video Calls</td>
<td>Video Calls</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>400</td>
</tr>
<tr>
<td></td>
<td>Audio Only Calls</td>
<td>Audio Only Calls</td>
</tr>
<tr>
<td></td>
<td>200</td>
<td>800</td>
</tr>
<tr>
<td>Small OVA (BE6000)</td>
<td>2,500</td>
<td>2,500</td>
</tr>
<tr>
<td></td>
<td>Video Calls</td>
<td>Video Calls</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Audio Only Calls</td>
<td>Audio Only Calls</td>
</tr>
<tr>
<td></td>
<td>200</td>
<td>200</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.

Small, medium, & CE500 can support Unified CM calls scaling up to 150 video or 300 audio per server.
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

• The 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>
Design and Deployment Considerations
Expressway & Jabber Service Discovery

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

Collaboration Services
Unified CM

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

Expressway
E Expressway
C
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 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 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, Advanced Control</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)

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

Unity Connection
Conferencing Resources
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
- The entire corporate directory needs to be sync’d on every Unified CM cluster for best contact search experience
Media Path Summary

Unified CM provides call control for both mobile and on-premise endpoints

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
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 or appliances throughout cluster
- Customers can deploy multiple clusters for the same domain
## Mobile & Remote Access Deployment Options

Customer domain shared across all Unified CM & IM&P clusters

<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>
Multi-Deployment Support

New feature in X8.5

- Single Expressway pair can now serve multiple domains
- Deployments partition UC services available to mobile and remote access (MRA) users
- Not a multi-tenant architecture
- Single certificate presented by Expressway-E needs to contain multiple domain names
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.
- Mobile and remote access requires a Expressway-C cluster for each Expressway-E cluster.
- Only one “Unified Communications services” 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 VCS-E, but will not allow for Unified Communication Services
- Not supported for the new mobile and remote access functionality introduced in X8.1
Combining features on a single cluster pair

Example #1

**Open Video Federation** supporting:
- SIP & H.323 (inbound & outbound)
- Outbound calling for CMR Cloud/Hybrid
- Inbound calling for CMR Premises

**XMPP Federation**

**Mobile & Remote Access** supporting:
- Cisco Jabber Desktop Clients
- Cisco Jabber Mobile Clients
- 7800 & 8800 Series IP Phones
- DX80, DX70, DX650 Collaboration Endpoints
- TC Series Telepresence Endpoints
Combining features across two cluster pairs

Example #2

Open Video Federation supporting:
- SIP & H.323 (inbound & outbound calling)
- Outbound calling for CMR Cloud/Hybrid
- Inbound calling for CMR Premises

Jabber Guest Inbound C2B Video calling

XMPP Federation

Mobile & Remote Access supporting:
- Cisco Jabber Clients
- 7800 & 8800 Series IP Phones
- DX80, DX70, DX650 Collaboration Endpoints
- TC Series Telepresence Endpoints

Pool all RMS licenses on pair #1
No RMS requirements on pair #2
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

  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

  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 or CMR (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 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

Unified CM Requirements
Expressway Mobile & Remote Access
from Unified CM perspective

- Remote access provided by Expressway is, for the most part, transparent to Unified CM
- Think SIP line integration, vs. 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 TelePresence 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 (or VCS-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 Trunk can interfere with remote registrations

SIP Video Endpoints

Collaboration Services

Unified CM

Inside firewall (Intranet)

DMZ

Outside firewall (Public Internet)

Internet

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

SIP Video

Collaboration Services

Unified CM

Inside firewall (Intranet)

DMZ

Outside firewall (Public Internet)

Internet
UDS Directory Search

- All Jabber clients connecting via Expressway will use UDS for directory search (assuming Unified CM 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 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
Supporting multiple Unified CM Clusters

Prerequisites

• Cross cluster UDS API calls are used to find Jabber user’s home cluster

https://<ucm>/cucm-uds/clusterUser?username=mdude

• Intercluster Lookup Service (ILS) networking needs to be established enterprise Unified CM clusters to allow for Unified CM cluster discovery

