



*TOMORROW  
starts here.*

Cisco *live!*



# Configuring and Troubleshooting Cisco Jabber MRA using Collaboration- Edge Deployment Model

BRKCRT-2602

Rami Kandah - Technical Architect

#clmel

Cisco *live!*



# Agenda

- Terminology Introduction
- CCNA and CCNP Collaboration
- Expressway Mobile & Remote Access Solution Overview
- MRA Configuration Procedure
- Cisco Unified Communications Manager Configuration
- Cisco Unified IM and Presence Configuration
- Expressway Series Configuration
- Troubleshooting
- Conclusion





# Terminology Introduction

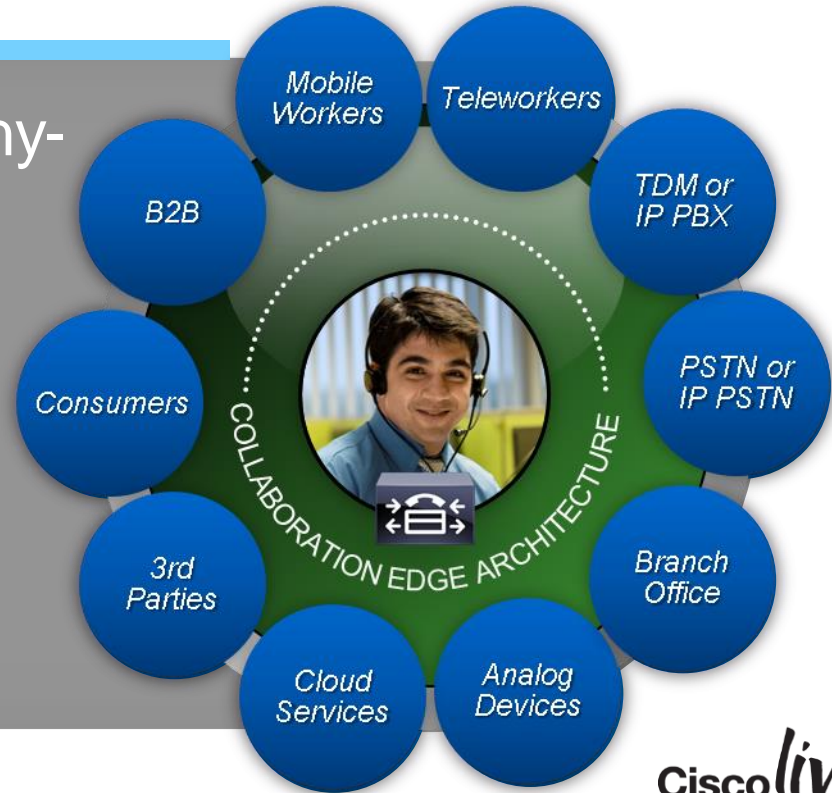


# Introducing Cisco Collaboration Edge Architecture

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

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

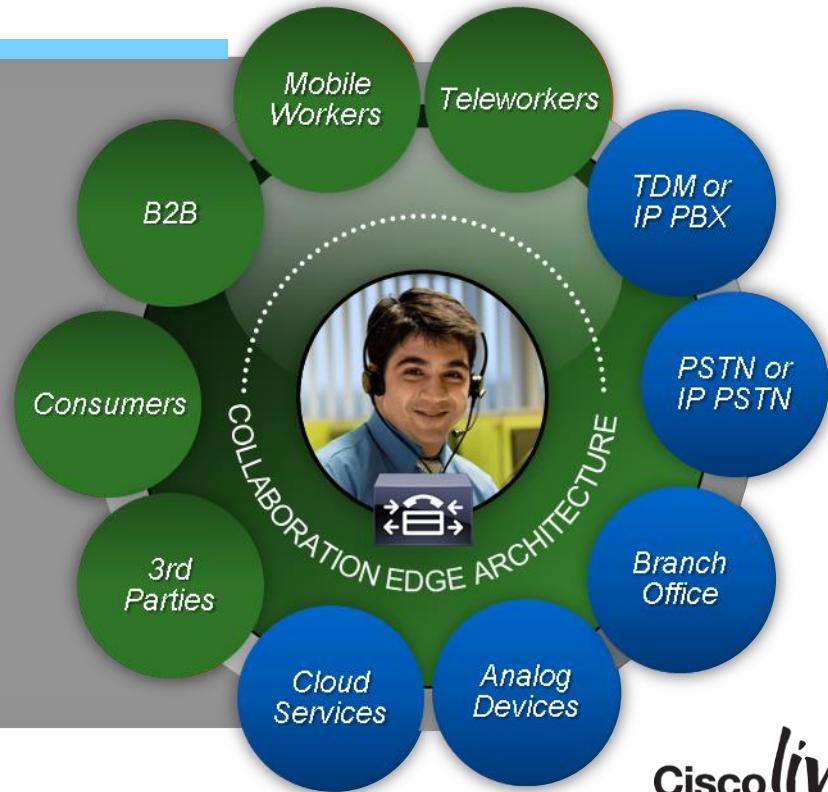
- TDM & analog gateways
- ISDN video gateways
- Session border control
- Firewall traversal
- Standards-based & secure



# Cisco Expressway

A gateway solving & simplifying business relevant use cases

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



# X8.1 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
- **Superset** of X8.1 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 X8.1 features
- No additional cost for server software licenses

# Branding Terminology Decode

## Collaboration Edge

umbrella term describing Cisco's entire collaboration architecture for edge  
... features and services that help bridge islands to enable any to any collaboration...  
...collaborate with anyone anywhere, on any device....

## Cisco VCS

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

## Cisco Expressway

**New** product line option for 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 X8.1 s/w  
Delivers VPN-less access to Jabber and Fixed Endpoints



A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with a glass railing spans across the street. The background features several modern buildings with lit windows and some streetlights. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

# Cisco CCNA and CCNP Collaboration Certification

Cisco *live!*

# Collaboration Engineer Evolving Skill Set

Voice and video skill sets converging to collaboration



- VoIP technologies
- Video end points
- Configuration of converged IP networks



- Integrated voice, video, web collaboration in converged network

# CCNA Collaboration



## Education

### What We Learn    How We Learn

- Unified Communications solutions
- Entry-level provisioning and support
- Video and conferencing concepts
- E-Learning Courses
- Instructor-Led Training



# Exams and Recommended Training

Required Exam(s)	Recommended Training*
210-060 CICD v1.0	Implementing Cisco Collaboration Devices (CICD v1.0)
210-065 CIVND v1.0	Implementing Cisco Video Network Devices, Part 1 (CIVND1 v1.0) – eLearning AND Implementing Cisco Video Network Devices, Part 2 (CIVND2 v1.0) – ILT

\*Delivered by Cisco Certified Learning Partners

# CCNP Collaboration

What We Learn    How We Learn

- Configuring Unified Communications Manager
- Implementing Video Mobility Features
- Troubleshooting
- Applications Management
- Instructor-led Training



Education

# Exams and Recommended Training

Required Exam(s)	Recommended Training*
300-070 CIPTV1 v1.0	Implementing Cisco IP Telephony & Video, Part 1 v1.0
300-075 CIPTV2 v1.0	Implementing Cisco IP Telephony & Video, Part 2 v1.0
300-080 CTCOLLAB v1.0	Troubleshooting Cisco IP Telephony & Video v1.0
300-085 CAPP5 v1.0	Implementing Cisco Collaboration Applications v1.0

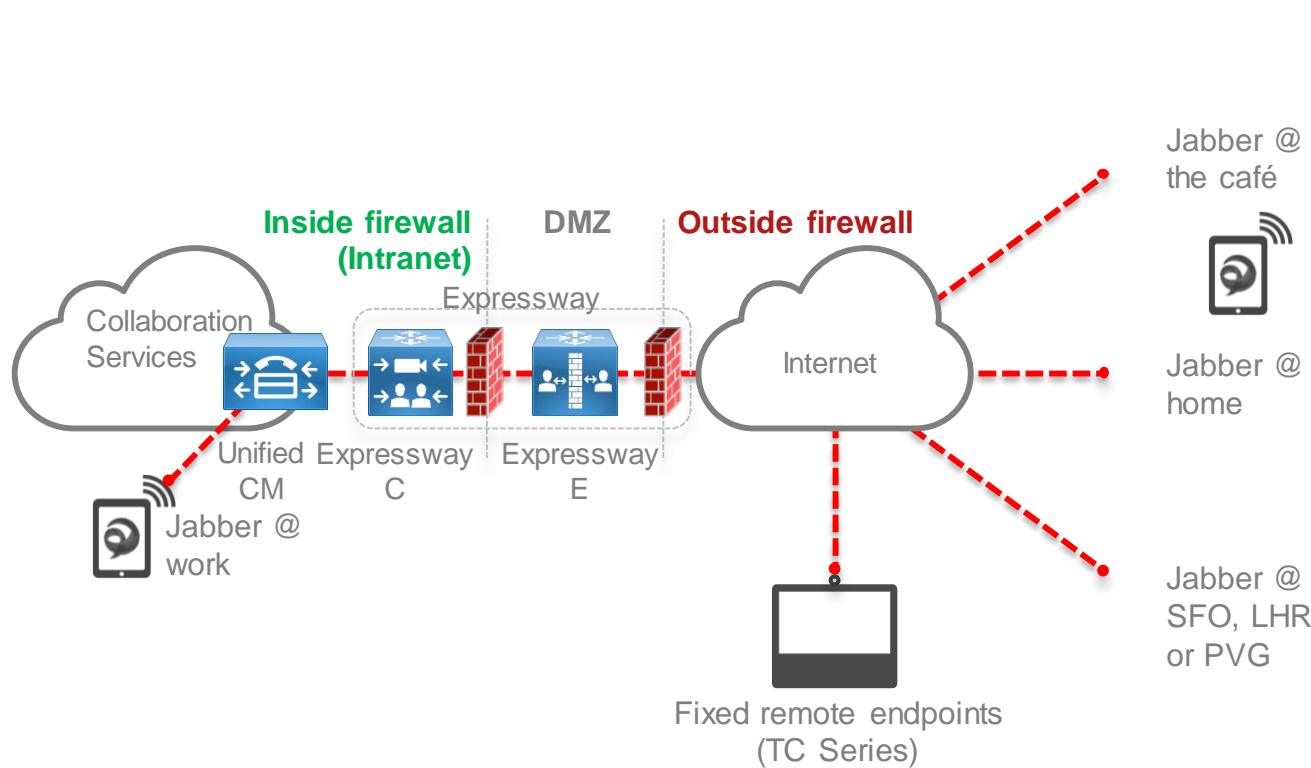
\*Delivered by Cisco Certified Learning Partners



A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with a glass railing spans across the street. The background features several modern buildings with lit windows and some colorful architectural lighting. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

# 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

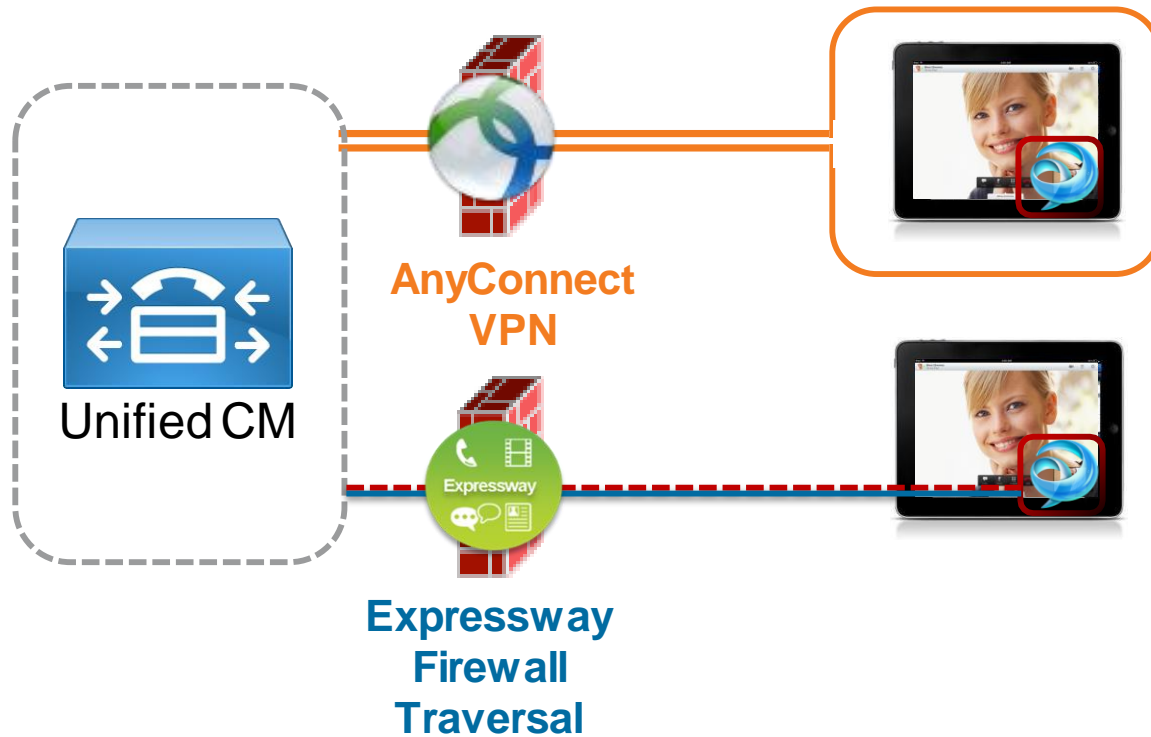
**Easy to use, easy to deploy:**  
Works with most firewall policies

**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

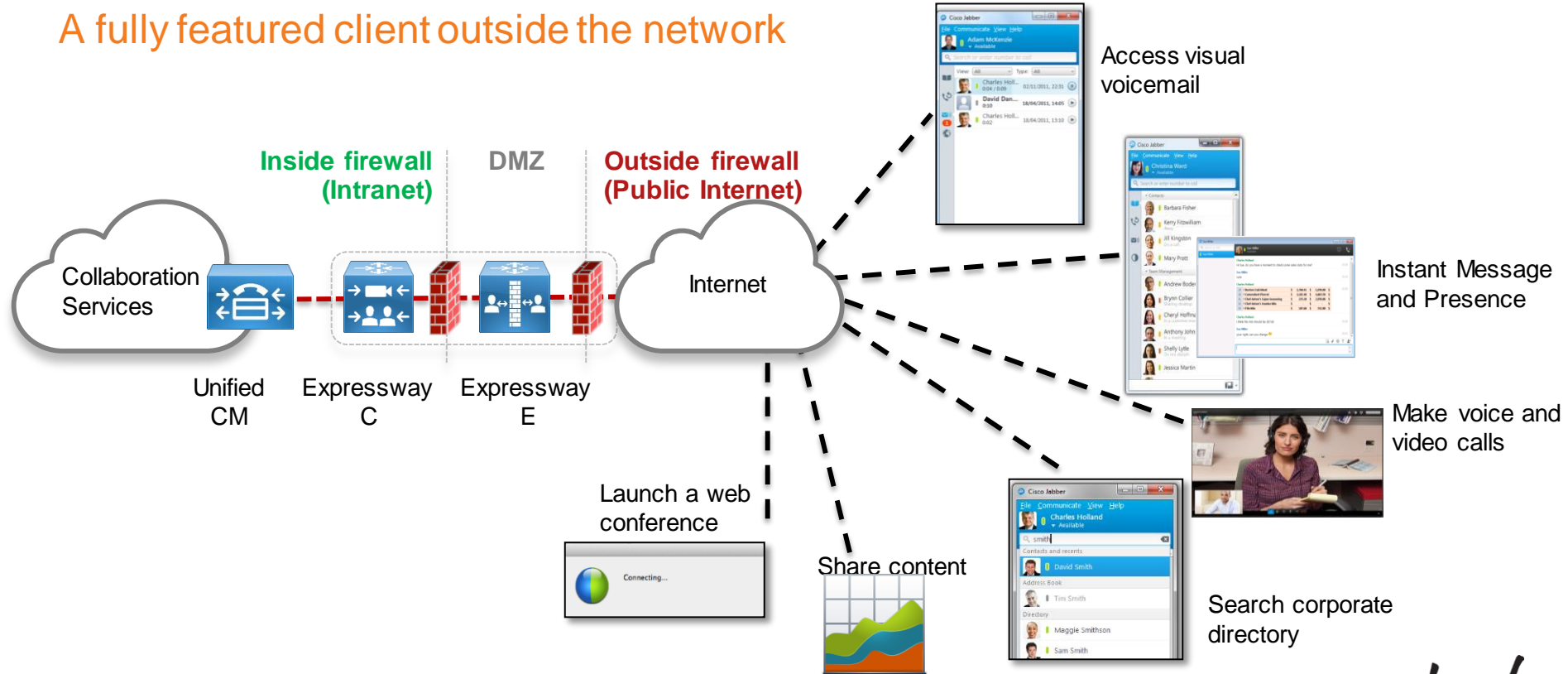


- Layer 3 VPN Solution
- Secures the entire device and it's contents
- AnyConnect allows users access to any permitted applications & data
- Session-based firewall traversal
- Secures access to collaboration applications ONLY
- Personal data not routed through enterprise network

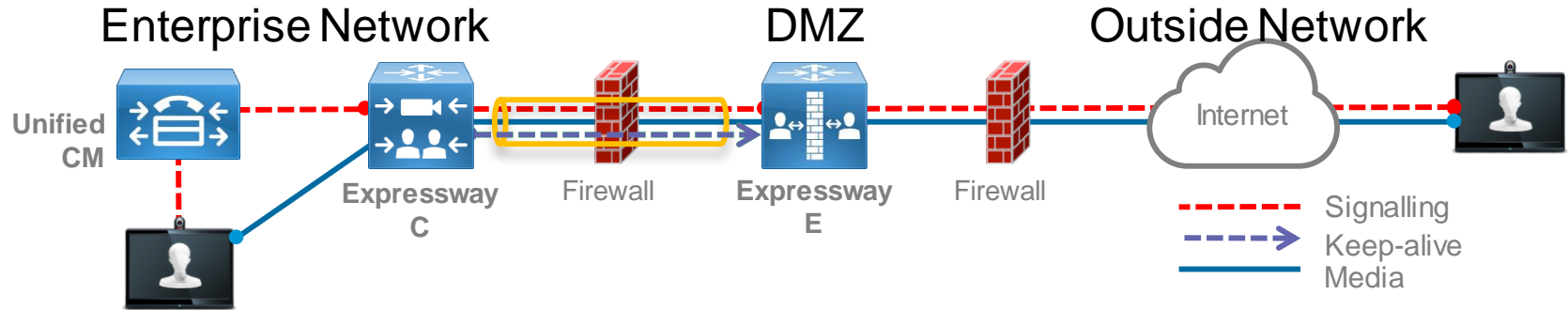


# What can a Jabber client do with Expressway?

A fully featured client outside the network

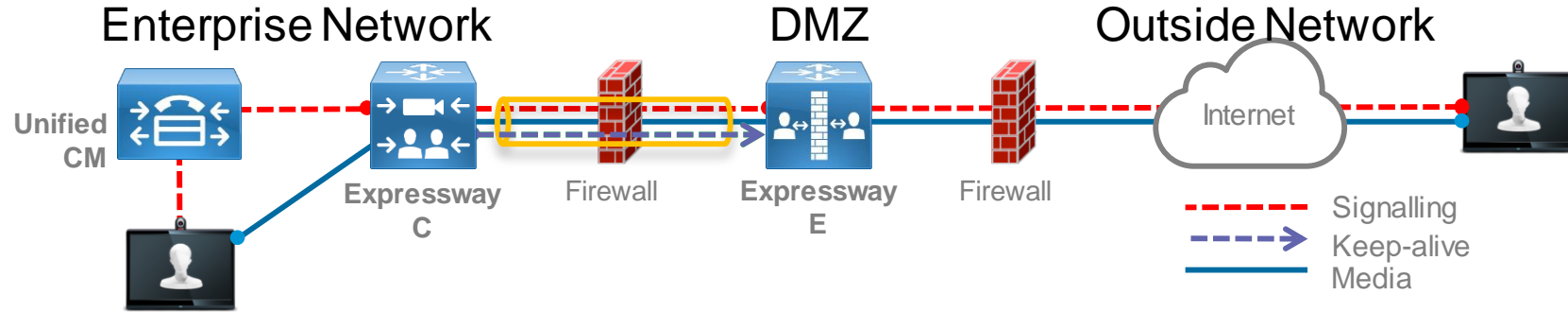


# Expressway Firewall Traversal Basics



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  
The call is established and media traverses the firewall securely over an existing traversal connection

# Expressway Firewall Traversal Basics

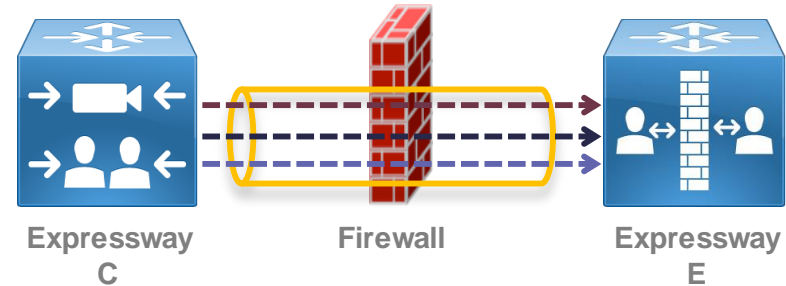


6. For outbound calls (from inside corporate), Unified CM will send a SIP Invite to Jabber with the Expressway-C IP address. (Unified CM knows that the Jabber client is registered through Expressway-C as proxy server)
7. Expressway-C forwards SIP Invite across the SSH Tunnel (Unified Communications Traversal Zone) to Expressway-E
8. Call forwarded to Remote Jabber client

# X8.1 Firewall Traversal Capabilities Expanded

The X8.1 release delivers 3 key capabilities enabling the Expressway Mobile and Remote Access feature

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

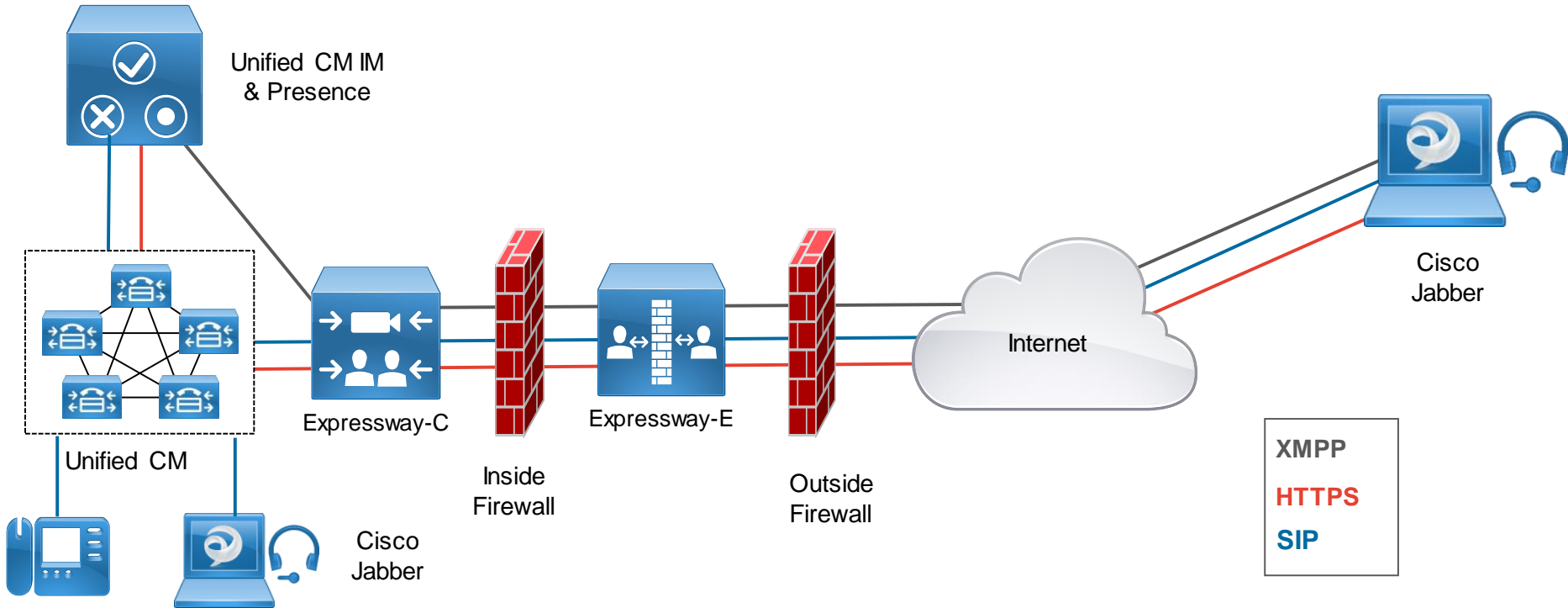


XCP is eXentsible Communications Platform

(details on new firewall port requirements covered later)



# Unified Communications Mobile and Remote Access Deployment



# Public (external) DNS SRV Requirements

Domain	Service	Protocol	Priority	Weight	Port	Target Host
collab10x.cisco.com	collab-edge	tls	10	10	8443	expressway-e.collab10x.cisco.com

