TOMORROW
starts here.

Cisco live!

Federation and Remote Access for Unified Communications Leveraging Collaboration Edge

BRKUCC-2666

Cheyne Mailhot

Consulting Systems Engineer

#clmel

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.

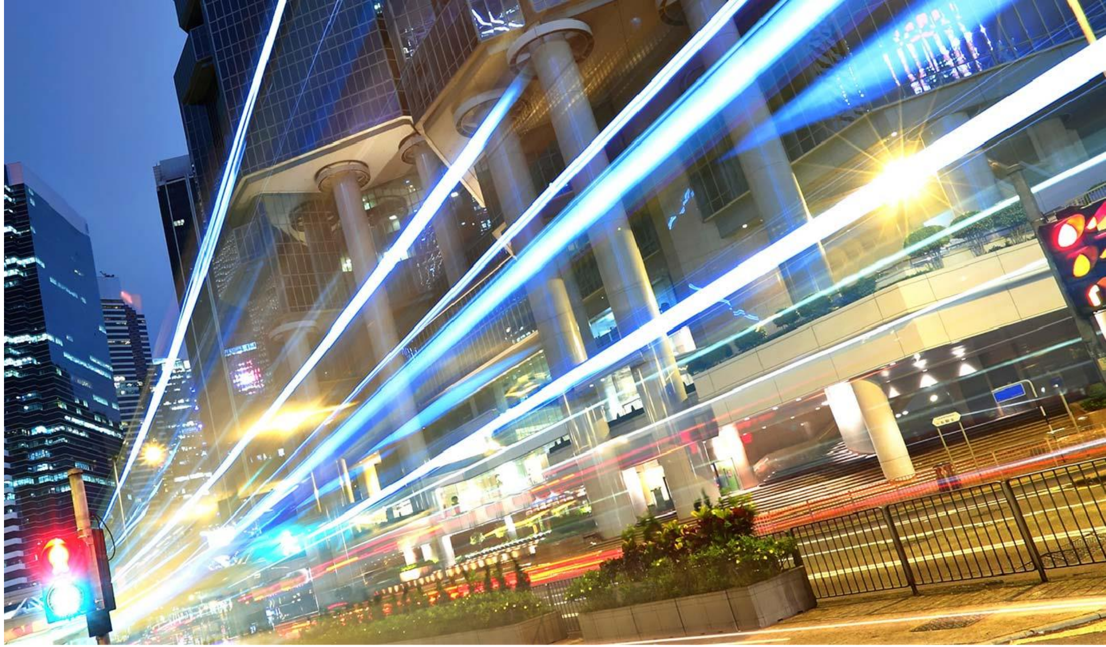
Remote Jabber clients will have access to voice/video, instant messaging and presence, visual voicemail, and directory look-up services.

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
- Expressway Solution Overview
- Product Line Options, Licensing, Scalability
- Design and Deployment Considerations
- Unified CM Requirements
- Authentication & Certificates
- Jabber 10.6 Single Sign On



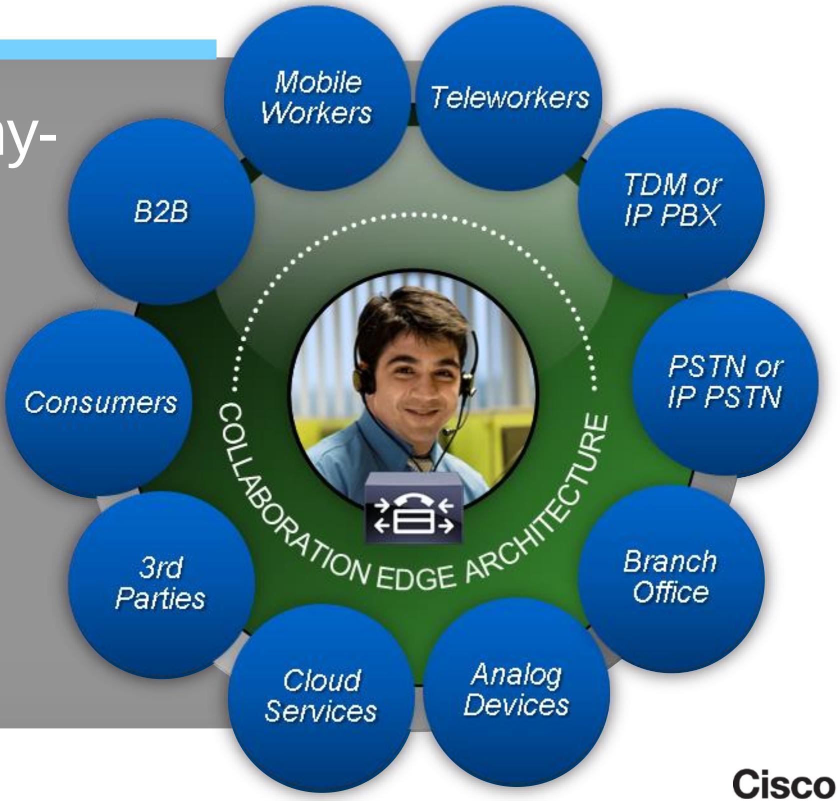
Terminology Introduction

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

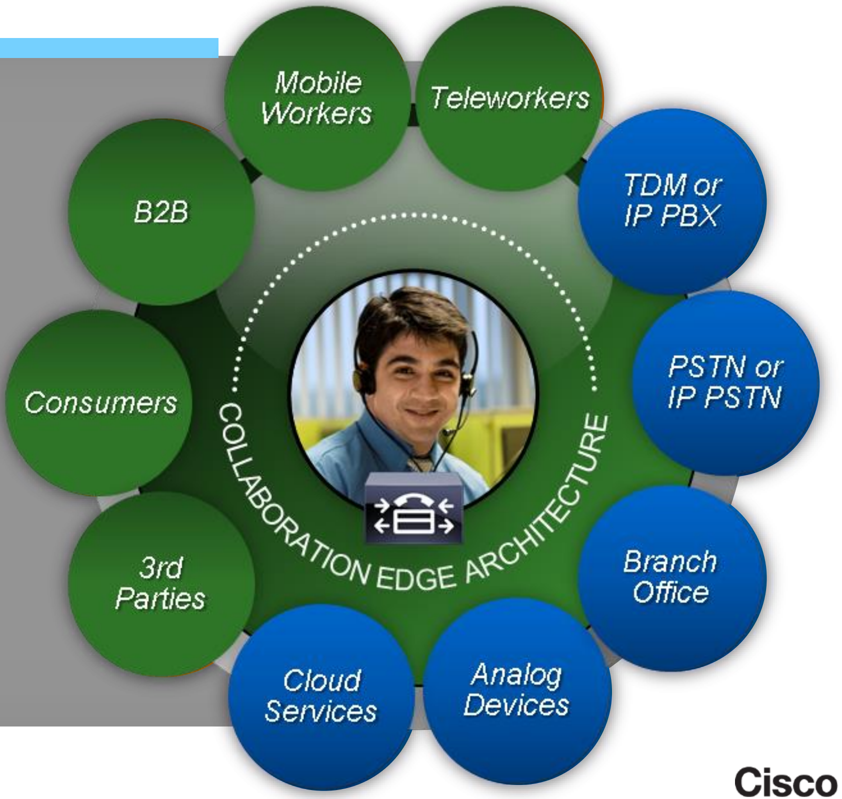
- TDM & analog gateways
- ISDN Video gateways
- Session border control
- Firewall traversal
- Standards-based & secure



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



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 C**ontrol and **VCS E**xpressway

Cisco Expressway

New product line option for Unified CM and Business Edition customers, providing firewall traversal & video interworking. Includes **Expressway C**ore and **Expressway E**dge

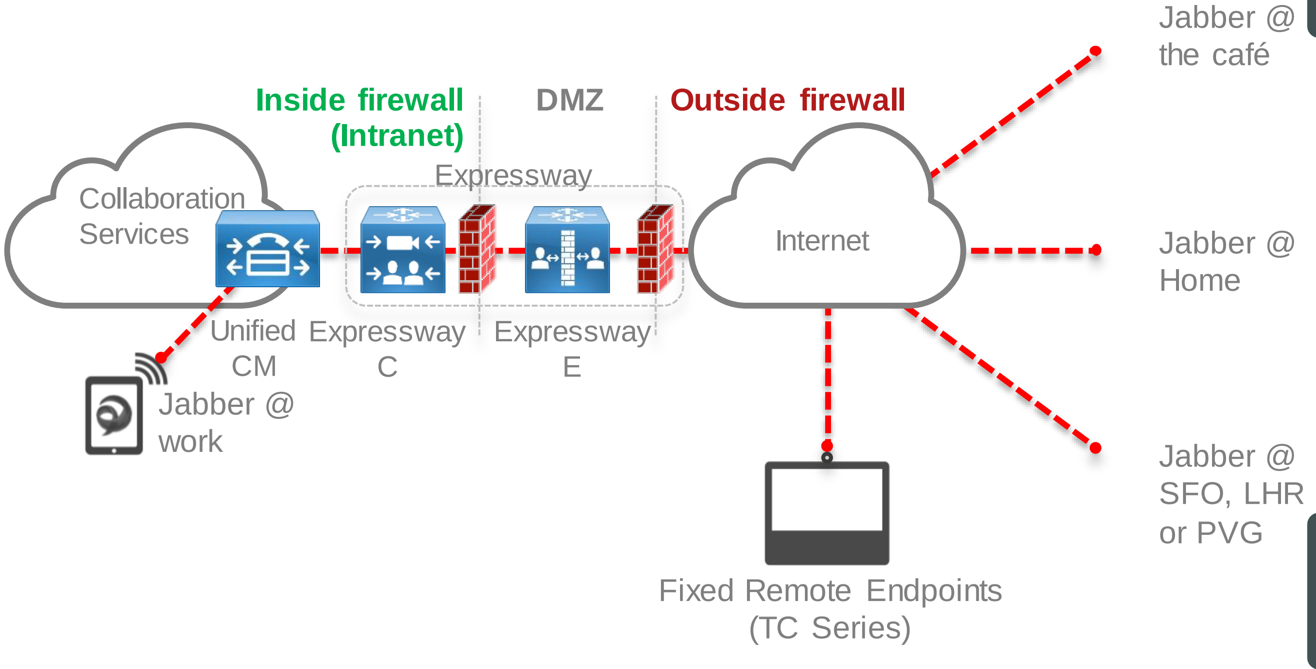
Mobile and Remote Access (MRA)

Feature available on **both** VCS and Expressway product lines with X8 software

Delivers VPN-less access to Jabber and Fixed Endpoints

Expressway Mobile and Remote Access Solution Overview

Mobile and Remote Collaboration with Expressway



Simple, Secure Collaboration: It just works...inside and outside the network, no compromises

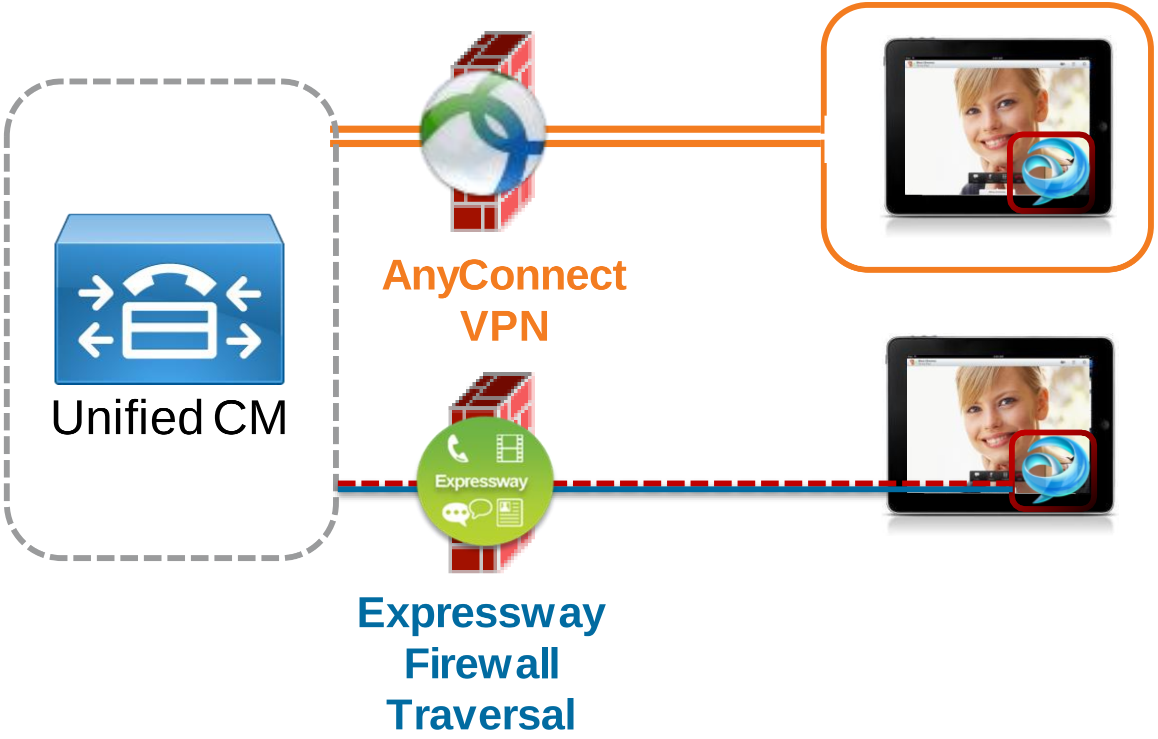
Easy to use, easy to deploy: Works with most firewall policies

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

Cisco Jabber Remote Access Options

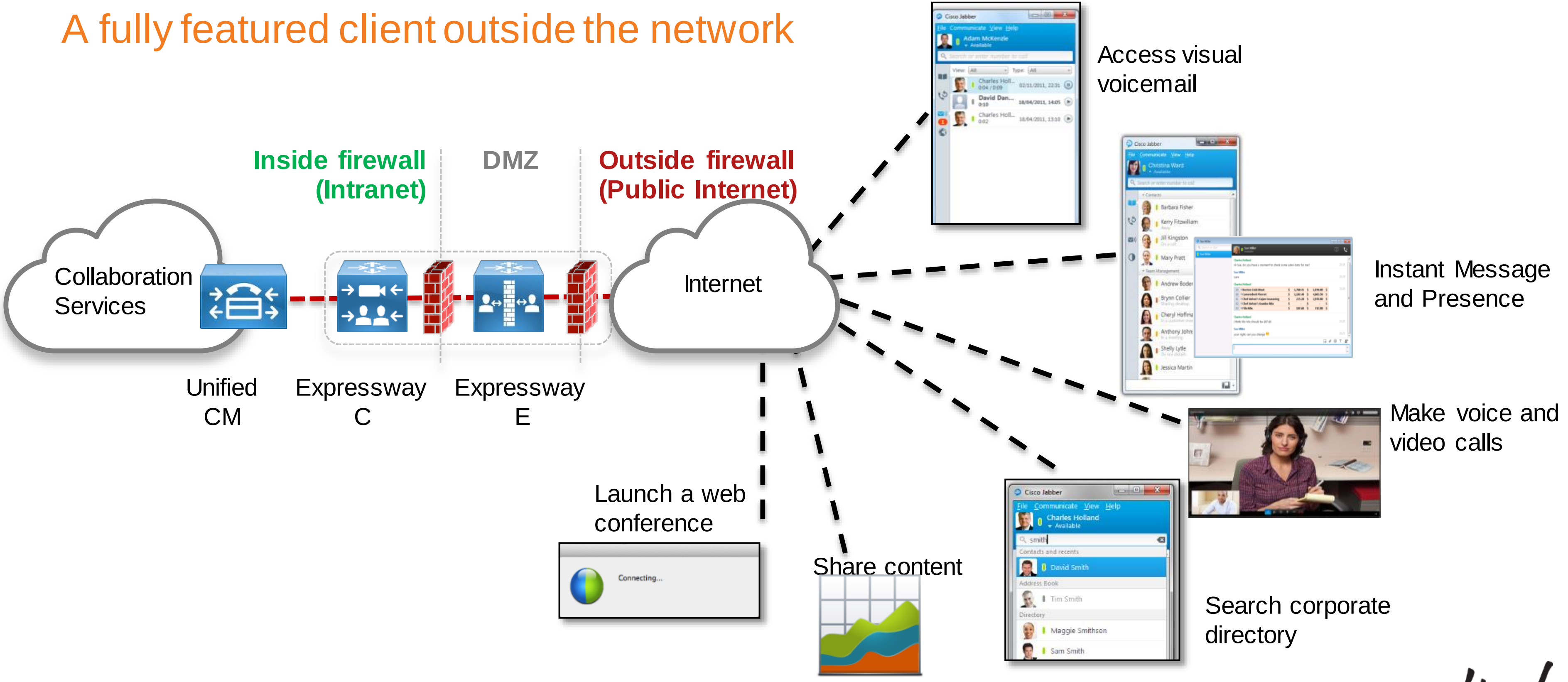


- Layer 3 VPN Solution
- Secures the entire device and it's contents
- AnyConnect allows users access to any permitted applications & data

- **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



Inside firewall (Intranet)

DMZ

Outside firewall (Public Internet)

Collaboration Services

Unified CM

Expressway C

Expressway E

Internet

Access visual voicemail

Instant Message and Presence

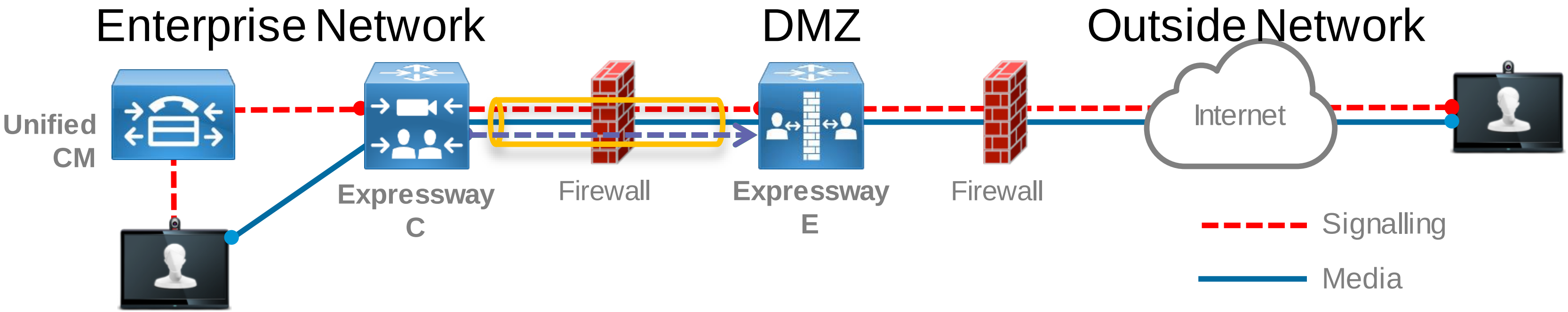
Make voice and video calls

Search corporate directory

Share content

Launch a web conference

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**.

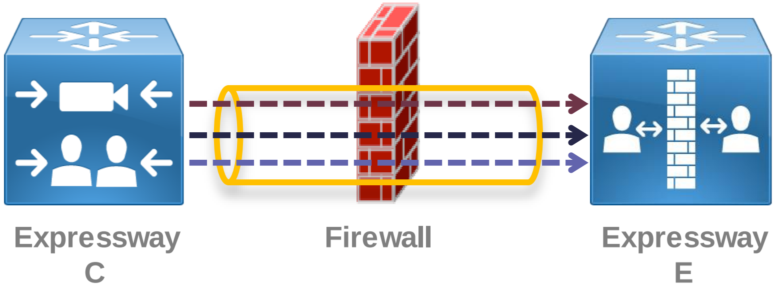
5. **Expressway-C** then routes the call to **Unified CM** to reach the called user or endpoint

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 and Remote Access Support

Minimum Software Requirements

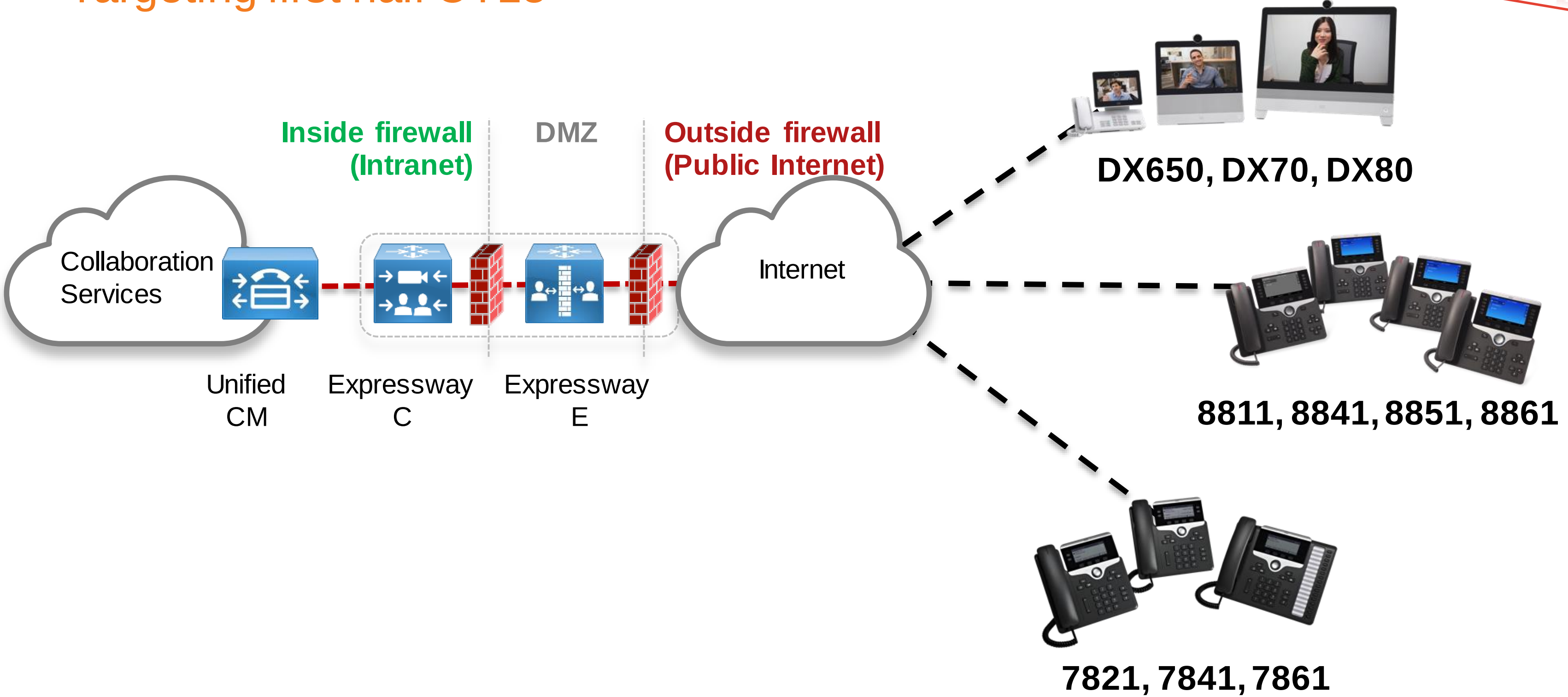
Component	Min Software Version	Projected Availability
Cisco Expressway (or Cisco VCS)	X8.1.1	Available
Unified CM	9.1(2) SU1	Available
Unified CM IM&P	9.1	Available
Unity Connection	8.6(1)	Available
Jabber for Windows	9.7	Available
Jabber for iPhone and iPad	9.6.1	Available
Jabber for Mac	9.6	Available
Jabber for Android	9.6	Available
EX/MX/SX/C Series TelePresence Endpoints	TC 7.1	Available

New Endpoint Support
Expressway Mobile & Remote Access

New Endpoint Support

Targeting first half CY15

TARGET DATES SUBJECT TO CHANGE



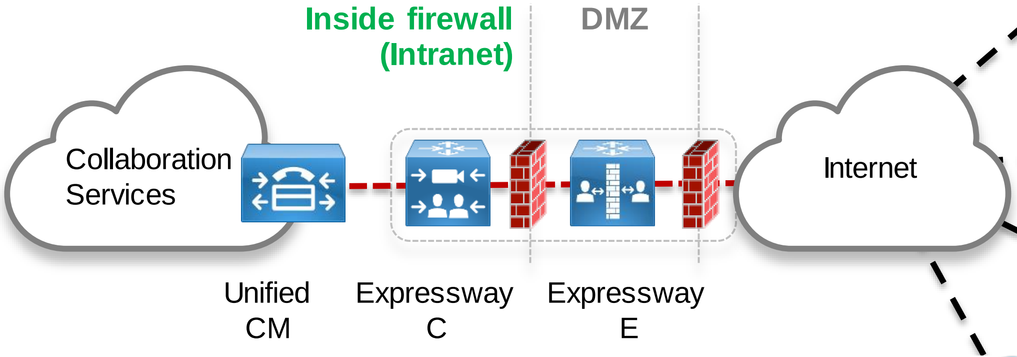
Target Use Case

DX Series + Expressway

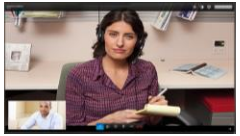
- Remote access for the collaboration desktop experience
- Ideal for teleworkers or employees that need flexibility to occasionally work from home to collaborate across time zones
- Allows remote workers to engage in rich multi-collaborative experience
- Alternative to AnyConnect VPN
- Expressway provides 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

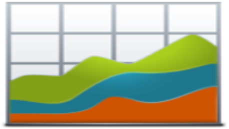
with Cisco Expressway



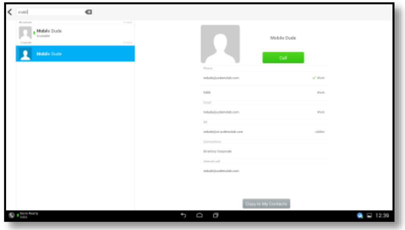
Voice and video calling, including content share



+



Search corporate directory



mobi

Mobile Dude
Available

Mobile Dude

Mobile Dude

Call

Phone

Work

Work

Email

Work

IM

Jabber

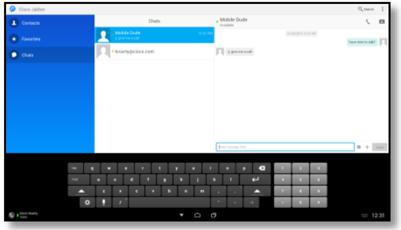
Directory: Corporate

Internet call

Copy to My Contacts

12:39

Instant Message and Presence, including escalation to Voice/Video



Cisco Jabber

Search

Contacts

Favorites

Chats

Mobile Dude
y, give me a call

kroarty@cisco.com

Mobile Dude
Available

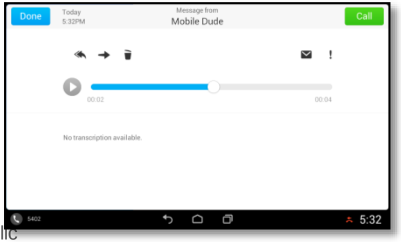
have time to talk?

y, give me a call

Send

12:31

Visual voicemail



Done

Today
5:32PM

Message from
Mobile Dude

Call

00:02

00:04

No transcription available.