• SIP URI replication over ILS is optional, not a requirement

• Unified CM’s Tomcat certificates need to be exchanged between Unified CM clusters for UDS clusterUser API calls to work
Unified CM Bulk Certificate Management

- Tool used to simplify Unified CM Cluster certificate exchange

- All Clusters **export** TFTP (CallManager), Tomcat, and CAPF certificates to central SFTP server

- Certificates are **consolidated** into PKCS12 files

- Consolidated set of certificates are then **imported** to each publisher

- Cisco Certificate Change Notification Service replicates trusted certificates throughout the cluster
Authentication & Certificates
Client Authentication at the Edge

Default deployment (non-SSO)

HTTPS

- Clients supply base64 encoded username and password to authenticate over HTTPS

  Authorization: Basic bWR1ZGU6dGhpc3Bhc3N3ZHdpbGxiZXJlc2V0

- Credentials are forwarded to Expressway-C and then used to authenticate against Unified CM, upon determination of the user’s home cluster

- Upon successful authentication, X-Auth token provided for future HTTPS requests (8 hour lifetime)

  Cookie: X-Auth=7f501814-e61f-483a-8620-ed0b5d3792db

SIP

- SIP Digest authentication used to authenticate users registering on tcp 5061

- No requirement to configure device for digest authentication on Unified CM
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

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

• No CTL requirement for Edge Server 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
- 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
Jabber Single Sign-On + Expressway Mobile & Remote Access
Why Single Sign-On?

• Security & Compliance: align with the broader enterprise authentication strategy
• Simplify user provisioning and deprovisioning
• 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

Highly recommended session for a deeper dive:
BRKCOL-2601 Directories Services and Single Sign-On for Collaboration
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 standard 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

- Directory
- Internal Network
- DMZ
- External Network
- Service Provider
- IdP
- Identity Infrastructure
- UCM
- Identity Provider
- EXPWY-C
- EXPWY-E
- Assertion Consumer Service
- Domain Name System
- Browser
- LDAP
- LDAP
- Proxy
- Service Provider
- IdP
- IdP
- SAML Request
- SAML Assertion

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

Jabber 10.6

MORE DETAILS IN APPENDIX C
SSO Transition Behavior

**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
# 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 →

[Image of popular IdPs: Ping Identity, OpenAM, ForgeRock, ADFS]
New Endpoint Support
Expressway Mobile & Remote Access
New Endpoint Support
Targeting first half CY15

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

Collaboration Services
Unified CM  Expressway C  Expressway E

Internet

DX650, DX70, DX80
8811, 8841, 8851, 8861
7821, 7841, 7861

TARGET DATES SUBJECT TO CHANGE
Target Use Case

DX Series + Expressway

• Remote access for the collaboration desktop experience
• Ideal for teleworkers or employees that need flexibility to occasionally work from home to collaborate across time zones
• Allows remote workers to engage in rich multi-collaborative experience
• Alternative to AnyConnect VPN
• Expressway provides enterprise firewall traversal for Phone and Jabber apps
• Other services (WebEx, email, box.com, etc.) consumed directly from cloud
• Endpoints can be shipped directly to remote workers, no required on-premises staging
Services available to DX series
with Cisco Expressway

- Voice and video calling, including content share
- Instant Message and Presence, including escalation to Voice/Video
- Visual voicemail
- Search corporate directory
- Collaboration Services
- Unified CM
- Expressway C
- Expressway E
- Inside firewall (Intranet)
- DMZ
- Internet
Target feature set

DX Series + Expressway

• 1080P 30fps HD video, plus BFCP content share/receive
• Single line support, with early media
• Encrypted signaling and media (UCM mixed mode not required)
• Access to corporate directory (UDS)
• Includes Jabber 10.6 client (IM&P only), with escalation from chat to video
• Unity Connection Visual Voicemail, Voicemail
• Call Forward, Transfer, Ad-hoc Conferencing, Do Not Disturb, MWI, iDivert, Mobile Connect
• Device management including configuration, firmware upgrades, reset/restart/applyConfig
Expressway-E certificate requirements

