TOMORROW starts here.
Configuring and Troubleshooting Cisco Jabber MRA using Collaboration-Edge Deployment Model

BRKCRT-2602

Rami Kandah - Technical Architect

#clmel
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

- Specialised video applications for video-only customer base and advanced video requirements
- **Superset** of X8.1 features
- No changes to existing licensing model

X8.1

- 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
Brandinng 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
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
- Unified Communications solutions
- Entry-level provisioning and support
- Video and conferencing concepts

How We Learn
- E-Learning Courses
- Instructor-Led Training
## Exams and Recommended Training

<table>
<thead>
<tr>
<th>Required Exam(s)</th>
<th>Recommended Training*</th>
</tr>
</thead>
<tbody>
<tr>
<td>210-060 CICD v1.0</td>
<td>Implementing Cisco Collaboration Devices (CICD v1.0)</td>
</tr>
<tr>
<td>210-065 CIVND v1.0</td>
<td>Implementing Cisco Video Network Devices, Part 1 (CIVN1 v1.0) – eLearning AND Implementing Cisco Video Network Devices, Part 2 (CIVN2 v1.0) – ILT</td>
</tr>
</tbody>
</table>

*Delivered by Cisco Certified Learning Partners*
CCNP Collaboration

What We Learn

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

How We Learn

- Instructor-led Training

Education
# Exams and Recommended Training

<table>
<thead>
<tr>
<th>Required Exam(s)</th>
<th>Recommended Training*</th>
</tr>
</thead>
<tbody>
<tr>
<td>300-070 CIPTV1 v1.0</td>
<td>Implementing Cisco IP Telephony &amp; Video, Part 1 v1.0</td>
</tr>
<tr>
<td>300-075 CIPTV2 v1.0</td>
<td>Implementing Cisco IP Telephony &amp; Video, Part 2 v1.0</td>
</tr>
<tr>
<td>300-080 CTCOLLAB v1.0</td>
<td>Troubleshooting Cisco IP Telephony &amp; Video v1.0</td>
</tr>
<tr>
<td>300-085 CAPPS v1.0</td>
<td>Implementing Cisco Collaboration Applications v1.0</td>
</tr>
</tbody>
</table>

*Delivered by Cisco Certified Learning Partners
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

Diagram:
- Collaboration Services
- Inside firewall (Intranet)
- DMZ
- Outside firewall
- Internet
- Expressway
- Unified CM
- Expressway C
- Expressway E
- Fixed remote endpoints (TC Series)
- Jabber @ work
- Jabber @ home
- Jabber @ the café
- Jabber @ SFO, LHR or PVG
Cisco Jabber Remote Access Options

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

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

Collaboration Services

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

Unified CM  Expressway C  Expressway E
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.
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

Unified CM IM & Presence

Expressway-C

Inside Firewall

Expressway-E

Outside Firewall

Internet

XMPP

HTTPS

SIP

Cisco Jabber

Unified CM

Cisco Jabber

Cisco Jabber
## Public (external) DNS SRV Requirements

<table>
<thead>
<tr>
<th>Domain</th>
<th>Service</th>
<th>Protocol</th>
<th>Priority</th>
<th>Weight</th>
<th>Port</th>
<th>Target Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>collab10x.cisco.com</td>
<td>collab-edge</td>
<td>tls</td>
<td>10</td>
<td>10</td>
<td>8443</td>
<td>expressway-e.collab10x.cisco.com</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Domain</th>
<th>Service</th>
<th>Protocol</th>
<th>Priority</th>
<th>Weight</th>
<th>Port</th>
<th>Target Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>collab10x.cisco.com</td>
<td>cisco-uds</td>
<td>tcp</td>
<td>10</td>
<td>10</td>
<td>8443</td>
<td>pub10x-hq.collab10x.cisco.com</td>
</tr>
<tr>
<td>collab10x.cisco.com</td>
<td>cuplogin</td>
<td>tcp</td>
<td>10</td>
<td>10</td>
<td>8443</td>
<td>imp10x-hq.collab10x.cisco.com</td>
</tr>
</tbody>
</table>
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

HTTP/1.1 200 OK
GET/cucm-uds/clusterUser?username=jdoe HTTP/1.1
HTTP/1.1 200 OK
GET/cucm-uds/clusterUser?email=jdoe@collab10x.cisco.com HTTP/1.1
HTTP/1.1 200 OK
127.0.0.1 HTTP/1.1 200 OK
Loopback address

HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
Registering Remote Cisco Jabber to Cisco Unified Communications Manager

Unified CM | Local DNS | CM IM & Presence | Expressway-C | Inside Firewall | Expressway-E | Outside Firewall | Public DNS | Cisco Jabber