5402

5:32

Target Feature Set

DX Series + Expressway

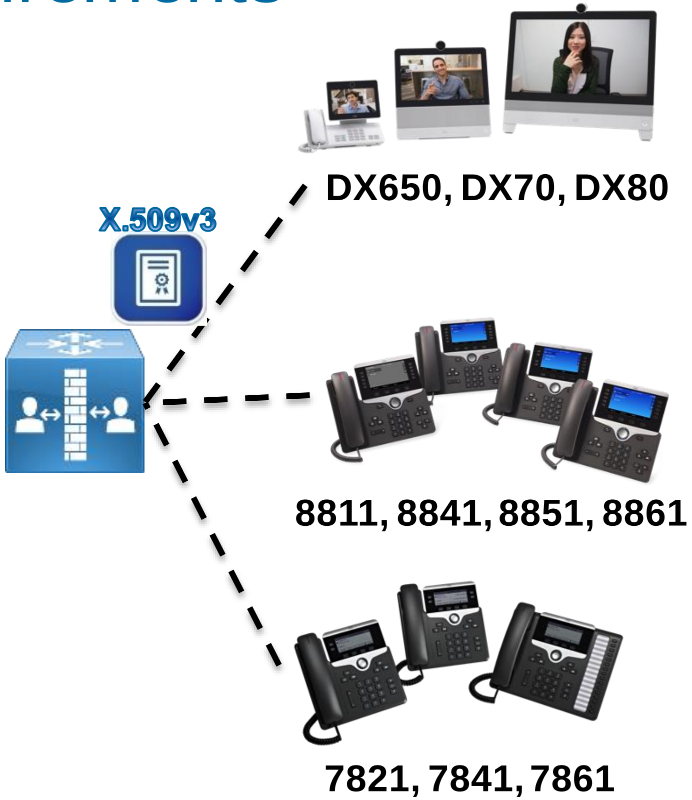
SUBJECT TO CHANGE

- 1080P 30fps HD video, plus BFCP content share/receive
- Single line support, with early media
- Encrypted signalling 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

Component	Min Software Version	Projected Availability
Cisco Expressway (or Cisco VCS)	X8.5.x	Target 1H CY15
Unified CM	9.1(2) SU1	Available
7821, 7841, 7861 IP Phones	10.3.1	Target 1H CY15
8811, 8841, 8851, 8861 IP Phones	10.3.1	Target 1H CY15
DX650, DX70, DX80 Collaboration Endpoints	10.2.4	Target 1H CY15

TARGET DATES SUBJECT TO CHANGE

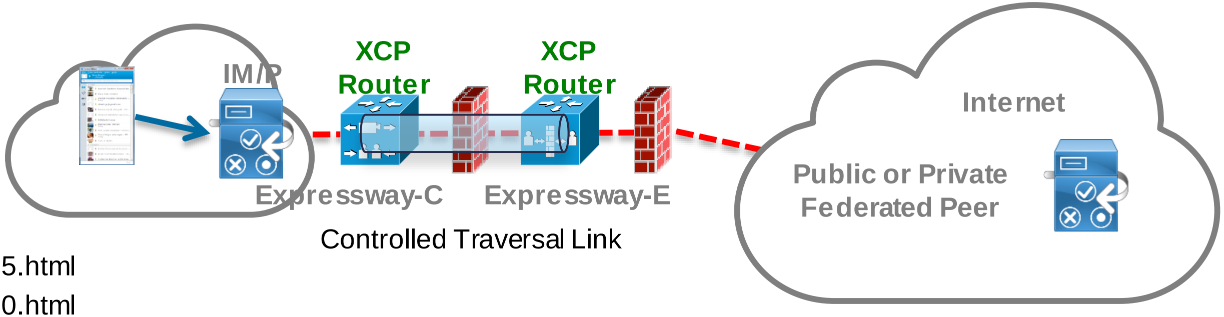
XMPP Federation Over Expressway

XMPP Federation Over Expressway

- ✓ Customers commonly need to federate either to a partner or subsidiary, or make IM&P server publically available
- ✓ Federation to all standard XMPP Clouds

Solution: Instant Message & Presence XMPP Federation over Edge

- Relies on firewall traversal technologies. No Firewall Punch holes



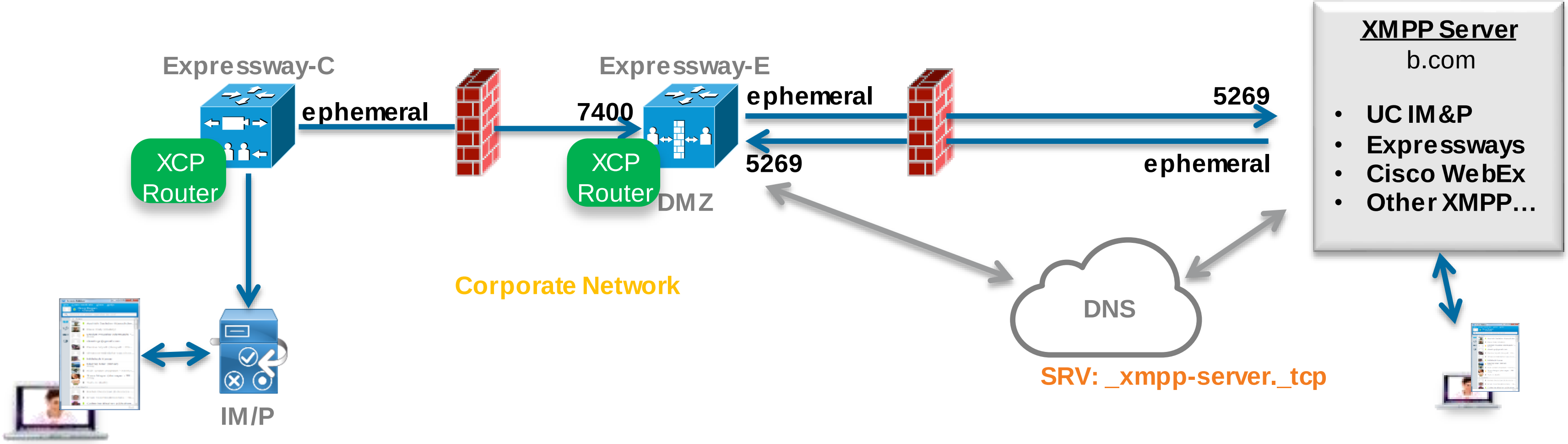
XMPP References

- http://tools.ietf.org/html/rfc3920
- http://tools.ietf.org/html/rfc3921
- http://xmpp.org/extensions/xep-0185.html
- http://xmpp.org/extensions/xep-0220.html
- http://xmpp.org/extensions/xep-0045.html

XMPP Federation Over Expressway

✓ Deploying Expressway for external XMPP Federation

- External XMPP federation enables users registered to Unified CM IM & Presence Server to communicate via the Expressway-E with users from a different XMPP deployment
- IM&P federation can eventually enhance possibility of B2B A/V escalation.



mike@b.com

XMPP Federation Support

Minimum Software Requirements

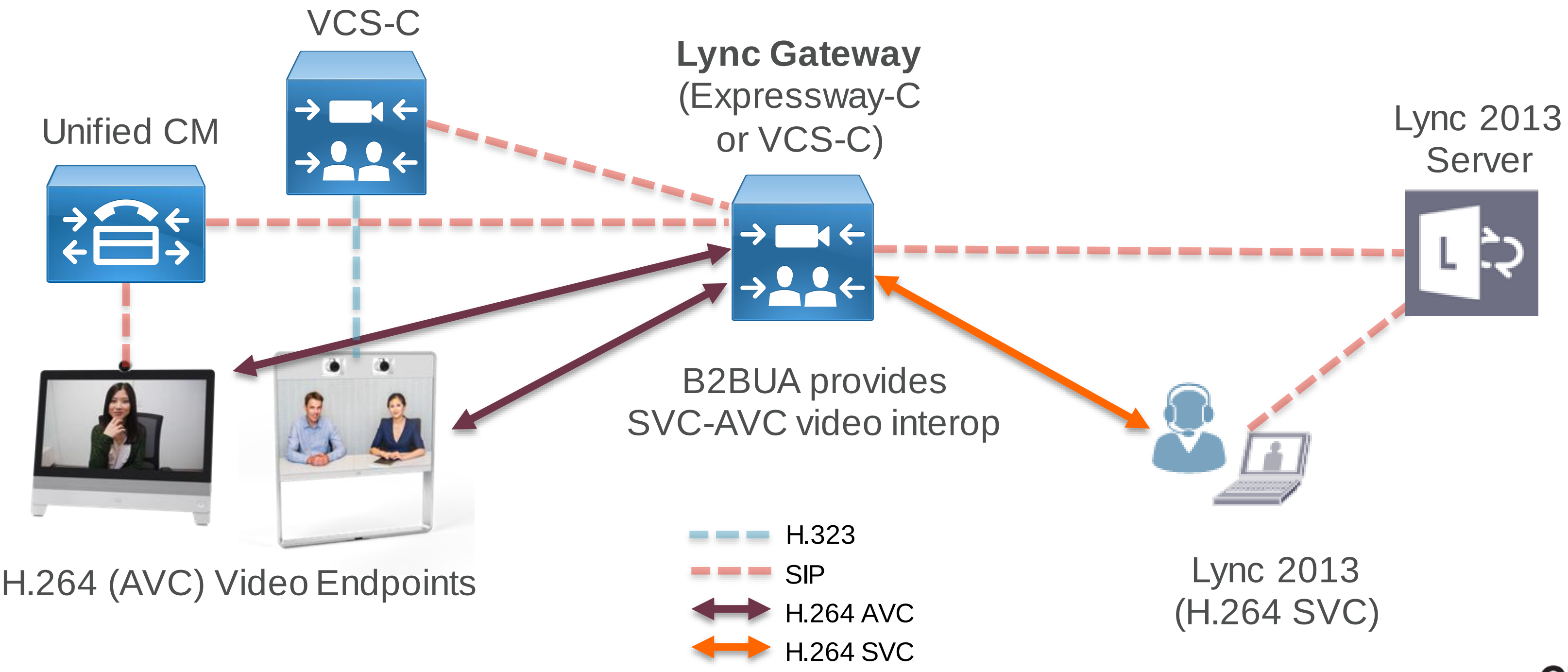
Component	Min Software Version	Projected Availability
Cisco Expressway (or Cisco VCS)	X8.2	Available
Unified CM	9.1(2)	Available
Unified CM IM&P	9.1(1)	Available
Jabber for Windows	9.7	Available
Jabber for iPhone and iPad	9.6.1	Available
Jabber for Mac	9.6	Available
Jabber for Android	9.6	Available
WebEx Connect	6.0	Available

Federate with WebEx Messenger cloud or any standards based XMPP server

Lync 2013 Video Interworking

Lync 2013 Video Interop Solution

SVC-AVC Gateway – 720p HD Video interop without transcoding



Lync 2013 Video Interop

Deployment Considerations

- Lync gateway function can be performed by either VCS-C or Expressway-C and supports up to 100 simultaneous calls.
- Only the VCS-C includes FindMe capability, which provides richer presence and enhances the integration
- Expressway-C is typically used as a Lync Gateway when providing interop with room based telepresence systems (not directly associated with users)
- One Lync Gateway Cluster per Lync domain
- Best practice is to dedicate VCS-C (or Expressway-C) to the Lync Gateway function
- Note: Lync Gateway function cannot exist on an Expressway-C or VCS-C used for Mobile and Remote Access

Lync 2013 Video Interop Support

Minimum Software Requirements

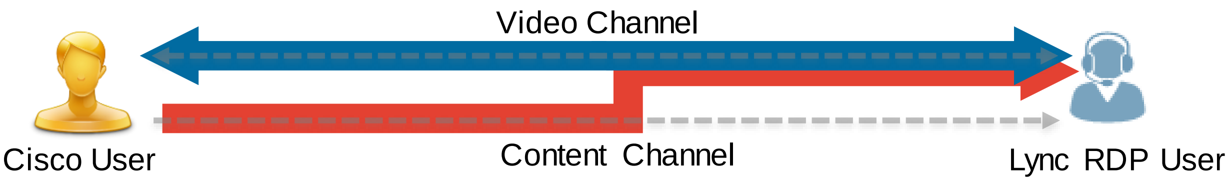
Component	Min Software Version	Projected Availability
Cisco Expressway (or Cisco VCS)	X8.1	Available
Microsoft Lync	2013	Available

Video Interop with Lync 2010 requires the Cisco Advanced Media Gateway (AMG)
Lync 2013 video interop does not require the AMG

Cisco TelePresence and Lync Interop for Content

Limitation: One Way Content Sharing Only

- Lync can't send content as video or share applications with standards-based endpoints
- Lync can receive applications and content embedded in video from standards-based endpoints

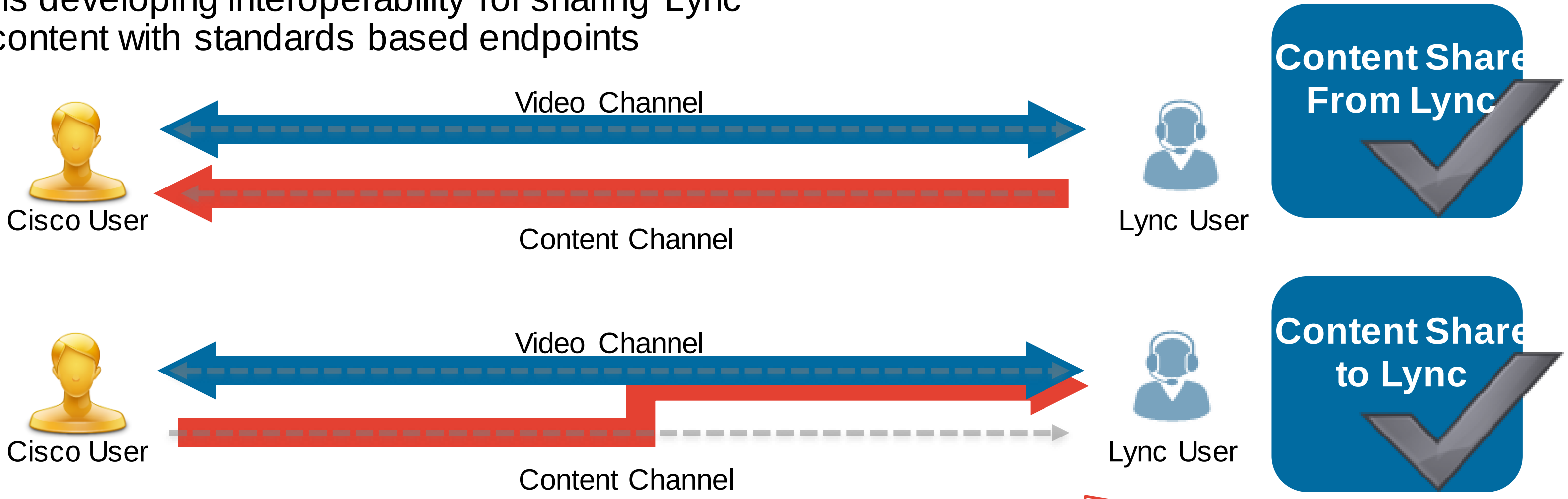


Two way HD video
One way content share
(content in video channel)

Cisco TelePresence and Lync Interop for Content

Solution

Cisco is developing interoperability for sharing Lync RDP content with standards based endpoints

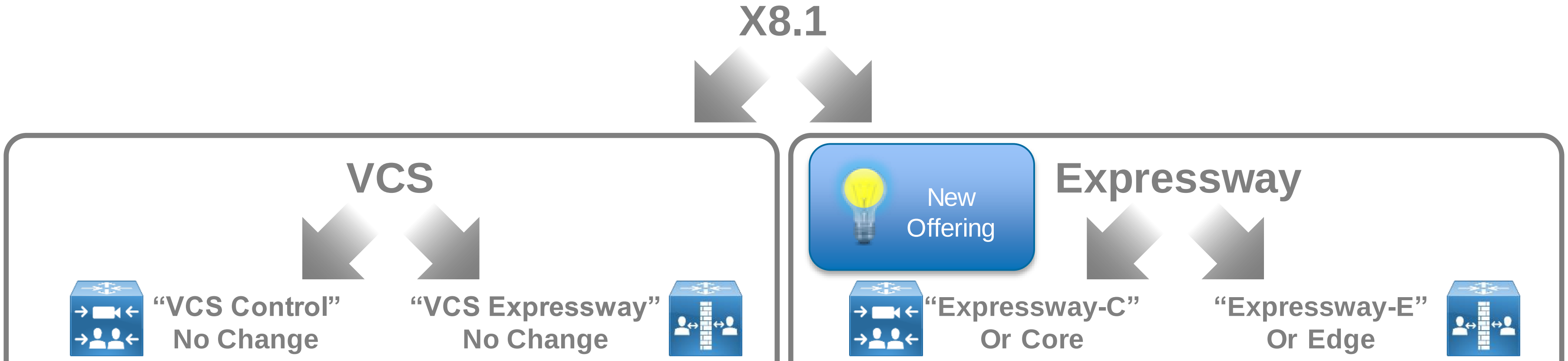


Two way HD video
Two way content share
Via Cisco Expressway (or VCS)

COMING IN 2015

Product Line Options, Licensing, Scalability

Product Line Options



X8.1

VCS

“VCS Control”
No Change

“VCS Expressway”
No Change

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

New Offering

Expressway

“Expressway-C”
Or Core

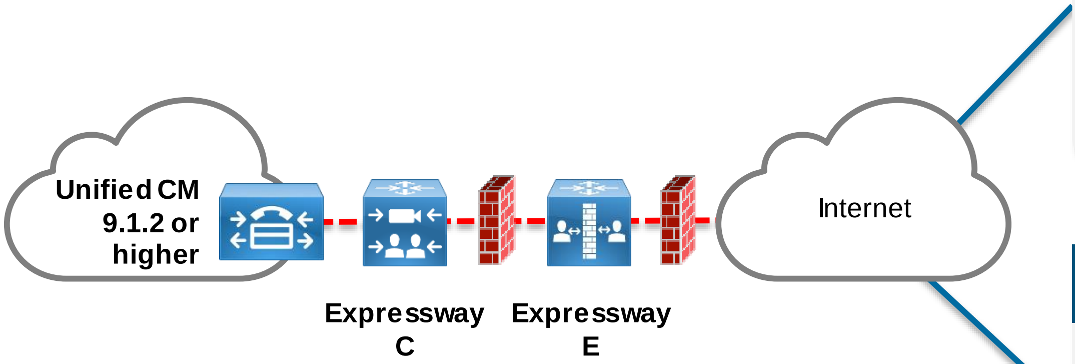
“Expressway-E”
Or Edge

- 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

Feature Comparison	Cisco Expressway Series	Cisco VCS Family
Mobile and Remote Access	Y	Y
Business to Business Video	Y	Y
Business to Consumer / Public to Enterprise Access with Jabber Guest	Y	Y
Video Interworking (IPv4 to IPv6, H.323-SIP, MS H.264 SVC-AVC, Standards-based 3rd Party Video endpoints)	Y	Y
Video / TelePresence Device Registration & Provisioning	N	Y
Video Session Management & Call Control	N	Y
CMR Cloud/Hybrid	Y	Y
XMPP Federation	Y	Y

Cisco Expressway Licensing



Fixed and Mobile Users at no additional cost

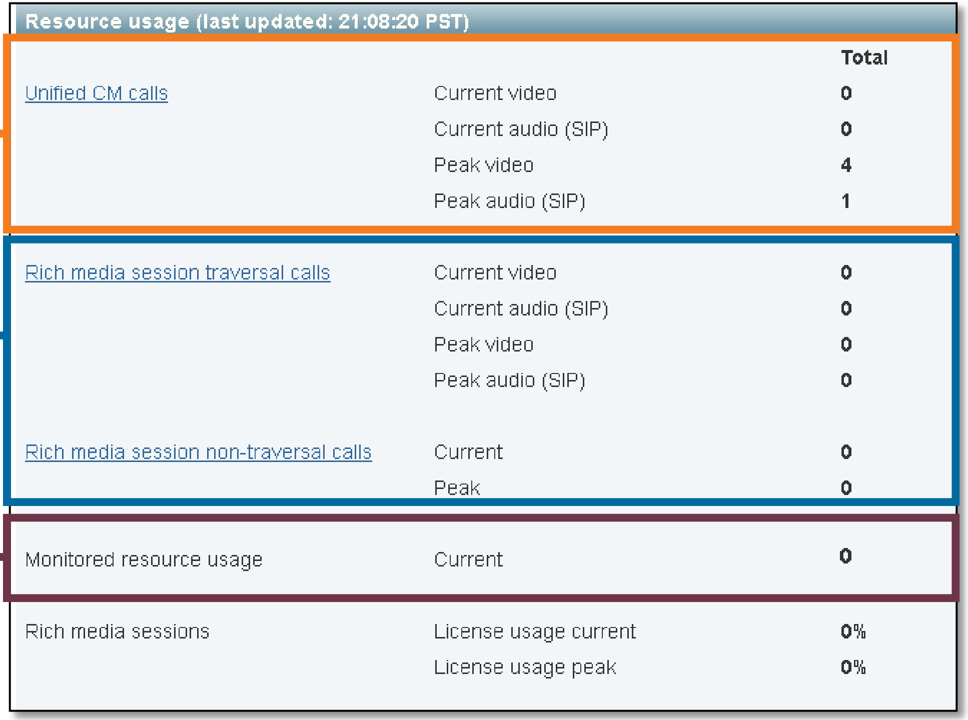
- Mobile and Fixed Endpoint registration
- IM & Presence
- Video and Audio Media Sessions
- Includes Virtual Edition Expressway Server Software
- **No Cost with Unified CM 9.1.2 or later**

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 (last updated: 21:08:20 PST)

		Total
Unified CM calls	Current video	0
	Current audio (SIP)	0
	Peak video	4
	Peak audio (SIP)	1
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
Rich media sessions	License usage current	0%
	License usage peak	0%

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

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

Compute Platform Options

Specs Based Virtual Machine Support

OVA Size	vCPU	Reserved RAM	Disk Space	vNIC(s)
Small	2 x 1.8 GHz	4GB	132GB	1Gb
Medium	2 x 2.4 GHz	6GB	132GB	1Gb
Large	8 x 3.2 GHz	8GB	132GB	10Gb

Appliance Support

New Offering

CE 500

CE 1000

- 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

	Server			Cluster		
Platform	MRA Registrations	Video Calls	Audio Only Calls	MRA Registrations	Video Calls	Audio Only Calls
Large OVA, CE1000	2,500	500	1,000	10,000	2,000	4,000
Medium OVA, CE500	2,500	100	200	10,000	400	800
Small OVA (BE6000)	2,500	100	200	2,500	100	200

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

License Description	PID	Expressway-C (EXPWY-VE-C-K9)	Expressway-E (EXPWY-VE-E-K9)
X8 Release Key	LIC-SW-EXP-K9	Included	Included
Expressway Series	LIC-EXP-SERIES	Included	Included
H323-SIP interworking Gateway	LIC-EXP-GW	Included	Included
Traversal Server Feature Set	LIC-EXP-E	N/A	Included
Advanced Networking Option	LIC-EXP-AN	N/A	Included
TURN Relay Option	LIC-EXP-TURN	N/A	Included
Expressway Rich Media Session	LIC-EXP-RMS	Optional	Optional
Microsoft Interoperability Option	LIC-EXP-MSFT	Optional	N/A