# Local (internal) DNS SRV Requirements (only in **internal** DNS)

Domain	Service	Protocol	Priority	Weight	Port	Target Host
collab10x.cisco.com	cisco-uds	tcp	10	10	8443	pub10x-hq.collab10x.cisco.com
collab10x.cisco.com	cuplogin	tcp	10	10	8443	imp10x-hq.collab10x.cisco.com

# Allowed Reverse Proxy Traffic

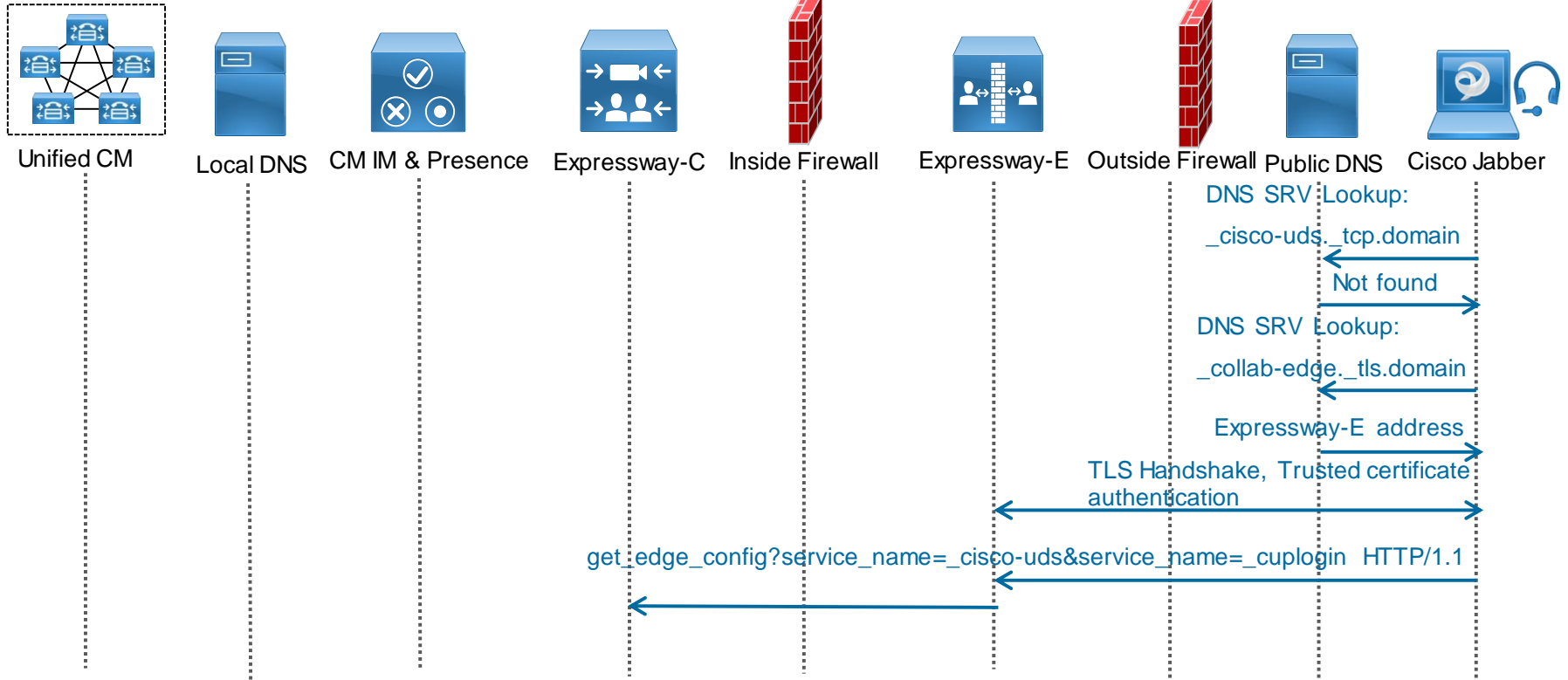
- Expressway-E server will be listening on TCP 8443 for HTTPS traffic
- Basic mobile & remote access configuration allows inbound authenticated HTTPS requests to the following destinations on the enterprise network
  - All discovered Unified CM nodes TCP 6970 (TFTP file requests) & TCP 8443 (UDS API)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



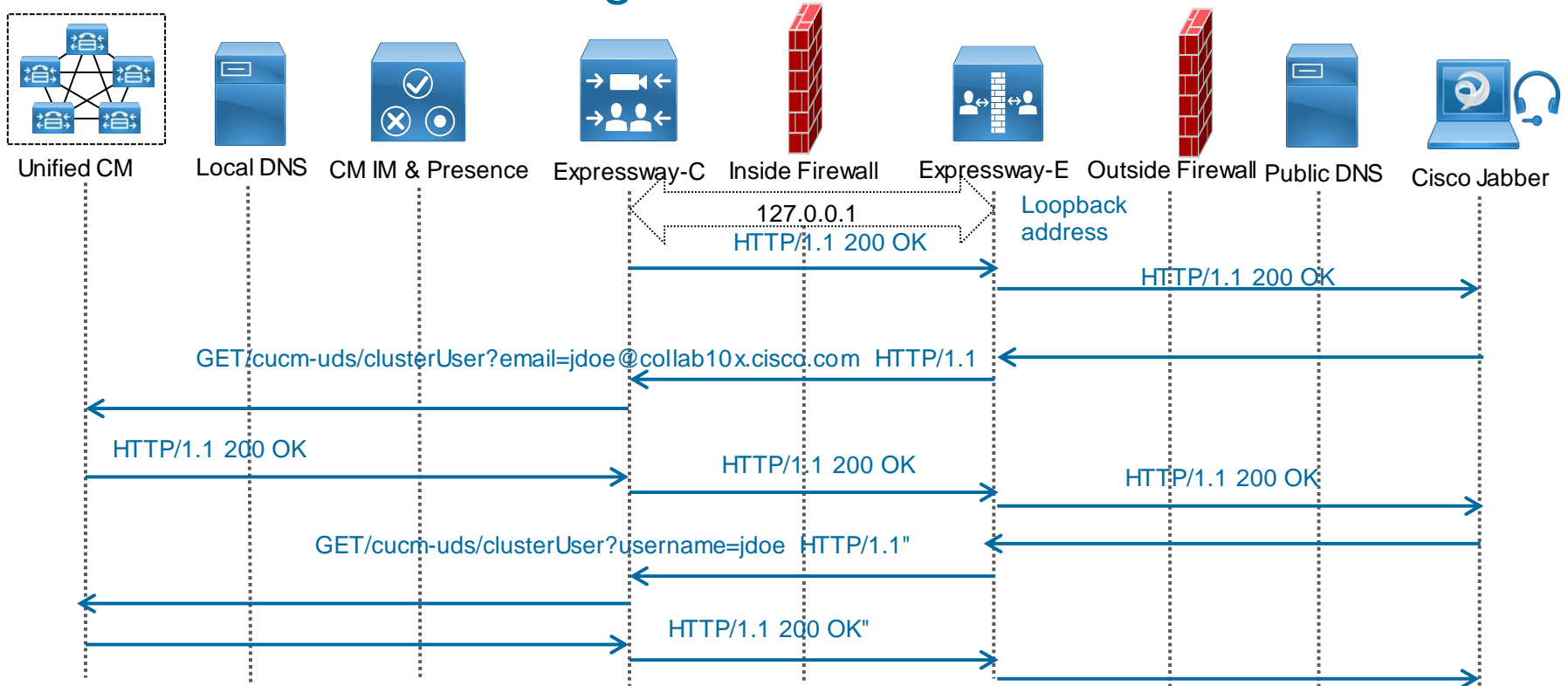
# Firewall Port Details

- **No inbound ports required to be opened on the internal firewall**
- Internal firewall needs to allow the following outbound connections from Expressway-C to Expressway-E
  - SIP: TCP 7001
  - Traversal Media: UDP 36000 to 36011
  - XMPP: TCP 7400
  - HTTPS (tunneled over SSH between C and E): TCP 2222
- External firewall needs to allow the following inbound connections to Expressway
  - SIP: TCP 5061
  - HTTPS: TCP 8443
  - XMPP: TCP 5222
  - Media: UDP 36002 to 59999

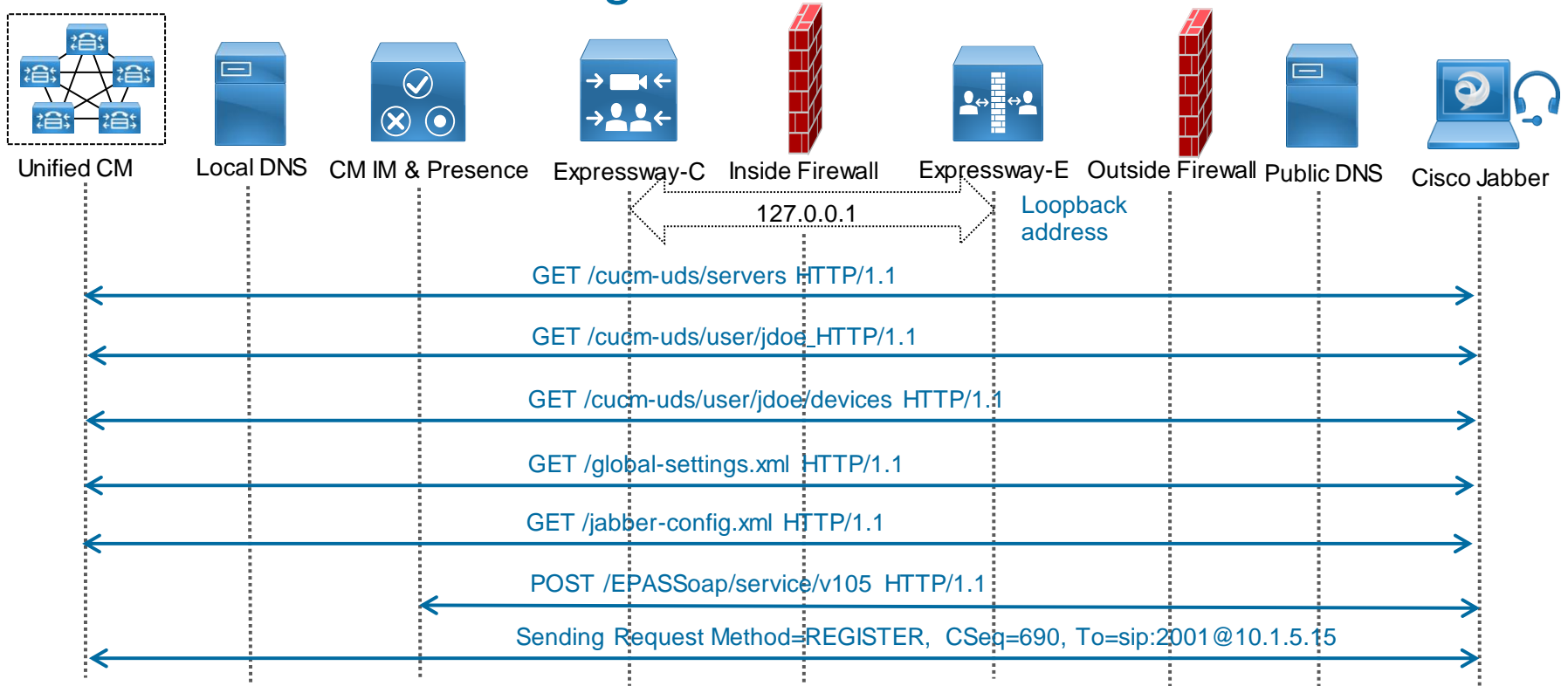
# Registering Remote Cisco Jabber to Cisco Unified Communications Manager



# Registering Remote Cisco Jabber to Cisco Unified Communications Manager



# Registering Remote Cisco Jabber to Cisco Unified Communications Manager





A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with a glass railing spans across the street. The background features several modern buildings with lit windows and some streetlights. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

# MRA Configuration Procedure

# Unified Communications Mobile and Remote Access Configuration Procedure

1. Configure Cisco Unified Communications Manager
2. Configure Cisco Unified IM and Presence
3. Configure Expressway Series



A nighttime photograph of a city street. In the foreground, there are long, curved light trails in shades of yellow, orange, and red, likely from a long-exposure shot of traffic. In the background, a modern cityscape is visible with illuminated buildings and a pedestrian bridge crossing the street. The sky is dark, and the overall scene is lit by city lights.

# Cisco Unified Communications Manager Configuration

# 1. Cisco Unified Communications Manager Configuration

- a) Configure SIP Trunk to Cisco Unified IM and Presence server
- b) Configure Domain and Publish SIP Trunk
- c) Configure Jabber in Cisco Unified Communications Manager
- d) Configure UC Service and Service Profile in Cisco Unified Communications Manager
- e) Enable User for Unified CM IM and Presence



# a) Configure SIP Trunk to Cisco Unified CM IM and Presence server

**Trunk Configuration**

Save Delete Reset Add New

**Status**  
Status: Ready

**SIP Trunk Status**  
Service Status: Unknown - OPTIONS Ping not enabled  
Duration: Unknown

**Device Information**

Product: SIP Trunk  
Device Protocol: SIP  
Trunk Service Type: None(Default)  
Device Name\*: IMP\_Trunk  
Description:  
Device Pool\*: Default

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Desti
1*	10.1.5.18		5060

MTP Preferred Originating Codec\*: 711ulaw  
BLF Presence Group\*: Standard Presence group  
SIP Trunk Security Profile\*: Non Secure SIP Trunk Profile  
Rerouting Calling Search Space: < None >  
Out-Of-Dialog Refer Calling Search Space: < None >  
SUBSCRIBE Calling Search Space: < None >  
SIP Profile\*: Standard SIP Profile [View Details](#)  
DTMF Signaling Method\*: No Preference

## b) Configure Domain and Publish SIP Trunk

Enterprise Parameters  
FQDN

Clusterwide Domain Configuration	
<a href="#">Organization Top Level Domain</a>	cisco.com
<a href="#">Cluster Fully Qualified Domain Name</a>	collab10x.cisco.com

<a href="#">Send SIP Multicast TTL in SDP</a> *	False
<a href="#">Default PUBLISH Expiration Timer</a> *	3600
<a href="#">Minimum PUBLISH Expiration Timer</a> *	60
<a href="#">IM and Presence Publish Trunk</a>	IMP_Trunk

Service Parameters  
Publish Trunk

This parameter specifies the SIP trunk that Cisco Unified Communications Manager uses to send PUBLISH messages that pertain to presence activities to Cisco Unified Presence (CUP).

# c) Configure Jabber in Cisco Unified Communications Manager

**Phone Configuration** Rela

Save Delete Copy Reset Apply Config Add New

**Status**  
Update successful

**Association**

1	Line [1] - 2001 in Internal pt
----- Unassigned Associated Items -----	
2	Line [2] - Add a new DN

**Phone Type**

**Product Type:** Cisco Unified Client Services Framework  
**Device Protocol:** SIP

**Real-time Device Status**

**Registration:** Registered with Cisco Unified Communications Manager 10.1.5.15  
**IPv4 Address:** 10.1.5.19  
**Active Load ID:** Jabber\_for\_Windows-10.6.0  
**Download Status:** None

**Device Information**

Device is Active  
 Device is trusted

**Device Name\*** CiscoJabber  
**Description**  
**Device Pool\*** Default  
**Common Device Configuration** < None >  
**Phone Button Template\*** Standard Client Services Framework  
**Common Phone Profile\*** Standard Common Phone Profile  
**Calling Search Space** Internal.CSS  
**AAR Calling Search Space** < None >

Device > Phone Type

Cisco Unified Client Services Framework (CSF)

Device Name

Any name – has no significance

## c) Configure Jabber in Cisco Unified Communications Manager

Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)
Owner User ID*	<input type="text" value="jdoe"/>

Protocol Specific Information	
Packet Capture Mode*	<input type="text" value="None"/>
Packet Capture Duration	<input type="text" value="0"/>
BLF Presence Group*	<input type="text" value="Standard Presence group"/>
SIP Dial Rules	<input type="text" value=" &lt; None &gt;"/>
MTP Preferred Originating Codec*	<input type="text" value="711ulaw"/>
Device Security Profile*	<input type="text" value="Cisco Unified Client Services Framework - Standar"/>
Rerouting Calling Search Space	<input type="text" value=" &lt; None &gt;"/>
SUBSCRIBE Calling Search Space	<input type="text" value=" &lt; None &gt;"/>
SIP Profile*	<input type="text" value="Standard SIP Profile"/>
Digest User	<input type="text" value=" &lt; None &gt;"/>



# c) Enable Video for Jabber in Cisco Unified Communications Manager

**Product Specific Configuration Layout**

Video Calling\* **Enabled**

Device CSF  
Enable Video Calling

**Region Configuration**

Save Delete Reset Apply Config Add New

**Region Information**

Name\* Default

**Region Relationships**






Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
Default	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	384 kbps
NOTE: Regions not displayed	Use System Default	Use System Default	Use System Default

System > Region  
Specify Video Bite Rate


## c) Configure Cisco Jabber Directory Number

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Applic

### Directory Number Configuration

 Save  Delete  Reset  Apply Config  Add New

**Status**

 Status: Ready

**Directory Number Information**

Directory Number\*

Route Partition

Description

**Directory Number Settings**

Voice Mail Profile

Calling Search Space

## d) Configure UC Services

**UC Service Configuration**

Save ~~Delete~~ Copy Reset Apply Config Add New

**Status**

Status: Ready

**UC Service Information**

**UC Service Type:** **IM and Presence**

Product Type\* Unified CM (IM and Presence)

Name\* IMP

Description

Host Name/IP Address\* 10.1.5.18

**UC Service Configuration**

Save ~~Delete~~ Copy Reset Apply Config Add New

**Status**

Status: Ready

**UC Service Information**

**UC Service Type:** **Directory**

Product Type\* Directory

Name\* UDS

Description

Host Name/IP Address\* 10.1.5.15

Port 389

Protocol TCP




### UC Service Type

UDS – Universal  
Directory Services on  
CUCM


## d) Configure Service Profile

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾

### Service Profile Configuration

Save  Delete  Copy  Add New

**Status**

 Status: Ready

**Service Profile Information**

Name\*

Description

Make this the default service profile for the system

**IM and Presence Profile**

Primary

Secondary

Tertiary

**Directory Profile**

Primary

Secondary

Tertiary

[Use UDS for Contact Resolution](#)

[Use Logged On User Credential](#)

[Username](#)

[Password](#)

[Search Base 1](#)

[Search Base 2](#)

[Search Base 3](#)

[Recursive Search on All Search Bases](#)

[Search Timeout \(seconds\)\\*](#)

## e) 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)

[Presence Viewer for User](#)

UC Service Profile:  [View Details](#)

---

### Device Information

Controlled Devices

Associate devices

Enable User for Unified CM and Presence



## e) End User Configuration

Allow Control of Device from CTI  
 Enable Extension Mobility Cross Cluster

---

**Directory Number Associations**

Primary Extension

Shared line

Enable Desk Phone Control  
Only for On-Prem

**Permissions Information**

Groups	Standard CCM End Users	▲
	Standard CTI Allow Call Monitoring	
	Standard CTI Allow Call Park Monitoring	
	Standard CTI Allow Call Recording	
	Standard CTI Allow Calling Number Modification	▼
Roles	Standard CTI Allow Calling Number Modification	▲
	Standard CTI Allow Control of All Devices	
	Standard CTI Allow Control of Phones supporting C	
	Standard CTI Allow Control of Phones supporting R	
	Standard CTI Enabled	▼

A nighttime photograph of a city street. In the foreground, there are long, curved light trails from traffic, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with blue lighting spans across the street. In the background, there are several tall buildings with lit windows and some flags on poles. The overall scene is illuminated by city lights.



# Cisco Unified CM IM and Presence Configuration

## 2. Cisco Unified CM IM and Presence Configuration


- a) Configure Service Parameters
- b) Configure Presence Settings
- c) Configure Presence Gateway
- d) Configure Client Settings
- e) Restart All Proxy Services
- f) Check System Dashboard and System Configuration Troubleshooter

# a) Configure Service Parameter

### Service Parameter Configuration

 Save  Set to Default

**Status**

 Status: Ready

**Select Server and Service**

Server\*

Service\*

All parameters apply only to the current server except parameters that are in the Clusterwide group(s).

**Cisco SIP Proxy (Active) Parameters on server 10.1.5.18--CUCM IM and Presence (Active)**

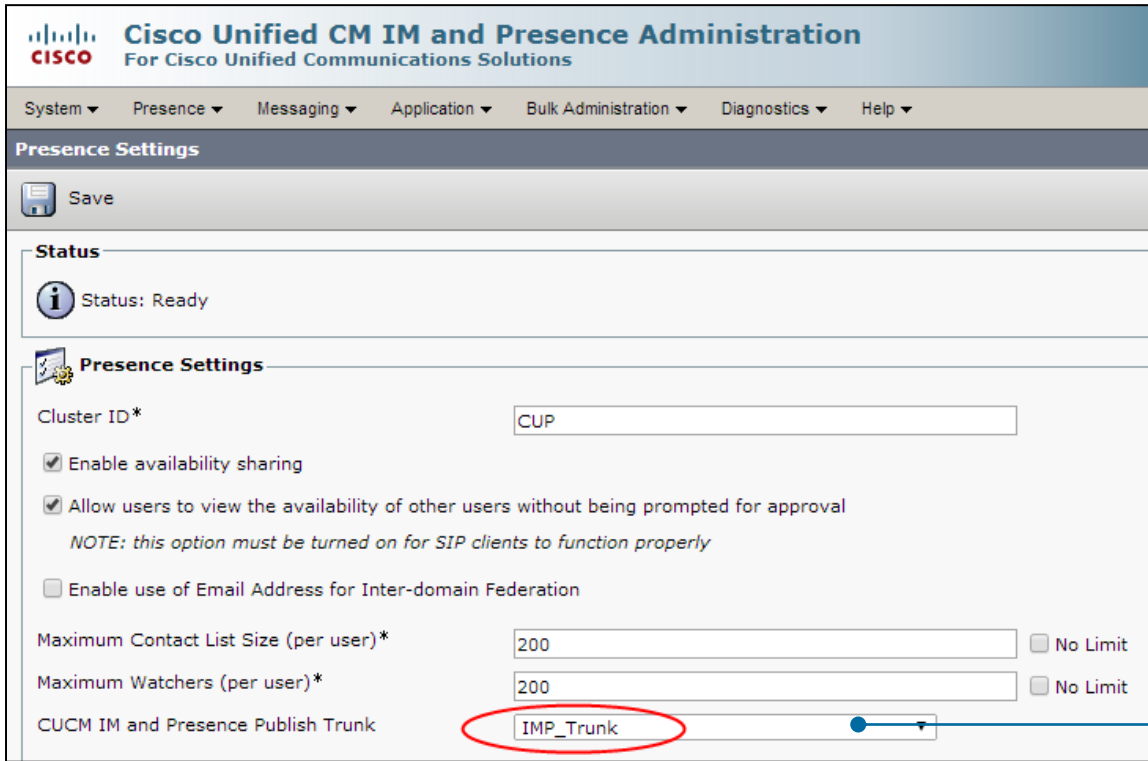
Parameter Name	Parameter Value
<b>General Proxy Parameters (Clusterwide)</b>	
<a href="#">Virtual IP Address (dotted-IPv4 format or IPv6)</a>	<input type="text"/>
<a href="#">SRV Cluster Name</a>	<input type="text"/>
<a href="#">CUCM Domain</a> *	<input type="text" value="collab10x.cisco.com"/>

CUCM Domain

Domain name configured in CUCM

**Cisco** live!

## b) Configure Presence Settings



The screenshot displays the Cisco Unified CM IM and Presence Administration interface. The top navigation bar includes 'System', 'Presence', 'Messaging', 'Application', 'Bulk Administration', 'Diagnostics', and 'Help'. The main content area is titled 'Presence Settings' and features a 'Save' button. Under the 'Status' section, it indicates 'Status: Ready'. The 'Presence Settings' section contains several configuration options: 'Cluster ID\*' is set to 'CUP'; 'Enable availability sharing' is checked; 'Allow users to view the availability of other users without being prompted for approval' is checked, with a note that this option must be turned on for SIP clients to function properly; 'Enable use of Email Address for Inter-domain Federation' is unchecked. Below these are two input fields for 'Maximum Contact List Size (per user)\*' and 'Maximum Watchers (per user)\*', both set to '200', each with a 'No Limit' checkbox. At the bottom, the 'CUCM IM and Presence Publish Trunk' is set to 'IMP\_Trunk', which is circled in red.

SIP Publish Trunk in  
CUCM

Cisco live!



## c) Configure Presence Gateway

**Presence Gateway Configuration**

Save Delete Add New

**Status**

Status: Ready

**Presence Gateway Settings (Cisco Unified Communications Manager)**

You can configure a Cisco Unified Communications Manager server as a presence gateway. The IM and Presence Service will then use this information (e.g. phone on/off hook status).