DX, 78XX, 88XX specific requirements

• Trust model based on broadly trusted Public Certificate Authorities

• Endpoint firmware includes 135 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
## New Endpoint 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.x</td>
<td>Target 1H CY15</td>
</tr>
<tr>
<td>Unified CM</td>
<td>9.1(2) SU1</td>
<td>Available</td>
</tr>
<tr>
<td>7821, 7841, 7861 IP Phones</td>
<td>10.3.1</td>
<td>Target 1H CY15</td>
</tr>
<tr>
<td>8811, 8841, 8851, 8861 IP Phones</td>
<td>10.3.1</td>
<td>Target 1H CY15</td>
</tr>
<tr>
<td>DX650, DX70, DX80 Collaboration Endpoints</td>
<td>10.2.4</td>
<td>Target 1H CY15</td>
</tr>
</tbody>
</table>

TARGET DATES SUBJECT TO CHANGE
Closing Thoughts
High Level 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

• Review TCP and UDP port requirements with firewall team

• 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
Key Takeaways

• Cisco Expressway: a product offering specifically for Unified CM 9.1+ and Business Edition customers
• Deploy Expressway with no added costs for mobile & remote users
• Expressway provides simple and secure VPN-less access, including support for Jabber Single Sign On
• New endpoint support (DX, 8800, 7800) coming very soon!
• Cisco VCS includes the complete set of X8 software features
• Cisco Expressway includes a subset of X8 software features
Call to Action

• Visit the World of Solutions for
  – Cisco Campus – Collaboration
  – Walk in Labs
  – Technical Solution Clinics

• Meet the Engineer

• Lunch time Table Topics

• DevNet zone related labs and sessions

• Recommended Reading: for reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2015
Complete Your **Online Session Evaluation**

- 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
Thank you.
Appendix A
Resources and Troubleshooting
Deployment Guides

- Expressway Basic Configuration Deployment Guide
- Expressway Mobile & Remote Access Deployment Guide
- Cisco Expressway Certificate Creation and Use Deployment Guide
- Cisco Jabber DNS Configuration Guide
- All other Expressway Configuration Guides
COP File for UDS Enhancements

No need to apply the COP file to 10.X or 9.1.2 SU2
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

• SIP messaging over the traversal zone from C to E will provide the mobile remote access configuration details established on the C
  – 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)

• NOTE: If the advanced networking license key is installed on the E, the 2\textsuperscript{nd} NIC is automatically enabled
  – When the 2\textsuperscript{nd} NIC is enabled, the E only listens for TCP 7400 on the 2\textsuperscript{nd} NIC interface
  – If you are not using the 2\textsuperscript{nd} NIC, you need to disable it on the System > IP menu
## Expressway-C Unified Communications Status

**Status > Unified Communications**

### Unified Communications

The Unified Communications status is `Enabled`. The Unified Communications services are `Active`. There are 2 IM and Presence servers, and 8 Unified CM servers.

### Activity

- Current provisioned sessions: 0
- Total provisioning requests since last restart: 0
- Total provisioned sessions since last restart: 0
- Unified CM calls: Current video: 0
- Unified CM calls: Current audio (SIP): 0

### Domains

<table>
<thead>
<tr>
<th>Name</th>
<th>Services</th>
<th>Associated zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>uccdemblab.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 san tunnel status
### Unified Communications proxy requests

<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>

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!