CMR Cloud + Expressway Traversal Sessions

Who	▪ For Cisco® based video deployments ▪ Cisco UCM (and BE) with Expressway C and E or VCS+ Expressway
What	▪ Long term: Connect to CMR Cloud through Expressway without needing licenses with CSR 11 (mid-2015) ▪ Short term: Get 125 time-bound traversal session licenses for every block of 250 CMR Cloud users
Where and When	▪ GPL Named Host using CCW ▪ GPL Active User, Employee Count using A2Q ▪ GRA Named Host, Active User, Employee Count using A2Q ▪ Current customers who already ordered CMR Cloud using A2Q
Why	▪ Simplify the CMR Cloud sales process ▪ Improve the customer purchase experience ▪ Lower total cost of the Cisco® end-to-end solution

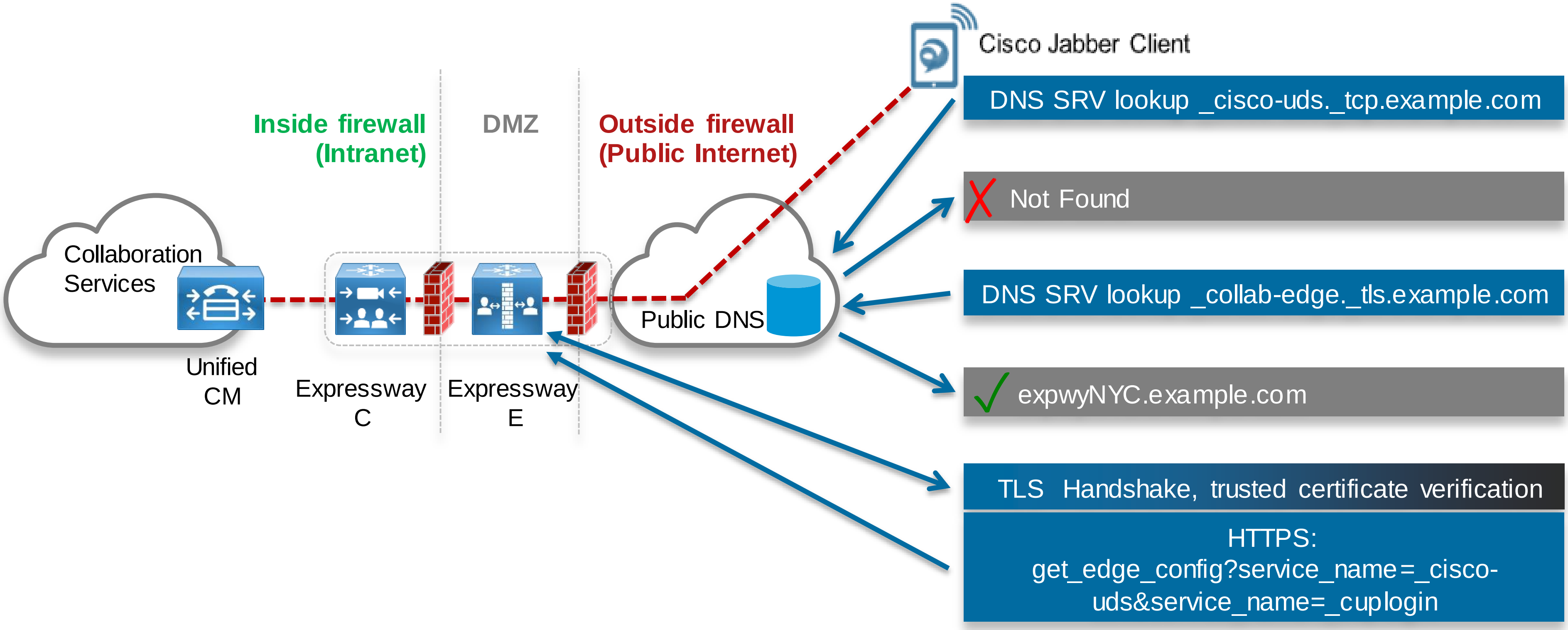
Example

Buy CMR Cloud Licenses	**Get Traversal Sessions**
1-250	125
251-500	250
501-750	375
….	…..
8001-8250	4125

Each traversal session = 2 RMS licenses

Design and Deployment Considerations

Expressway and Jabber Service Discovery



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

Split DNS SRV Record Requirements

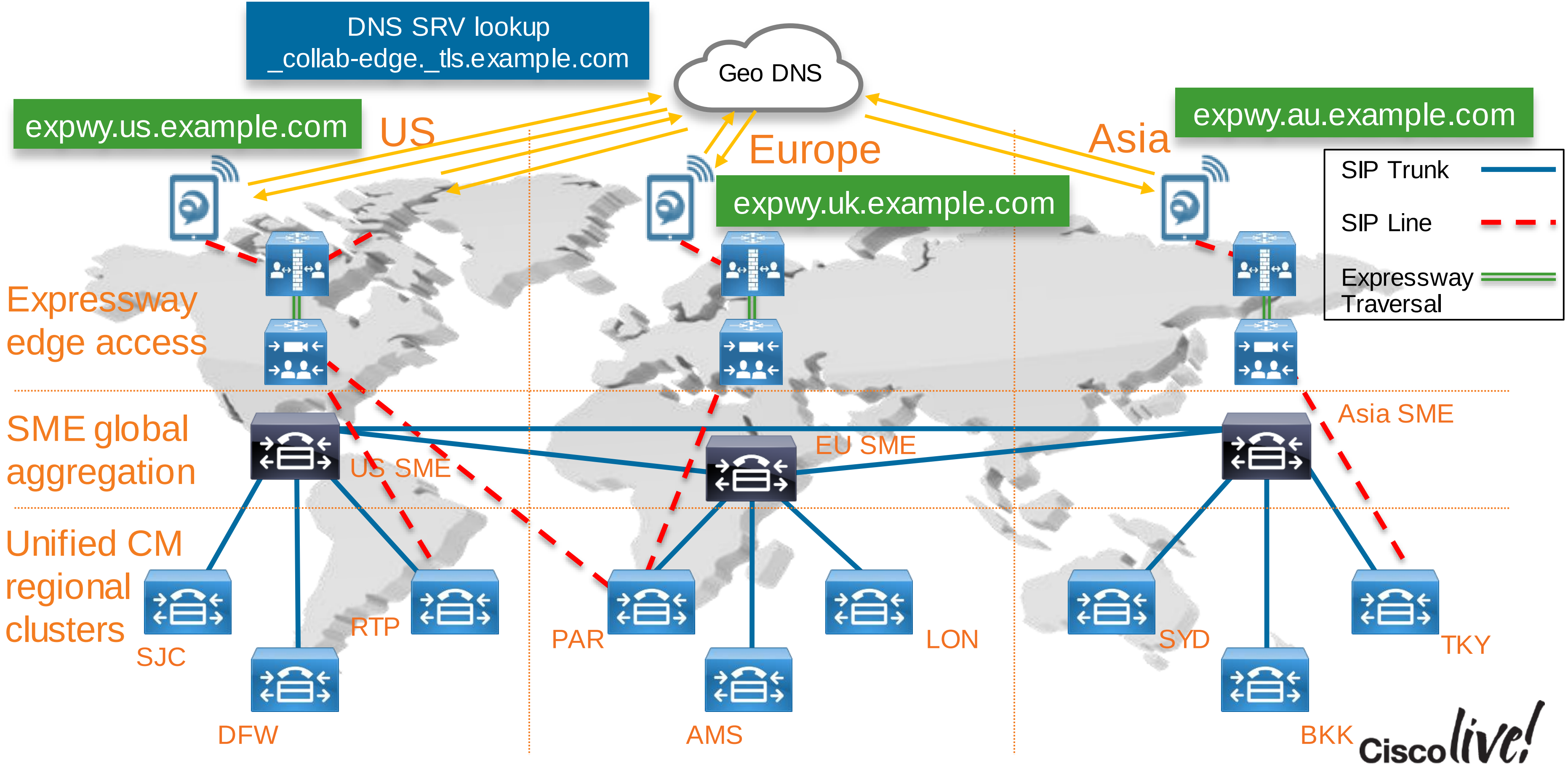
- **_collab-edge** record needs to be available in **public** DNS
- Multiple SRV records (and Expressway-E hosts) should be deployed for HA
- A GEO DNS service can be used to provide unique DNS responses by geographic region

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

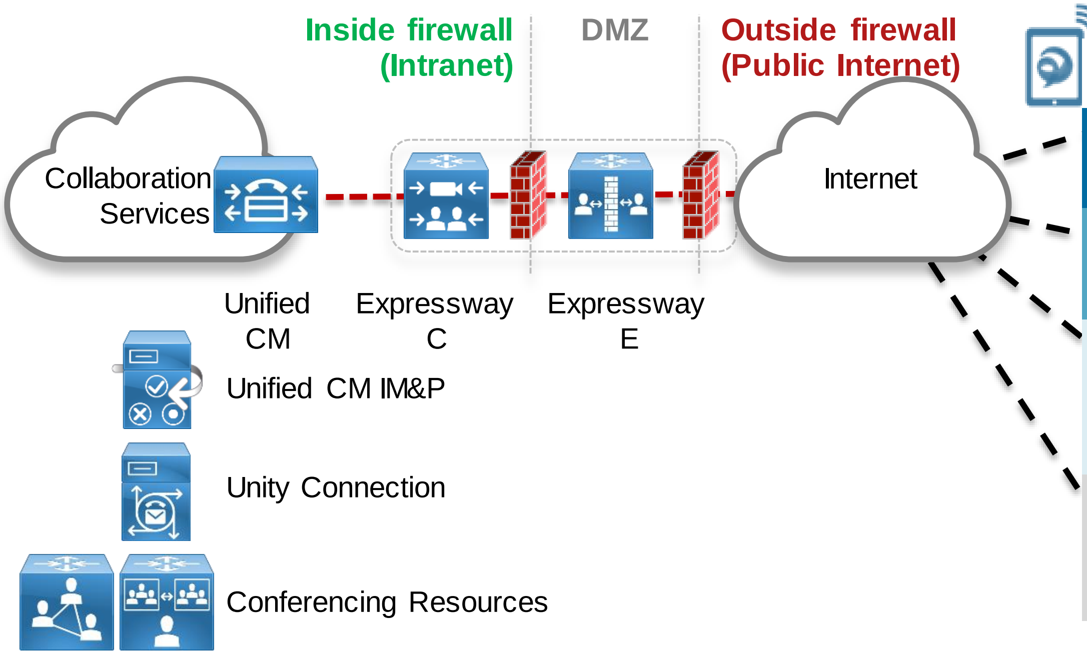
- **_cisco-uds** record needs to be available **only** in **internal** DNS

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

Global Deployment Topology and Geo DNS

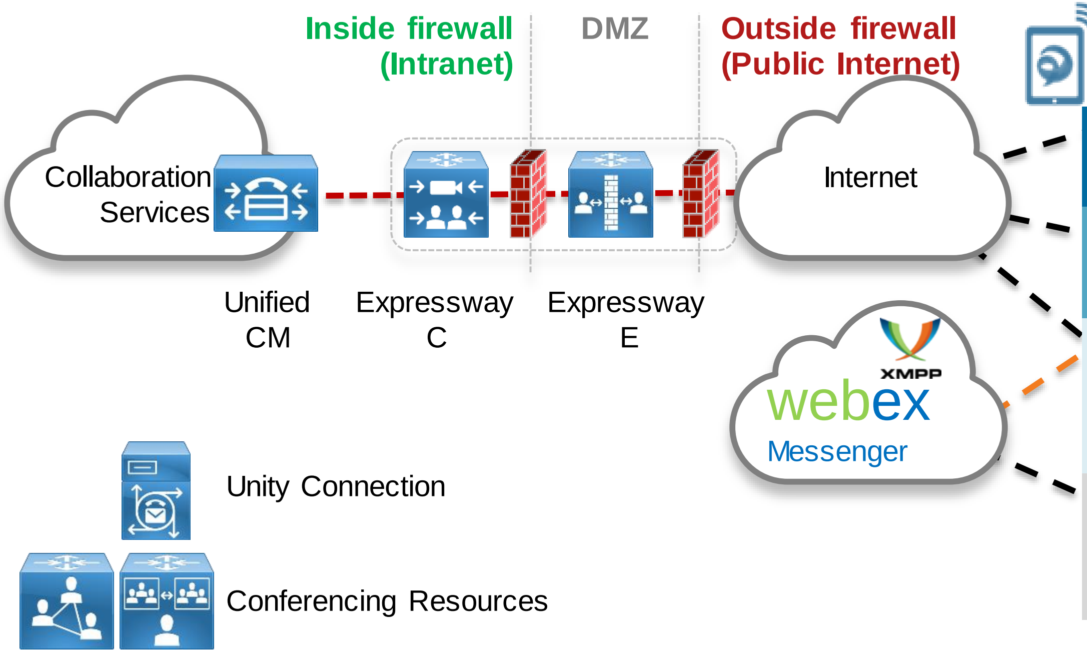


Protocol Workload Summary



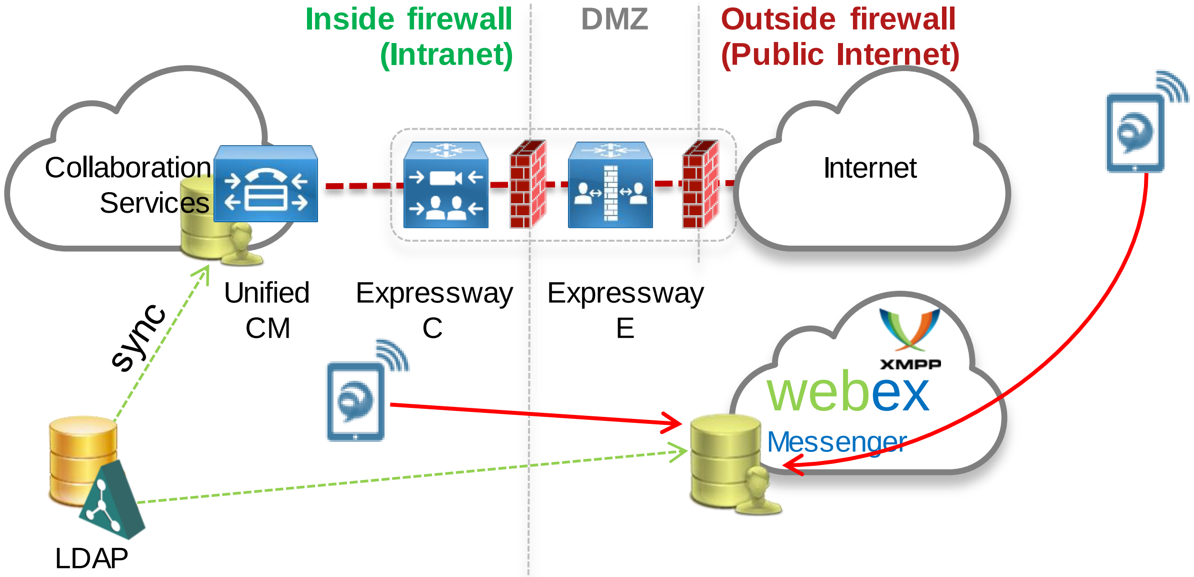
Protocol	Security	Service
SIP	TLS	Session Establishment – Register, Invite, etc.
Media	SRTP	Audio, Video, Content Share, Advanced Control
HTTPS	TLS	Logon, Provisioning/Configuration, Contact Search, Visual Voicemail
XMPP	TLS	Instant Messaging, Presence

Hybrid Deployment - Cloud Based IM&P



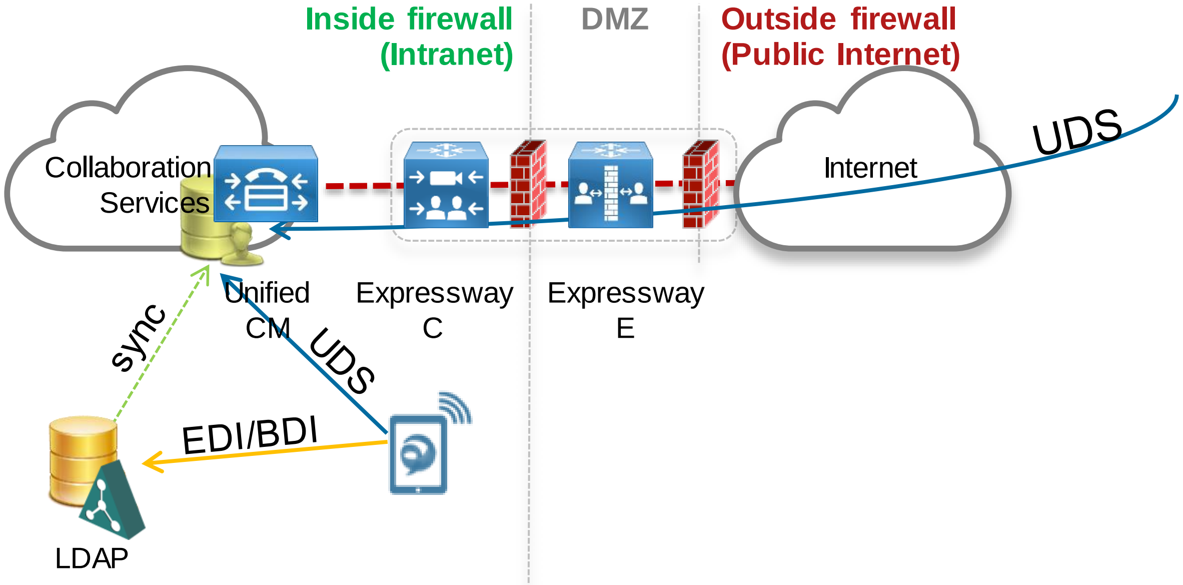
Protocol	Security	Service
SIP	TLS	Session Establishment – Register, Invite, etc.
Media	SRTP	Audio, Video, Content Share, Advanced Control
HTTPS	TLS	Logon, Provisioning/Configuration, **Contact Search**, Visual Voicemail
XMPP	TLS	Instant Messaging, Presence

Contact Search Considerations (Cloud Based IM&P)



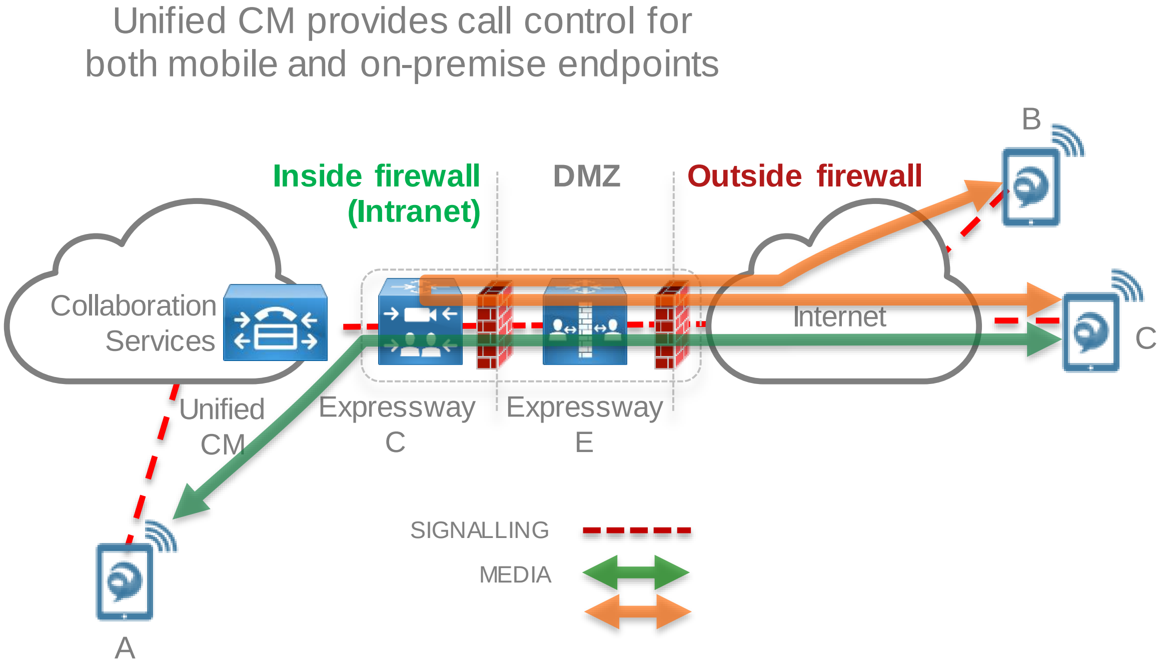
- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to Unified CM
- Corporate directory is also exported to WebEx Messenger cloud
- All Jabber clients will use WebEx Messenger cloud as a contact source for contact search

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



Media Traversal

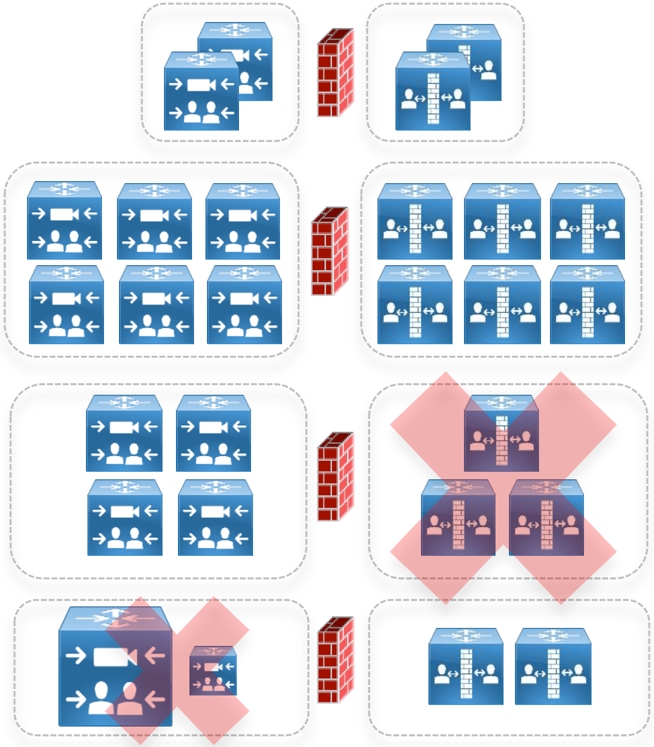
- Call between "C" and "A" on-premise
- Expressway provides firewall traversal for signalling & media
- Expressway-C de-multiplexes media and forwards toward "A"
- Media stream always SRTP encrypted between "C" and Expressway-C
- Media stream only SRTP encrypted between "A" and Expressway-C when both 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



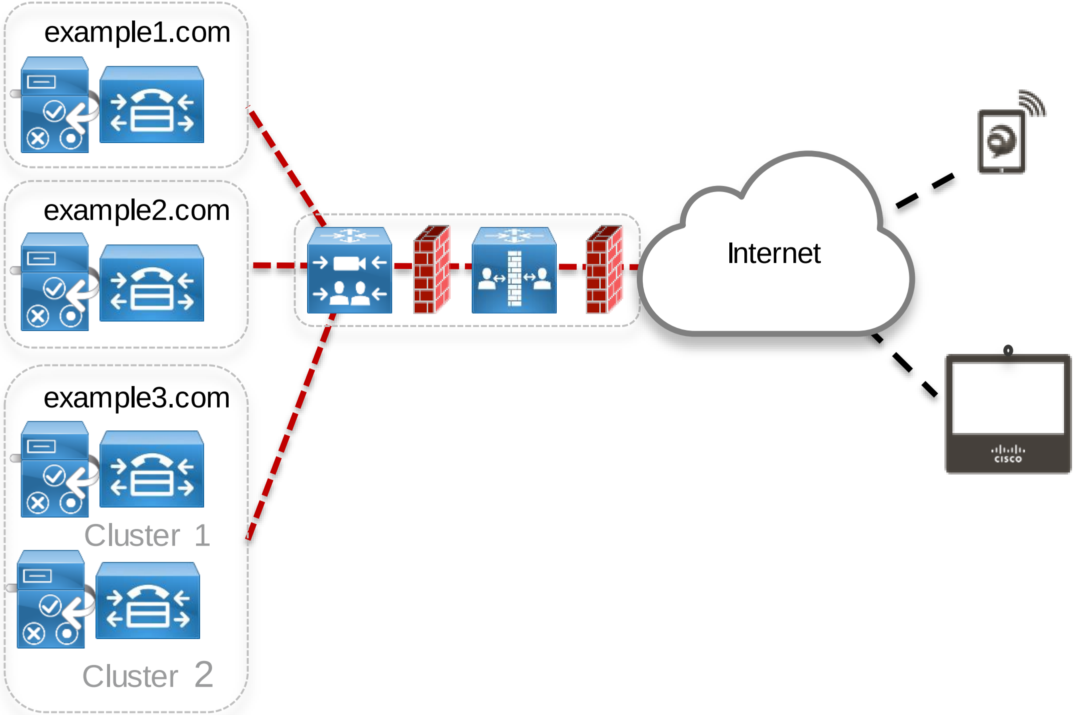
Mobile and Remote Access Deployment Options

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

Unified CM Clusters	Expressway-C Clusters	Expressway-E Clusters	Comments
1	1	1	Single Expressway deployment providing remote access to a central Unified CM cluster
1	2+	2+	Regional Expressway deployments providing remote access to a central Unified CM cluster
2+	1	1	Single Expressway deployment providing remote access to a multiple Unified CM clusters
2+	2+	2+	Regional Expressway deployments providing remote access to multiple Unified CM Clusters