Presence Gateway Type\* CUCM

Description\* CUCM


Presence Gateway\* 10.1.5.15

Presence Gateway  
IP Address of CUCM


## d) Configure Client Settings

TFTP Servers  
Phone Control

### Client Settings

 Save

**Status**

 Status: Ready

**TFTP Servers**

Primary TFTP Server

Backup TFTP Server

Backup TFTP Server

**Cisco Unified Personal Communicator Security Certificates Setting**

CSF certificate directory (relative to CSF install directory)


## e) Restart All Proxy Services

### Proxy Configuration Settings

 Save

---

**Status**

 Status: Ready

---

**Restart**

**Restart All Proxy Services**

---

**General Configuration**

CVP Enable ACL Configuration

Method/Event Routing Status\*

Preferred Proxy Listener

# f) Check System Dashboard

**Cisco Unified CM IM and Presence Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM IM and Presence Administration

System | Presence | Messaging | Application | Bulk Administration | Diagnostics | Help

### System Dashboard

**System**

Troubleshooter Status ✓ 💬

CUCM Publisher 10.1.5.1

Sync Status **Completed**

Total End Users [1 view x](#)

Logged-in XMPP Users [1 view x](#)

**Federated Domains**

No federated domains currently provisioned [add >>](#)

**Cisco Jabber**

Troubleshooter Status ✓ 💬

**Calendar Integration**

No calendaring gateway currently provisioned [add >>](#)

**Topology**

Troubleshooter Status ✓ 💬

**System Troubleshooter Status (Click to anchor tooltip)**

System Troubleshooter			
Test Description	Outcome	Problem	Solution
Verify the size of the database for the node 10.1.5.18	<span>✓</span>		
Verify users are not at or exceeding the currently set Contact List Size limit (per user)	<span>✓</span>		
Verify users are not at or exceeding the currently set Watcher limit (per user)	<span>✓</span>		
Verify nodes in cluster are synchronised to the same NTP server	<span>✓</span>		
Verify Cisco IM and Presence Data Monitor service is running on all nodes.	<span>✓</span>		

Sync Agent Troubleshooter			
Test Description	Outcome	Problem	Solution
Verify AXL settings entry exists	<span>✓</span>		
Verify valid AXL user-id	<span>✓</span>		

## f) System Configuration Troubleshooter

The screenshot shows the 'System Configuration Troubleshooter' interface. At the top, there are navigation tabs: System, Presence, Messaging, Application, Bulk Administration, Diagnostics, and Help. Below the tabs is a 'Key' section with four items: Test Passed (green checkmark), Test Failed (red X), Test Warning (yellow triangle), and Information Only (blue circle with 'i'). The 'Results' section contains two tables. The first table, titled 'System Troubleshooter', has columns for 'Test Description', 'Outcome', and 'Problem'. It lists five tests, all with green checkmarks in the 'Outcome' column, which are circled in red. The second table, titled 'Sync Agent', has columns for 'Test Description' and 'Outcome' and shows one test: 'Verify AXL settings entry exists'.

Test Description	Outcome	Problem
Verify the size of the database for the node 10.1.5.18	✓	
Verify users are not at or exceeding the currently set Contact List Size limit (per user)	✓	
Verify users are not at or exceeding the currently set Watcher limit (per user)	✓	
Verify nodes in cluster are synchronised to the same NTP server	✓	
Verify Cisco IM and Presence Data Monitor service is running on all nodes.	✓	

Test Description	Outcome
Verify AXL settings entry exists	

Troubleshooting GUI for:

- System
- Sync Agent
- Presence Engine
- Sip Proxy
- Topology
- Cisco Jabber
- XCP
- User



A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in yellow and orange, indicating motion blur. In the middle ground, a pedestrian bridge with a glass railing spans across the street. The background features several modern buildings with lit windows and some streetlights. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

# Expressway Series Configuration

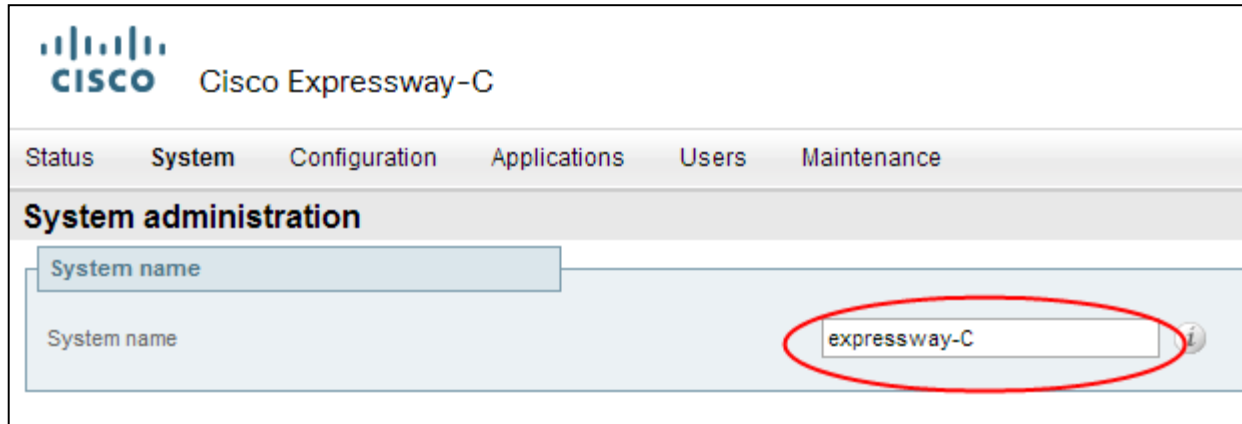
# 3. Expressway Series Configuration

- a) Setup basic configurations on Expressway Series
- b) Configure domains and supported services on Expressway-C
- c) Enable MRA on Expressway Series
- d) Configure Unified CM Servers on Expressway-C
- e) Configure IM and Presence Server on Expressway-C
- f) Check Status of servers and Search Rules on Expressway-C
- g) Expressway server certificates requirements
- h) Subject Alternative Name (SAN) requirements
- i) Generate CSR on Expressway-C

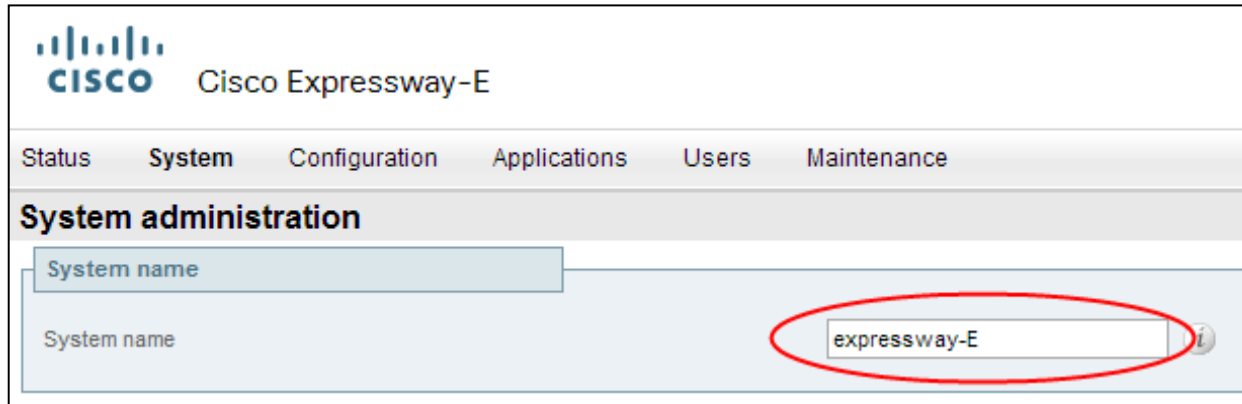
## 3. Expressway Series Configuration

- j) Generate CSR on Expressway-E
- k) Download Expressway certificates for signing by CA
- l) Upload signed certificates
- m) Upload CA certificate to Expressway-C and Expressway-E
- n) Configure Traversal Client on Expressway-C
- o) Configure Traversal Server on Expressway-E
- p) Verification

# a) Basic Configuration - System Name

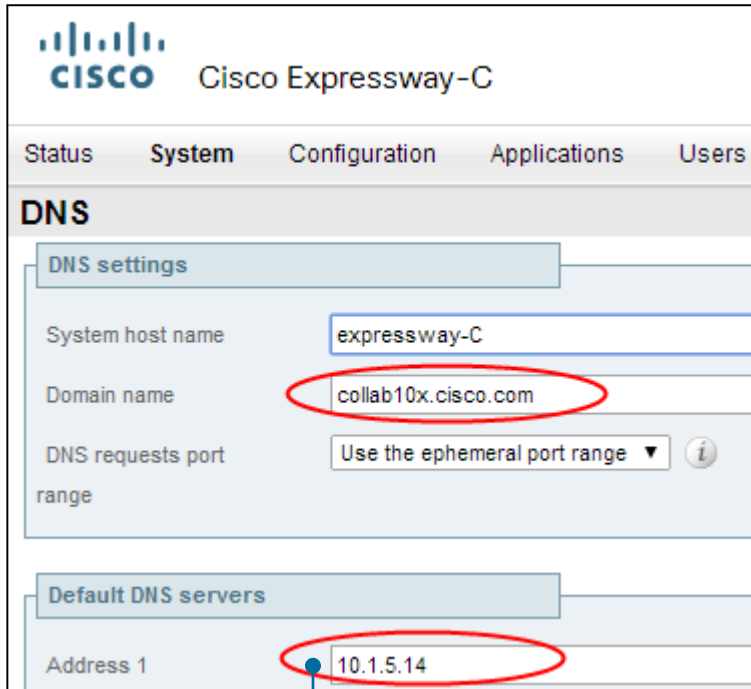


The screenshot shows the Cisco Expressway-C configuration interface. At the top left is the Cisco logo and the text "Cisco Expressway-C". Below this is a navigation bar with tabs for "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". The "System" tab is selected. Underneath is a section titled "System administration". A form field labeled "System name" is highlighted with a blue box. Below this, the current system name "expressway-C" is displayed in a white box with a red oval around it. A small information icon is visible to the right of the text.



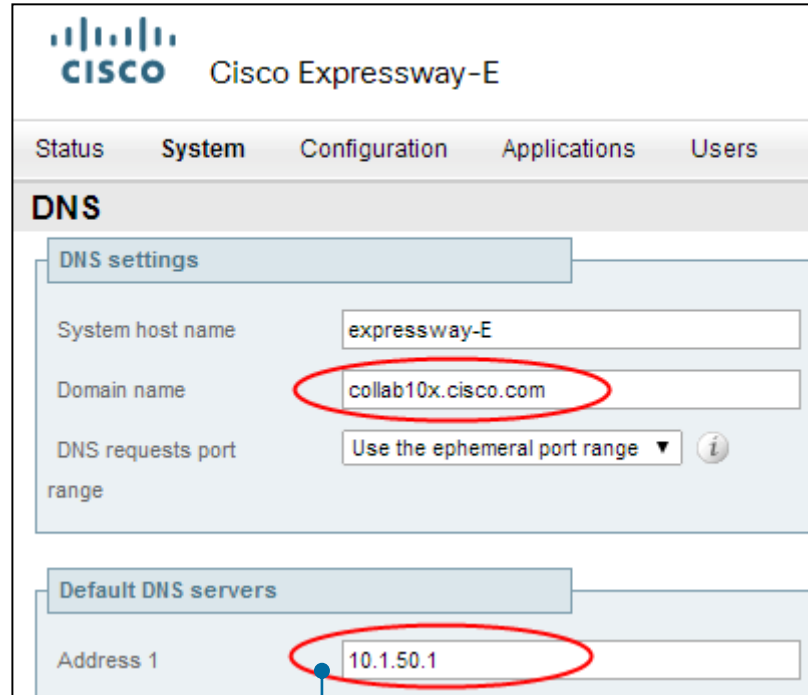
The screenshot shows the Cisco Expressway-E configuration interface. At the top left is the Cisco logo and the text "Cisco Expressway-E". Below this is a navigation bar with tabs for "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". The "System" tab is selected. Underneath is a section titled "System administration". A form field labeled "System name" is highlighted with a blue box. Below this, the current system name "expressway-E" is displayed in a white box with a red oval around it. A small information icon is visible to the right of the text.

# a) Basic Configuration - DNS



The screenshot shows the Cisco Expressway-C configuration page for DNS. The 'DNS settings' section includes: System host name: expressway-C; Domain name: collab10x.cisco.com (circled in red); DNS requests port range: Use the ephemeral port range. The 'Default DNS servers' section includes: Address 1: 10.1.5.14 (circled in red with a blue dot and line pointing to the label 'Corporate DNS' below).

Corporate DNS

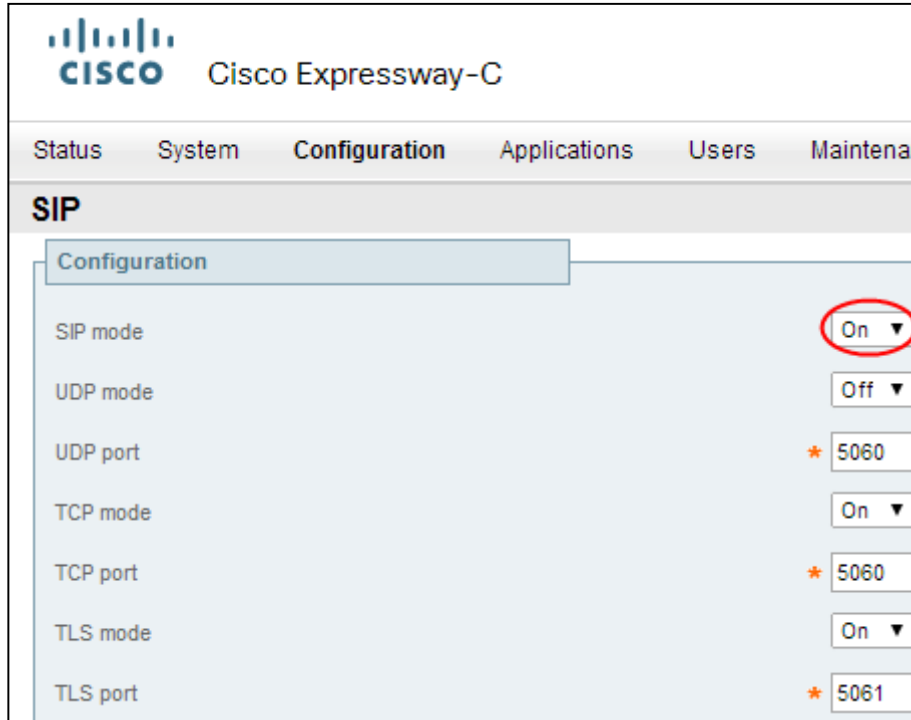


The screenshot shows the Cisco Expressway-E configuration page for DNS. The 'DNS settings' section includes: System host name: expressway-E; Domain name: collab10x.cisco.com (circled in red); DNS requests port range: Use the ephemeral port range. The 'Default DNS servers' section includes: Address 1: 10.1.50.1 (circled in red with a blue dot and line pointing to the label 'Public DNS' below).

Public DNS

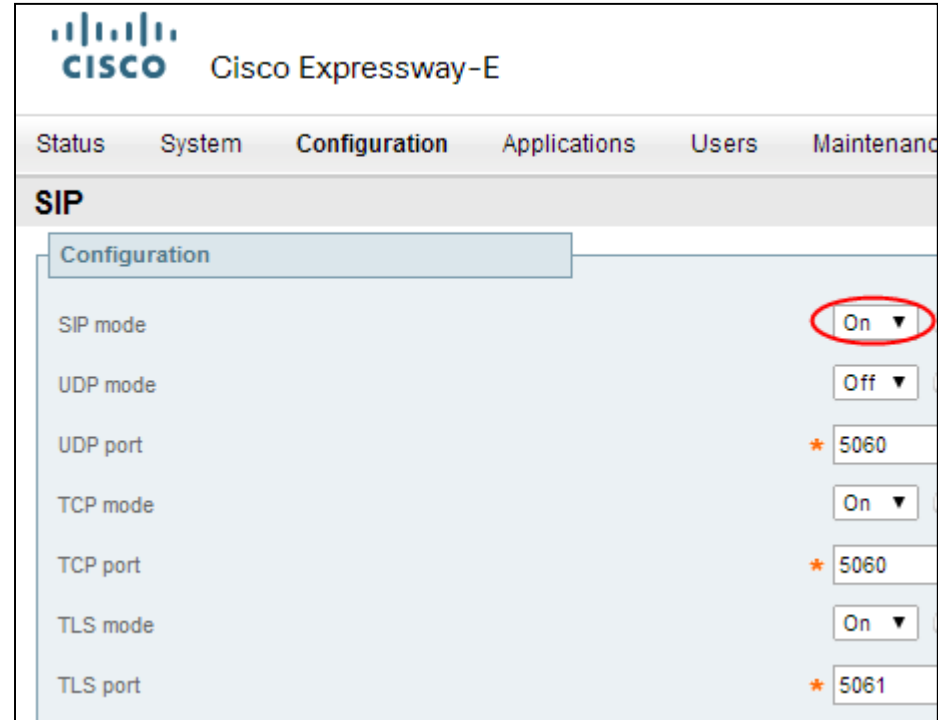


# a) Basic Configuration - SIP



The screenshot shows the Cisco Expressway-C configuration interface. The 'SIP' section is expanded to show the 'Configuration' tab. The 'SIP mode' dropdown menu is circled in red and set to 'On'. Other settings include UDP mode (Off), UDP port (5060), TCP mode (On), TCP port (5060), TLS mode (On), and TLS port (5061).

Parameter	Value
SIP mode	On
UDP mode	Off
UDP port	5060
TCP mode	On
TCP port	5060
TLS mode	On
TLS port	5061



The screenshot shows the Cisco Expressway-E configuration interface. The 'SIP' section is expanded to show the 'Configuration' tab. The 'SIP mode' dropdown menu is circled in red and set to 'On'. Other settings include UDP mode (Off), UDP port (5060), TCP mode (On), TCP port (5060), TLS mode (On), and TLS port (5061).

Parameter	Value
SIP mode	On
UDP mode	Off
UDP port	5060
TCP mode	On
TCP port	5060
TLS mode	On
TLS port	5061

## b) Configure Domains and Supported Services on Expressway-C

The screenshot displays the Cisco Expressway-C configuration interface. At the top, the Cisco logo and 'Cisco Expressway-C' are visible. Below this is a navigation bar with tabs for 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The 'Configuration' tab is selected, and the 'Domains' section is expanded. Under 'Domains', there is a 'Configuration' sub-section. The 'Domain name' field is set to 'collab10x.cisco.com', which is circled in red. Below this, the 'Supported services for this domain' section is expanded, showing three services: 'SIP registrations and provisioning on Unified CM' (set to 'On'), 'IM and Presence Service' (set to 'On'), and 'XMPP federation' (set to 'Off'). Each service has a dropdown menu and an information icon, with the 'On' dropdowns circled in red.

**CISCO** Cisco Expressway-C

Status System **Configuration** Applications Users Maintenance

### Domains

Configuration

Domain name \* collab10x.cisco.com

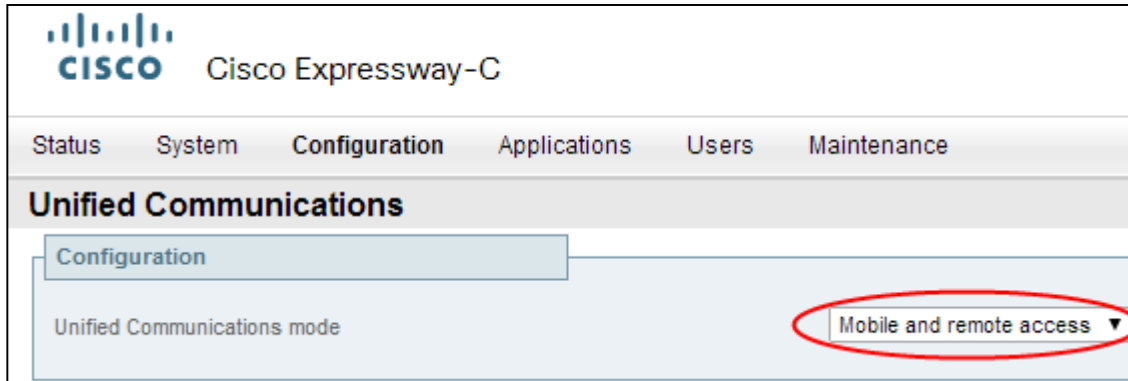
Supported services for this domain

SIP registrations and provisioning on Unified CM On ▼ ⓘ

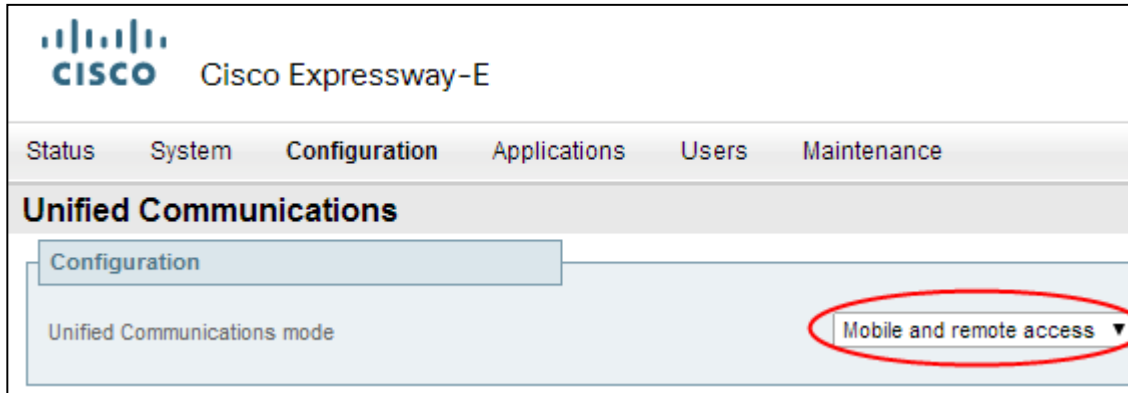
IM and Presence Service On ▼ ⓘ

XMPP federation Off ▼ ⓘ

## c) Enable MRA



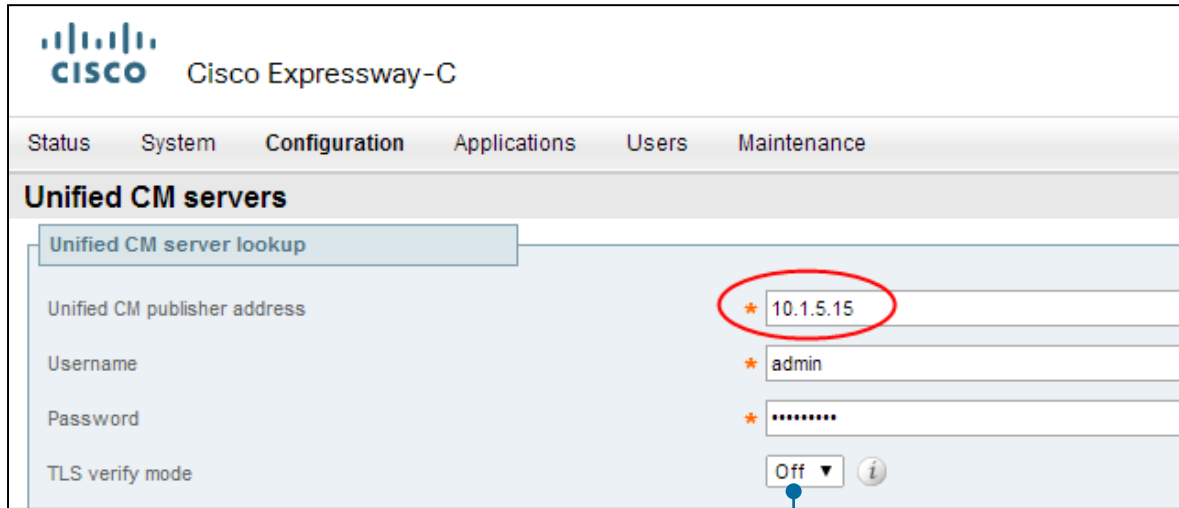
The screenshot shows the Cisco Expressway-C configuration interface. At the top left is the Cisco logo and the text "Cisco Expressway-C". Below this is a navigation bar with tabs for "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". The "Configuration" tab is selected. Underneath, there is a "Unified Communications" section with a "Configuration" sub-section. In the "Unified Communications mode" area, the "Mobile and remote access" dropdown menu is highlighted with a red circle.



The screenshot shows the Cisco Expressway-E configuration interface, which is identical in layout to the Expressway-C page. It features the Cisco logo, "Cisco Expressway-E" title, and the same navigation and configuration structure. The "Mobile and remote access" dropdown menu in the "Unified Communications mode" section is also highlighted with a red circle.