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.

```
<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 bWR1ZGU6dGhpc3Bhc3N3ZjdpbGxiZXJlJcV0
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 /dWNkZW1vbGFiLmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0N/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

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

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>

  - <clusterUser
      uri="https://cucm1-1.eft.cisco.com:8443/cucm-uds/clusterUser?username=mjackson" version="9.1.2">{}
  
  - <clusterUser
      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
      version="10.0.1" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/clusterUser?username=mjackson">{}
  
  - <result found="true" url="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>
      <adminProvisionMode>false</adminProvisionMode>
  
  </homeClusterDetails>

  </clusterUser>
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 /dWNkZW1vbGFilmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0NDM/cucm-uds/clusterUser?username=mdude

GET /dWNkZW1vbGFilmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0NDM/cucm-uds/servers

GET /dWNkZW1vbGFilmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0NDM/cucm-uds/user/mdude

GET /dWNkZW1vbGFilmNvbS9odHRwL2N1Y20tcHVilNvJzGVtb2xhYi5jb20vNjk3MA/SP3d2e8a13-21da-2a19-fb54-c36848840d66.cnf.xml

GET /dWNkZW1vbGFilmNvbS9odHRwL2N1Y20tcHVilNvJzGVtb2xhYi5jb20vNjk3MA/global-settings.xml

GET /dWNkZW1vbGFilmNvbS9odHRwL2N1Y20tcHVilNvJzGVtb2xhYi5jb20vNjk3MA/jabber-config.xml

POST /dWNkZW1vbGFilmNvbS9odHRwcy9pbXAxLnVjZGVtb2xhYi5jb20vODQ0Mw/EPASSoap/service/v80
Cisco Jabber Client Initialization

Base64 decoded HTTPS requests

GET /base64(ucdemolab.com)/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin

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
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://collabedge1e.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://collabedge1e.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
Edge Config & Services (1 of 2)

No need to define this SRV serviceConfig details returned here are a result of Expressway-C DNS SRV lookups

SRV is not required, but may exist when using on-prem IM&P

You will need one or more of _cisco-uds SRV records

The tftpServer entry is an exception, these details are not based on a SRV lookup. Ignore, no longer used by the clients
Every member of the Expressway-E cluster is returned as a sipEdgeServer

One route string is provided to clients for each Expressway-C in the cluster

Every member of the Expressway-E cluster is returned as a xmppEdgeServer

Every member of the Expressway-E cluster is 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.
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”

![Network Log Filter Example]

• 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

- Use the diagnostic logging feature when you want to capture network and event logs in the same file and download for analysis
Appendix B
Expressway Server Certificate Details
Subject Alternative Name (SAN) requirements

Expressway-E Server Certificate

• Customer’s service discovery domain is 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

• This is a security measure that allows clients to verify connections to edge servers authoritative for their domain (RFC 6125)
Unified CM Mixed Mode & Expressway-C SANs

- 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
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

Common name
- Common name: FQDN of Expressway cluster
- Common name as it will appear: cluster.collabedge1.ucdemolab.com

Alternative name
- Subject alternative names
- Additional alternative names (comma separated)
- IM and Presence chat node aliases (federated group chat)
- Unified CM phone security profile names
- Alternative name as it will appear

Only required for XMPP federation

Only required when using encrypted devices with UCM in mixed mode
Expressway-E Certificate Signing Request

<table>
<thead>
<tr>
<th>Generate CSR</th>
<th>You are here: Maintenance ▶ Security certificates ▶ Generate CSR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common name</strong></td>
<td>FQDN of Expressway cluster ▼ i</td>
</tr>
<tr>
<td>Common name as it will appear</td>
<td>collabedge1.ucdemolab.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alternative name</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject alternative names</strong></td>
<td>FQDN of Expressway cluster plus FQDNs of all peers in the cluster ▼ i</td>
<td></td>
</tr>
<tr>
<td><strong>Additional alternative names (comma separated)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Unified CM registrations domains</strong></td>