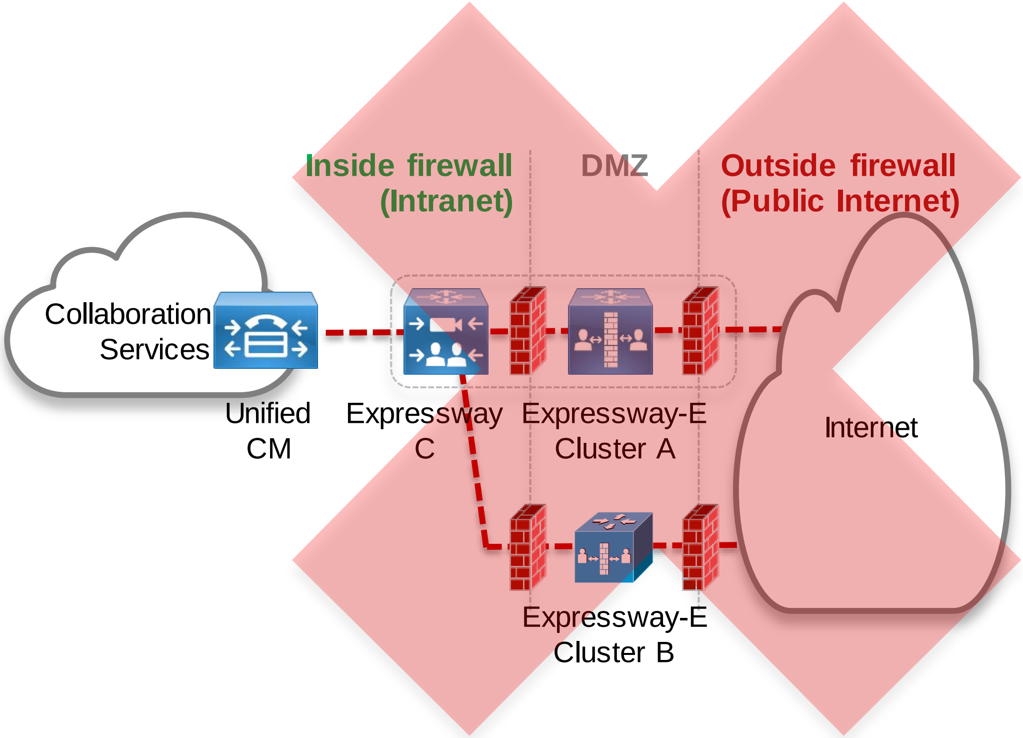
Multi-Deployment Support

New feature in X8.5



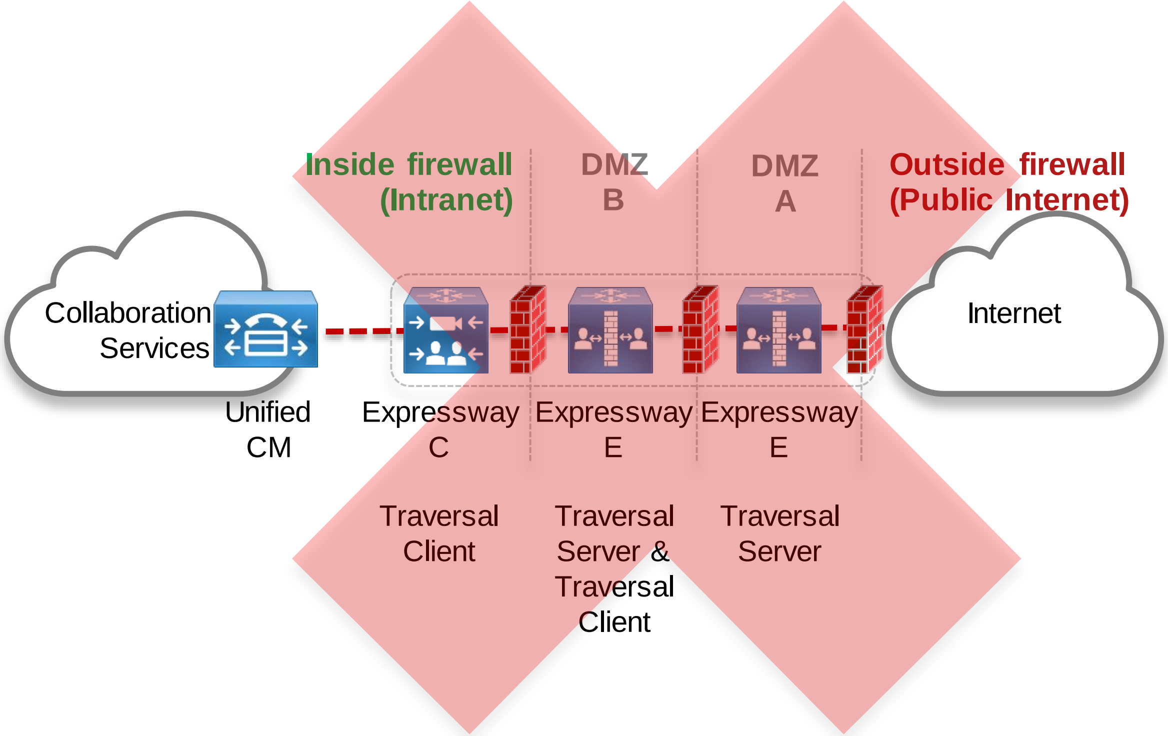
- Single Expressway pair can now serve multiple domains
- Deployments partition UC services available to mobile and remote access (MRA) users
- Not a multi-tenant architecture
- Single certificate presented by Expressway-E needs to contain multiple domain names

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**

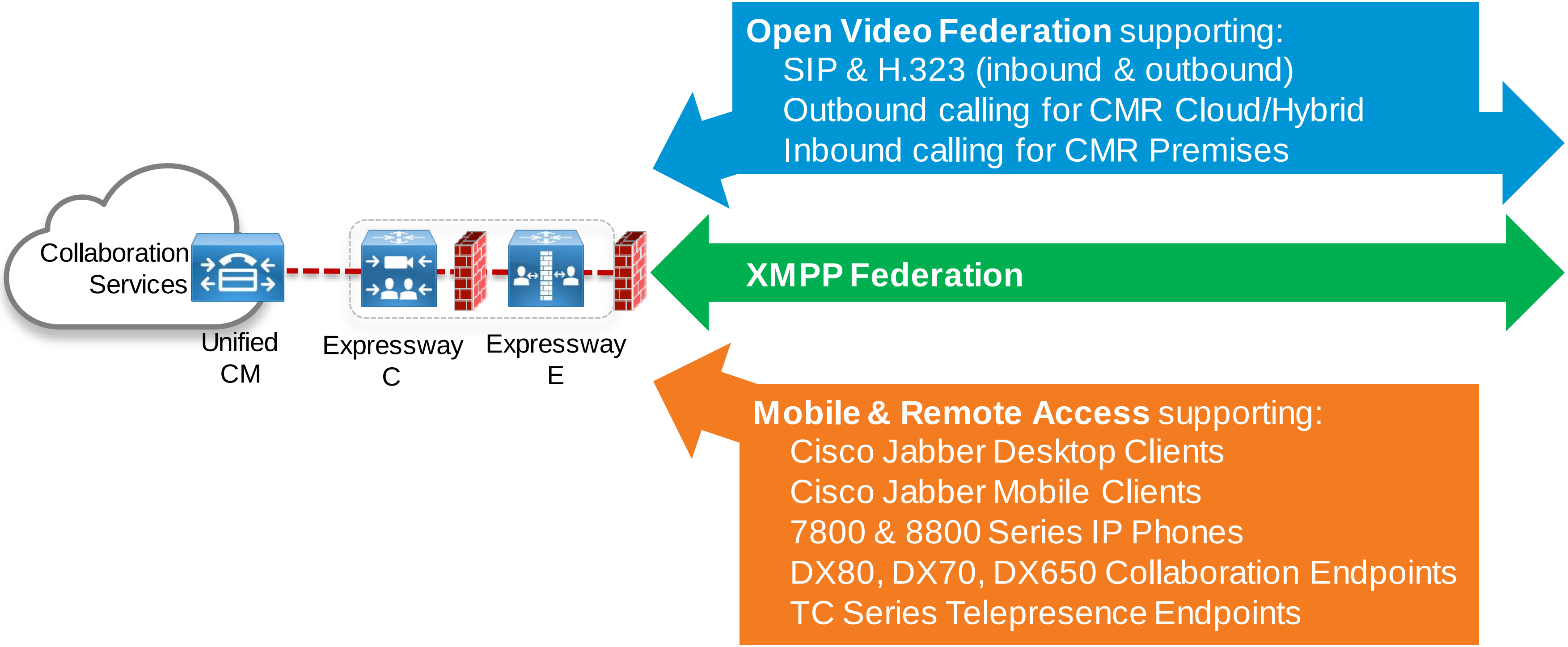
Unsupported: Expressway Chained Traversal



- 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



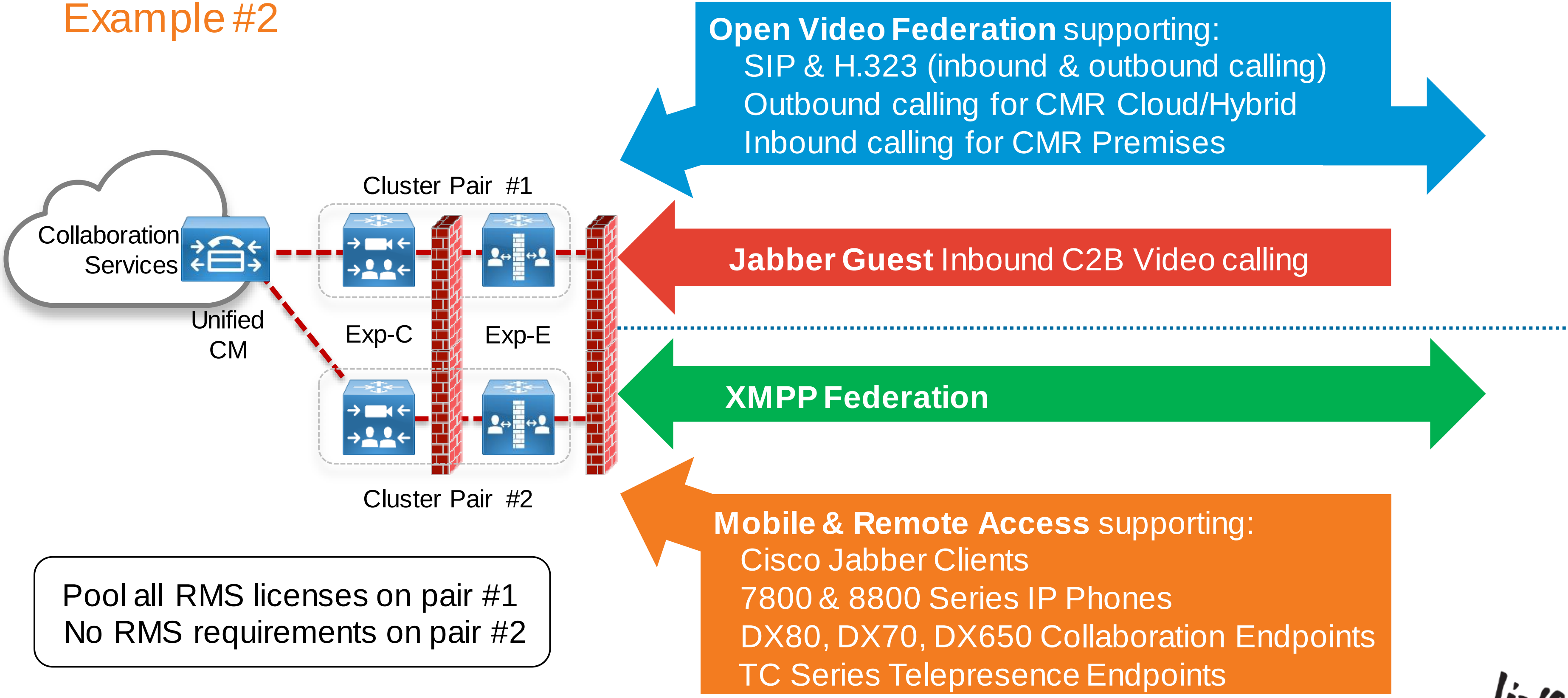
Open Video Federation supporting:
- SIP & H.323 (inbound & outbound)
- Outbound calling for CMR Cloud/Hybrid
- Inbound calling for CMR Premises

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

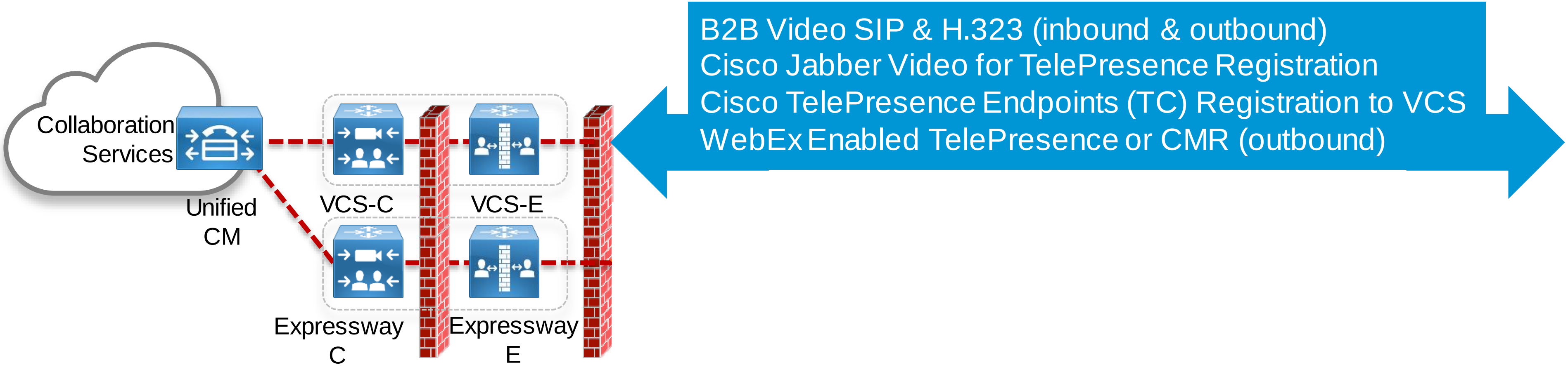
  Will the number of remote Jabber users making calls over Expressway crush my existing TelePresence deployment?

- 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 and 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 and 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

  http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_CollabEdge.html

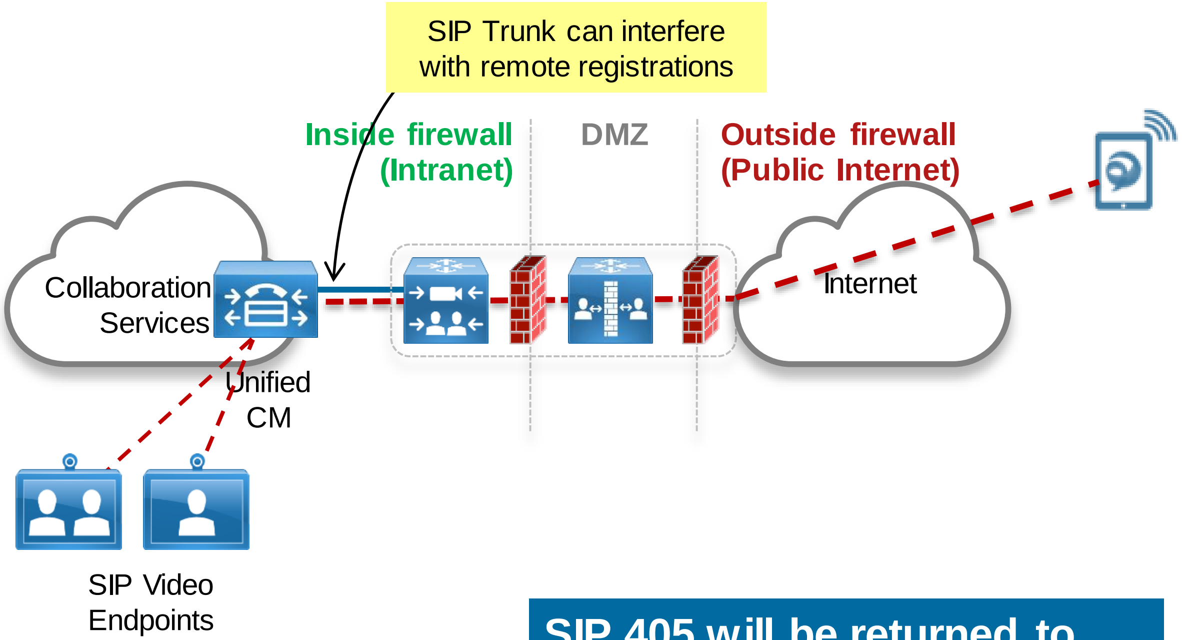
Unified CM Requirements

Expressway Mobile and 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



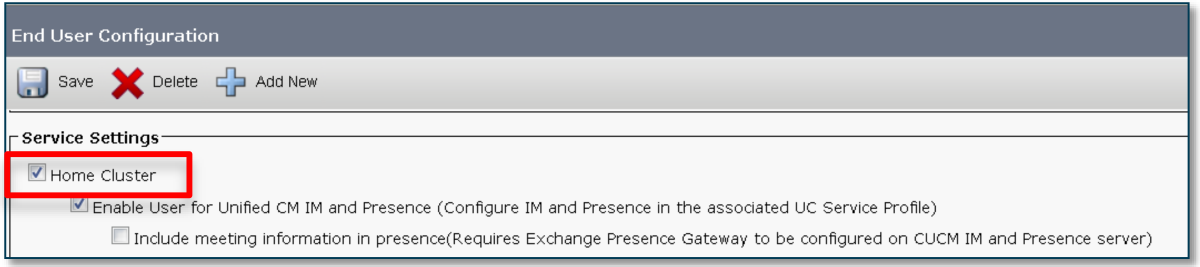
SIP Trunk can interfere with remote registrations
Inside firewall (Intranet)
DMZ
Outside firewall (Public Internet)
Collaboration Services
Unified CM
Internet
SIP Video Endpoints

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

- 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

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



End User Configuration

Service Settings

☑ Home Cluster

☑ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

□ Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

- Unified CM clusters support 80K end users, and can scale as high as 160K with BU approval

Supporting Multiple Unified CM Clusters

Prerequisites

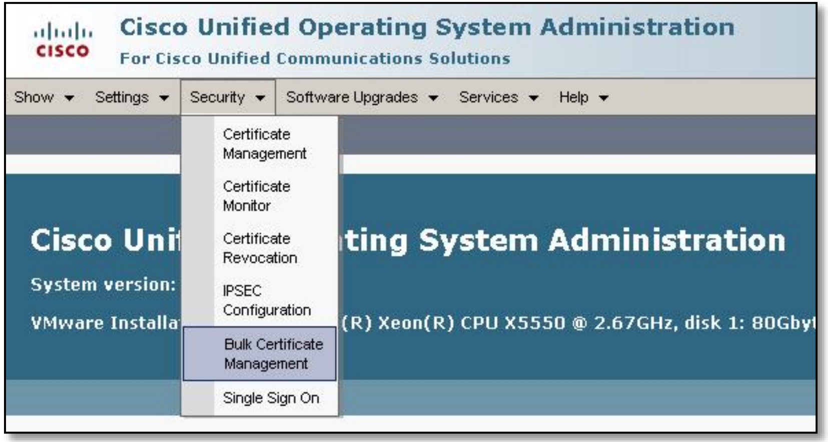
- Cross cluster UDS API calls are used to find Jabber user’s home cluster

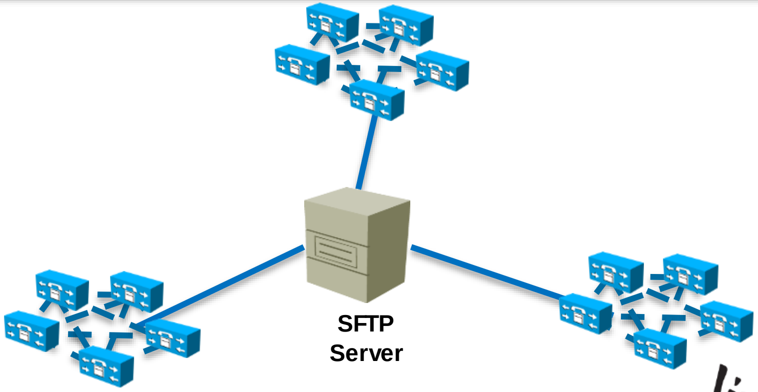
```
https://<ucm>/cucm-uds/clusterUser?username=mdude
```

- 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 and Certificates

Client Authentication at the Edge

Default deployment (non-SSO)

HTTPS

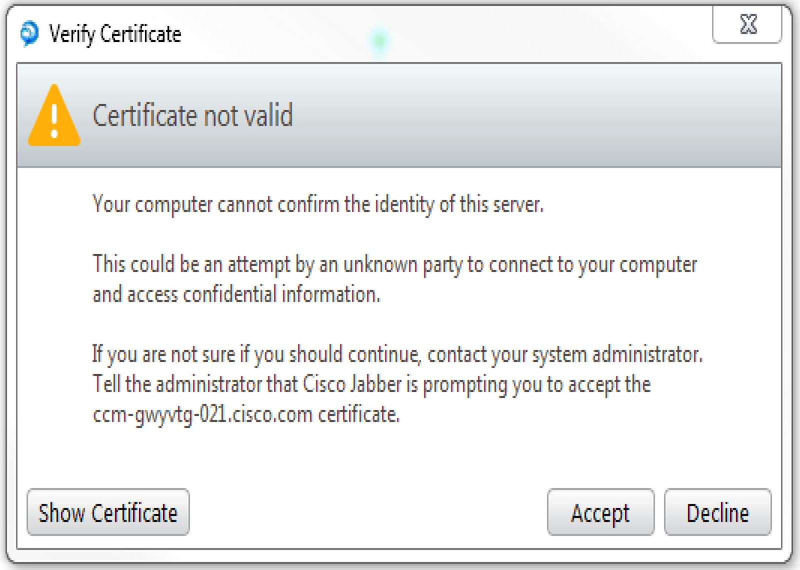
- Clients supply base64 encoded username and password to authenticate over HTTPS **`Authorisation: Basic bWR1ZGU6dGhpc3Bhc3N3ZHdpbGxiZXJlc2V0`**
- Credentials are forwarded to Expressway-C and then used to authenticate against Unified CM, upon determination of the user’s home cluster
- Upon successful 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



Certificate not valid

Your computer cannot confirm the identity of this server.

This could be an attempt by an unknown party to connect to your computer and access confidential information.

If you are not sure if you should continue, contact your system administrator. Tell the administrator that Cisco Jabber is prompting you to accept the ccm-gwyvtg-021.cisco.com certificate.