Enable Mobile and Remote Access

## d) Configure Unified CM Servers on Expressway-C



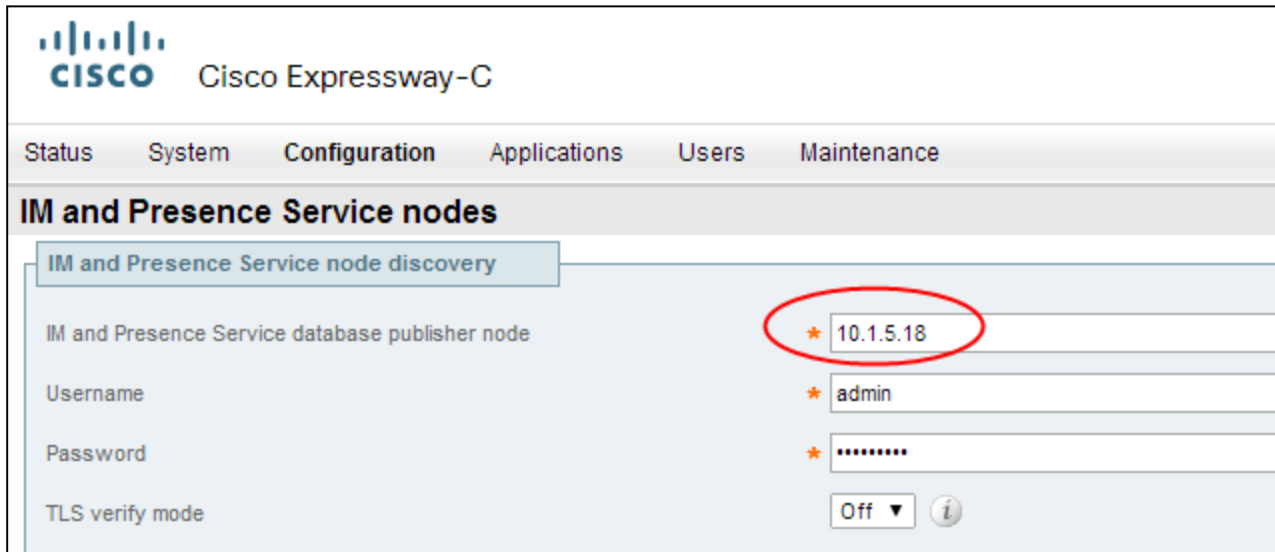
The screenshot shows the Cisco Expressway-C configuration interface. At the top, there is a navigation menu with tabs for Status, System, Configuration, Applications, Users, and Maintenance. The 'Configuration' tab is selected. Below the navigation, the 'Unified CM servers' section is active, showing a 'Unified CM server lookup' form. The form contains the following fields:

Field	Value
Unified CM publisher address	10.1.5.15
Username	admin
Password	*****
TLS verify mode	Off

The IP address '10.1.5.15' is circled in red. The 'TLS verify mode' dropdown is set to 'Off' and has a blue dot below it with a line pointing to the explanatory text.

If TLS verify mode is enabled, the Unified CM system's FQDN or IP address must be contained within the X.509 certificate. The certificate itself must also be valid and signed by a trusted certificate authority.

## e) Configure IM and Presence Server on Expressway-C



The screenshot shows the Cisco Expressway-C configuration interface. The top navigation bar includes 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The main heading is 'IM and Presence Service nodes'. A sub-section titled 'IM and Presence Service node discovery' is active. The configuration fields are as follows:

Field	Value
IM and Presence Service database publisher node	* 10.1.5.18
Username	* admin
Password	* .....
TLS verify mode	Off ▼ ⓘ

The IP address '10.1.5.18' in the first row is circled in red.



# f) Check Status of Servers on Expressway-C

Cisco Expressway-C

Status System Configuration Applications Users Maintenance

**Unified CM servers**

You are here: Configuration > Unified CM servers

Publisher address	Username	TLS verify mode	Nodes discovered by this lookup
<input type="checkbox"/> 10.1.5.15	admin	Off	10.1.5.16, 10.1.5.15

New Delete Select all Unselect all Refresh servers

Click Refresh servers to refresh the details of the nodes associated with this publisher address.

**Currently found Unified CM nodes**

Publisher address	Name	Protocol	Version	Status
10.1.5.15	10.1.5.15	TCP	10.0.1	TCP: Active
10.1.5.15	10.1.5.16	TCP	10.0.1	TCP: Active

Publisher & Subscriber nodes

Cisco Expressway-C

Status System Configuration Applications Users Maintenance

**IM and Presence Service nodes**

You are here: Configuration > Unified Communications > IM and Presence Service nodes

Publisher address	Username	TLS verify mode	Nodes discovered by this lookup
<input type="checkbox"/> 10.1.5.18	admin	Off	10.1.5.18

New Delete Select all Unselect all Refresh servers

Click Refresh servers to refresh the details of the nodes associated with this publisher address.

**Currently found IM and Presence Service nodes**

Publisher address	Name	Version	Status
10.1.5.18	10.1.5.18	10.5.2	Active

IM and Presence node

## g) Check Search Rules

Cisco Expressway-C

This system has 6 alarms

Status System **Configuration** Applications Users Maintenance

You are here: Configuration > Dial plan > Search rules

Priority	Rule name	Protocol	Source	Authentication required	Mode	Pattern type	Pattern string	Pattern behavior	On match	Target	State	Actions
45	<a href="#">CEtcp-10.1.5.15</a>	SIP	Any	No	Alias pattern match	Prefix	10.1.5.15;transport=TCP	Leave	Stop	<a href="#">CEtcp-10.1.5.15</a>	✓ Enabled	<a href="#">View</a>   <a href="#">Clone</a>
45	<a href="#">CEtcp-10.1.5.16</a>	SIP	Any	No	Alias pattern match	Prefix	10.1.5.16;transport=TCP	Leave	Stop	<a href="#">CEtcp-10.1.5.16</a>	✓ Enabled	<a href="#">View</a>   <a href="#">Clone</a>
<input type="checkbox"/> 50	<a href="#">LocalZoneMatch</a>	Any	Any	No	Any alias				Continue	LocalZone	✓ Enabled	<a href="#">View/Edit</a>   <a href="#">Clone</a>

Automatic search  
rules created

CEtcp-10.1.5.15 and CEtcp-10.1.5.16 or  
CEtls-10.1.5.15 and CETls-10.1.5.16 if using TLS Verify ON

## h) Expressway Server Certificates Requirements

- 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

# i) 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 **collab10x.cisco.com**

DNS X509v3 Subject Alternative Name: DNS:collab10x.cisco.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)



# i) Subject Alternative Name (SAN) Requirements

## Expressway-E Server Certificate

```
[rc\cert\common\BaseCertVerifier.cpp(250)] [csf.cert.]  
[cert::BaseCertVerifier::checkIdentity] - About to verify the Subject Alt  
Name.  
2015-01-30 12:42:47,022 DEBUG [0x00006ea0]  
[ls\src\cert\common\CertVerifier.cpp(154)] [csf.cert]  
[cert::CertVerifier::checkIdentifier] - Verifying identity 'expressway-  
E.collab10x.cisco.com'  
2015-01-30 12:42:47,022 DEBUG [0x00006ea0]  
[rc\cert\utils\AltNameParserImpl.cpp(309)] [csf.cert.utils]  
[cert::AltNameParserImpl::verify] - Looking for match with expressway-  
E.collab10x.cisco.com  
2015-01-30 12:42:47,022 DEBUG [0x00006ea0]  
[rc\cert\utils\AltNameParserImpl.cpp(318)] [csf.cert.utils]  
[cert::AltNameParserImpl::verify] - Match found in dnsNames index: 0  
2015-01-30 12:42:47,022 DEBUG [0x00006ea0]  
[rc\cert\common\BaseCertVerifier.cpp(321)] [csf.cert.]  
[cert::BaseCertVerifier::checkIdentifiers] - Verification of identity  
succeeded. Matched identifier : 'expressway-E.collab10x.cisco.com'
```





# j) Generate CSR: Expressway-C

**Generate CSR**

**Common name**

Common name: \_\_\_\_\_ FQDN of Expressway: \_\_\_\_\_  
Common name as it will appear: expressway-C.collab10x.cisco.com

**Alternative name**

Additional alternative names (comma separated): \_\_\_\_\_ ⓘ  
Unified CM phone security profile names: \_\_\_\_\_ ⓘ  
Alternative name as it will appear: DNS:expressway-C.collab10x.cisco.com

**Additional information**

Key length (in bits): 4096 ⓘ  
Country: \* US ⓘ  
State or province: \* CA ⓘ  
Locality (town name): \* SJC ⓘ  
Organization (company name): \* Cisco ⓘ  
Organizational unit: \* L@C ⓘ

**Generate CSR**

## k) Generate CSR: Expressway-E

### Generate CSR

**Common name**

Common name FQDN of Expressway

Common name as it will appear expressway-E.collab10x.cisco.com

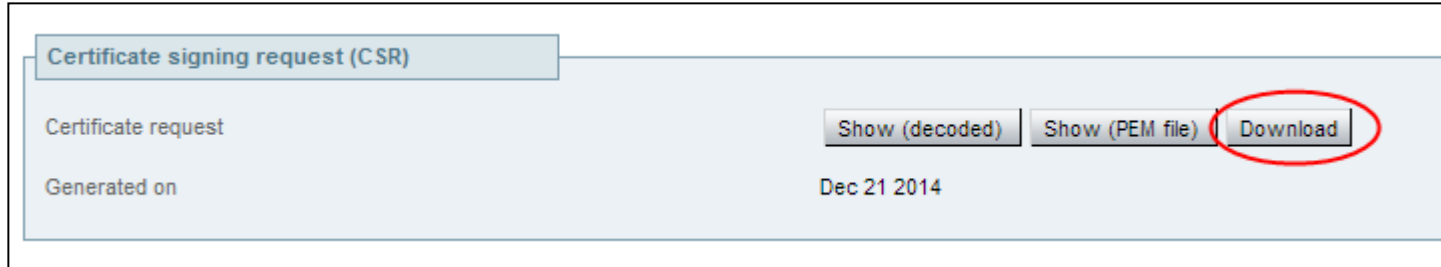
**Alternative name**

Additional alternative names (comma separated)

Unified CM registrations domains  Format:

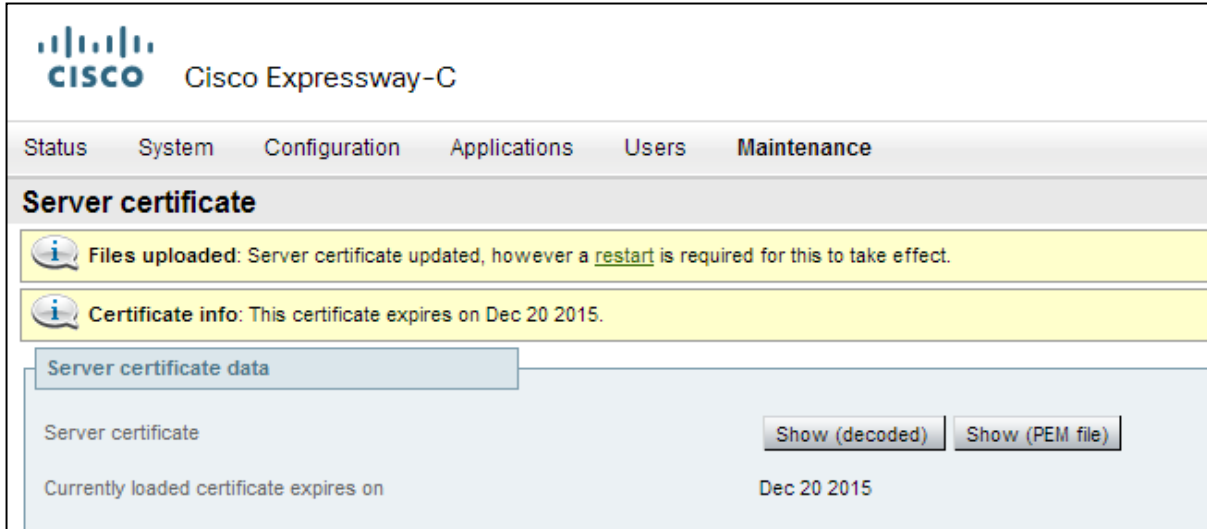
Alternative name as it will appear DNS: expressway-E.collab10x.cisco.com  
SRV: \_collab-edge.\_tls.collab10x.cisco.com

# I) Download Expressway Certificates for Signing by CA



Expressway-E Server certificates should be signed by 3rd party Public CA  
(Certificate signing covered in Appendix A)

# m) Upload Signed Certificates



**CISCO** Cisco Expressway-C

Status System Configuration Applications Users **Maintenance**

### Server certificate

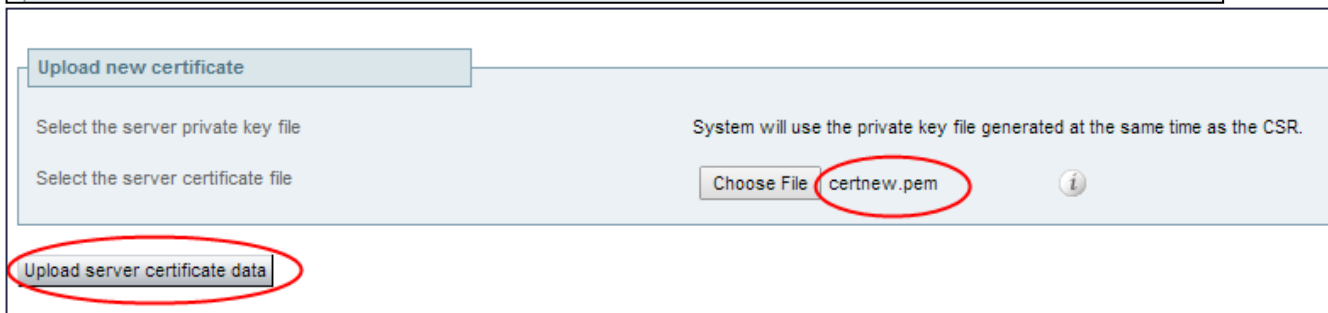
**Files uploaded:** Server certificate updated, however a [restart](#) is required for this to take effect.

**Certificate info:** This certificate expires on Dec 20 2015.

**Server certificate data**

Server certificate Show (decoded) Show (PEM file)

Currently loaded certificate expires on Dec 20 2015



**Upload new certificate**

Select the server private key file System will use the private key file generated at the same time as the CSR.

Select the server certificate file Choose File **certnew.pem** i

**Upload server certificate data**

# n) Upload CA Certificate to Expressway-C and Expressway-E

**CISCO** Cisco Expressway-E

Status System Configuration Applications Users Maintenance

### Trusted CA certificate

**File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.**

Type	Issuer
<input type="checkbox"/> Certificate	O=Temporary CA d634b5d8-7f89-11e3-af0c-005056b41ed3, OU=Temporary CA d634b5d8-7f89-005056b41ed3
<input type="checkbox"/> Certificate	CN=v360-V360-SERVER-CA

Show all (decoded) Show all (PEM file) Delete Select all Unselect all

**Upload**

Select the file containing trusted CA certificates  No file chosen



## o) Configure Traversal Client on Expressway-C

**Configuration**

Name

Type Unified Communications traversal

Hop count  *i*

**Connection credentials**

Username

Password

**SIP**

Port  *i*

Accept proxied registrations  *i*

ICE support  *i*

Create Zone  
Unified Communications  
Traversal

## p) Configure Traversal Client on Expressway-C

Location	
Peer 1 address	<input type="text" value="expressway-E.collab10x.cisco.com"/>
Peer 2 address	<input type="text"/>
Peer 3 address	<input type="text"/>
Peer 4 address	<input type="text"/>
Peer 5 address	<input type="text"/>
Peer 6 address	<input type="text"/>

# q) Configure Traversal Server on Expressway-E

**Configuration**

Name:

Type: Unified Communications traversal

Hop count:  ⓘ

**Connection credentials**

Username:

Password: [Add/Edit local authentication database](#)

**SIP**

Port:  ⓘ

TLS verify subject name:

Accept proxied registrations:  ⓘ

Transport TLS  
SSH Tunnel only  
supports TLS

## r) Verify Traversal Zone Status

Location

Peer 1 address  ⓘ

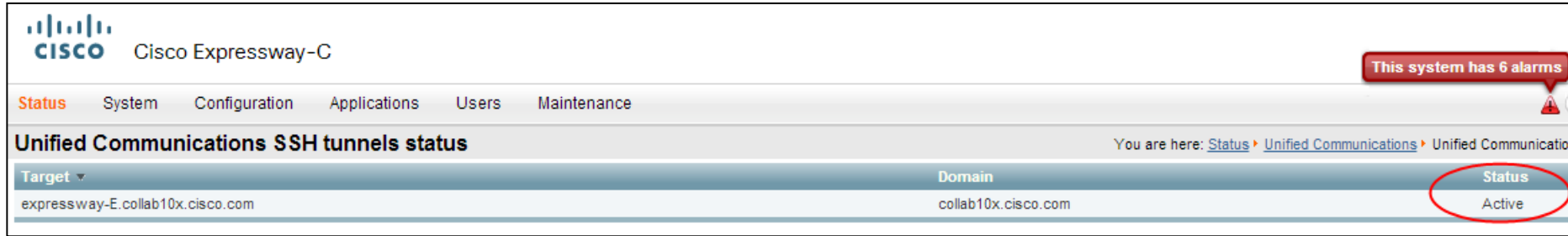
Peer 2 address  ⓘ

SIP: Reachable: 10.1.5.20:7001

Status	
State	Active
Number of calls to this zone	0
Bandwidth used on this Expressway	0 kbps
Total bandwidth used across this cluster	0 kbps
Search rules targeting this zone	0

Configuration > Zones  
Check traversal zone  
status to Expressway-E

## r) Verify SSH Tunnel Status

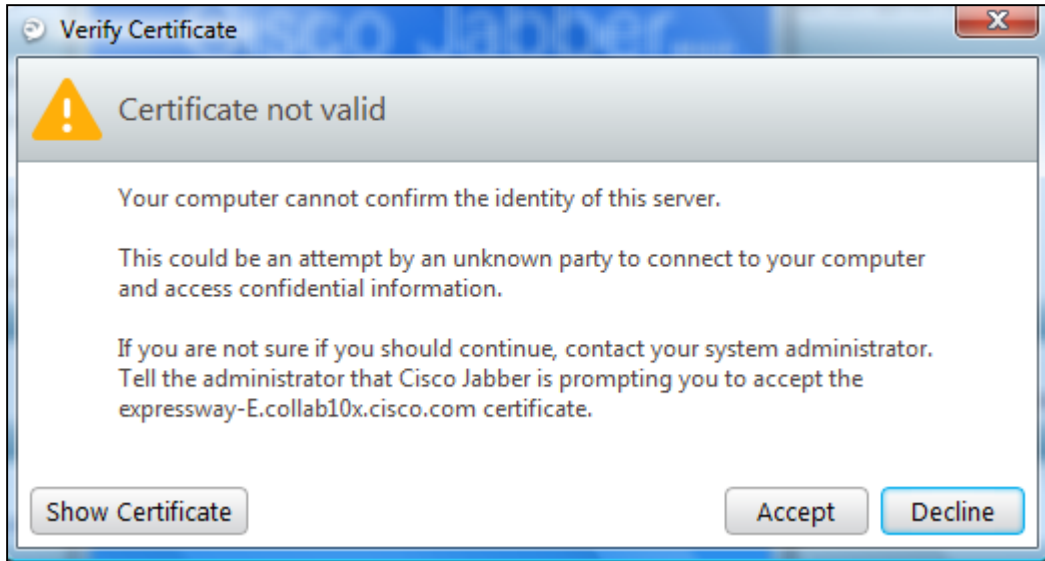


The screenshot shows the Cisco Expressway-C management interface. At the top left is the Cisco logo and the text "Cisco Expressway-C". A navigation menu includes "Status" (highlighted in orange), "System", "Configuration", "Applications", "Users", and "Maintenance". A red alarm notification bubble in the top right corner states "This system has 6 alarms". Below the navigation menu, the page title is "Unified Communications SSH tunnels status". A breadcrumb trail reads "You are here: Status > Unified Communications > Unified Communication". A table displays the SSH tunnel status for the target "expressway-E.collab10x.cisco.com" with the domain "collab10x.cisco.com" and a status of "Active". The "Active" status is circled in red.

Target	Domain	Status
expressway-E.collab10x.cisco.com	collab10x.cisco.com	Active



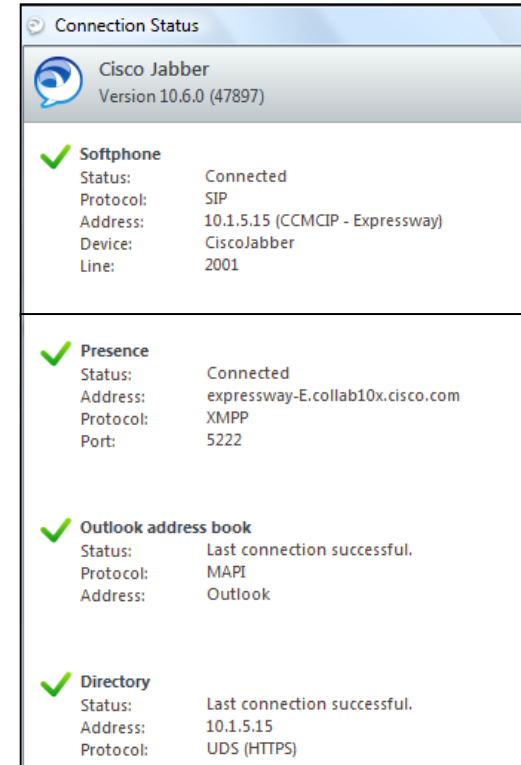
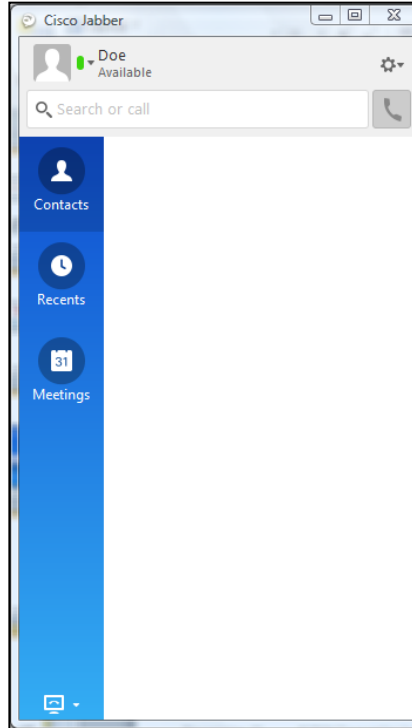
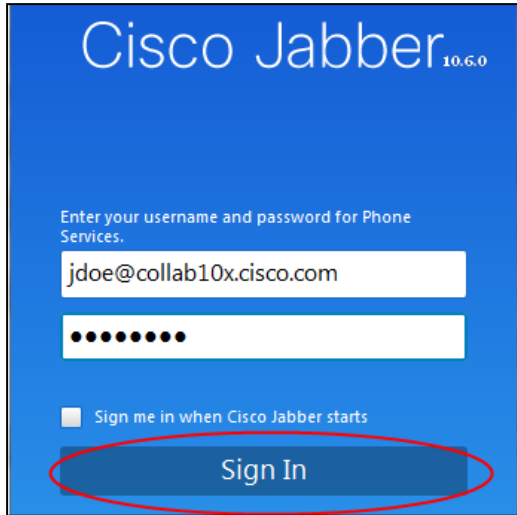
## s) Verification: Login to Cisco Jabber



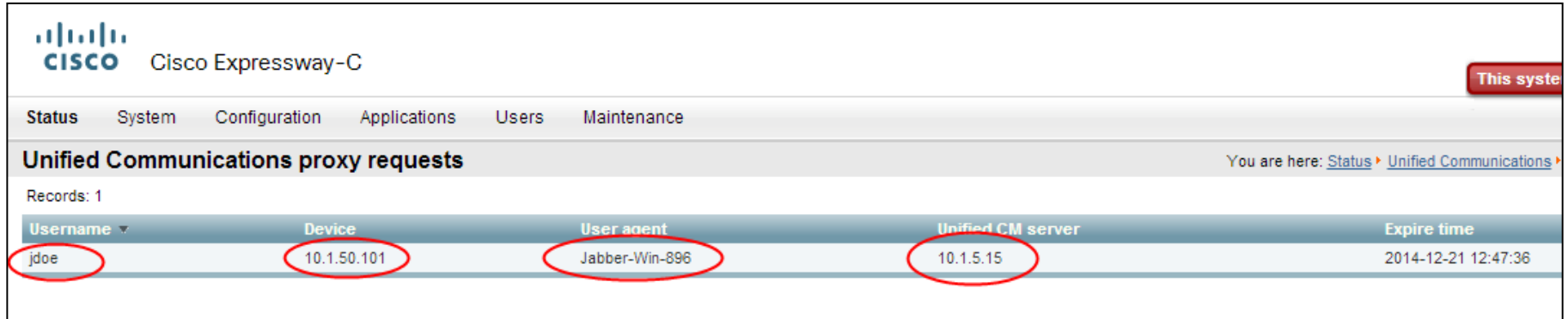
Certificate not valid. Appears if Expressway-E certificate is not trusted by PC platform.



## s) Verification: Login to Cisco Jabber



## s) Verification: Check Status on Expressway-C



The screenshot shows the Cisco Expressway-C web interface. At the top left is the Cisco logo and the text "Cisco Expressway-C". On the top right, there is a red button labeled "This system". Below the header is a navigation menu with tabs for "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". The "Status" tab is selected. The main content area is titled "Unified Communications proxy requests" and includes a breadcrumb trail: "You are here: Status > Unified Communications >". Below the title, it says "Records: 1". A table displays the following data:

Username	Device	User agent	Unified CM server	Expire time
jdoo	10.1.50.101	Jabber-Win-896	10.1.5.15	2014-12-21 12:47:36

In the original image, the values "jdoo", "10.1.50.101", "Jabber-Win-896", and "10.1.5.15" are circled in red. A blue line with a dot at the top points from the "Status" breadcrumb in the screenshot to the text below.