<td>ucdemolab.com</td>
<td>Format: DNS ▼ i</td>
</tr>
<tr>
<td><strong>XMPP federation domains</strong></td>
<td>ucdemolab.com</td>
<td>Format: DNS ▼ i</td>
</tr>
<tr>
<td><strong>IM and Presence chat node aliases (federated group chat)</strong></td>
<td>lab1MP1.ucdemolab.com, conference-2-ucdemolab/lab1MP1</td>
<td>Format: DNS ▼ i</td>
</tr>
<tr>
<td><strong>Alternative name as it will appear</strong></td>
<td>DNS: collabedge1.ucdemolab.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS: ucdemolab.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS: conference-1-ucdemolab/lab1MP1.ucdemolab.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS: conference-2-ucdemolab/lab1MP1.ucdemolab.com</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<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=Digital Signature Trust Co., CN=DST Root CA X3</td>
<td>O=Cisco Systems, CN=Cisco SSCA2</td>
<td>Oct 22 2015</td>
<td>Valid</td>
<td>View [decoded]</td>
</tr>
<tr>
<td>Certificate</td>
<td>O=Cisco, OU=CTG-TME, CN=Kroarty-lab</td>
<td>Matches Issuer</td>
<td>Jul 18 2016</td>
<td>Valid</td>
<td>View [decoded]</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>
</tr>
</tbody>
</table>

**Upload**

Select the file containing trusted CA certificates

**Append CA certificate**  **Reset to default CA certificate**
# 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>
Single Sign On over Mobile and Remote Access

UC Applications SSO enabled

Expressway-C SSO Enabled

DMZ

Expressway-E SSO Enabled

Circle of Trust

Client

POST SAML Assertion

Resource Request

Resource

Authentication

POST SAML Assertion

IDP Redirection

1

2

3

4

5

6

7

Client

UC Applications SSO enabled

Expressway-C SSO Enabled

DMZ

Expressway-E SSO Enabled

Circle of Trust
New Expressway APIs for Edge SSO

• In order to implement EDGE SSO support Jabber avails of two new API’s on Expressways.

• “get_edge_sso” API enables Jabber to query the Expressways for SSO support. **NOTE:** This API takes the username or discovery address as parameter because the home cluster needs to be located and finally checked for SSO enablement.

• The “authorize” API enables Jabber to request for OAuth tokens to be used for SSO. **NOTE:** Jabber will receive 3 OAuth tokens. More details later
The Browser is the "OAuth Client". The Browser accesses some resources on the Service.

GET /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.

POST /authorize_proxy

The SAML Assertion contains end user is 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.

200OK [access_token] Set-Cookie= SP_Cookie

POST /token/authorize_proxy
Authorization: Basic 3(service-autz secret)
Host: CUCM
Content-Type: application/x-www-from-urlencoded
grant_type=urn:ietf:params:oauth:grant-type:saml2-bearer &assertion=xxx &scope=resource

Simplified Call-Flow
OAuth

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)

Access Token is Provided to Jabber

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)
SSO Resource Request Flowchart

Resource Request → Valid SP Cookie → Access Token Expired

- YES: Set SP Cookie and New Access Token → Resource
- NO: Valid IDP Cookie

- YES: Set SP Cookie and New Access Token → Resource
- NO: Authentication Process

- Authentication Process → Set IDP Cookie

- Set IDP Cookie → Valid IDP Cookie

- NO: Valid SP Cookie → Access Token Expired

- YES: Set SP Cookie and New Access Token → Resource
Edge SSO Timers

A) IdP Session timeout
   - Configured on the IdP (e.g. ADFS2, OpenAM, Ping)
   - 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 D
TelePresence Endpoint Provisioning
TC 7.1 Edge Endpoint Provisioning

Provisioning Wizard

Start
TC 7.1 Edge Endpoint Provisioning

Configure Your TelePresence Unit

Select infrastructure:
- Cisco VCS
- WebEx Telepresence
- Cisco UCM
- Cisco UCM via Expressway

Cancel  Next
TC 7.1 Edge Endpoint Provisioning

Configure Your TelePresence Unit

Infrastructure: Cisco UCM via Expressway
Username: kroarty
Domain: ucdemolab.com
Password: *******

- Delete old certificate files (CTL, ITL)
- Manually override Expressway address

Cancel  Register
TC 7.1 Edge Endpoint Provisioning

Please wait...

Your system is being configured.
Your Cisco EX90 has been registered!

Your Cisco EX90 has now been registered and is ready for use. Your contacts can reach you on the following URI: kroarty@ucdemolab.com

OK
TC 7.1 Edge Endpoint Provisioning
TC 7.1 Edge Endpoint Provisioning

System Upgrade

The system will automatically be upgraded in 53 seconds

The upgrade will make your system unavailable for approximately 5 minutes.

Postpone for 6 hours Upgrade Now