Expressway Server Certificates

MORE DETAILS IN APPENDIX B

- 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
```

X.509v3

- 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

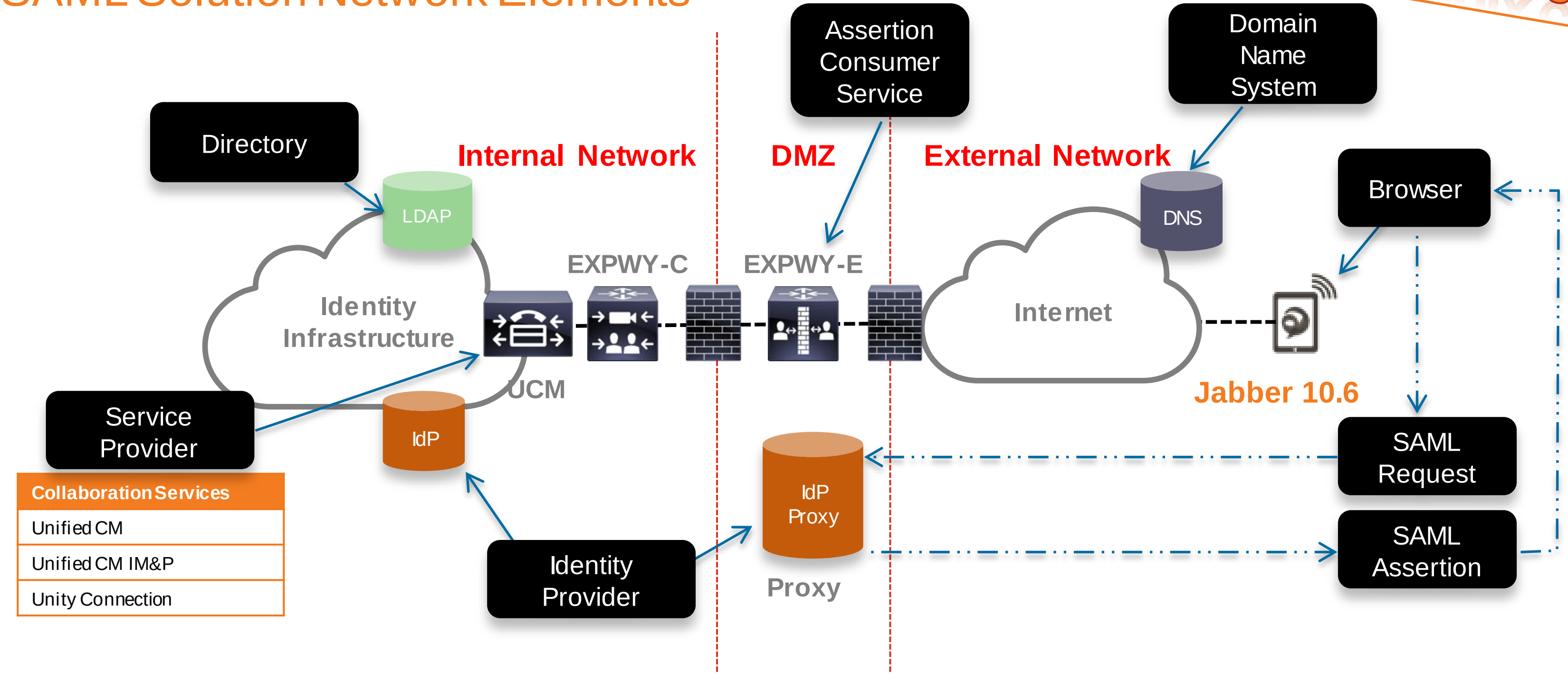
What’s Involved with SSO and Edge?

- 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 authorisation
- Tokens & Cookies
- Export & import metadata to form trust relationships between IdP, Expressway, Unified CM, Unity Connection

Jabber + Expressway SSO Solution

SAML Solution Network Elements

MORE DETAILS IN APPENDIX C



Collaboration Services
Unified CM
Unified CM IM&P
Unity Connection

SSO Transition Behaviour

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

Component	Min Software Version	Projected Availability
Cisco Expressway (or Cisco VCS)	X8.5.1	Available
Unified CM	10.5(2)	Available
Unified CM IM&P	10.5(2)	Available
Unity Connection	10.5(2)	Available
Jabber for Windows	10.6	Available
Jabber for iPhone and iPad	10.6	Available
Jabber for Mac	10.6	Available
Jabber for Android	10.6	Available

Your SAML v2.0 IdP must be reachable from internet

Cisco has tested the most popular IdPs ⟶

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

Q&A

Complete Your Online Session Evaluation

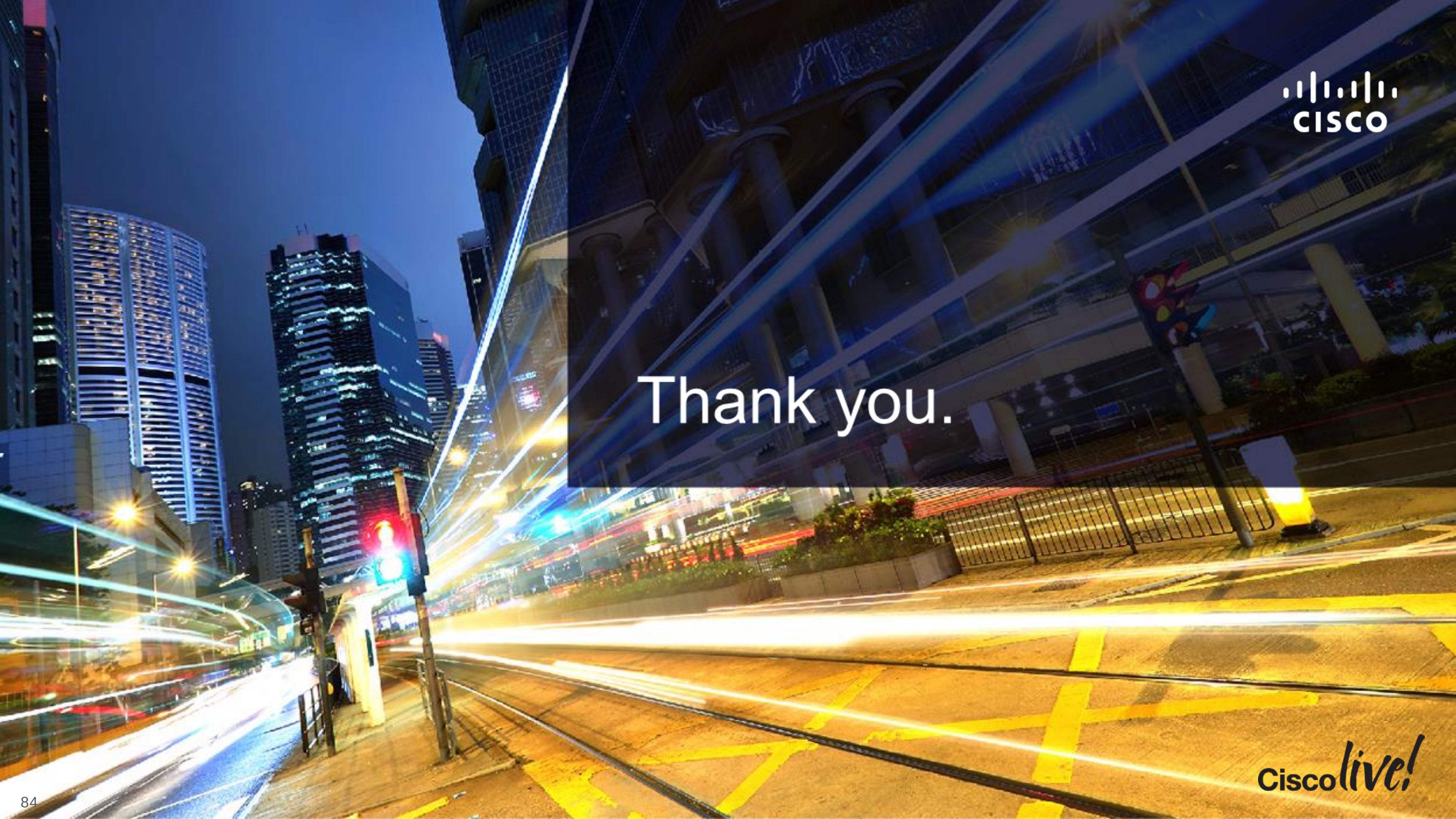
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com



Thank you.

cisco

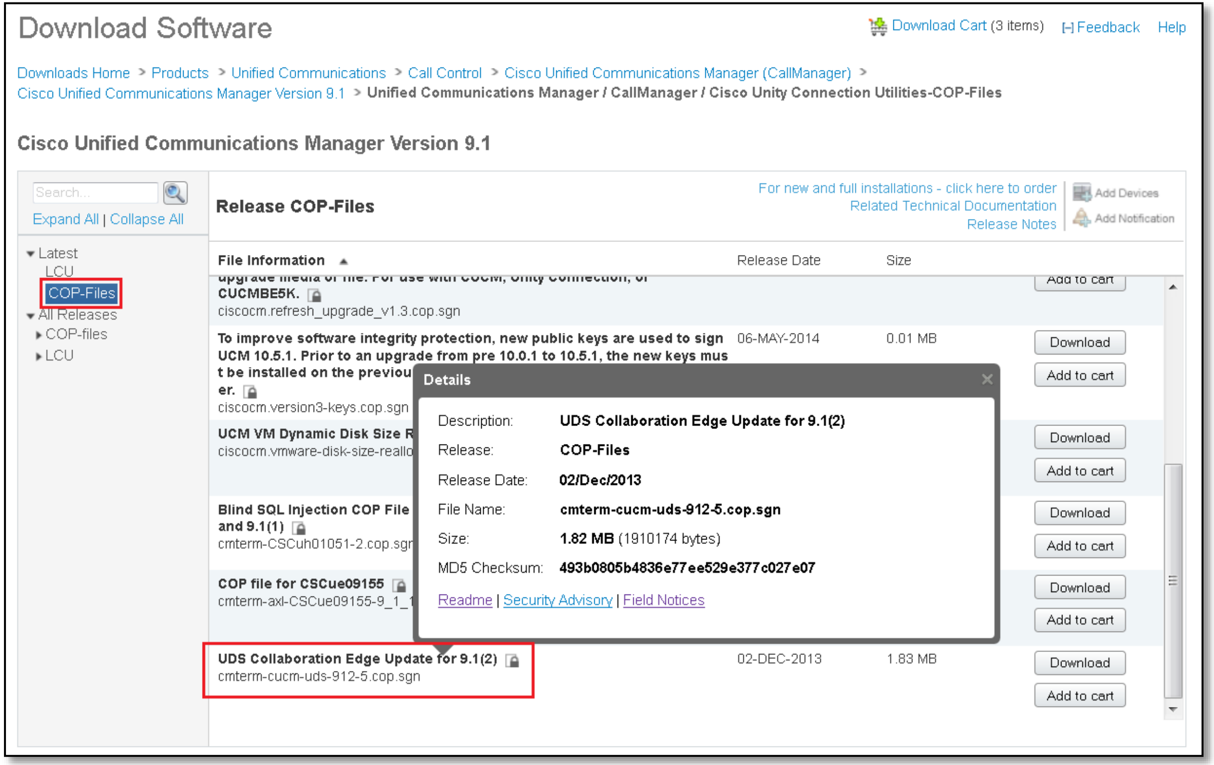
Appendix A
Resources and Troubleshooting

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



Download Software

Download Cart (3 items) [-] Feedback Help

Downloads Home > Products > Unified Communications > Call Control > Cisco Unified Communications Manager (CallManager) > Cisco Unified Communications Manager Version 9.1 > **Unified Communications Manager / CallManager / Cisco Unity Connection Utilities-COP-Files**

Cisco Unified Communications Manager Version 9.1

Search...
Expand All | Collapse All
Latest
LCU
COP-Files
All Releases
COP-files
LCU
For new and full installations - click here to order
Related Technical Documentation
Release Notes
Add Devices
Add Notification

Release COP-Files

File Information	Release Date	Size	
upgrade media or file. For use with CUCM, Unity Connection, or **CUCMBE5K.** ciscocm.refresh_upgrade_v1.3.cop.sgn			Add to cart
To improve software integrity protection, new public keys are used to sign UCM 10.5.1. Prior to an upgrade from pre 10.0.1 to 10.5.1, the new keys mus t be installed on the previou er. ciscocm.version3-keys.cop.sgn	06-MAY-2014	0.01 MB	Download Add to cart
UCM VM Dynamic Disk Size R ciscocm.vmware-disk-size-reallo			Download Add to cart
Blind SQL Injection COP File and 9.1(1) cmterm-CSCuh01051-2.cop.sgr			Download Add to cart
COP file for CSCue09155 cmterm-axl-CSCue09155-9_1_1			Download Add to cart
UDS Collaboration Edge Update for 9.1(2) cmterm-cucm-uds-912-5.cop.sgn	02-DEC-2013	1.83 MB	Download Add to cart

Details

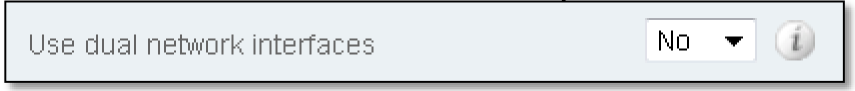
Description:	**UDS Collaboration Edge Update for 9.1(2)**
Release:	**COP-Files**
Release Date:	**02/Dec/2013**
File Name:	**cmterm-cucm-uds-912-5.cop.sgn**
Size:	**1.82 MB** (1910174 bytes)
MD5 Checksum:	**493b0805b4836e77ee529e377c027e07**

Readme | Security Advisory | Field Notices

Starting Point for Troubleshooting

Verify Expressway Traversal Connections

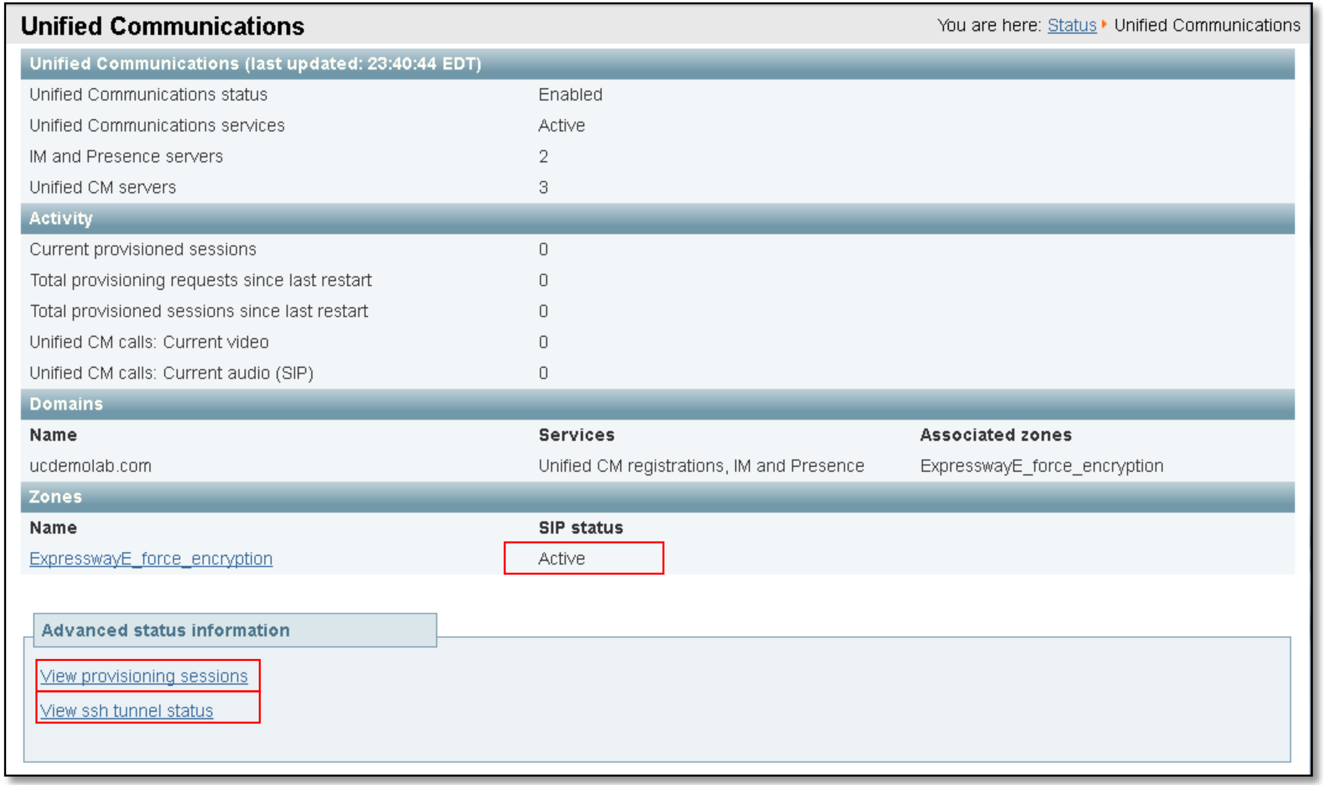
- The SIP connection between Expressway C and E needs to be established first
  - If you don't have an active SIP traversal connection verify DNS, NTP, SSL certificates, and the trusted CA certificates on both C and E, also check firewall
- SIP messaging over the traversal zone from C to E will provide 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 2nd NIC is automatically enabled
  - When the 2nd NIC is enabled, the E only listens for TCP 7400 on the 2nd NIC interface
  - If you are not using the 2nd NIC, you need to disable it on the System > IP menu



Use dual network interfaces: No

Expressway-C Unified Communications Status

Status > Unified Communications



Unified Communications

You are here: Status ▸ Unified Communications

Unified Communications (last updated: 23:40:44 EDT)

Unified Communications status	Enabled
Unified Communications services	Active
IM and Presence servers	2
Unified CM servers	3

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

Name	Services	Associated zones
ucdemolab.com	Unified CM registrations, IM and Presence	ExpresswayE_force_encryption

Zones

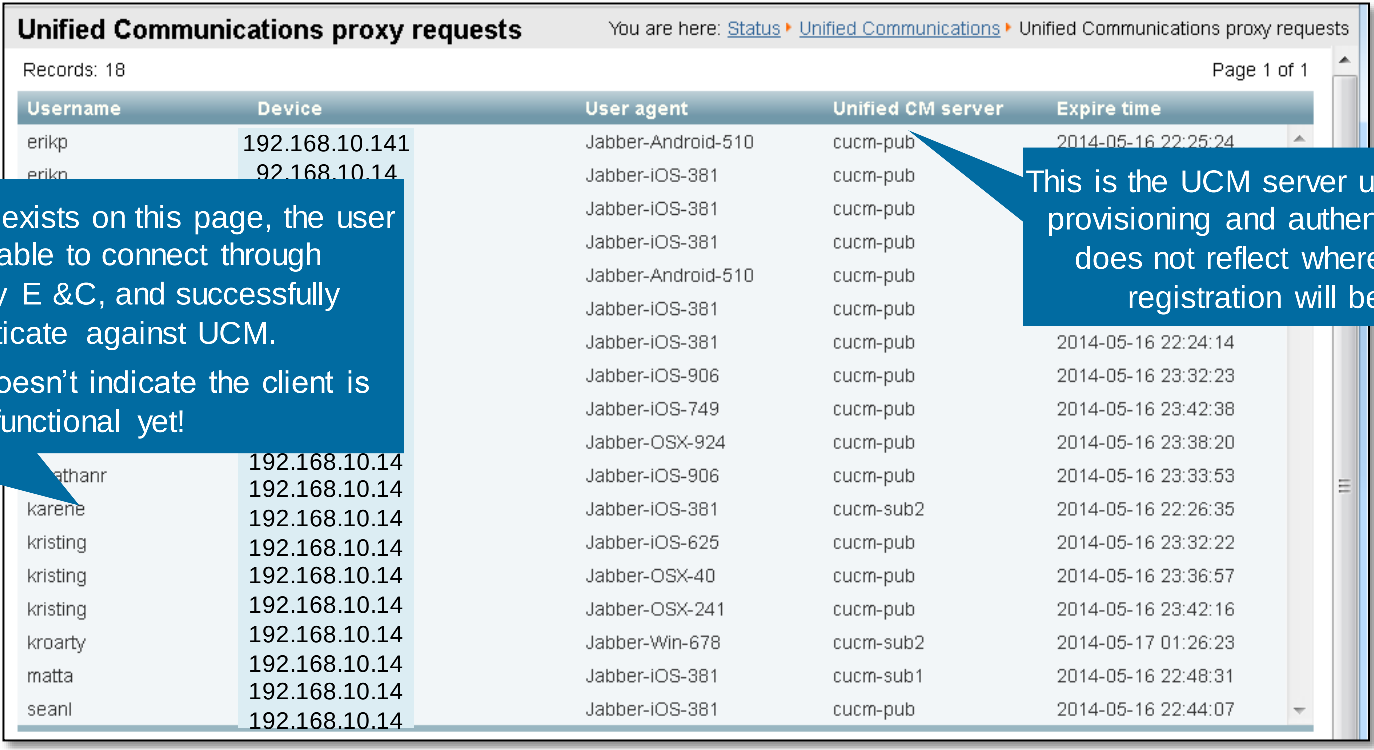
Name	SIP status
ExpresswayE_force_encryption	Active

Advanced status information

View provisioning sessions

View ssh tunnel status

View Provisioning Sessions on Expressway-C



Unified Communications proxy requests

You are here: Status ▸ Unified Communications ▸ Unified Communications proxy requests

Records: 18

Page 1 of 1

Username	Device	User agent	Unified CM server	Expire time
erikp	192.168.10.141	Jabber-Android-510	cucm-pub	2014-05-16 22:25:24
erikp	92.168.10.14	Jabber-iOS-381	cucm-pub	
		Jabber-iOS-381	cucm-pub	
		Jabber-iOS-381	cucm-pub	
		Jabber-Android-510	cucm-pub	
		Jabber-iOS-381	cucm-pub	
		Jabber-iOS-381	cucm-pub	2014-05-16 22:24:14
		Jabber-iOS-906	cucm-pub	2014-05-16 23:32:23
		Jabber-iOS-749	cucm-pub	2014-05-16 23:42:38
	192.168.10.14	Jabber-OSX-924	cucm-pub	2014-05-16 23:38:20
athanr	192.168.10.14	Jabber-iOS-906	cucm-pub	2014-05-16 23:33:53
karene	192.168.10.14	Jabber-iOS-381	cucm-sub2	2014-05-16 22:26:35
kristing	192.168.10.14	Jabber-iOS-625	cucm-pub	2014-05-16 23:32:22
kristing	192.168.10.14	Jabber-OSX-40	cucm-pub	2014-05-16 23:36:57
kristing	192.168.10.14	Jabber-OSX-241	cucm-pub	2014-05-16 23:42:16
kroarty	192.168.10.14	Jabber-Win-678	cucm-sub2	2014-05-17 01:26:23
matta	192.168.10.14	Jabber-iOS-381	cucm-sub1	2014-05-16 22:48:31
seanl	192.168.10.14	Jabber-iOS-381	cucm-pub	2014-05-16 22:44:07

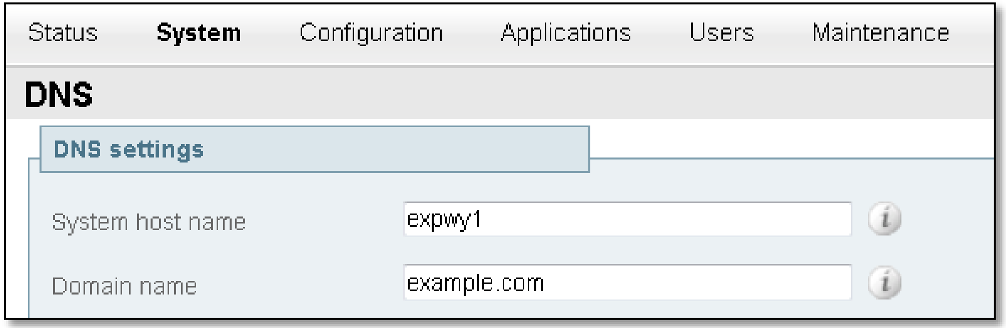
When an entry exists on this page, the user has been able to connect through Expressway E &C, and successfully authenticate against UCM.

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



DNS

DNS settings

System host name: expwy1

Domain name: example.com

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

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 bWR1ZGU6dGhpc3Bhc3N3ZHdpbGxiZXJlc2V0
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
```

X-Auth token

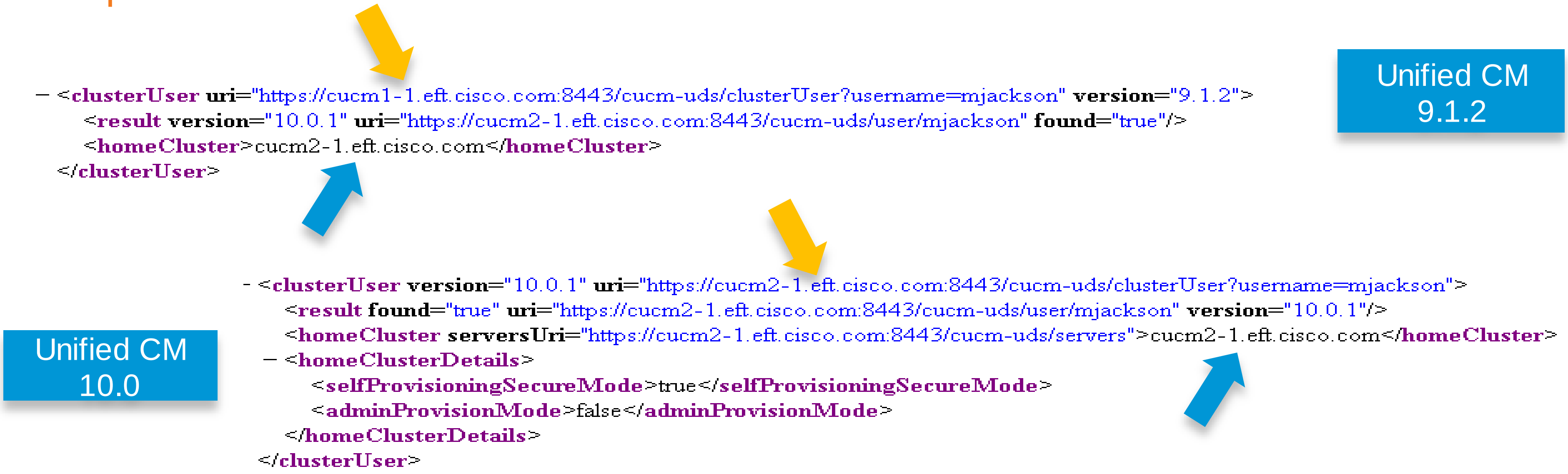
Base64 decode = ucdemolab.com/https/cucm-pub.ucdemolab.com/8443

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>



Unified CM 9.1.2

```
– <clusterUser uri="https://cucm1-1.eft.cisco.com:8443/cucm-uds/clusterUser?username=mjackson" version="9.1.2">
    <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>
```

Unified CM 10.0

```
- <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>
      <adminProvisionMode>false</adminProvisionMode>
    </homeClusterDetails>
  </clusterUser>
```

Cisco Jabber Client Initialisation

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 Initialisation

Sampling of initial Jabber HTTPS requests

```
GET /dWNkZW1vbGFiLmNvbQ/get_edge_config?service_name=_cisco-uds

GET /dWNkZW1vbGFiLmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0NDM/cucm-uds/clusterUser?username=mdude

GET /dWNkZW1vbGFiLmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0NDM/cucm-uds/servers

GET /dWNkZW1vbGFiLmNvbS9odHRwcy9jdWNtLXN1YjIudWNkZW1vbGFiLmNvbS84NDQz/cucm-uds/user/mdude

GET /dWNkZW1vbGFiLmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0NDM/cucm-uds/user/mdude/devices

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 Initialisation

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
```