Status > Unified Communications  
View provisioning  
Sessions

# s) Verification: Check Status in Cisco Unified Communications Manager

**Find and List Phones** Related Links: [Actively Logged](#)



[+](#) Add New [Select All](#) [Clear All](#) [Delete Selected](#) [Reset Selected](#) [Apply Config to Selected](#)

**Status**  
2 records found

**Phone (1 - 2 of 2)**

Find Phone where

Select item or enter search text

<input type="checkbox"/>		Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IPv4 Address
<input type="checkbox"/>		<a href="#">CiscoJabber</a>		<a href="#">Default</a>	SIP	Registered with 10.1.5.15	10.1.5.19
<input type="checkbox"/>		<a href="#">SEPECC88211512B</a>	SEPECC88211512B	<a href="#">Default</a>	SIP	Registered with 10.1.5.15	<a href="#">10.1.110.11</a>

Device> Phone  
Cisco Jabber shows IP  
address of Expressway-C

## s) Verification: Check Call Status



Cisco Expressway-C

Status System Configuration Applications Users Maintenance

**Call status**

Records: 1

Start time ^	Duration	Source	Destination	Type	Protocol
<input type="checkbox"/> <a href="#">2014-12-21 15:32:25</a>	1 minute 12 seconds	sip:2001@10.1.5.15	sip:3001@10.1.5.15	Traversal	Multiple components

Traversal Call



Cisco Expressway-E

Status System Configuration Applications Users Maintenance

**Call status**

Records: 1

Start time ^	Duration	Source	Destination	Type	Protocol	Peer
<input type="checkbox"/> <a href="#">2014-12-21 15:32:25</a>	4 minutes 23 seconds	sip:2001@10.1.5.15	sip:3001@10.1.5.15	Traversal	SIP <-> SIP	This system

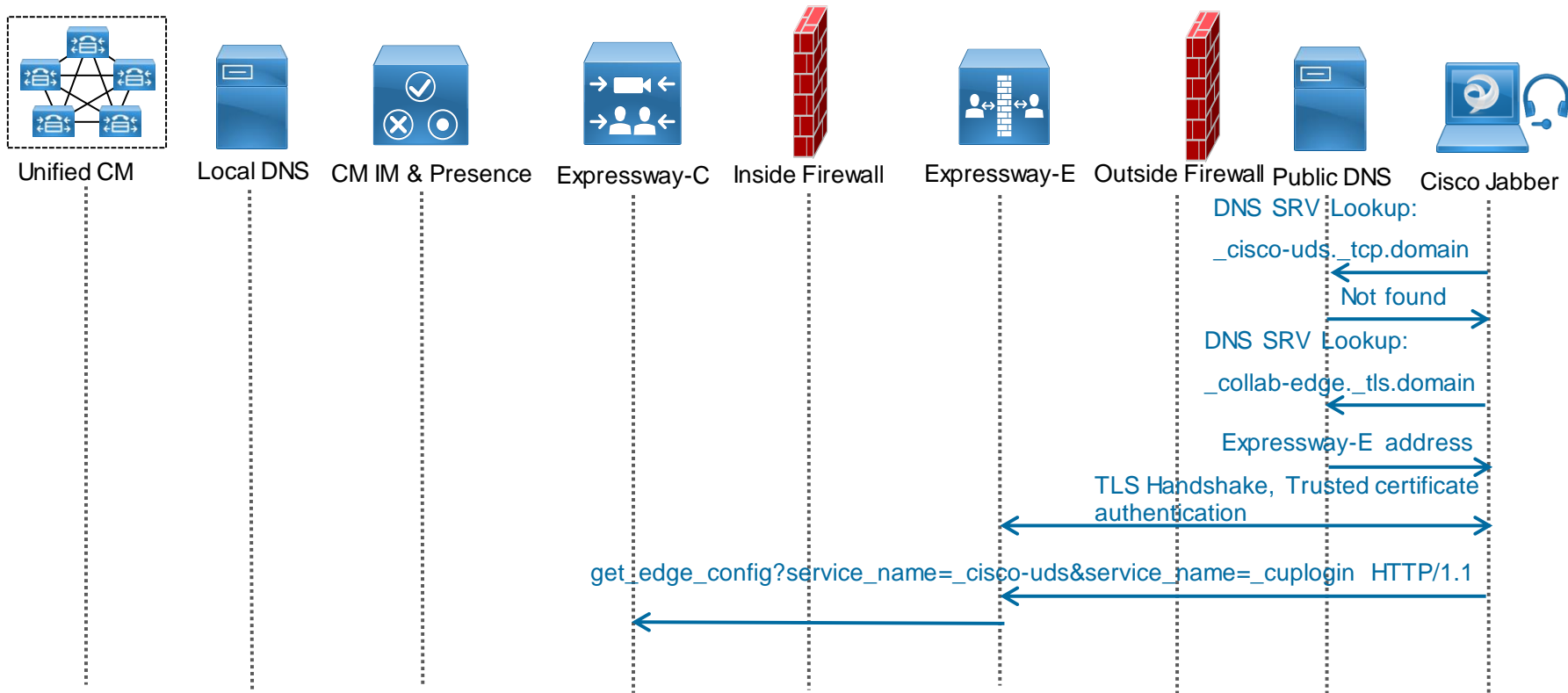




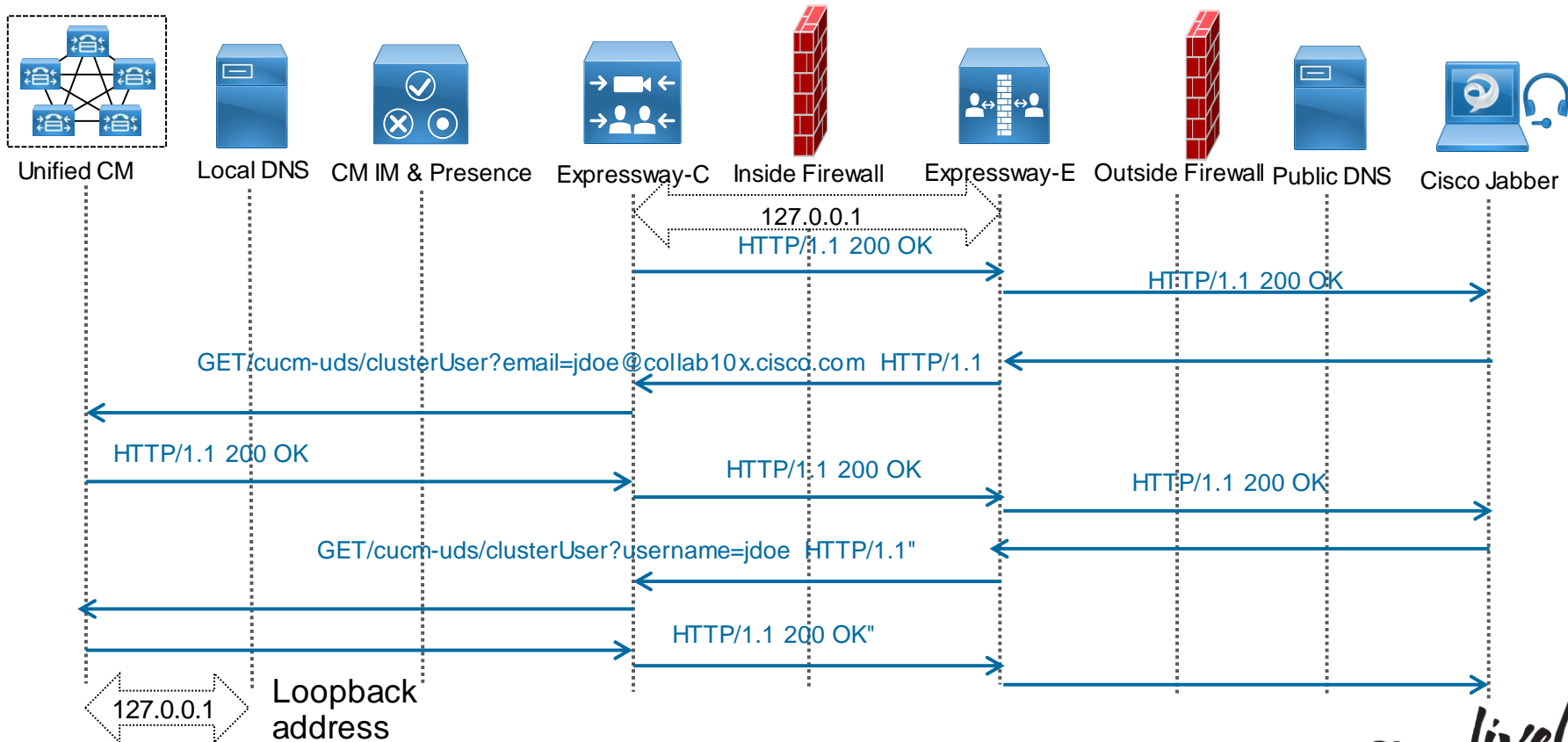
# Troubleshooting



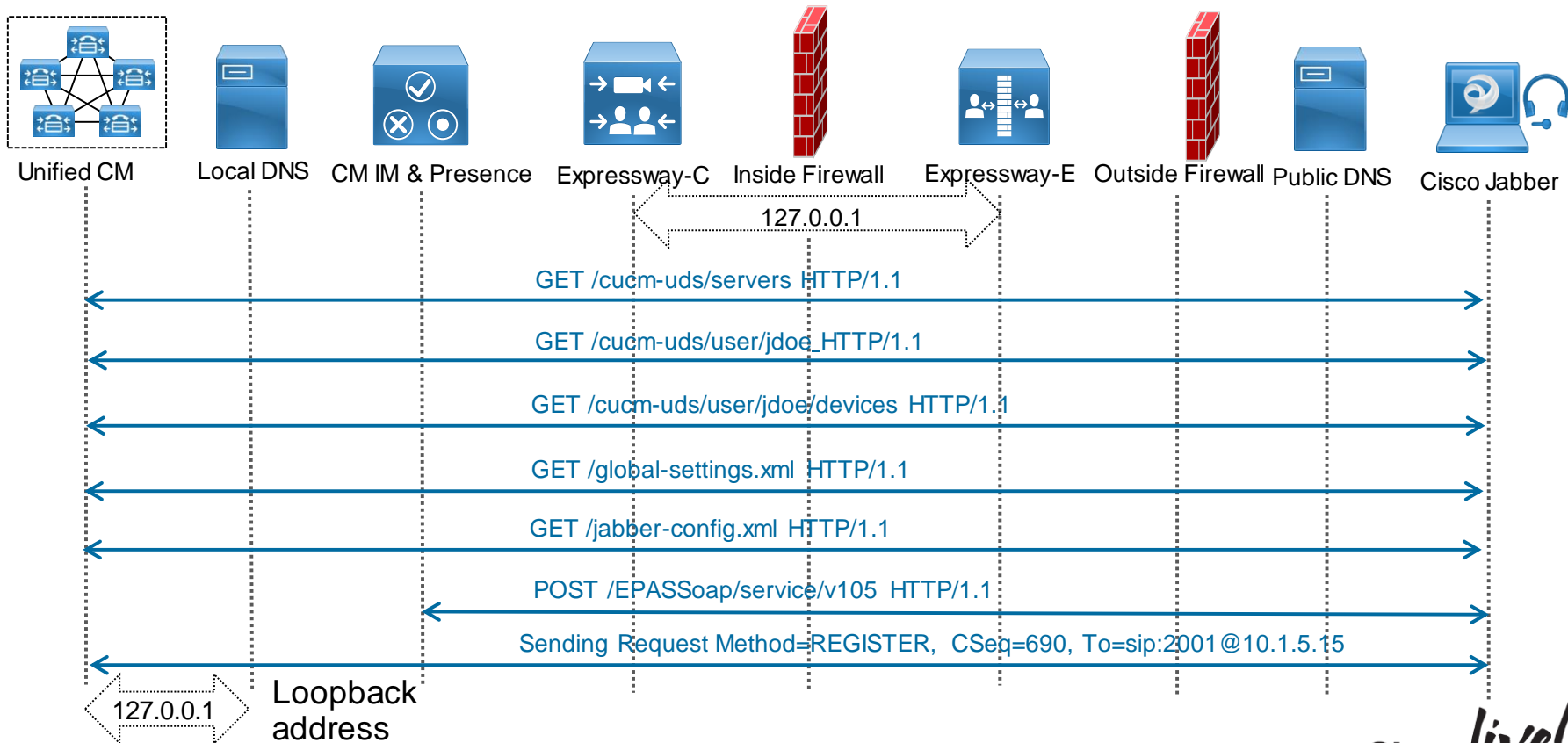
# Registering Remote Cisco Jabber to Cisco Unified Communications Manager



# Registering Remote Cisco Jabber to Cisco Unified Communications Manager



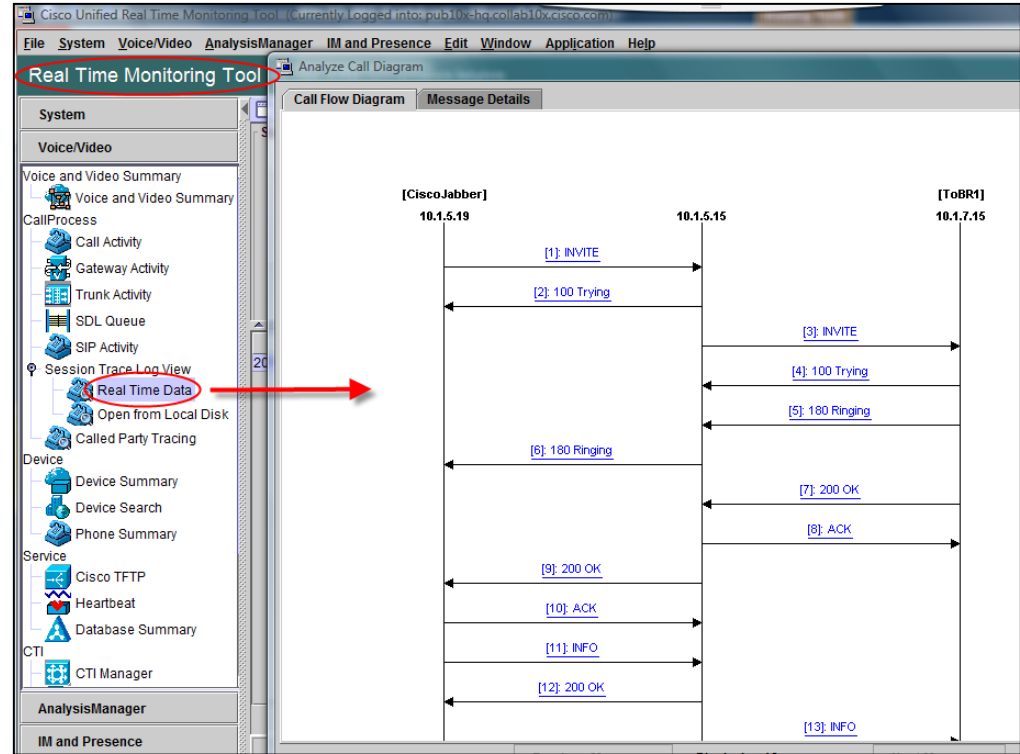
# Registering Remote Cisco Jabber to Cisco Unified Communications Manager



# Tools: Cisco Unified Communications Manager

## Real Time Monitoring Tool

- Call Activity
  - Session Trace Log View
  - Call Activity
  - SDL Trace
  - Called Party Tracing
- (These are some examples)



# Tools: Expressway Series

## Network Log

- Status > Logs > Network Log
- Filter network.http.trafficserver
- Filter network.sip

Cisco Expressway-C

Status System Configuration Applications Users Maintenance

**Network Log**

Filter

Contains all of the words:  [more options](#)

[Configure log settings](#) | [Download this page](#)

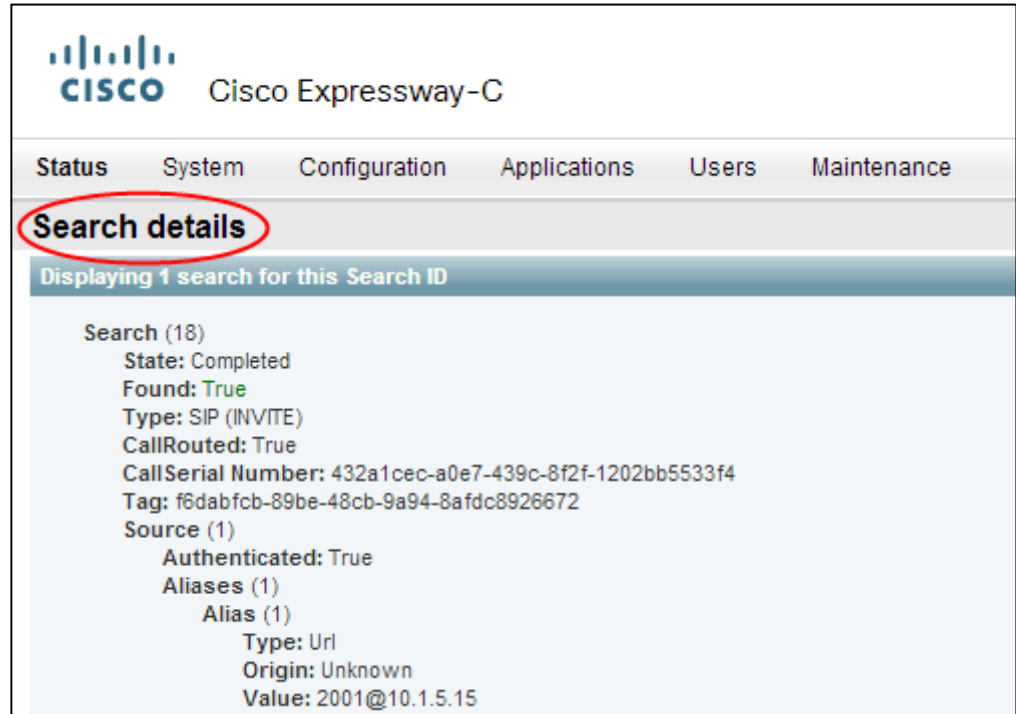
**Results**

2015-02-05T22:08:51+00:00	traffic_server[31381]: UTCTime="2015-02-05 22:08:51.473" Module="network.http.trafficserver" Level="INFO": Detail="Sending Response" Txn-id="243" Dst-ip="127.0.0.1"
2015-02-05T22:08:51+00:00	traffic_server[31381]: UTCTime="2015-02-05 22:08:51.472" Module="network.http.trafficserver" Level="INFO": Detail="Receive Response" Txn-id="243" Src-ip="10.1.5.18"
2015-02-05T22:08:51+00:00	traffic_server[31381]: UTCTime="2015-02-05 22:08:51.193" Module="network.http.trafficserver" Level="INFO": Detail="Sending Request" Txn-id="243" Dst-ip="10.1.5.18" Ds
2015-02-05T22:08:51+00:00	traffic_server[31381]: UTCTime="2015-02-05 22:08:51.174" Module="network.http.trafficserver" Level="INFO": Detail="Receive Request" Txn-id="243" Src-ip="127.0.0.1" S
2015-02-05T22:08:51+00:00	traffic_server[31381]: UTCTime="2015-02-05 22:08:51.122" Module="network.http.trafficserver" Level="INFO": Detail="Sending Response" Txn-id="241" Dst-ip="127.0.0.1"
2015-02-05T22:08:51+00:00	traffic_server[31381]: UTCTime="2015-02-05 22:08:51.121" Module="network.http.trafficserver" Level="INFO": Detail="Receive Response" Txn-id="241" Src-ip="10.1.5.18"
2015-02-05T22:08:50+00:00	traffic_server[31381]: UTCTime="2015-02-05 22:08:50.473" Module="network.http.trafficserver" Level="INFO": Detail="Sending Request" Txn-id="241" Dst-ip="10.1.5.18" Ds

# Tools: Expressway Series

## Search History

- Status > Search History
- Search details of call
- View call information
- View all events for the call



**CISCO** Cisco Expressway-C

Status System Configuration Applications Users Maintenance

**Search details**

Displaying 1 search for this Search ID

Search (18)

- State: Completed
- Found: True
- Type: SIP (INVITE)
- CallRouted: True
- CallSerial Number: 432a1cec-a0e7-439c-8f2f-1202bb5533f4
- Tag: f6dabfcb-89be-48cb-9a94-8afdc8926672
- Source (1)
  - Authenticated: True
  - Aliases (1)
    - Alias (1)
      - Type: Url
      - Origin: Unknown
      - Value: 2001@10.1.5.15



# Tools: Cisco Jabber

## Network Log

- %user\_profile%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs

```
2015-02-05 14:37:53,253 DEBUG [0x00003b38]
[rc\media\cpve\CpveVideoProvider.cpp(881)] [csf.ecc.media.term]
[ecc::CpveVideoProvider::getCodecList] - getCodecList()
2015-02-05 14:37:53,254 INFO [0x00003b38]
[src\media\MediaConfiguration.cpp(278)] [csf.ecc]
[ecc::MediaConfiguration::getFilteredCodecs] - getFilteredCodecs:
codecs=H264 with whitelist=G711, G7221_24, G7221_32, G722, G729A, H264
2015-02-05 14:37:53,254 DEBUG [0x00003b38]
[src\media\MediaConfiguration.cpp(288)] [csf.ecc]
[ecc::MediaConfiguration::getFilteredCodecs] - Supporting whitelisted
Codec: H264
2015-02-05 14:37:53,254 DEBUG [0x00003b38]
[honewrapper\CC_SIPCCVcmBinding.cpp(2734)] [csf.ecc.vcm]
[ecc::SIPCCVcmBinding::vcmGetVideoCodecList] - codec_mask=0x0080
2015-02-05 14:37:53,254 WARN [0x00003b38]
[src\common\thread\Timeout.cpp(139)] [csf.ecc] [cancel] - Cancelling
Timer. Thread ID: 00003B38
```

# Scenario 1: Cannot Find Services

- ✓ Does Cisco Jabber register locally?
- ✓ Is \_cisco-uds SRV request blocked?
- ✗ Do we get a response to \_collab-edge.tls SRV request?



# Scenario 1: Cannot Find Services

10.1.50.101	10.1.5.1	DNS	87 Standard query 0x034c SRV _collab-edge._tls.cisco.com
10.1.5.1	10.1.50.101	DNS	164 Standard query response 0x034c <b>No such name</b>

```
> set type=all
> _collab-edge._tls.cisco.com
Server: UnKnown
Address: 10.1.5.1

*** UnKnown can't find _collab-edge._tls.cisco.com: Non-existent domain
> _
```

```
Domain Name System (response)
  [Request In: 211]
  [Time: 0.024181000 seconds]
  Transaction ID: 0x034c
  Flags: 0x8583 Standard query response, No such name
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
  Queries
    [collab-edge._tls.cisco.com] type SRV, class IN
      Name: _collab-edge._tls.cisco.com
      Type: SRV (Service location)
      Class: IN (0x0001)
    Authoritative nameservers
      [cisco.com] type SOA, class IN, mname collab10x.cisco.com
        Name: cisco.com
        Type: SOA (Start of zone of authority)
        Class: IN (0x0001)
        Time to live: 1 day
        Data length: 56
        Primary name server: collab10x.cisco.com
        Responsible authority's mailbox: mb1.cisco.com
        Serial Number: 3628166845
        Refresh Interval: 21600 (6 hours)
        Retry Interval: 900 (15 minutes)
        Expire limit: 7776000 (90 days)
```

Wireshark Trace

Domain Name System

# Scenario 2: Cannot Communicate with Server

- ✓ Does Cisco Jabber register locally?
- ✓ Is \_cisco-uds SRV request blocked?
- ✓ Do we get a response to \_collab-edge.tls SRV request?
- ✓ Can the Expressway-E IP address be resolved?
- ✗ Is the SSH Tunnel OK?



# Scenario 2: Cannot Communicate with Server

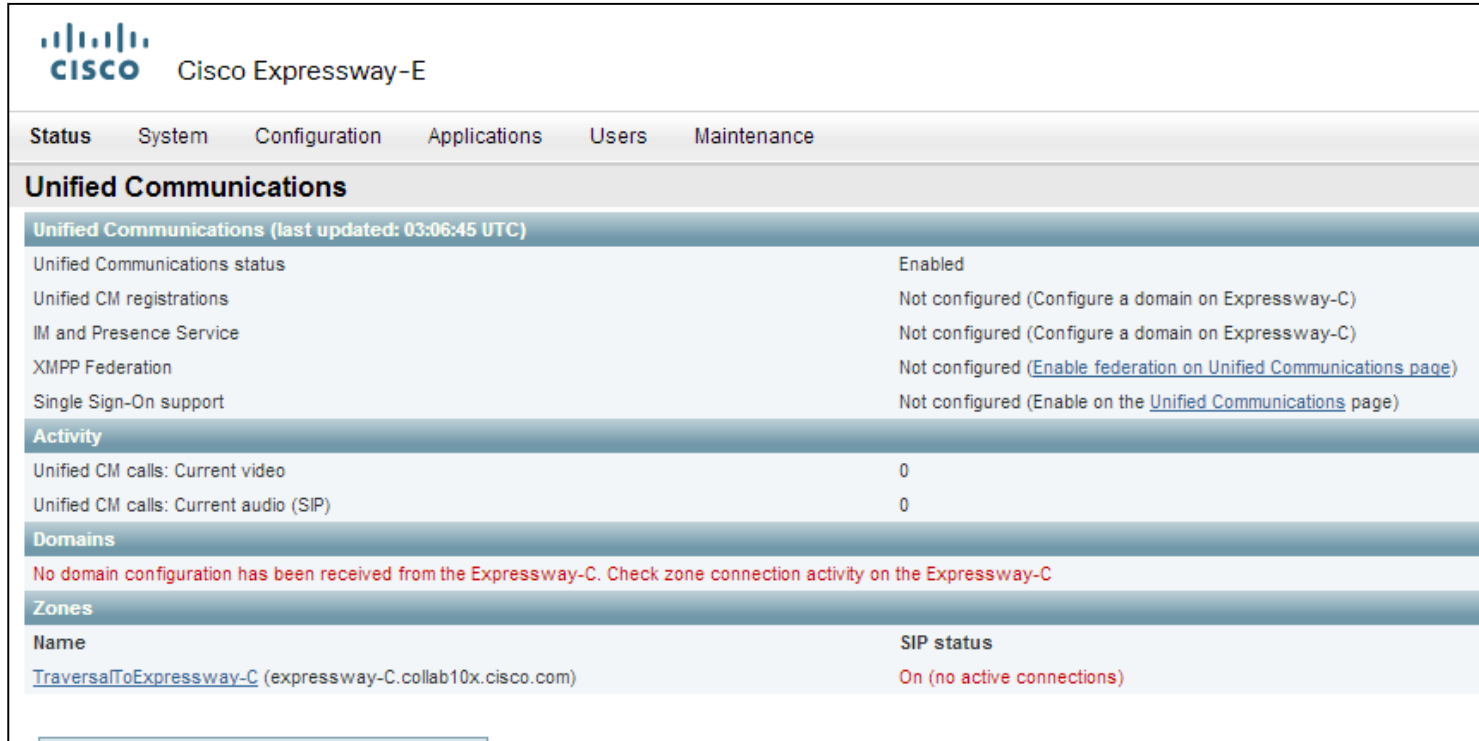
The screenshot displays the Cisco Expressway-C web interface. At the top, the Cisco logo and 'Cisco Expressway-C' are visible. Below the navigation tabs (Status, System, Configuration, Applications, Users, Maintenance), the 'Unified Communications' section is active. It includes a sub-section for 'Unified Communications (last updated: 03:03:30 UTC)' with a table of status items. Below that is an 'Activity' section with call statistics. The 'Domains' section contains a table with columns for Name, Services, and Associated zones. The 'Zones' section has a table with columns for Name and SIP status. The 'SIP status' for the 'TraversalToExpressway-E' zone is circled in red and shows 'Failed'. The 'Servers' section lists IM and Presence Service nodes, Unified CM servers, and Unity Connection servers.

Name	Services	Associated zones
<a href="#">collab10x.cisco.com</a>	Unified CM registrations, IM and Presence Service	TraversalToExpressway-E

Name	SIP status
<a href="#">TraversalToExpressway-E</a>	Failed

# Scenario 2: Cannot Communicate with Server



The screenshot shows the Cisco Expressway-E web interface. At the top left is the Cisco logo and the text "Cisco Expressway-E". Below this is a navigation bar with tabs for "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". The "Configuration" tab is selected, and the "Unified Communications" section is expanded. A sub-section header "Unified Communications (last updated: 03:06:45 UTC)" is visible. Below this, a table lists various settings:

Setting	Value
Unified Communications status	Enabled
Unified CM registrations	Not configured (Configure a domain on Expressway-C)
IM and Presence Service	Not configured (Configure a domain on Expressway-C)
XMPP Federation	Not configured ( <a href="#">Enable federation on Unified Communications page</a> )
Single Sign-On support	Not configured (Enable on the <a href="#">Unified Communications</a> page)

Below the table is an "Activity" section with two rows:

Activity	Count
Unified CM calls: Current video	0
Unified CM calls: Current audio (SIP)	0

Next is a "Domains" section with a red error message: "No domain configuration has been received from the Expressway-C. Check zone connection activity on the Expressway-C".

Finally, there is a "Zones" section with a table:

Name	SIP status
<a href="#">TraversalToExpressway-C</a> (expressway-C.collab10x.cisco.com)	On (no active connections)



# Scenario 2: Cannot Communicate with Server

Type	Issuer
<input type="checkbox"/> Certificate	O=Temporary CA d634b5d8-7f89-11e3-af0c-005056b41ed3, OU=Temporary CA d634b5d8-7f89-11e3-af0c-005056b41ed3

Uses Temporary CA

Fix by applying CA  
certificate used to sign  
CSR

# Scenario 3: Cannot Communicate with Server

- ✓ Does Cisco Jabber register locally?
- ✓ Is \_cisco-uds SRV request blocked?
- ✓ Do we get a response to \_collab-edge.tls SRV request?
- ✓ Can the Expressway-E IP address be resolved?
- ✓ Is the SSH Tunnel OK?



# Scenario 3: Cannot Communicate with Server

✓ get\_edge\_config OK?

✗ GET/cucm-uds/clusterUser?email=jdoe@collab10x.cisco.com HTTP/1.1



# Scenario 3: Cannot Communicate with Server

```
Detail="Sending Response" Txn-id="251" Dst-ip="10.1.50.101" Dst-port="52142" Msg="HTTP/1.1 403 Forbidden"  
Detail="Receive Request" Txn-id="251" Src-ip="10.1.50.101" Src-port="52142" Msg="GET https://oauthcb HTTP/1.1"
```

## Expressway-E Network Log

Filter on 'trafficserver' to  
view HTTPS traffic

## Cisco Jabber Log

AppData\Local\Cisco\Unified  
Communications\Jabber

DNS name

collab10x.cisco.com does  
not exist

```
[cert::CertVerifier::checkIdentifier] - Verifying identity 'collab-  
edge.collab10x.cisco.com'  
2015-01-30 12:42:47,023 DEBUG [0x00006ea0]  
[rc\cert\utils\AltNameParserImpl.cpp(309)] [csf.cert.utils]  
[cert::AltNameParserImpl::verify] - Looking for match with collab-  
edge.collab10x.cisco.com  
2015-01-30 12:42:47,023 ERROR [0x00006ea0]  
[rc\cert\utils\AltNameParserImpl.cpp(353)] [csf.cert.utils]  
[cert::AltNameParserImpl::verify] - No Match Found  
2015-01-30 12:42:47,023 ERROR [0x00006ea0]  
[rc\cert\common\BaseCertVerifier.cpp(316)] [csf.cert.]  
[cert::BaseCertVerifier::checkIdentifiers] - verification of identity:  
'collab10x.cisco.com' 'collab-edge.collab10x.cisco.com' failed.  
2015-01-30 12:42:47,023 DEBUG [0x00006ea0] [sf-  
netutils\src\common\PolicySet.cpp(76)] [csf.common.PolicySet]  
[common::PolicySet::getPolicy] - Searching a policy with nature
```

# Scenario 3: Cannot Communicate with Server

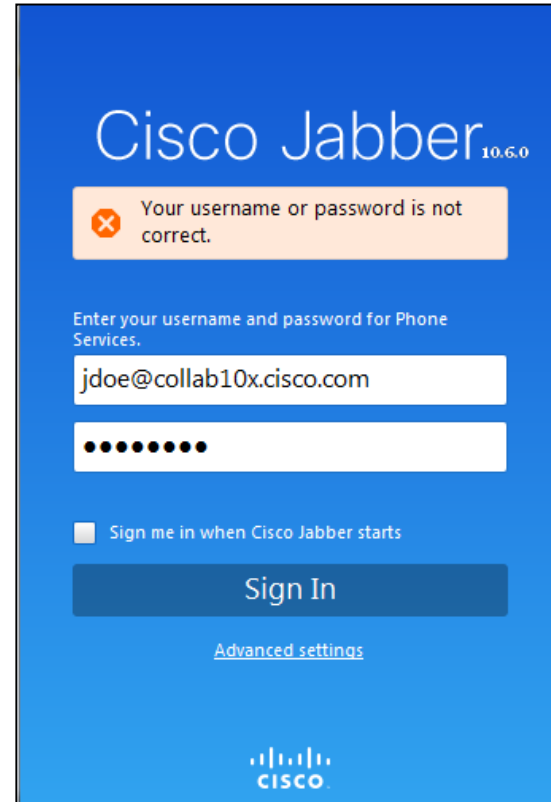
## Expressway-E DNS

DNS name cisco.com does not match name requested by Cisco Jabber

The screenshot shows the Cisco Expressway-E configuration interface. At the top, there is a navigation bar with tabs for Status, System, Configuration, Applications, Users, and Maintenance. The 'DNS' section is active, showing 'DNS settings' and 'Default DNS servers'. In the 'DNS settings' section, the 'System host name' is 'expressway-E', the 'Domain name' is 'cisco.com', and the 'DNS requests port range' is 'Use the ephemeral port range'. In the 'Default DNS servers' section, 'Address 1' is '10.1.5.100' and 'Address 2' is empty. Red circles highlight the 'cisco.com' domain name and the '10.1.5.100' IP address.

# Scenario 4: Username/Password Not Valid

- ✓ Does Cisco Jabber register locally?
- ✓ Is \_cisco-uds SRV must blocked?
- ✓ Do we get a response to \_collab-edge.tls SRV request?
- ✓ Can the Expressway-E IP address be resolved?
- ✓ Is the SSH Tunnel OK?



Cisco Jabber<sup>10.6.0</sup>


 Your username or password is not correct.

Enter your username and password for Phone Services.

Sign me in when Cisco Jabber starts

[Sign In](#)

[Advanced settings](#)





# Scenario 4: Username/Password Not Valid

X get\_edge\_config OK?

```
[\DnsEdgeServiceDiscoveryRequest.cpp(162)] [service-discovery]
[DnsEdgeServiceDiscoveryRequest::getServiceInformationFromEdge] - Edge
discovery has finished with the return value FAILED_EDGE_AUTHENTICATION
2015-01-30 12:42:47,273 DEBUG [0x00006ea0]
[scopy\ServiceDiscoveryHandler.cpp(754)] [service-discovery]
[isCucmServiceInformationAvailable] - service discovery result is empty
```



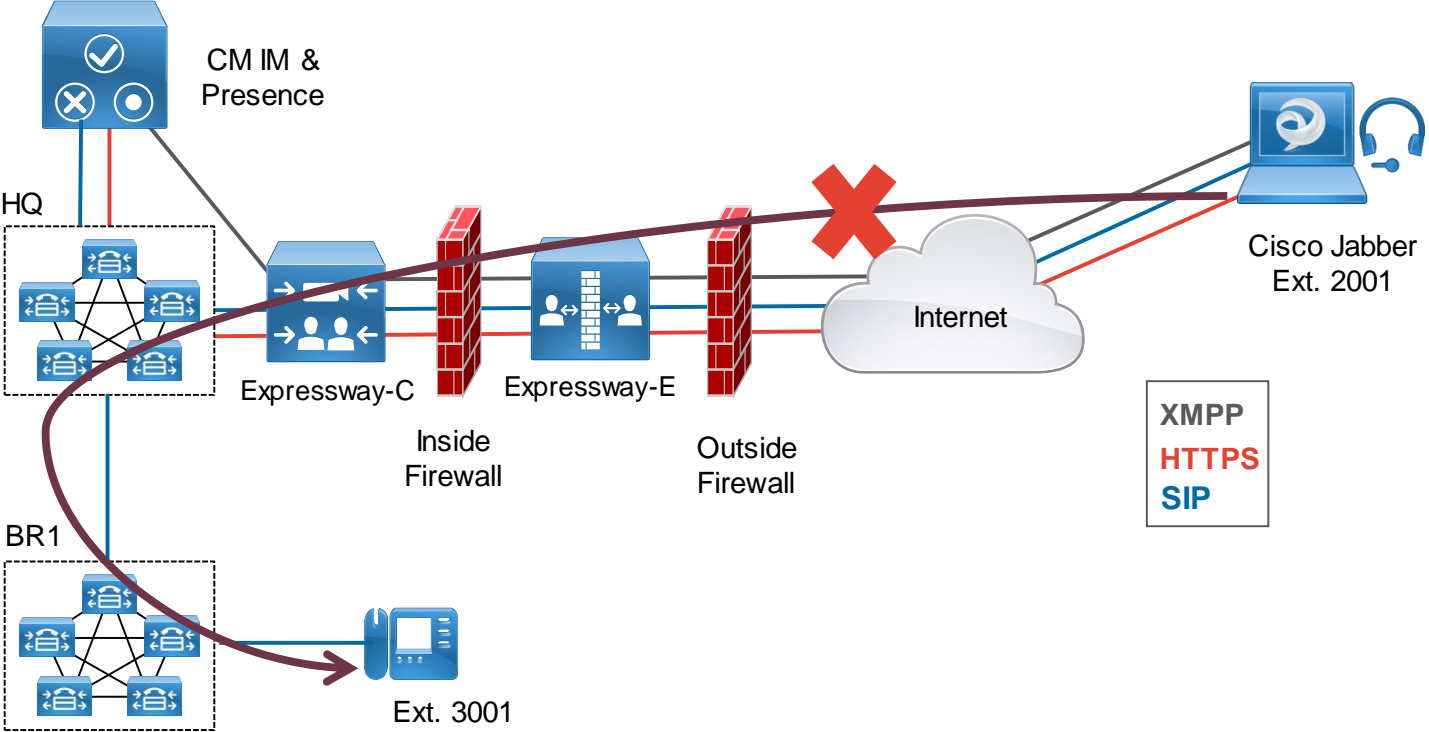
```
edgeconfigprovisioning UTCTime="2015-01-30 20:22:40.911" Module="network.http.sso.server" Level="DEBUG" Action="Sent" Local-ip="127.0.0.1" Local-port="22111" Dst-ip="127.0.0.1" Dst-port="34955" Code="503"
HTTPMSG:
(HTTP/1.1 503 Service Unavailable
Server: [GE_C_ECS])

|
edgeconfigprovisioning UTCTime="2015-01-30 20:22:40.910" Module="network.http.sso.server" Level="DEBUG" Action="Received" Local-ip="127.0.0.1" Local-port="22111" Src-ip="127.0.0.1" Src-port="34955" Uri="/nodom
ain/status" Method="GET"
HTTPMSG:
|GET /nodomain/status HTTP/1.1
Host: [*127.0.0.1:22111]
Accept-Encoding: [gzip, deflate]
User-Agent: [Python-httpplib2/0.9 (gzip)]
```

# Scenario 4: Username/Password Not Valid

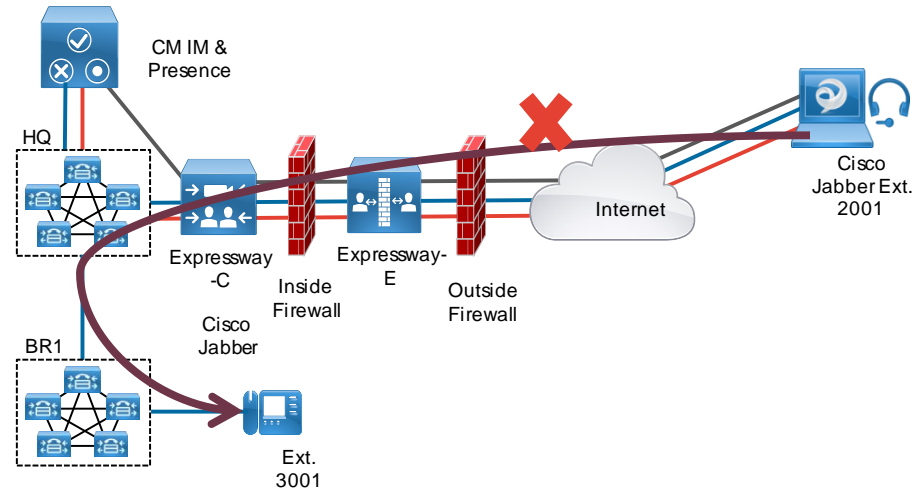
The image shows a side-by-side comparison of a configuration page and a login page. On the left is the Cisco Expressway-C configuration interface. The 'Domains' section is expanded to 'Configuration', where the 'Domain name' is set to 'cisco.com'. Below this, under 'Supported services for this domain', 'SIP registrations and provisioning on Unified CM' and 'IM and Presence Service' are both set to 'On', while 'XMPP federation' is set to 'Off'. On the right is the Cisco Jabber 10.6.0 login page. It displays an error message: 'Your username or password is not correct.' Below the error, the login fields show the username 'jdoe@collab10x.cisco.com' and a masked password. A red arrow points from the 'cisco.com' domain in the configuration to the '@collab10x.cisco.com' domain in the login field. A red diagonal watermark reads 'Mismatched Service Domain'.

# Scenario 5: Cannot Place Calls



# Scenario 5: Cannot Place Calls

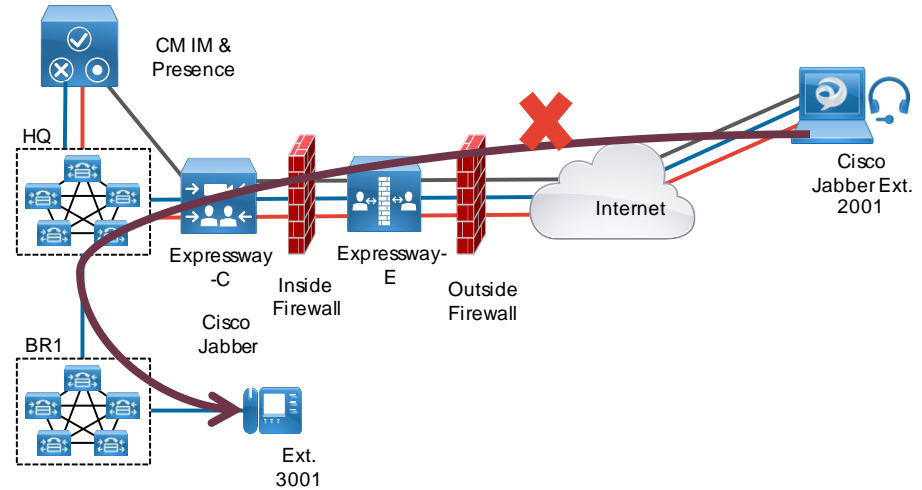
- ✓ Is the SIP Invite received by Expressway-E?
- ✓ Is the SIP Invite forwarded to Expressway-C through the Unified Communications Traversal Zone?
- ✓ Is the Expressway-C forwarding the SIP Invite to the Unified Communications Manager through the CEtcp-@ neighbour zone?
- ✓ Is the SIP Invite received by Unified Communications Manager at HQ?



# Scenario 5: Cannot Place Calls

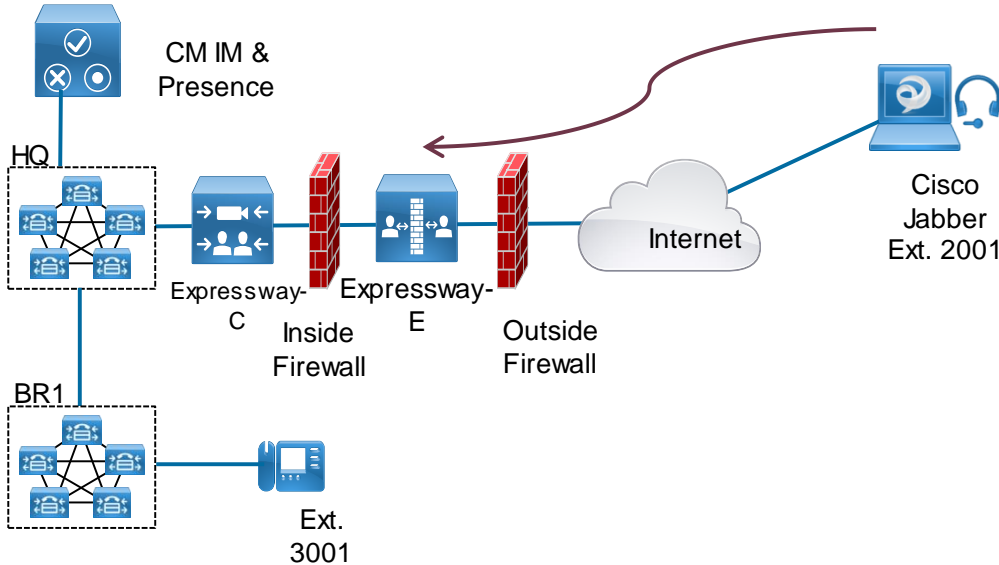
✓ Is the SIP Invite received by Unified Communications Manager at BR1?

✗ Can BR1 reach device at 3001?



# Scenario 5: Cannot Place Calls

✓ Is the Invite received by Expressway-E?



**CISCO** Cisco Expressway-E

Status System Configuration Applications Users Maintenance

### Search details

Displaying 1 search for this Search ID

Search (5)

- State: Completed
- Found: **False**
- Reason: **Not Found**
- Type: SIP (INVITE)
- CallSerial Number: ede3a009-5e24-4ae7-887f-231da0c810b3
- Tag: 6f8cfe48-31c3-4a8a-9979-7eff2f907d1c

Source (1)

- Authenticated: True
- Aliases (1)
  - Alias (1)
    - Type: Uri
    - Origin: Unknown
    - Value: 2001@10.1.5.15
- Zone (1)
  - Name: CollaborationEdgeZone
  - Type: Default
- Path (1)
  - Hop (1)
    - Address: 10.1.50.101:58779

Destination (1)

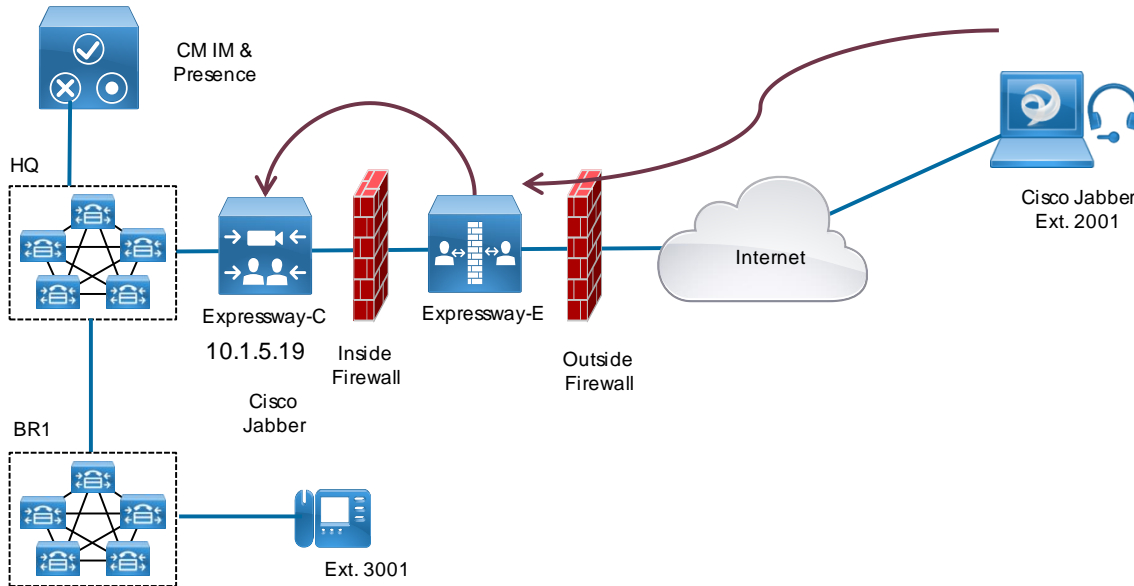
- Alias (1)
  - Type: Uri
  - Origin: Unknown
  - Value: sip:3001@10.1.5.15;user=phone

StartTime: 2015-01-21 22:06:42



# Scenario 5: Cannot Place Calls

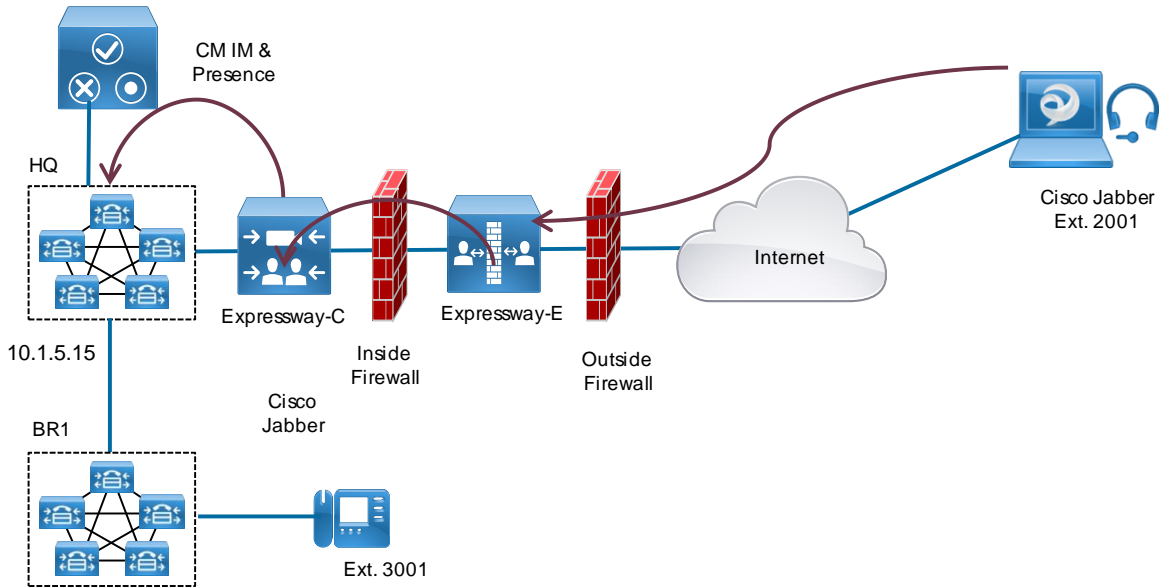
✓ Is the Invite forwarded to Expressway-C through the Unified Communications Traversal Zone?



```
SubSearch (1)
Type: Admin Policy
Action: Proxy
ResultAlias (1)
  Type: H323Id
  Origin: Unknown
  Value: sip:3001@10.1.5.15;user=phone
Zone (1)
  Name: TraversalToExpressway-C
  Type: TraversalServer
  Protocol: SIP
  Found: False
  Reason: Not Found
  StartTime: 2015-01-21 22:06:42
  Duration: 10.29
  Gatekeeper (1)
    Address: 10.1.5.19:25004
    Alias (1)
      Type: H323Id
      Origin: Unknown
      Value: sip:3001@10.1.5.15;user=phone
```

# Scenario 5: Cannot Place Calls

- ✓ Is the Expressway-C forwarding the Invite to HQ Unified Communications Manager through the CEtcp-@ neighbour zone?