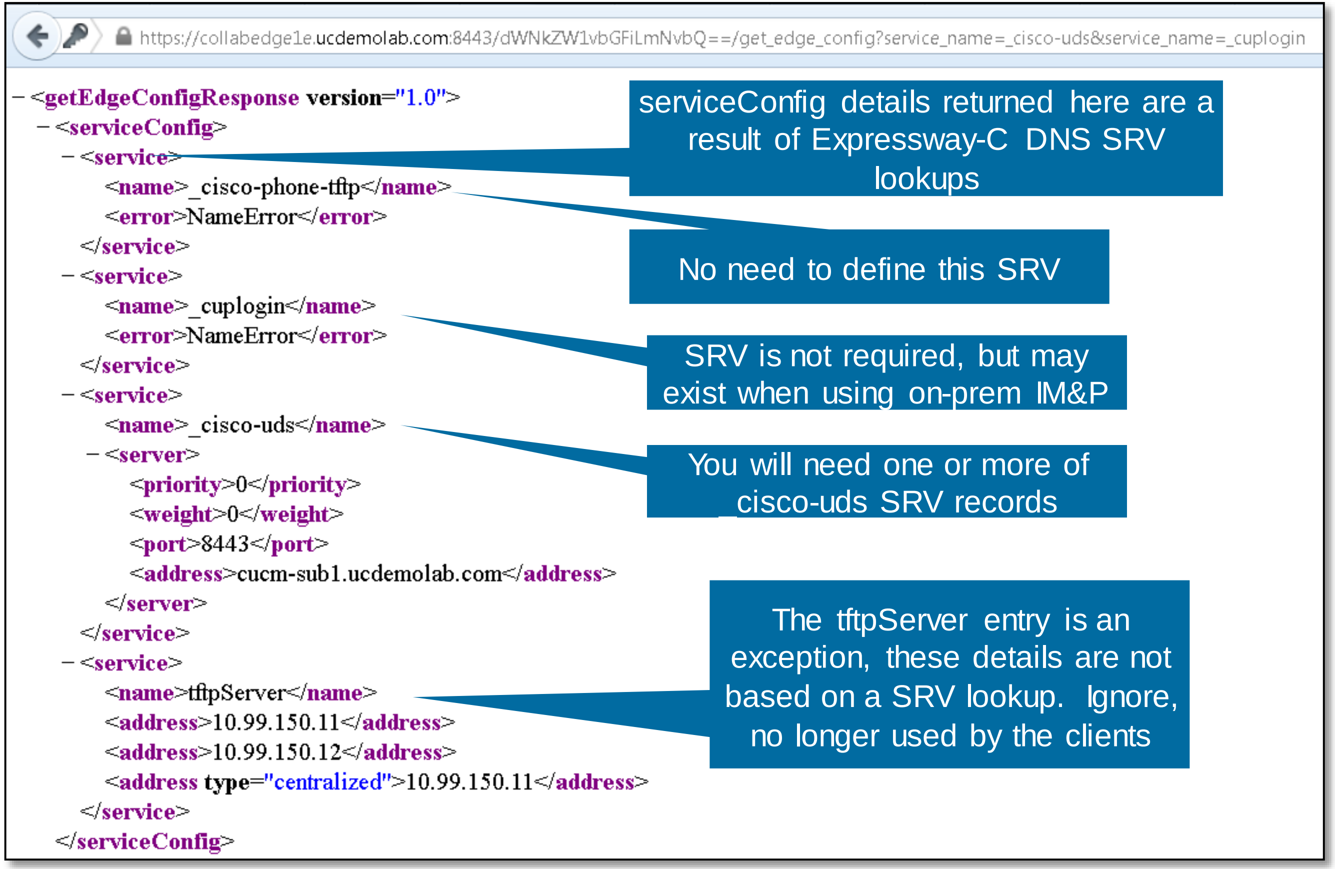
Request Edge Config in Your Browser

- 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)



https://collabedge1e.ucdemolab.com:8443/dWNkZW1vbGFiLmNvbQ==/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin

```
– <getEdgeConfigResponse version="1.0">
  – <serviceConfig>
    – <service>
        <name>_cisco-phone-tftp</name>
        <error>NameError</error>
      </service>
    – <service>
        <name>_cuplogin</name>
        <error>NameError</error>
      </service>
    – <service>
        <name>_cisco-uds</name>
      – <server>
          <priority>0</priority>
          <weight>0</weight>
          <port>8443</port>
          <address>cucm-sub1.ucdemolab.com</address>
        </server>
      </service>
    – <service>
        <name>tftpServer</name>
        <address>10.99.150.11</address>
        <address>10.99.150.12</address>
        <address type="centralized">10.99.150.11</address>
      </service>
  </serviceConfig>
```

serviceConfig details returned here are a result of Expressway-C DNS SRV lookups

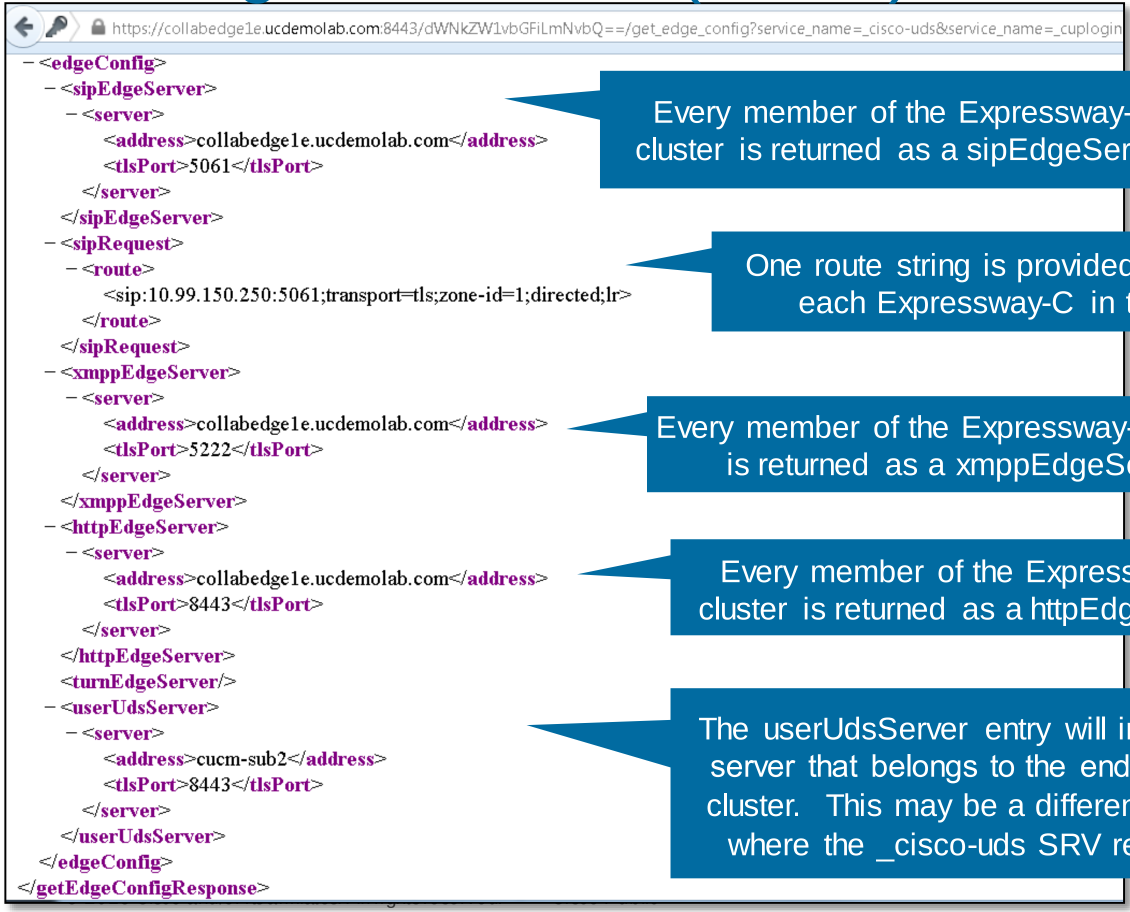
No need to define this SRV

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

Edge Config & Services (2 of 2)



https://collabedge1e.ucdemolab.com:8443/dWNkZW1vbGFiLmNvbQ==/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin

```
– <edgeConfig>
  – <sipEdgeServer>
    – <server>
        <address>collabedge1e.ucdemolab.com</address>
        <tlsPort>5061</tlsPort>
      </server>
    </sipEdgeServer>
  – <sipRequest>
    – <route>
        <sip:10.99.150.250:5061;transport=tls;zone-id=1;directed;lr>
      </route>
    </sipRequest>
  – <xmppEdgeServer>
    – <server>
        <address>collabedge1e.ucdemolab.com</address>
        <tlsPort>5222</tlsPort>
      </server>
    </xmppEdgeServer>
  – <httpEdgeServer>
    – <server>
        <address>collabedge1e.ucdemolab.com</address>
        <tlsPort>8443</tlsPort>
      </server>
    </httpEdgeServer>
    <turnEdgeServer/>
  – <userUdsServer>
    – <server>
        <address>cucm-sub2</address>
        <tlsPort>8443</tlsPort>
      </server>
    </userUdsServer>
  </edgeConfig>
</getEdgeConfigResponse>
```

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

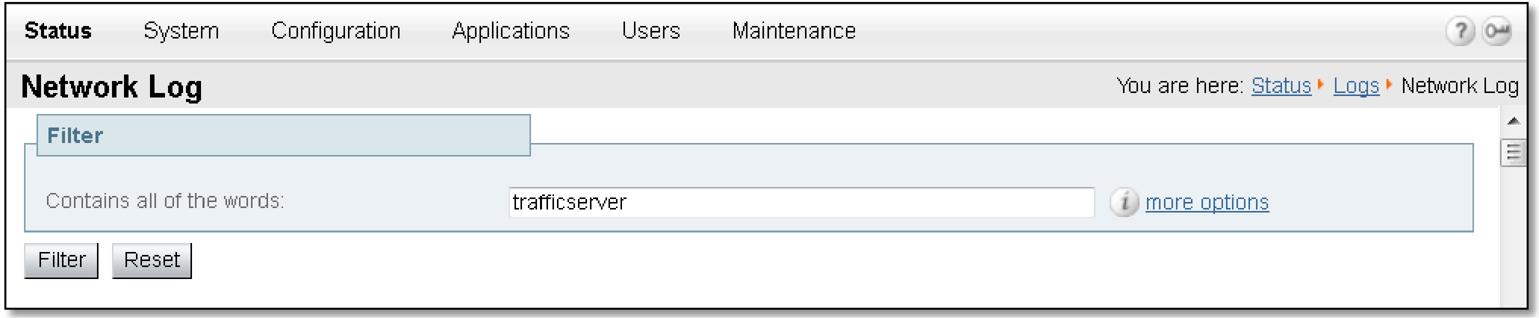
Every member of the Expressway-E cluster is returned as a xmppEdgeServer

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

You are here: Status ▸ Logs ▸ Network Log

Filter

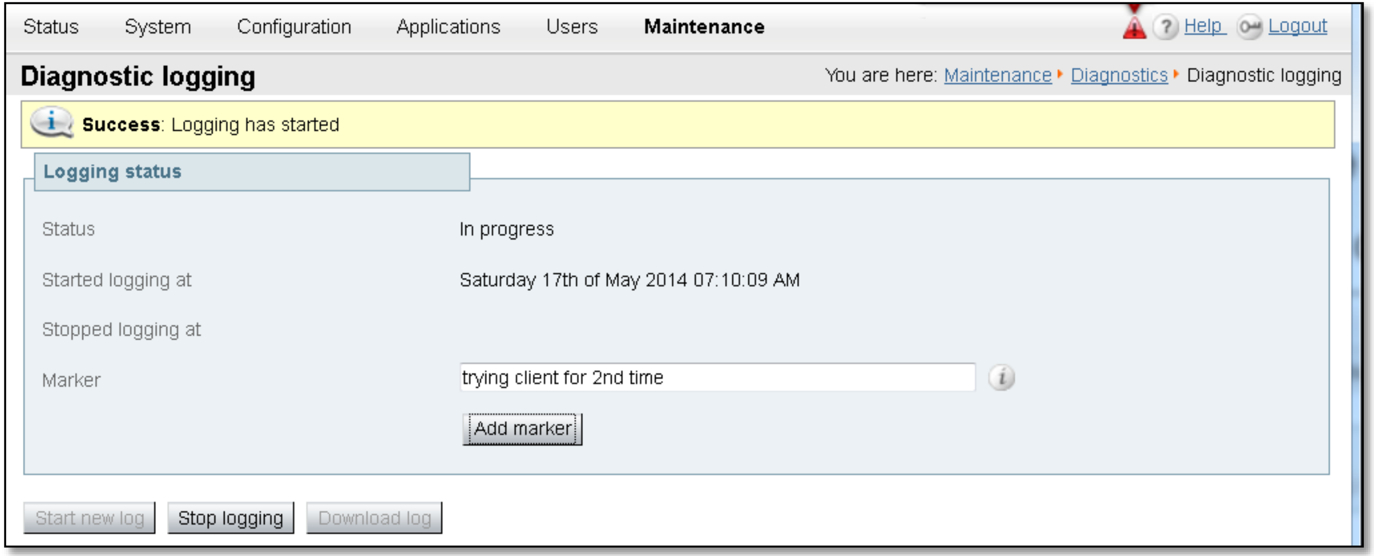
Contains all of the words: trafficserver

- 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

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



Diagnostic logging

You are here: Maintenance ▸ Diagnostics ▸ Diagnostic logging

Success: Logging has started

Logging status

Status	In progress
Started logging at	Saturday 17th of May 2014 07:10:09 AM
Stopped logging at	
Marker	trying client for 2nd time

Appendix B
Expressway Server Certificate Details

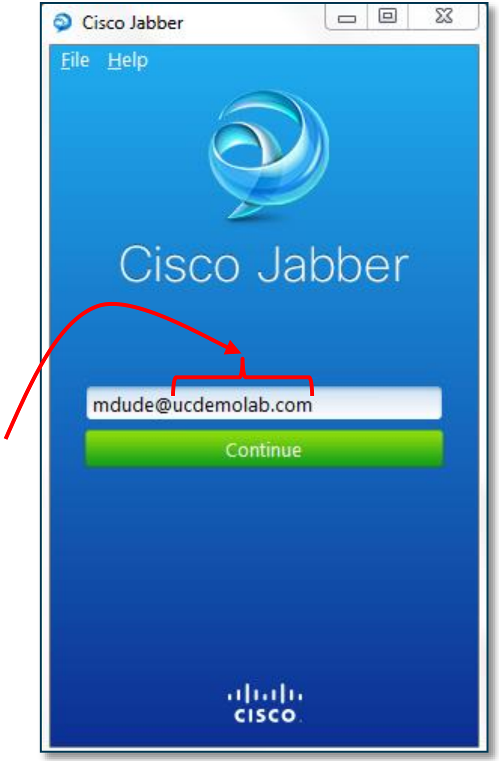
Subject Alternative Name (SAN) Requirements

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)



mdude@ucdemolab.com

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 authorise the TLS registration on TCP 5061

Optional SANs for XMPP Federation

Applies to on-prem IM&P customers only

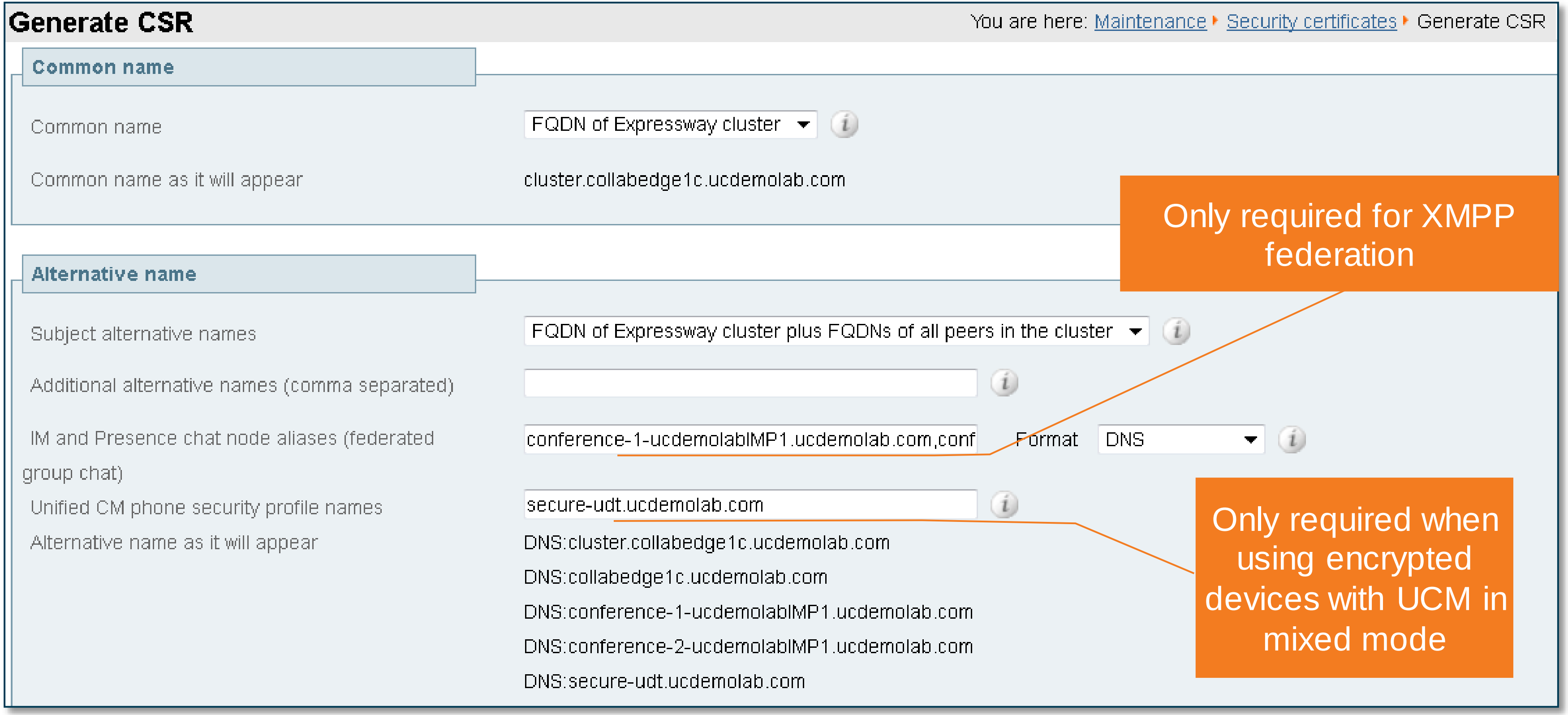
- The Expressway Server Certificate Generate CSR page will also insert “IM&P chat node aliases” as SANs
- These specific SANS will allow for **TLS XMPP federation**

```
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

X.509v3

Expressway-C Certificate Signing Request



Generate CSR

You are here: Maintenance ▸ Security certificates ▸ Generate CSR

Common name

Common name	FQDN of Expressway cluster ▾
Common name as it will appear	cluster.collabedge1c.ucdemolab.com

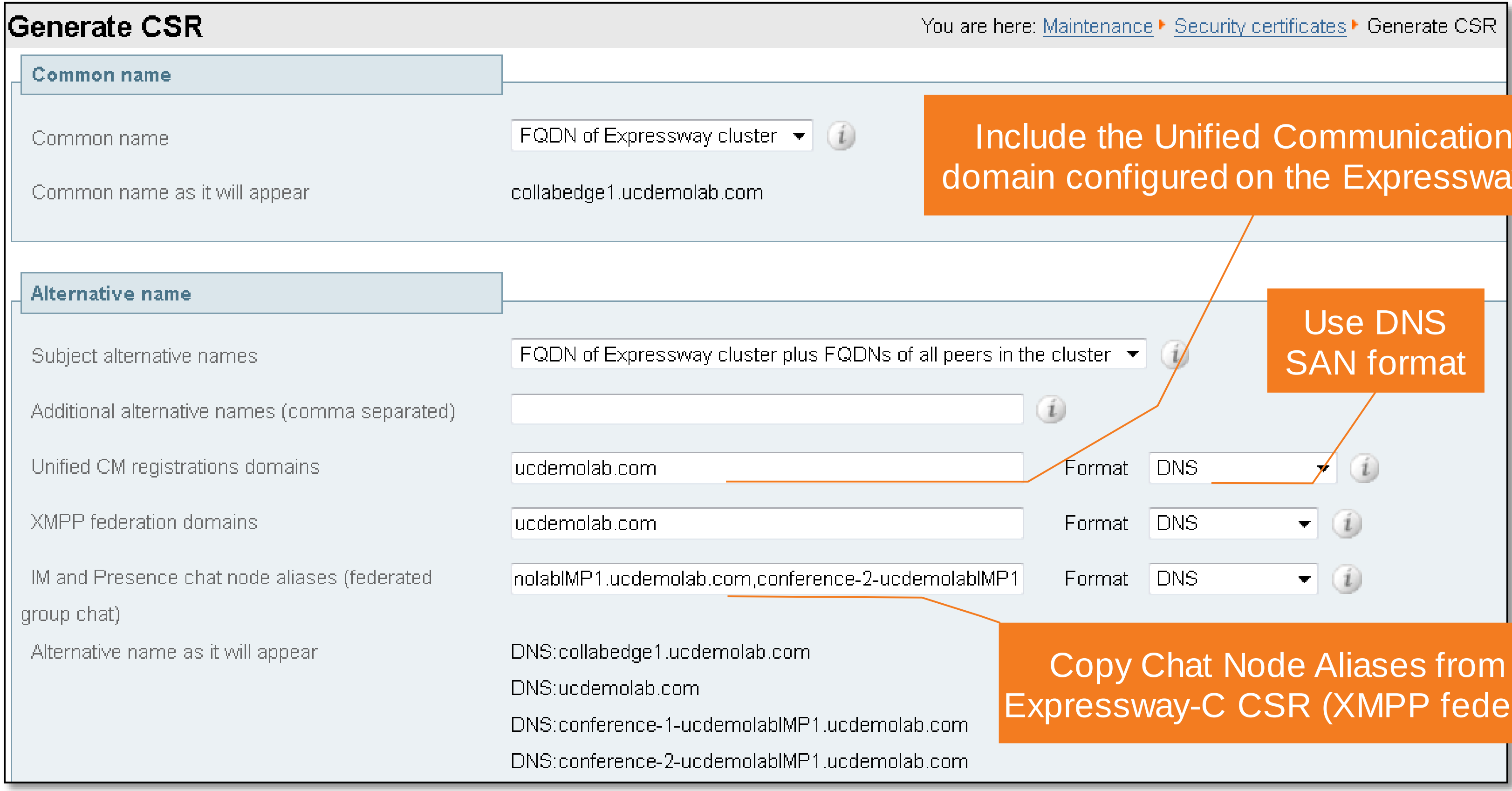
Alternative name

Subject alternative names	FQDN of Expressway cluster plus FQDNs of all peers in the cluster ▾
Additional alternative names (comma separated)	
IM and Presence chat node aliases (federated group chat)	conference-1-ucdemolabIMP1.ucdemolab.com,conf Format DNS ▾
Unified CM phone security profile names	secure-udt.ucdemolab.com
Alternative name as it will appear	DNS:cluster.collabedge1c.ucdemolab.com DNS:collabedge1c.ucdemolab.com DNS:conference-1-ucdemolabIMP1.ucdemolab.com DNS:conference-2-ucdemolabIMP1.ucdemolab.com DNS:secure-udt.ucdemolab.com

Only required for XMPP federation

Only required when using encrypted devices with UCM in mixed mode

Expressway-E Certificate Signing Request



Generate CSR

You are here: Maintenance ▸ Security certificates ▸ Generate CSR

Common name

Common name: FQDN of Expressway cluster

Common name as it will appear: collabedge1.ucdemolab.com

Alternative name

Subject alternative names: FQDN of Expressway cluster plus FQDNs of all peers in the cluster

Additional alternative names (comma separated):

Unified CM registrations domains: ucdemolab.com — Format: DNS

XMPP federation domains: ucdemolab.com — Format: DNS

IM and Presence chat node aliases (federated group chat): nolabIMP1.ucdemolab.com,conference-2-ucdemolabIMP1 — Format: DNS

Alternative name as it will appear:
DNS:collabedge1.ucdemolab.com
DNS:ucdemolab.com
DNS:conference-1-ucdemolabIMP1.ucdemolab.com
DNS:conference-2-ucdemolabIMP1.ucdemolab.com

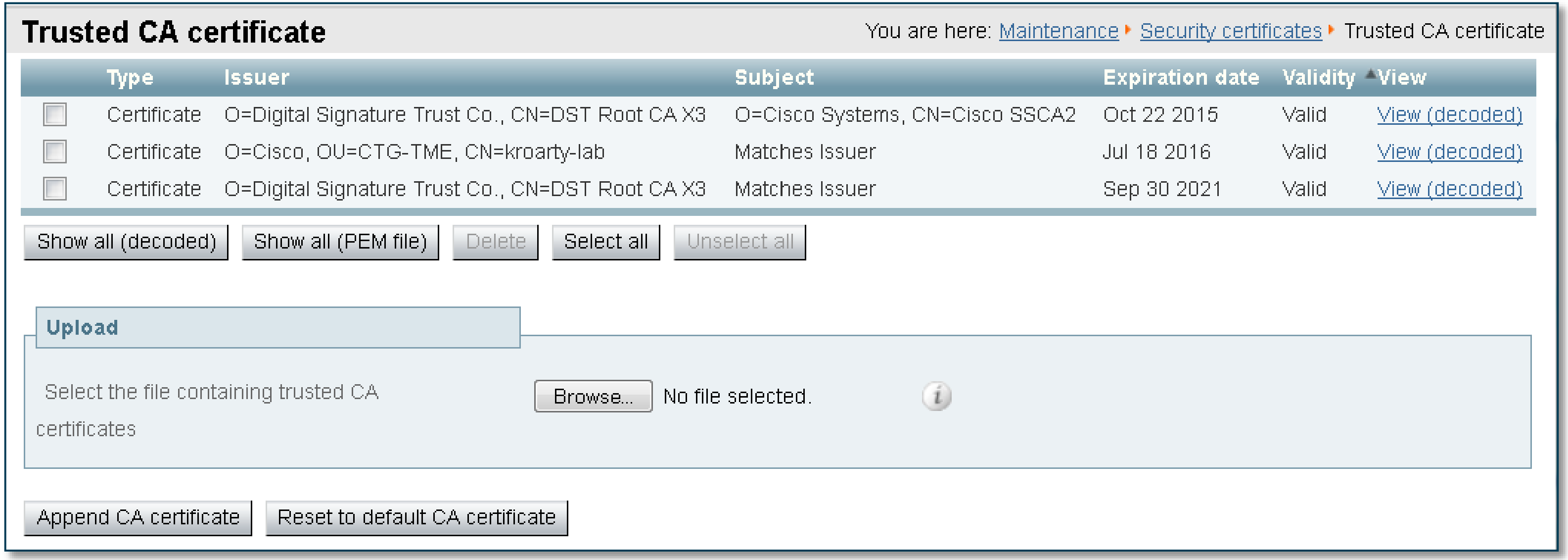
Include the Unified Communications domain configured on the Expressway-C

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



Trusted CA certificate

You are here: Maintenance ▸ Security certificates ▸ Trusted CA certificate

	Type	Issuer	Subject	Expiration date	Validity ▲	View
□	Certificate	O=Digital Signature Trust Co., CN=DST Root CA X3	O=Cisco Systems, CN=Cisco SSCA2	Oct 22 2015	Valid	View (decoded)
□	Certificate	O=Cisco, OU=CTG-TME, CN=kroarty-lab	Matches Issuer	Jul 18 2016	Valid	View (decoded)
□	Certificate	O=Digital Signature Trust Co., CN=DST Root CA X3	Matches Issuer	Sep 30 2021	Valid	View (decoded)

Upload

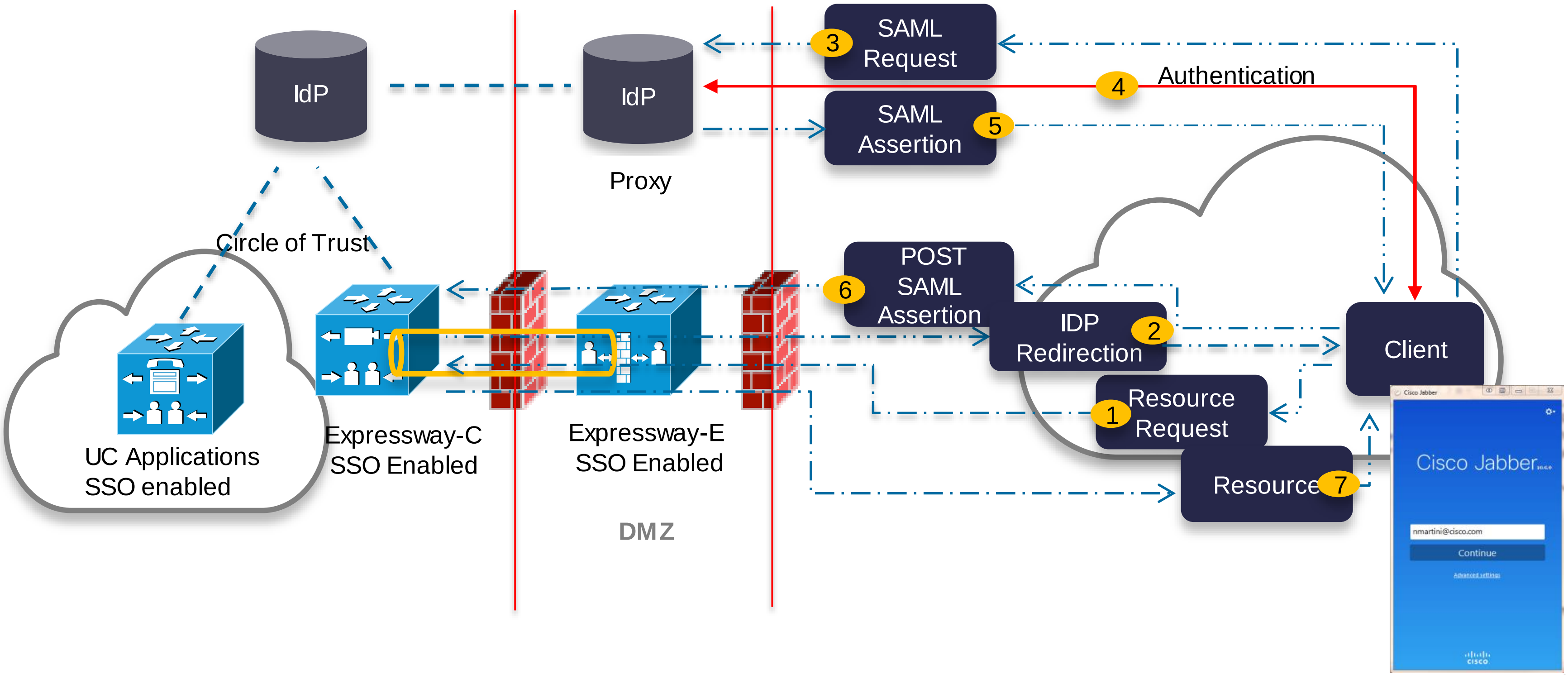
Select the file containing trusted CA certificates — Browse... No file selected.

Expressway Trusted CA Certificates

Certificate Type	Expressway-C Trusted CA	Expressway-E Trusted CA	Comments
Public CA cert chain used to sign Expressway-E certificate	☑	☑	Required to establish Traversal Zone MTLS connections
Public (or Enterprise) CA cert chain used to sign Expressway-C certificate	☑	☑	Required to establish Traversal Zone MTLS connections
Unified CM Tomcat certificates or CA cert chain	☑	☒	Only required when Expressway-C configured to use TLS Verify mode on Unified CM discovery
Unified CM CallManager CA cert chain	☑	☒	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
Unified CM IM&P Tomcat certificates or CA cert chain	☑	☒	Only required when Expressway-C configured to use TLS Verify mode on IM&P discovery

Appendix C
Jabber SSO + Expressway Resources

Single Sign On Over Mobile and Remote Access



IdP

IdP

Proxy

Circle of Trust

UC Applications
SSO enabled

Expressway-C
SSO Enabled

Expressway-E
SSO Enabled

DMZ