**CISCO** Cisco Expressway-C

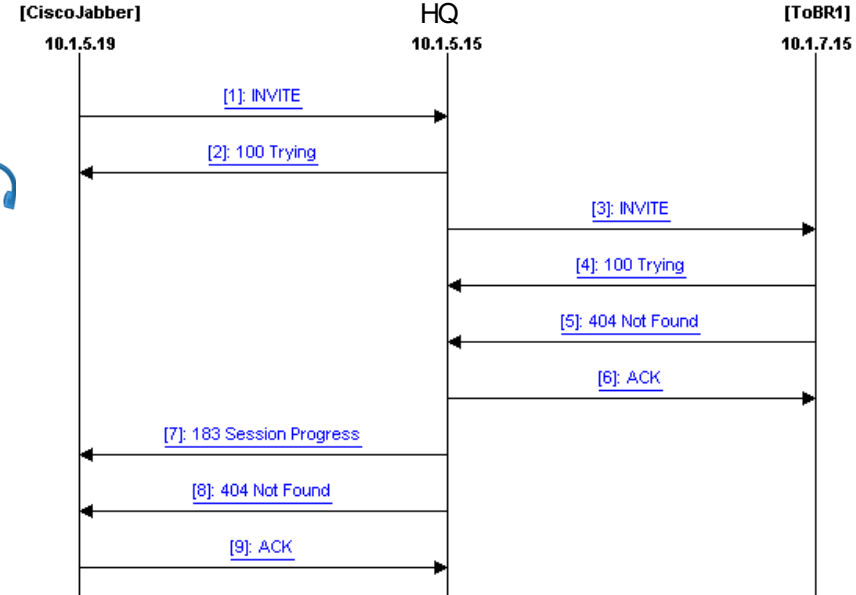
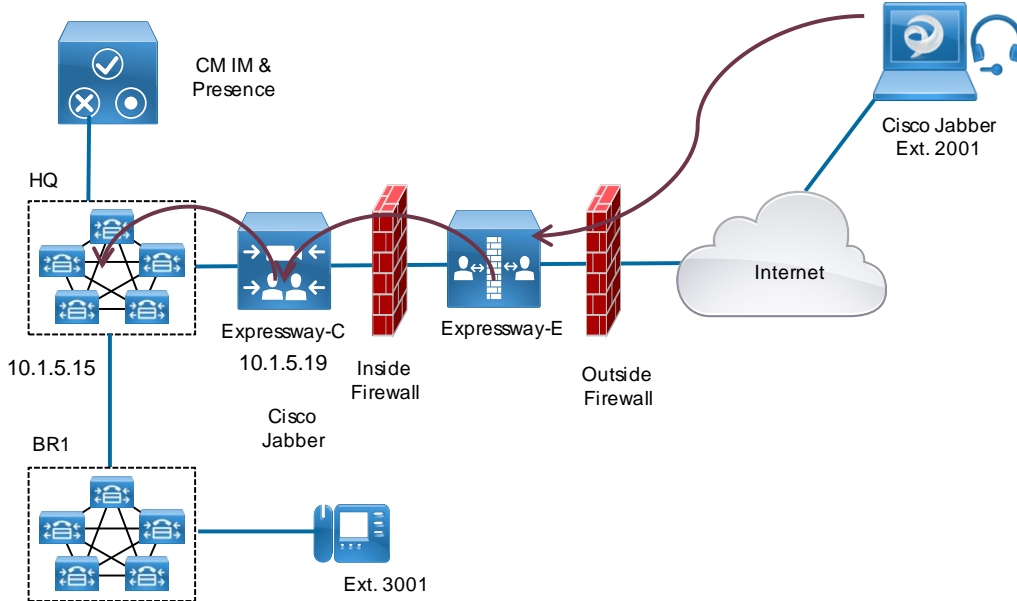
Status System Configuration Applications Users Maintenance

**Search details**

- Destination (1)
  - Alias (1)
    - Type: Url
    - Origin: Unknown
    - Value: sip:3001@10.1.5.15;user=phone
  - StartTime: 2015-01-21 22:06:43
  - Duration: 10.22
- SubSearch (1)
  - Type: Directed
  - Path (1)
    - Hop (1)
      - Address: CEtcp101515
    - Hop (2)
      - Address: 10.1.5.15
  - SubSearch (1)
    - Type: Admin Policy
    - Action: Proxy
    - ResultAlias (1)
      - Type: H323Id
      - Origin: Unknown
      - Value: sip:3001@10.1.5.15;user=phone
    - Zone (1)**
      - Name: CEtcp-10.1.5.15**
      - Type: Neighbor
      - Protocol: SIP
      - Found: **False**
      - Reason: **Not Found**
      - StartTime: 2015-01-21 22:06:43
      - Duration: 10.21
      - Gatekeeper (1)
        - Address: 10.1.5.15:5060
      - Alias (1)
        - Type: H323Id
        - Origin: Unknown
        - Value: sip:3001@10.1.5.15;user=phone

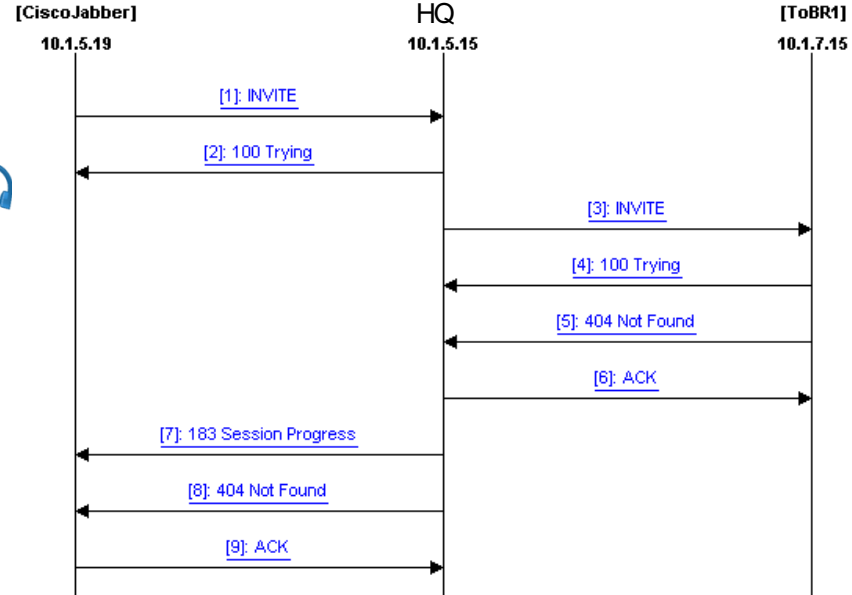
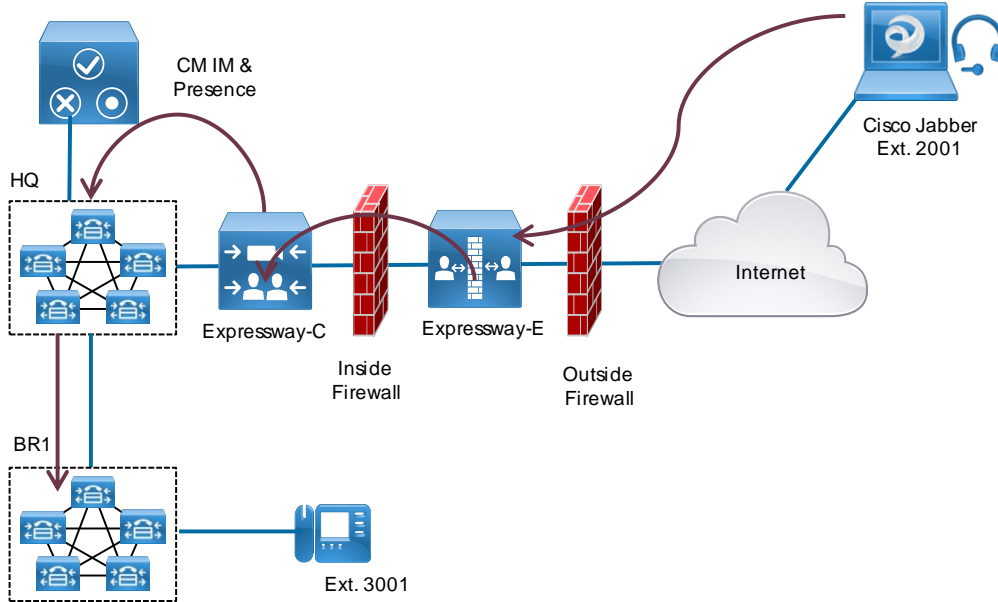
# Scenario 5: Cannot Place Calls

✓ Is the Invite received by Unified Communications Server at HQ?



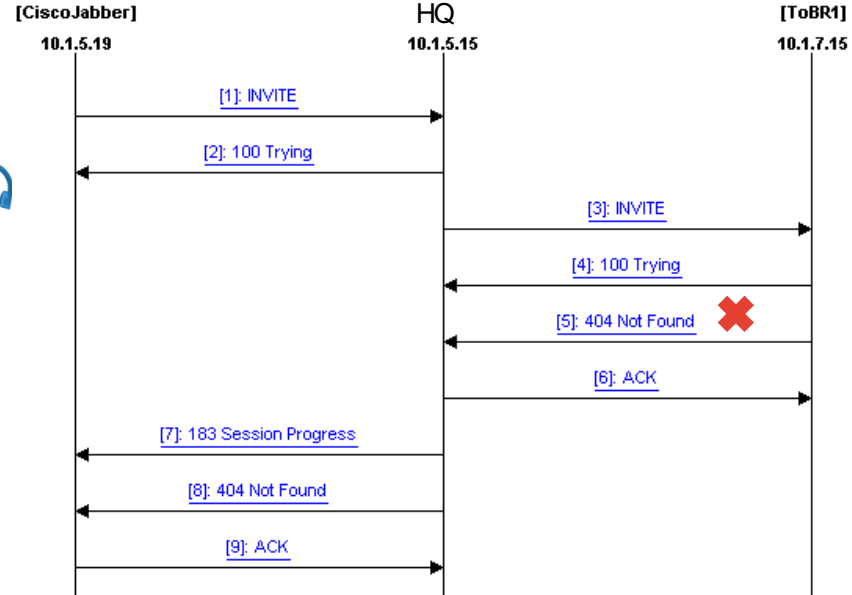
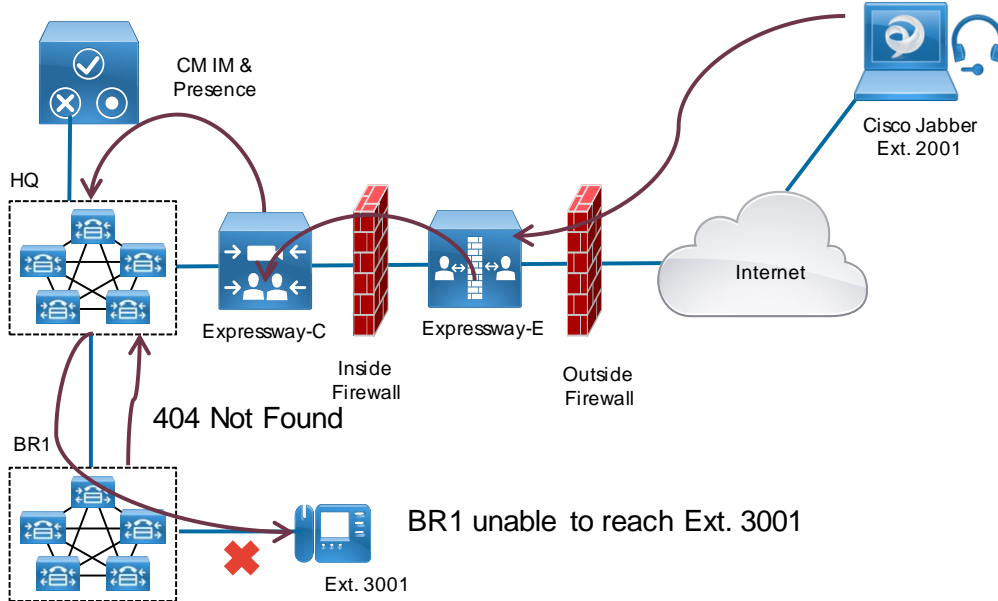
# Scenario 5: Cannot Place Calls

✓ Is the Invite received by Unified Communications Server at BR1?



# Scenario 5: Cannot Place Calls

✗ Can BR1 reach device at 3001?







Q&A

Cisco *live!*

# 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](http://www.CiscoLiveAPAC.com)





Thank you.

Cisco *live!*



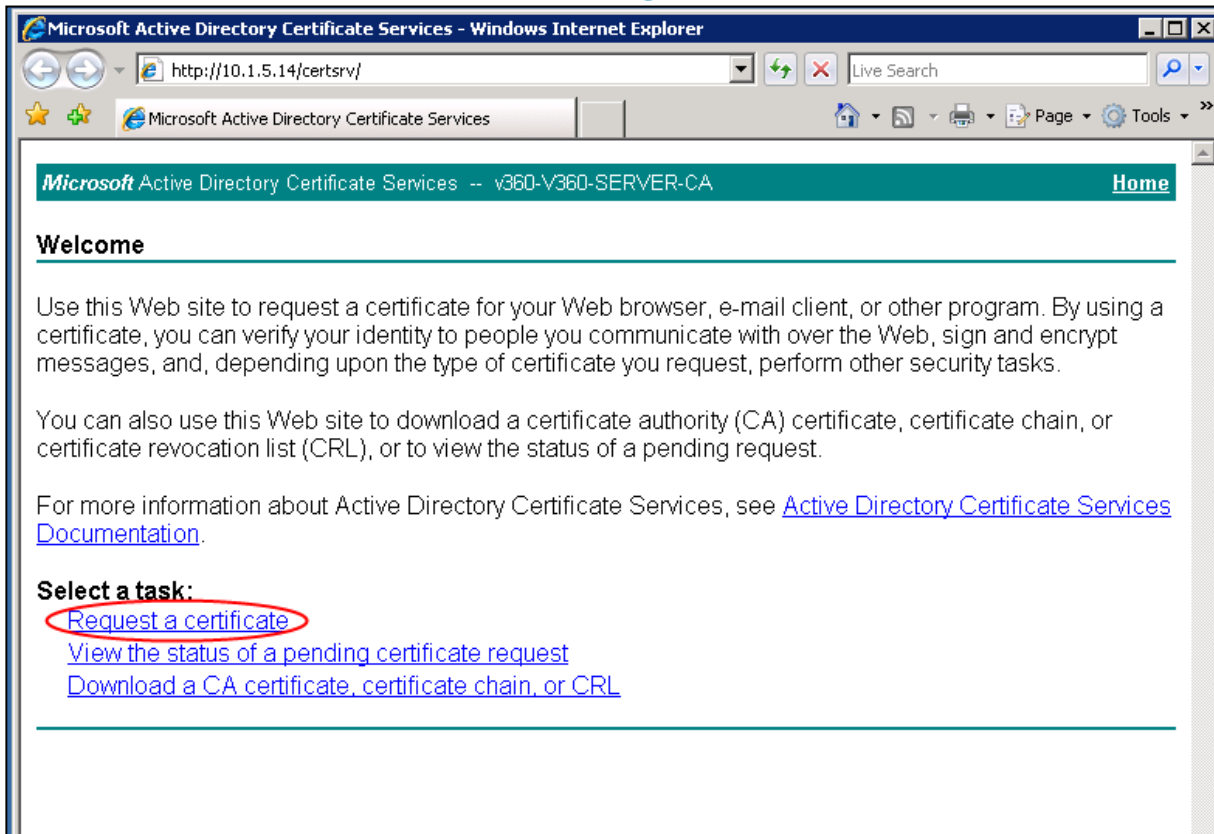
**CISCO**



A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern pedestrian bridge with blue lighting spans across the street. Tall buildings with illuminated windows and signs are visible, along with several flags on poles to the left. The overall scene is a dynamic urban environment.

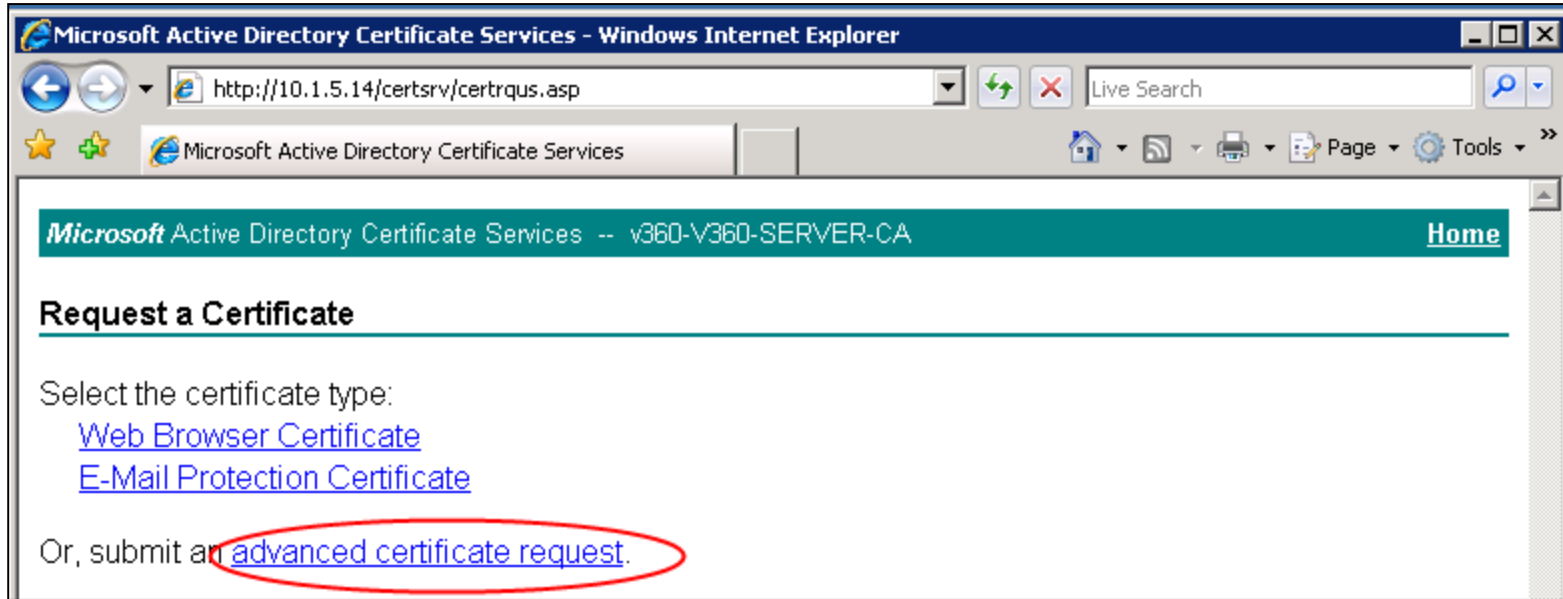
# Appendix A Certificates

# Request a Certificate using Microsoft CA



The screenshot shows a Windows Internet Explorer browser window displaying the Microsoft Active Directory Certificate Services website. The address bar shows the URL `http://10.1.5.14/certsrv/`. The page title is "Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA". The main content area features a "Welcome" section with a horizontal line, followed by a paragraph explaining the site's purpose: "Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks." Below this is another paragraph: "You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request." A link to "Active Directory Certificate Services Documentation" is provided. A "Select a task:" section follows, with three links: "Request a certificate" (circled in red), "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

# Submit an Advanced Certificate Request



# Submit a Certificate Request

Microsoft Active Directory Certificate Services - Windows Internet Explorer

http://10.1.5.14/certsrv/certrqad.asp

Microsoft Active Directory Certificate Services

Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA [Home](#)

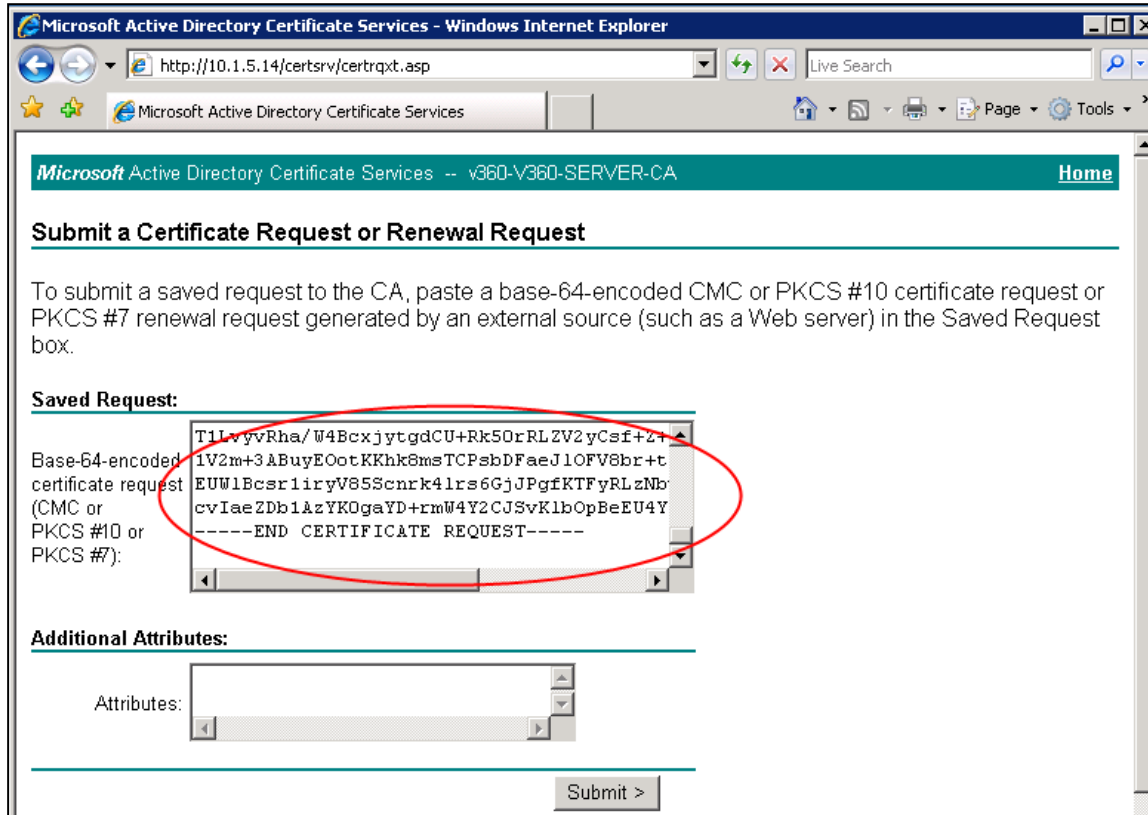
## Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- [Create and submit a request to this CA.](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)



# Paste Certificate from CSR file



The screenshot shows a web browser window titled "Microsoft Active Directory Certificate Services - Windows Internet Explorer". The address bar shows the URL "http://10.1.5.14/certsrv/certrqxt.asp". The page content includes a header "Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA" and a "Home" link. The main heading is "Submit a Certificate Request or Renewal Request". Below this, there is a paragraph explaining that users can submit a saved request by pasting a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request. A section titled "Saved Request:" contains a text area with a red circle around it. The text in the text area is a base-64 encoded certificate request. Below the text area is an "Additional Attributes:" section with a text input field and a "Submit >" button.

**Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA** [Home](#)

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
T1LvyvRha/W4BcxjytdCU+Rk5OrRLZV2yCsf+2t  
1V2m+3ABuyEOotKKhk8msTCPsbDFaeJ10FV8br+t  
EUW1Bc8r1iryV85Scnrk41rs6GjJPgfKTFyRLzNb  
cvIaeZDb1AzYK0gaYD+rmW4Y2CJSvK1bOpBeEU4Y  
-----END CERTIFICATE REQUEST-----
```

**Additional Attributes:**

Attributes:

# Certificate Pending



The screenshot shows a Windows Internet Explorer browser window. The title bar reads "Microsoft Active Directory Certificate Services - Windows Internet Explorer". The address bar contains the URL "http://10.1.5.14/certsrv/certifnsh.asp". The page content includes a header for "Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA" with a "Home" link. The main heading is "Certificate Pending". The text below the heading states: "Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested." It then says "Your Request Id is 18" and "Please return to this web site in a day or two to retrieve your certificate." A note at the bottom reads: "Note: You must return with this web browser within 10 days to retrieve your certificate".

Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA [Home](#)

## Certificate Pending

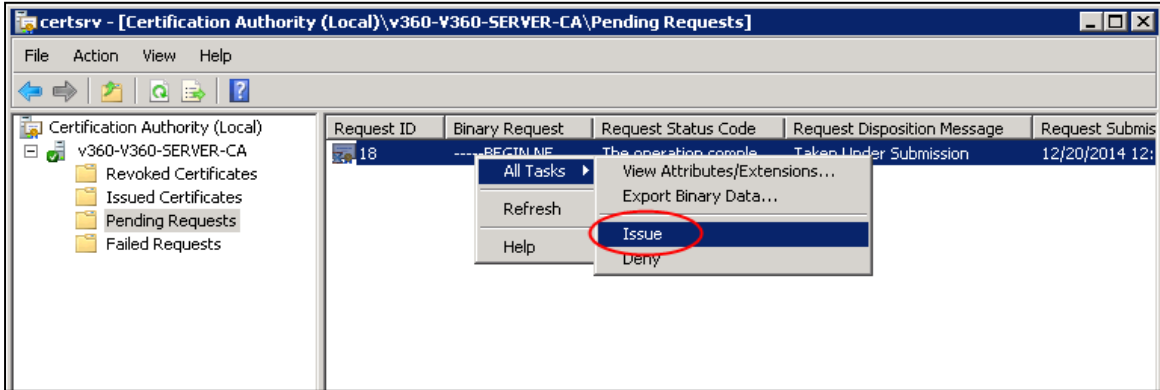
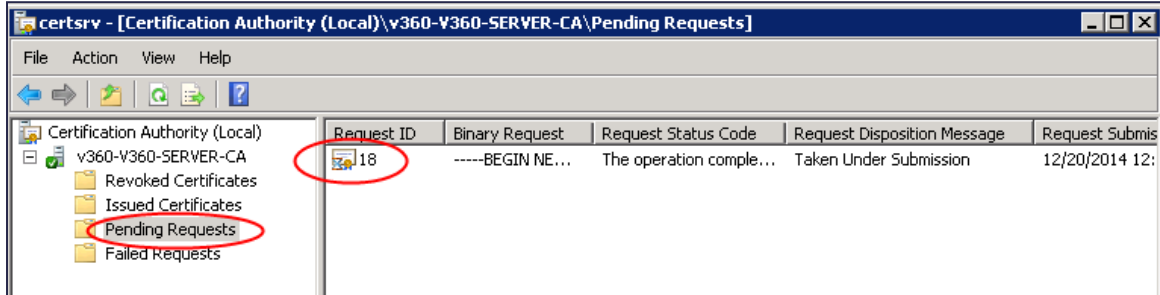
Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 18

Please return to this web site in a day or two to retrieve your certificate.

**Note:** You must return with **this** web browser within 10 days to retrieve your certificate

# Issue Certificate from CA



# View Status: MS Active Directory Certificate Services

Microsoft Active Directory Certificate Services - Windows Internet Explorer

http://10.1.5.14/certsrv/

Microsoft Active Directory Certificate Services

Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA [Home](#)

## Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

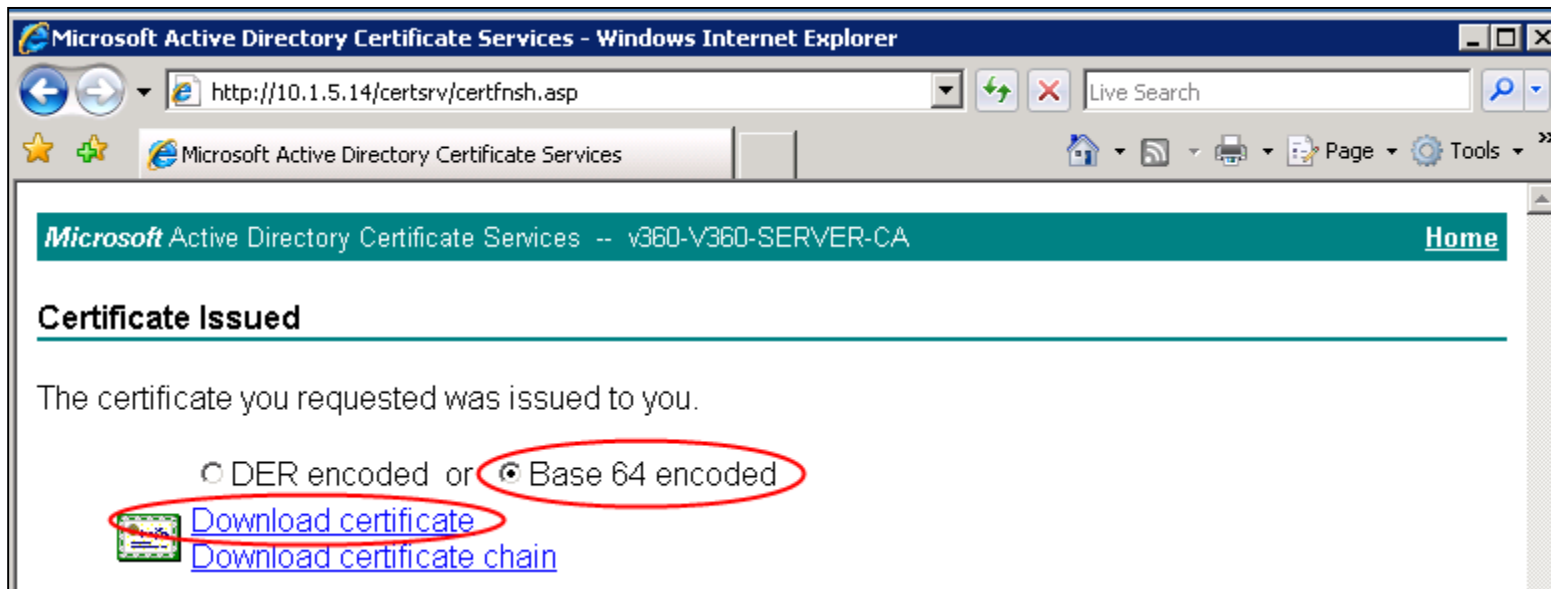
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

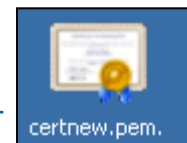
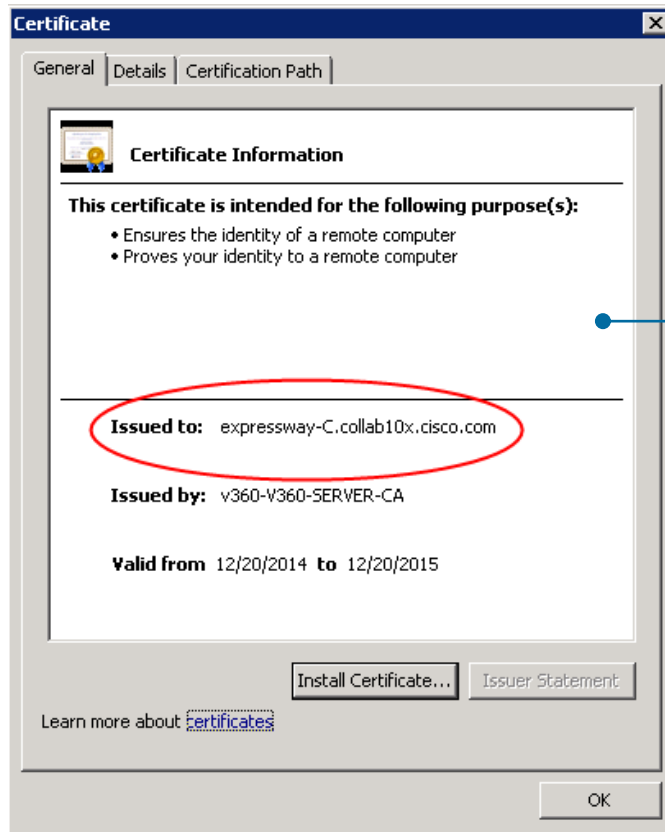
**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

# Download Certificate



# Check Certificate





# Download CA Certificate

Microsoft Active Directory Certificate Services - Windows Internet Explorer

http://10.1.5.14/certsrv/

Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA [Home](#)

## Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

# Download CA Certificate

Microsoft Active Directory Certificate Services - Windows Internet Explorer

http://10.1.5.14/certsrv/certcarc.asp

Microsoft Active Directory Certificate Services -- v360-V360-SERVER-CA [Home](#)

## Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

**CA certificate:**

Current [v360-V360-SERVER-CA]

**Encoding method:**

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

Appendix B  
Single Sign On  
over Collaboration Edge



# Overview

- x8.5 supports SSO.
- Jabber 10.6 has added Edge to its SSO login flow
- This support is an extension of the existing SSO login and discovery features added in 10.5
- This feature adds no visible change to the existing login flows
- Jabber also discovers if edge is SSO enabled. Edge credential prompt via SSO if available

# API's

In order to implement EDGE SSO two new API's added on VCS/Expressways:

1. “*get\_edge\_sso*”: an API enables Jabber to query if the Edge server supports SSO
2. The “*authorise*”: an API enable Jabber to request tokens used for SSO from the VCS/Expressway server



## /get\_edge\_sso

- The get\_edge\_sso API takes a single parameter that identifies the user making the request. This can be the user name, the user's email address or the user identifier
  - GET [https://edge.com:8443/#\(domain\)/get\\_edge\\_sso?username=USER-NAME](https://edge.com:8443/#(domain)/get_edge_sso?username=USER-NAME)
  - GET [https://edge.com:8443/#\(domain\)/get\\_edge\\_sso?email=EMAIL](https://edge.com:8443/#(domain)/get_edge_sso?email=EMAIL)
  - GET [https://edge.com:8443/#\(domain\)/get\\_edge\\_sso?userid=USER-IDENTIFIER](https://edge.com:8443/#(domain)/get_edge_sso?userid=USER-IDENTIFIER)
- The Expressway always replies to the /get\_edge\_sso request with a 200 OK response
- Response is an XML formatted message that indicates whether or not SSO is currently supported for the user



# /authorise

- Used by the client to initiate the authentication of the user (by the Identity Provider)
- Authorisation tokens for HTTP, XMPP and SIP access to the enterprise.
- The API takes a number of parameters
  - *response\_type* - Must be set to “token”
  - *client\_id* - Identifies the type of client (Jabber for Android etc.)
  - *device\_id* - Uniquely identifies the client device (e.g. MAC address)
  - *Realm* - Set to “local”
  - *Username, email or useridentifier* - Only one of these must be specified
  - *Service* - Unity tokens. It indicates the URL of the Cisco Unity Connection server: base64 hash of domain/protocol/address/port

# /authorise: Examples

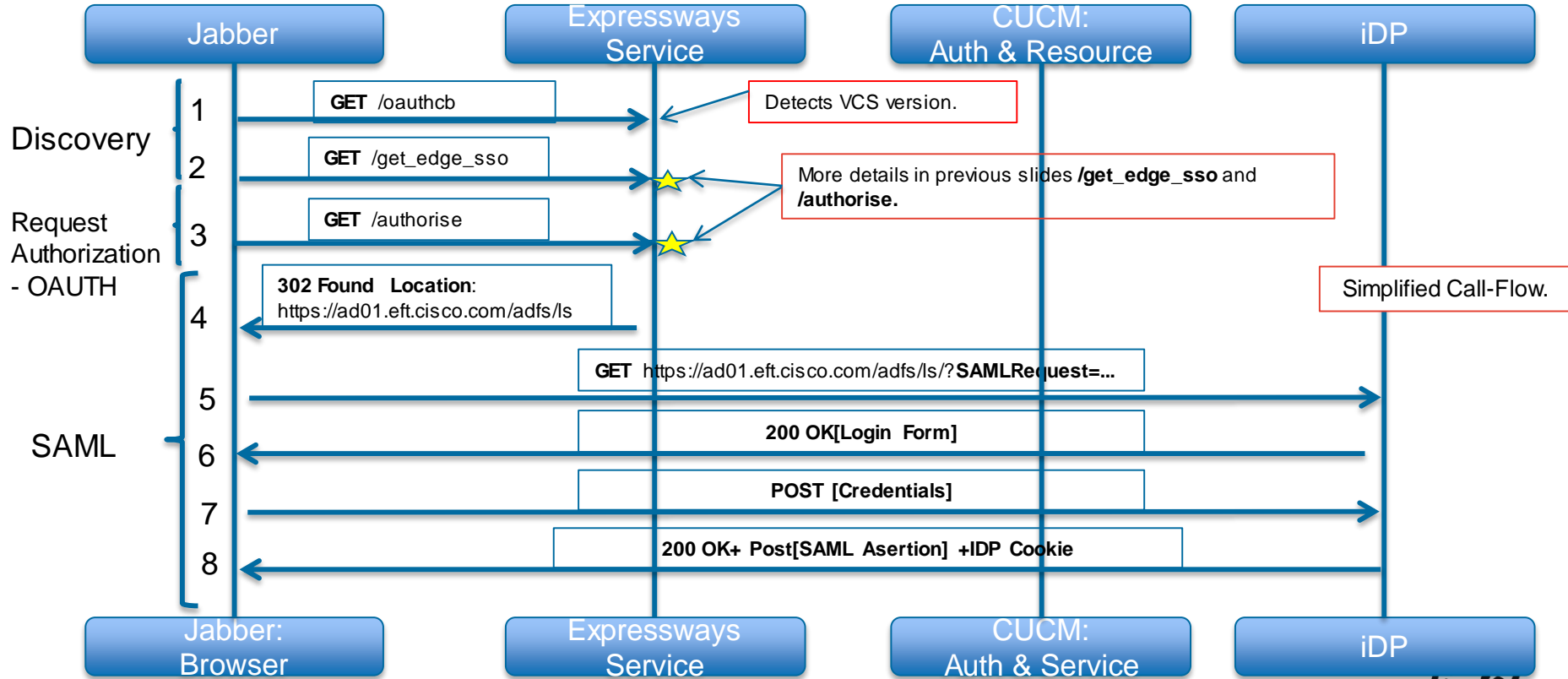
- *VCS/CUCM/CUP Authorization Request*

[https://edge.com:8443/#\(domain\)/authorize?response\\_type=token&client\\_id=CLIENT-ID&realm=local&device\\_id=DEVICE-ID&username=USER-NAME](https://edge.com:8443/#(domain)/authorize?response_type=token&client_id=CLIENT-ID&realm=local&device_id=DEVICE-ID&username=USER-NAME)

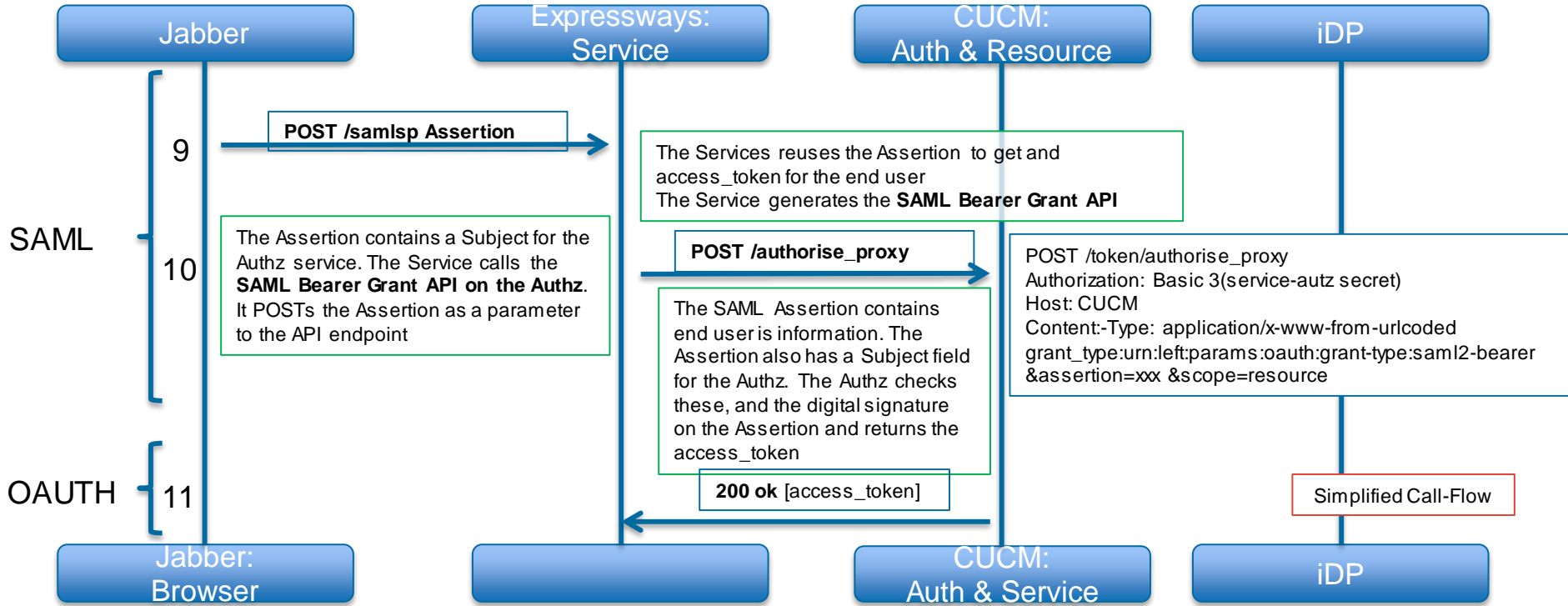
- *Cisco Unity Connection Authorisation Request*

[https://edge.com:8443/#\(domain\)/authorize?response\\_type=token&client\\_id=CLIENT-ID&realm=local&device\\_id=DEVICE-ID&service=#\(domain/protocol/address/port\)&username=USER-NAME](https://edge.com:8443/#(domain)/authorize?response_type=token&client_id=CLIENT-ID&realm=local&device_id=DEVICE-ID&service=#(domain/protocol/address/port)&username=USER-NAME)

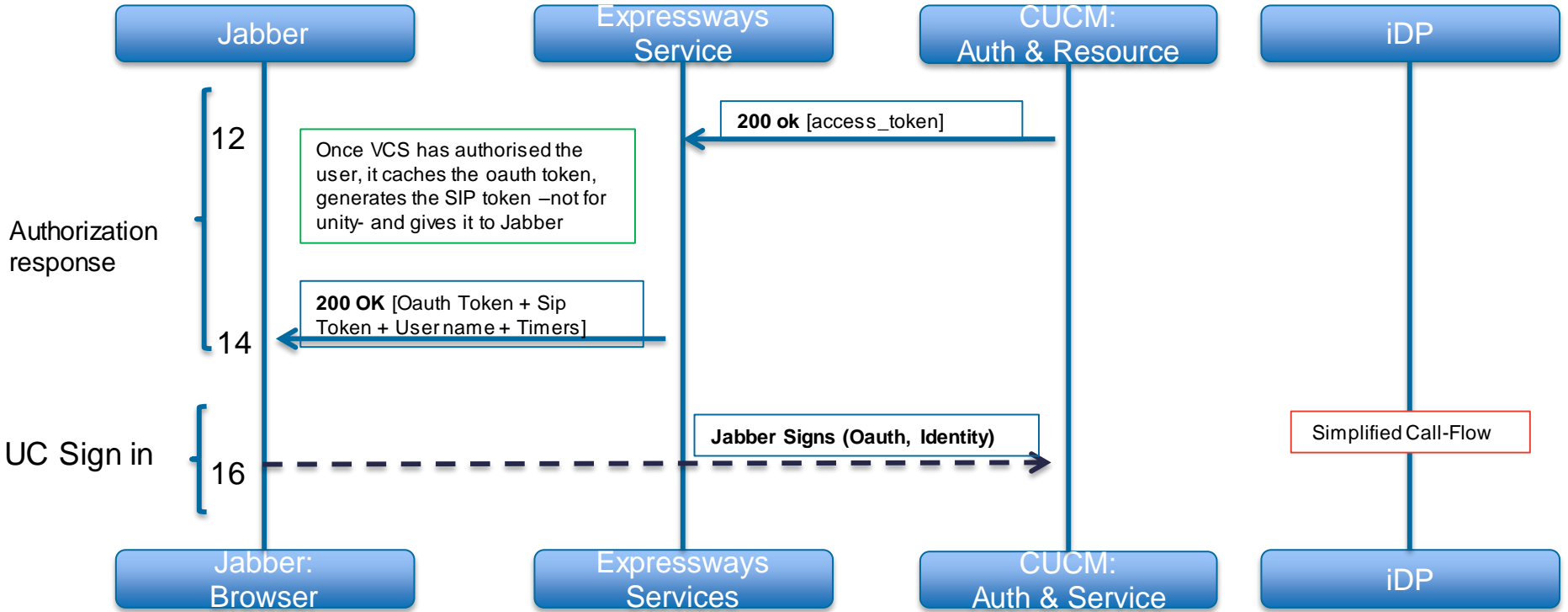
# EDGE SSO - Call Flow Sequence



# EDGE SSO - Call Flow Sequence



# EDGE SSO - Call Flow Sequence



# Edge SSO Tokens

- Jabber receives three token via two different calls to the VCS authorise API.
- First request to VCS Jabber retrieves the **CUCM OAUTH Token** which is used to authenticate all **HTTP** and **XMPP** traffic traversing the edge.
- Same request also provides Jabber with a **SIP token** which is required for SIP traffic to traverse the edge. This token has a longer lifetime than the CUCM token.
- Subsequent request to VCS Jabber retrieves the **Unity OAUTH Token** for use by voicemail HTTP traffic.



# 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

- CUCM - Default 60 minutes

## C) SIP Token Extra TTL

- Configured on VCS-C / Expressway-C
- Value is added onto OAuth Token expiry to get SIP Token Expiry
- Default 0, Max 48 hours

## D) SIP REGISTER expiry refresh

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 is 2 minutes.

SIP stack attempts to refresh register 1 minute 55 seconds after last successful one using Voicemail, Unity OAUTHToken expiry

# Edge Transition Behaviour

- If you login to Jabber while on Edge and then transition to an on-prem network while still logged in then Jabber will seamlessly reconnect as the tokens issued by VCS are valid for CUCM and Unity.
- However, if you login to jabber while on-prem, and then transition to Edge, then the tokens that were issued directly by CUCM and Unity will not be valid for traffic through VCS.
- Jabber must re-authenticate with VCS and the user may be prompted to do this via the standard re-establish SSO session pop-up, if the cookie has expired otherwise it will be invisible to the user.
- If logging in on-prem with SSO and then transitioning to a non SSO Edge results Jabber going offline. The client must sign out to reestablish connection.

# Logs

- This line is the result from checking if the VCS/Expressway server is a version capable of SSO.
  - `[EdgeSSODetector::Impl::isSSOSupported]` - VCS has `<SUPPORTED>` SSO and it `<was/wasn't>` previously SSO Enabled
- This is the log message that shows we have discovered the VCS/Expressway and the users cluster to be SSO enabled. We should now do an SSO Login.
  - `[EdgeSSODetector::Impl::discoverSSO]` - `ssoConfiguration->isSSOEnabled: 1`

# Logs

- This means that the client needs credentials for the VCS server, and will use SSO to get a token.
  - `[LifeCycleImpl::Impl::OnCredentialsRequired]` - SSO Enabled and ServiceID: 1001 is configured for SSO - `doSingleSignOn`
- Any successful navigation to get a token will be framed by "navigate to:" and "[SingleSignOn::Impl::gotOAuthTokenInResult]". There may be one or more [SingleSignOn::Impl::noTokenInResult] in between, which can represent the login page or intermediate redirects.
  - `[SingleSignOn::Impl::authorizeNext]` - About to navigate to: <URL> for authenticationService: 1001
  - `[SingleSignOn::Impl::gotOAuthTokenInResult]` - Got an OAuth Token for service: 1001

# Logs to look for

- If there were any issues, or the token was not retrieved, you can check [BrowserListenerImpl::OnNavigationCompleted], this should show the error type the browser experienced and may be followed by the URL that was navigated to, depending on the error.
- After initial sign in, you can find refreshes and attempts to reauthenticate after a failed use of a token by looking for:

```
[SingleSignOn::Impl::appendAndAuthenticate] -  
appendAndAuthenticate for authenticatorId [1001]
```



**CISCO**