3 SAML Request

4 Authentication

SAML Assertion 5

6 POST SAML Assertion

IDP Redirection 2

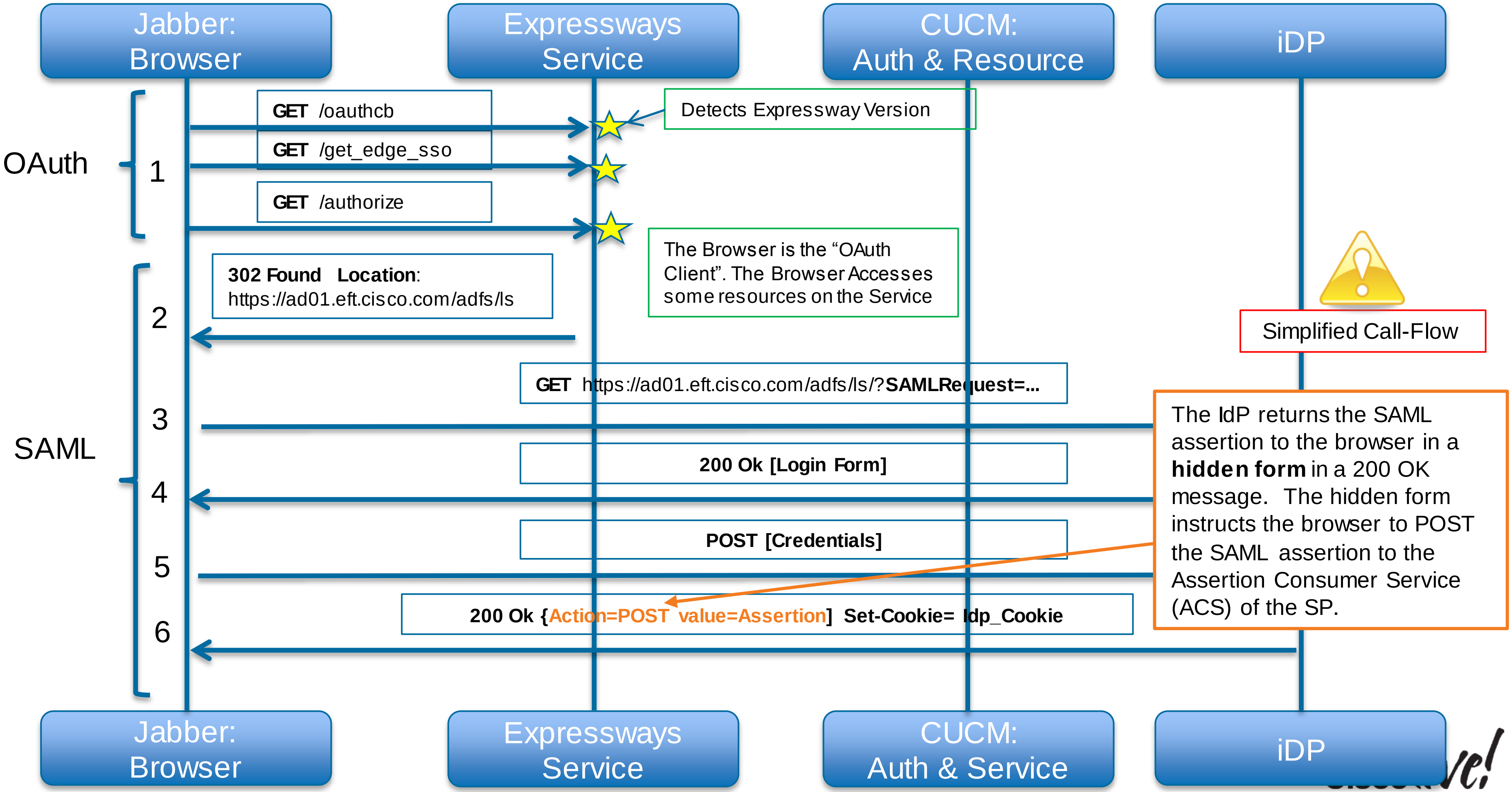
1 Resource Request

Resource 7

Client

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 ***"authorise"*** API enables Jabber to request for OAuth tokens to be used for SSO. **NOTE:** Jabber will receive 3 OAuth tokens. More details later



Jabber: Browser

Expressways Service

CUCM: Auth & Resource

iDP

OAuth

1

GET /oauthcb

Detects Expressway Version

GET /get_edge_sso

GET /authorize

The Browser is the “OAuth Client”. The Browser Accesses some resources on the Service

Simplified Call-Flow

SAML

2

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

3

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

4

200 Ok [Login Form]

5

POST [Credentials]

6

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

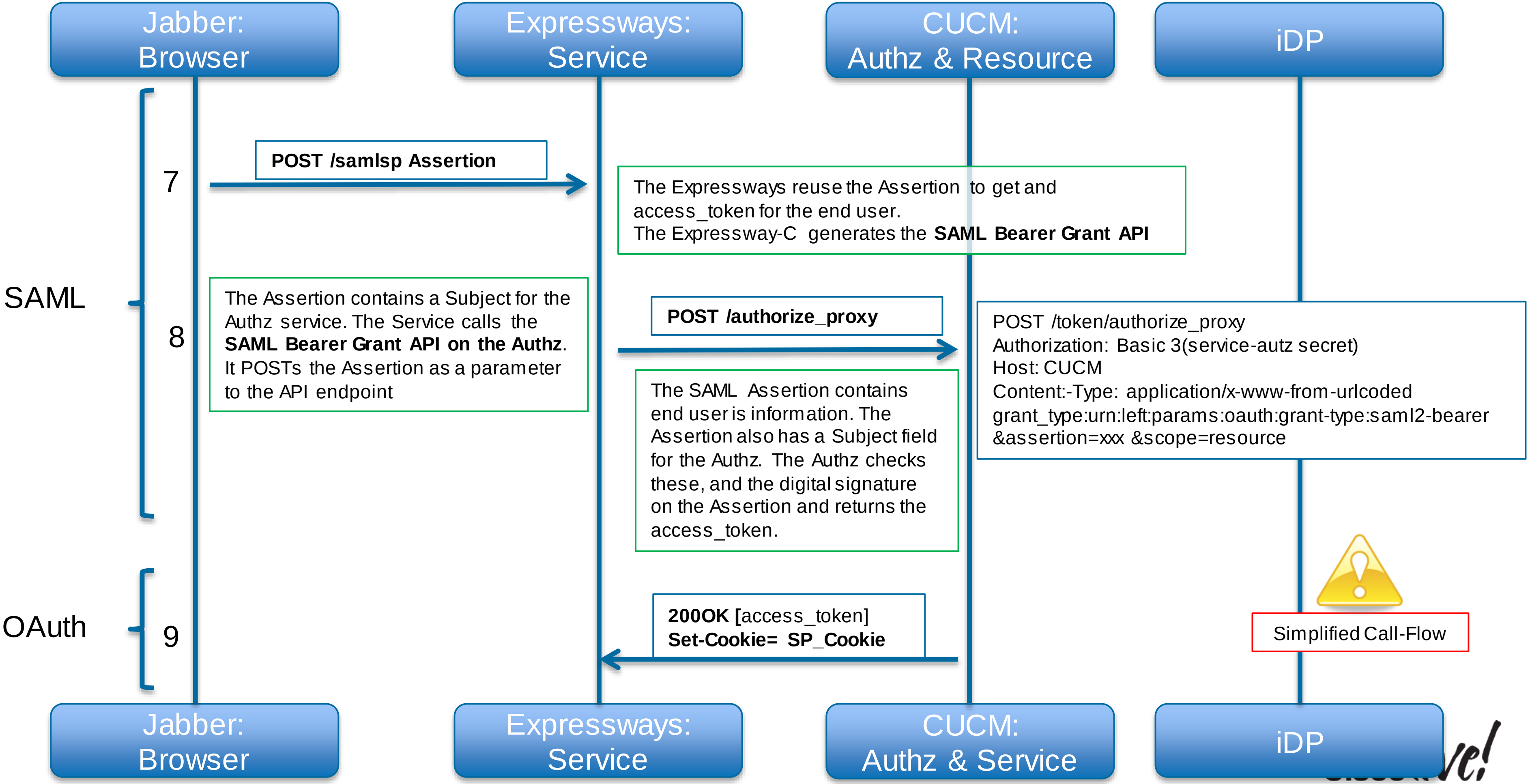
The IdP returns the SAML assertion to the browser in a **hidden form** in a 200 OK message. The hidden form instructs the browser to POST the SAML assertion to the Assertion Consumer Service (ACS) of the SP.

Jabber: Browser

Expressways Service

CUCM: Auth & Service

iDP



Jabber: Browser

Expressways: Service

CUCM: Authz & Resource

iDP

SAML

7

POST /samlsp Assertion

The Expressways reuse the Assertion to get and access_token for the end user.
The Expressway-C generates the **SAML Bearer Grant API**

8

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

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

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.

OAuth

9

200OK [access_token]
Set-Cookie= SP_Cookie

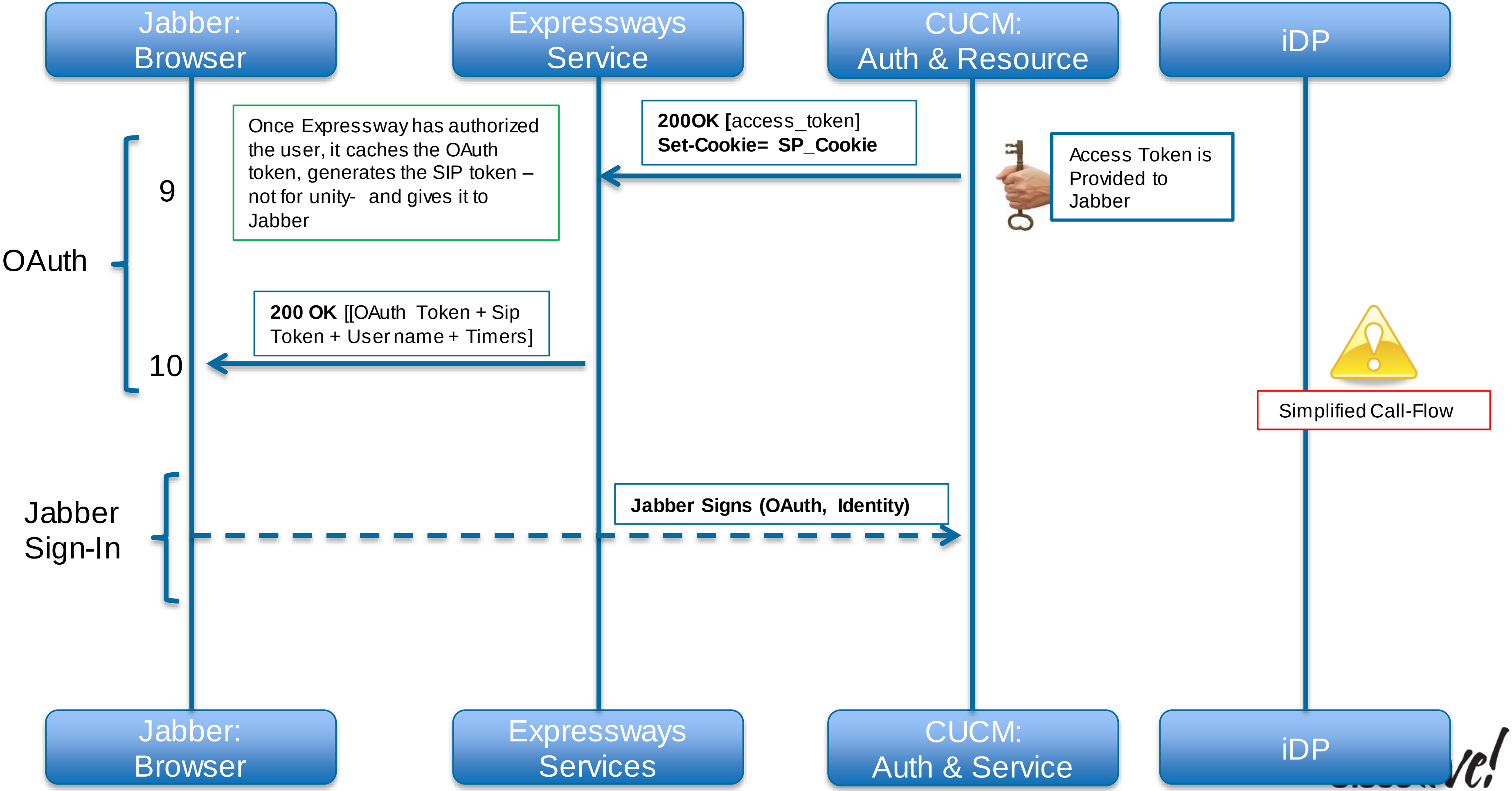
Simplified Call-Flow

Jabber: Browser

Expressways: Service

CUCM: Authz & Service

iDP



Jabber: Browser

Expressways Service

CUCM: Auth & Resource

iDP

OAuth

9

Once Expressway has authorized the user, it caches the OAuth token, generates the SIP token – not for unity- and gives it to Jabber

200OK [access_token]
Set-Cookie= SP_Cookie

Access Token is Provided to Jabber

10

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

Simplified Call-Flow

Jabber Sign-In

Jabber Signs (OAuth, Identity)

Jabber: Browser

Expressways Services

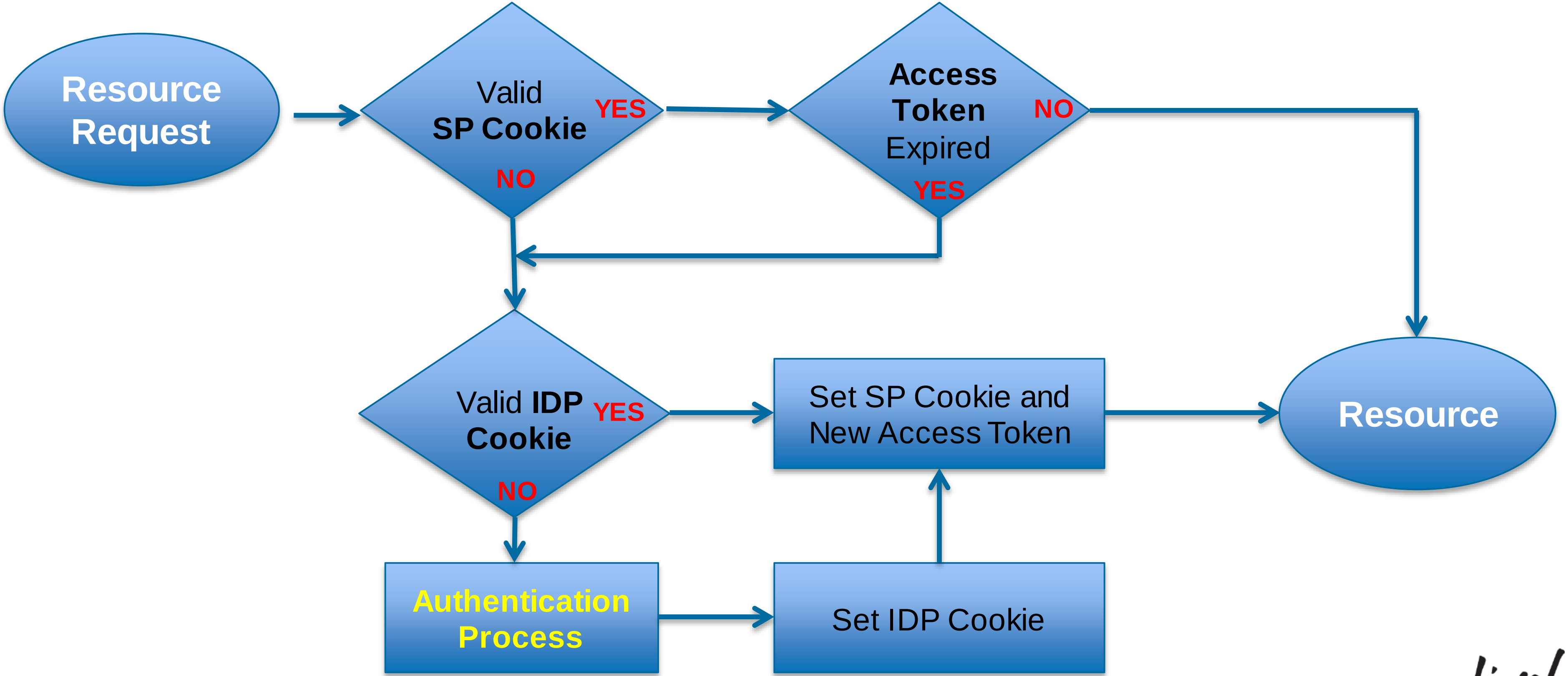
CUCM: Auth & Service

iDP

Edge SSO Tokens

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



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

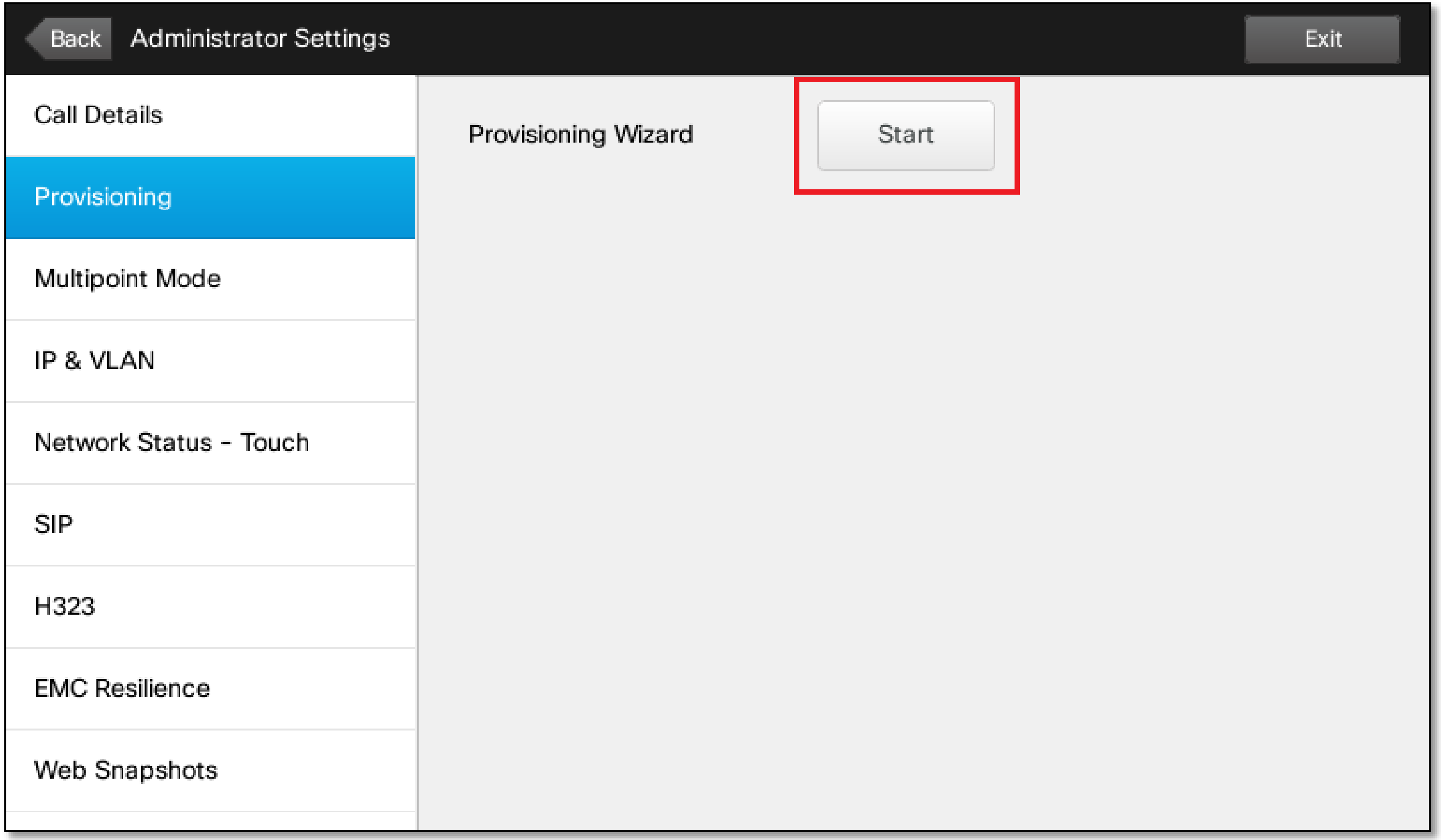
With 12 minute register expiry, sip stack attempts to refresh register 10 minutes after last successful one

For all other devices (including CSF) register expires = 2 minutes –

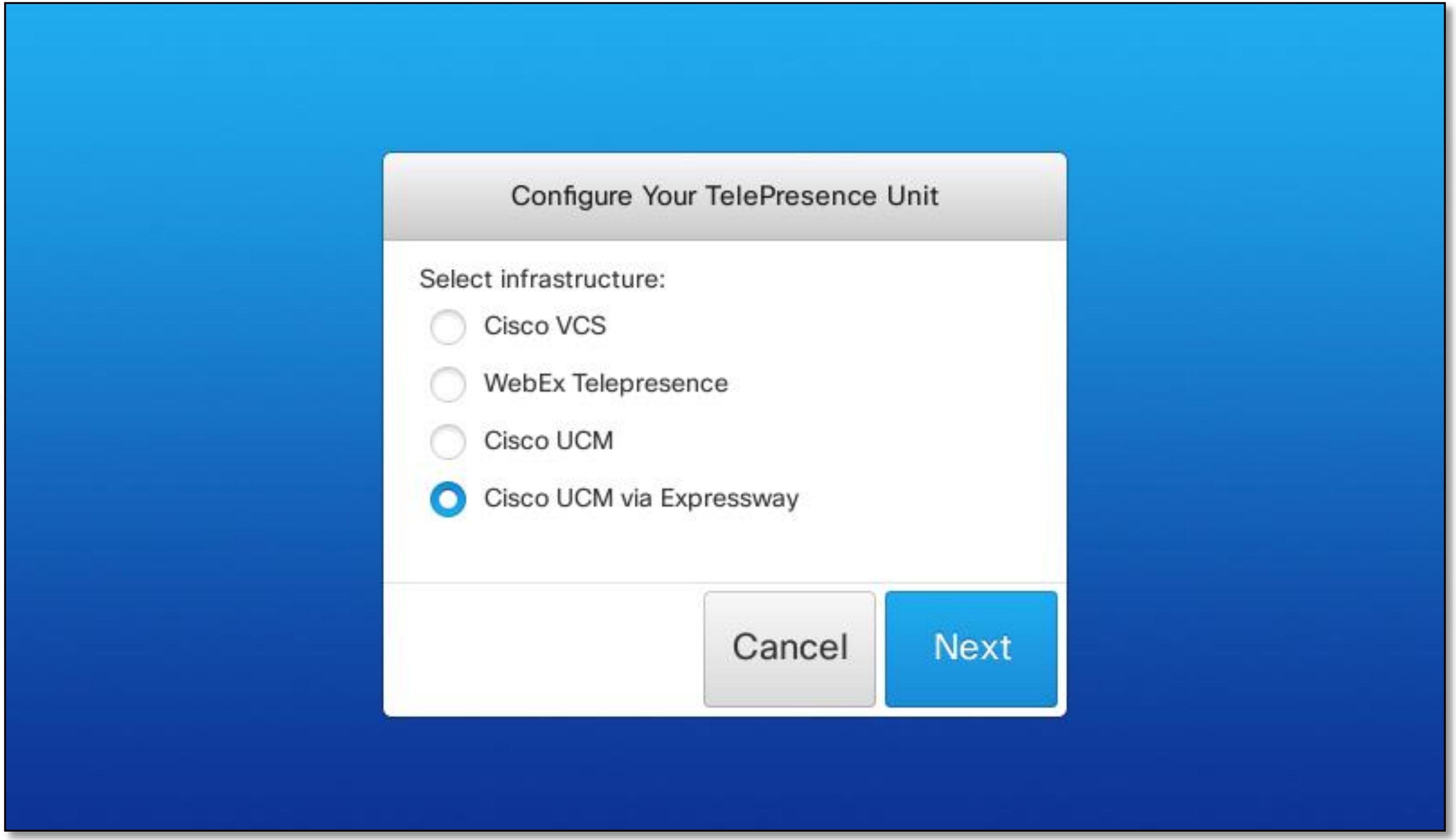
SIP stack attempts to refresh register 1 minute 55 seconds after last successful one

Appendix D
TelePresence Endpoint Provisioning

TC 7.1 Edge Endpoint Provisioning



TC 7.1 Edge Endpoint Provisioning



Configure Your TelePresence Unit

Select infrastructure:

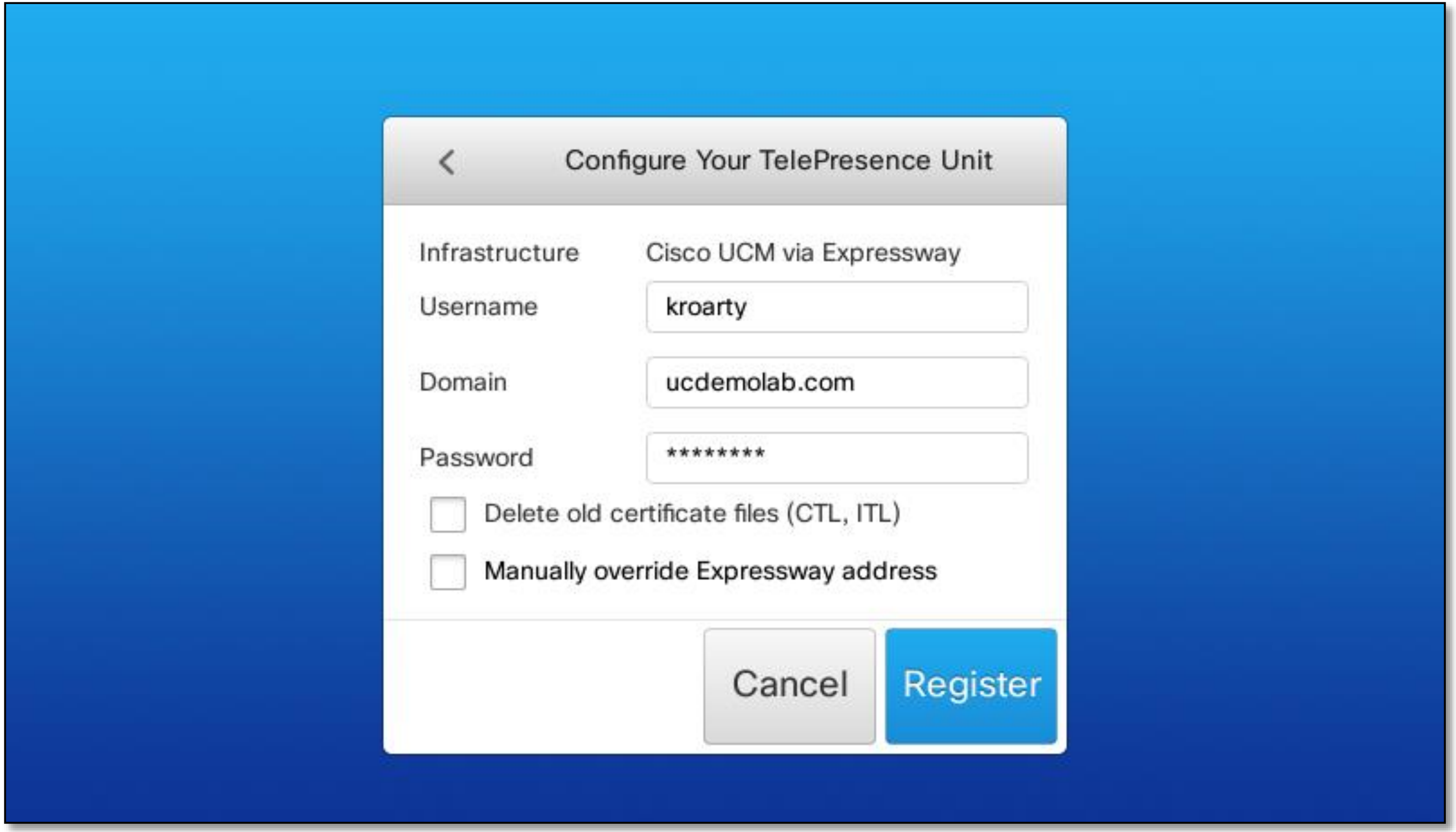
○ Cisco VCS

○ WebEx Telepresence

○ Cisco UCM

● Cisco UCM via Expressway

TC 7.1 Edge Endpoint Provisioning



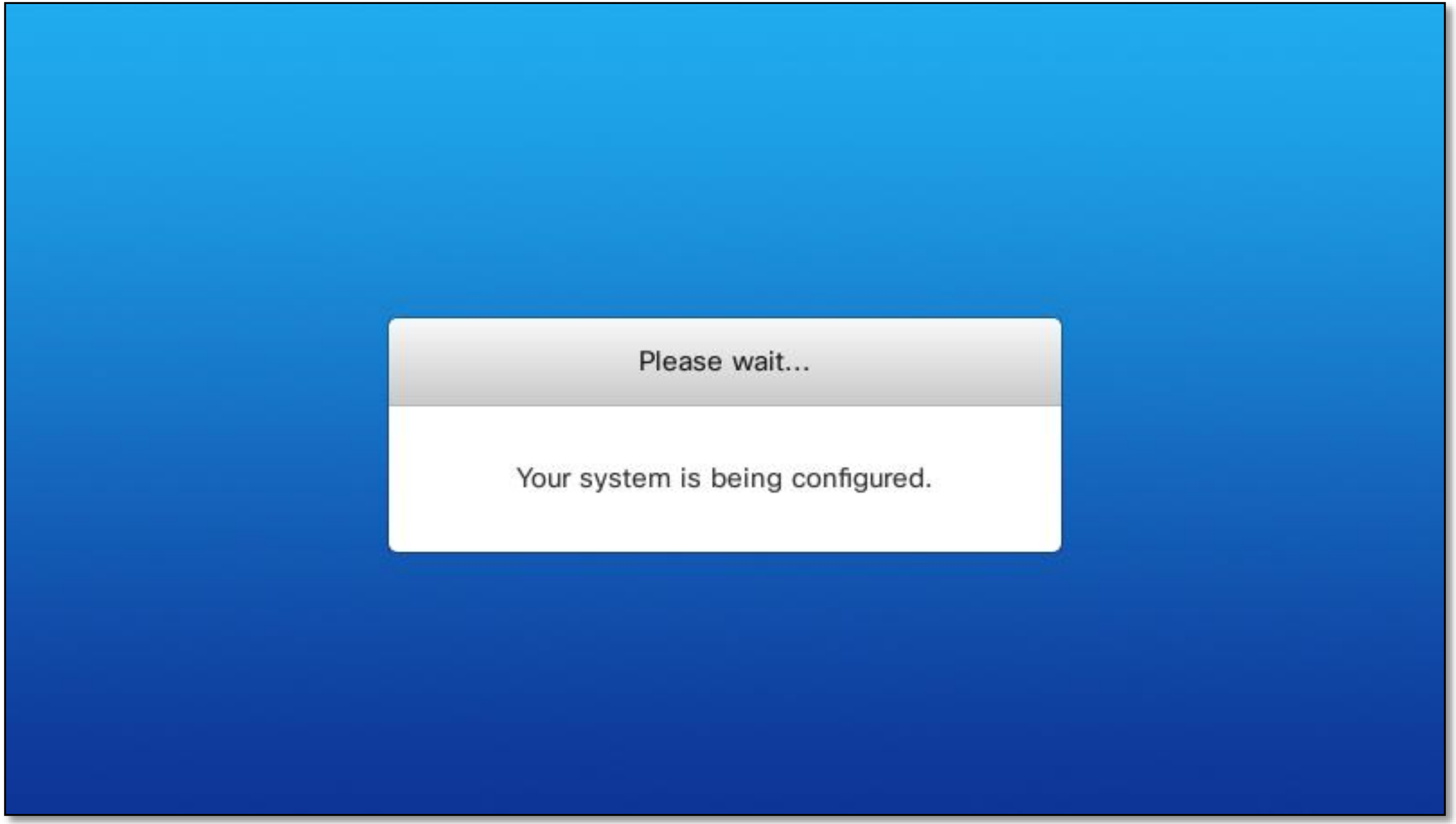
Configure Your TelePresence Unit

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

□ Delete old certificate files (CTL, ITL)

□ Manually override Expressway address

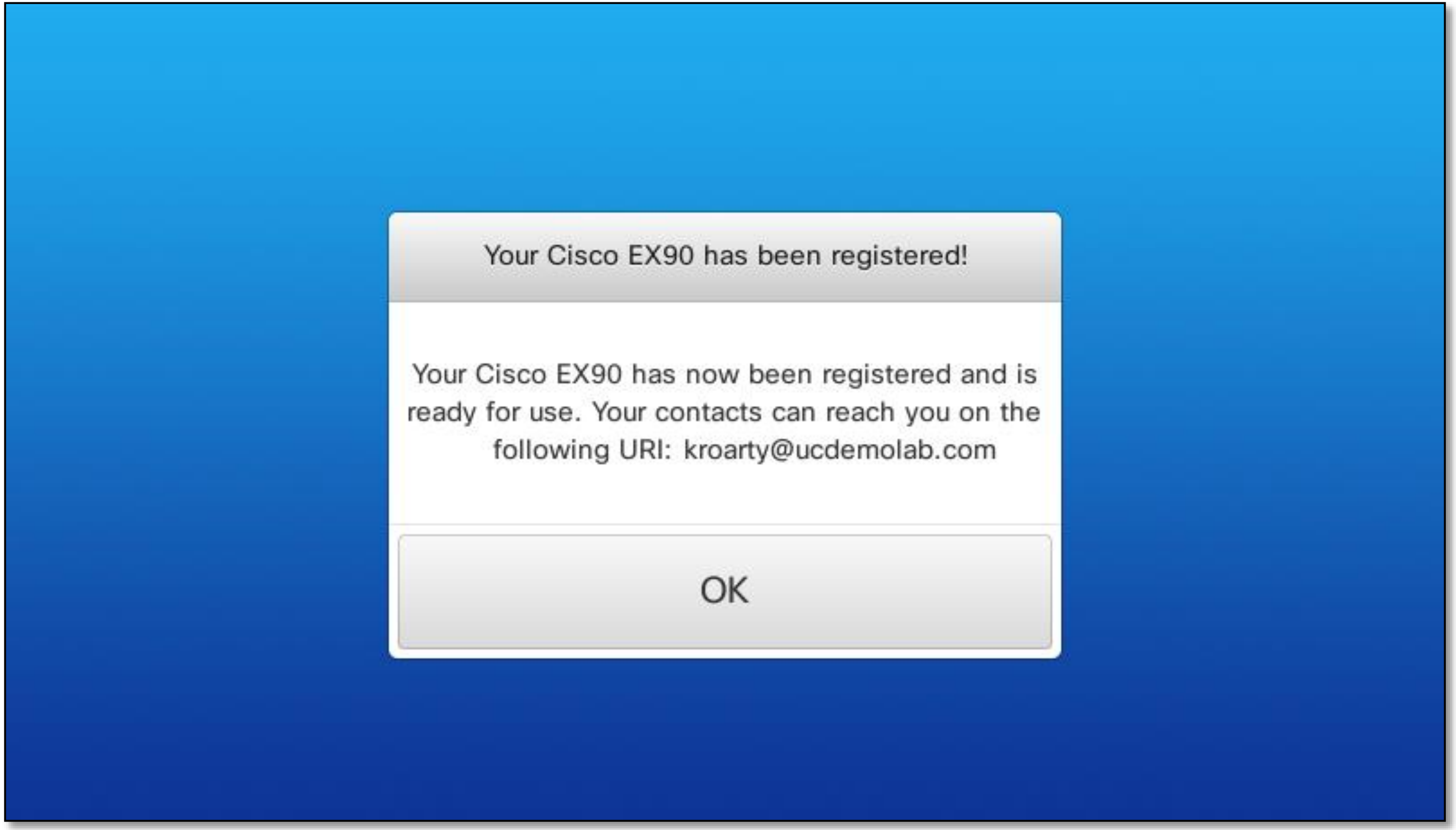
TC 7.1 Edge Endpoint Provisioning



Please wait...

Your system is being configured.

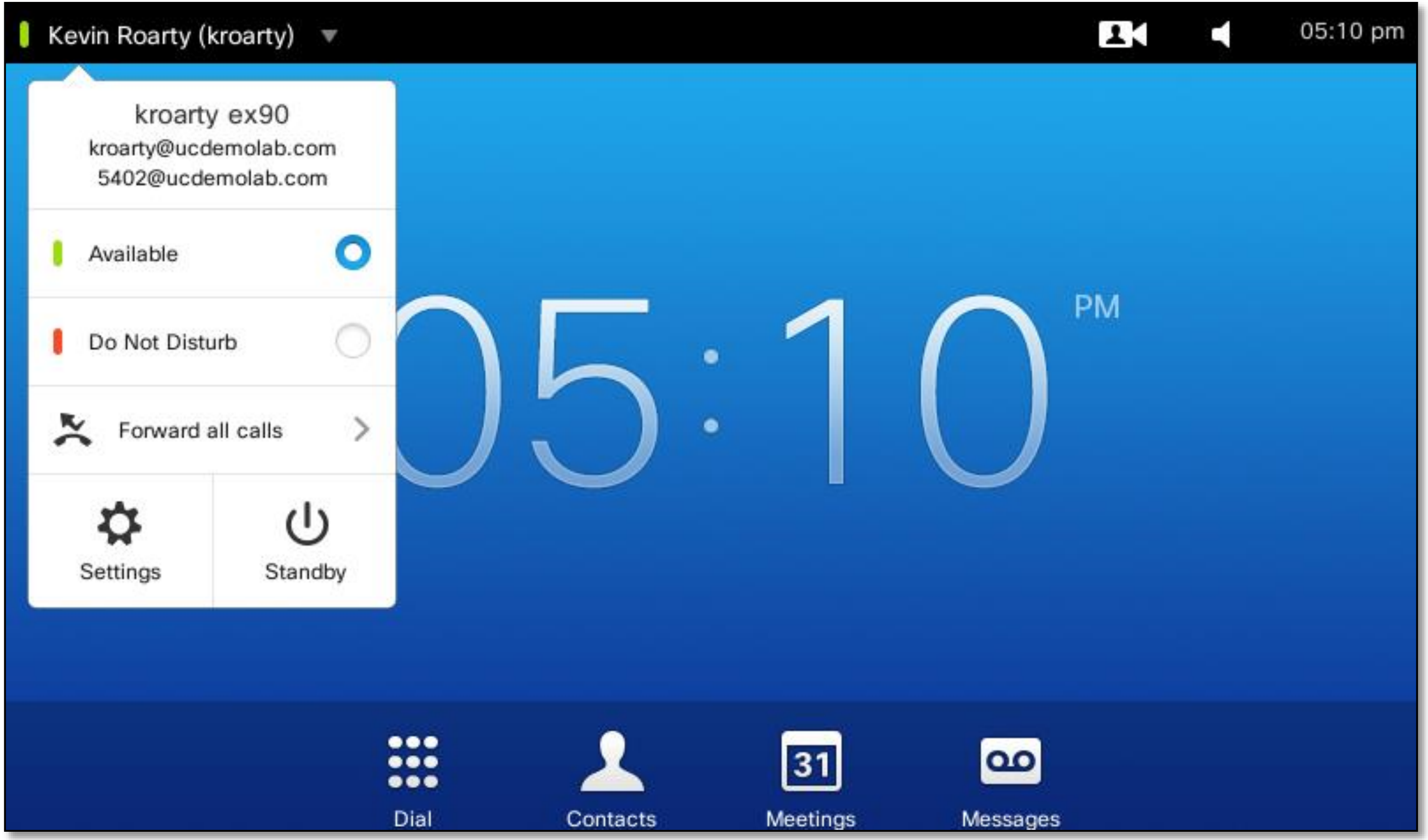
TC 7.1 Edge Endpoint Provisioning



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

TC 7.1 Edge Endpoint Provisioning



Kevin Roarty (kroarty)

05:10 pm

kroarty ex90

kroarty@ucdemolab.com

5402@ucdemolab.com

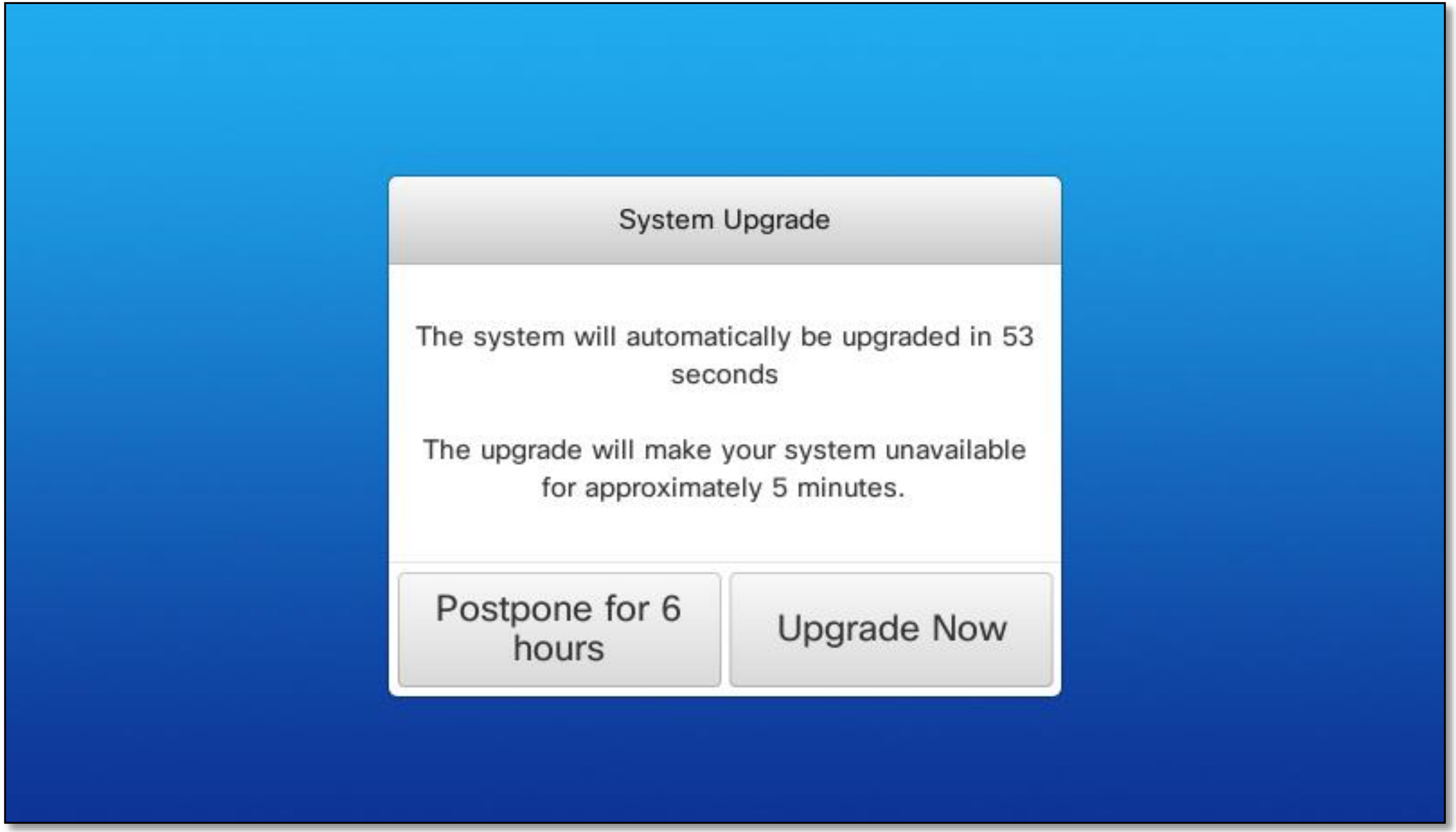
Available ●

Do Not Disturb ○

Forward all calls

05:10 PM

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.

CISCO