GET /cucm-uds/servers HTTP/1.1
GET /cucm-uds/user/jdoe HTTP/1.1
GET /cucm-uds/user/jdoe/devices HTTP/1.1
GET /global-settings.xml HTTP/1.1
GET /jabber-config.xml HTTP/1.1
POST /EPASSoap/service/v105 HTTP/1.1

Sending Request Method=REGISTER, CSeq=690, To=sip:2001@10.1.5.15

Loopback address: 127.0.0.1
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
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

Device Information:
- Product: SIP
- Device Protocol: SIP
- Trunk Service Type: Standard Presence Group
- Device Name: IMP_Trunk
- Description: Optional

SIP Information:
- Destination Address: 10.1.5.18
- Destination Address IPv6: 5050
- Non-Secure SIP Trunk Profile
- Standard SIP Profile
- Standard Presence Group
- 711law
- No Preference
b) Configure Domain and Publish SIP 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

<table>
<thead>
<tr>
<th>Phone Configuration</th>
<th>Rela</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td></td>
</tr>
<tr>
<td><img src="image1" alt="Image of the status section" /></td>
<td></td>
</tr>
<tr>
<td><strong>Association</strong></td>
<td></td>
</tr>
<tr>
<td><img src="image2" alt="Image of the association section" /></td>
<td></td>
</tr>
<tr>
<td><strong>Device Information</strong></td>
<td></td>
</tr>
<tr>
<td><img src="image3" alt="Image of the device information section" /></td>
<td></td>
</tr>
</tbody>
</table>

- **Device > Phone Type**
  - Cisco Unified Client Services Framework (CSF)

- **Device Name**
  - Any name – has no significance
c) Configure Jabber in Cisco Unified Communications Manager

![Diagram showing Jabber configuration settings]

- Owner: User
- Owner User ID: jdoe
- Protocol Specific Information:
  - Packet Capture Mode: None
  - BLF Presence Group: Standard Presence Group
  - SIP Dial Rules: < None >
  - MTP Preferred Originating Codec: 711ulaw
  - Device Security Profile: Cisco Unified Client Services Framework - Standard
  - SIP Profile: Standard SIP Profile
  - Digest User: < None >
c) Enable Video for Jabber in Cisco Unified Communications Manager

- Enable Video Calling
- Specify Video Bite Rate
c) Configure Cisco Jabber Directory Number

![Image of Cisco Jabber Directory Number configuration interface]

- **Directory Number Configuration**
- **Status**: Status: Ready
- **Directory Number Information**
  - Directory Number*: 2001
  - Route Partition: Internal_pt
- **Directory Number Settings**
  - Voice Mail Profile: < None >
  - Calling Search Space: Internal.CSS
d) Configure UC Services

UC Service Type
UDS – Universal Directory Services on CUCM
d) Configure Service Profile

**Service Profile Configuration**
- **Save**, **Delete**, **Copy**, **Add New**

**Status**
- Status: Ready

**Service Profile Information**
- Name: ServProf
- Description
- Make this the default service profile for the system

**IM and Presence Profile**
- Primary: IMP
- Secondary: <None>
- Tertiary: <None>

**Directory Profile**
- Primary: UDS
- Secondary: <None>
- Tertiary: <None>

- 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

Enable User for Unified CM and Presence

Associate devices
e) End User Configuration

- Enable Desk Phone Control
  - Only for On-Prem
- Shared line
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

Status

Status: Ready

Select Server and Service

Server*: 10.1.5.18--CUCM IM and Presence (Active)
Service*: Cisco SIP Proxy (Active)

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)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Proxy Parameters (Clusterwide)</td>
<td></td>
</tr>
<tr>
<td>Virtual IP Address (dotted-IPv4 format or IPv6)</td>
<td></td>
</tr>
<tr>
<td>SRV Cluster Name</td>
<td></td>
</tr>
<tr>
<td>CUCM Domain *</td>
<td>collab10x.cisco.com</td>
</tr>
</tbody>
</table>
b) Configure Presence Settings

<table>
<thead>
<tr>
<th>Presetne Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cluster ID</strong></td>
</tr>
<tr>
<td><strong>Enable availability sharing</strong></td>
</tr>
<tr>
<td><strong>Allow users to view the availability of other users without being prompted for approval</strong></td>
</tr>
<tr>
<td><strong>Note:</strong> this option must be turned on for SIP clients to function properly</td>
</tr>
<tr>
<td><strong>Enable use of Email Address for Inter-domain Federation</strong></td>
</tr>
<tr>
<td><strong>Maximum Contact List Size (per user)</strong></td>
</tr>
<tr>
<td><strong>Maximum Watchers (per user)</strong></td>
</tr>
<tr>
<td><strong>CUCM IM and Presence Publish Trunk</strong></td>
</tr>
</tbody>
</table>

**SIP Publish Trunk in CUCM**
c) Configure Presence Gateway

<table>
<thead>
<tr>
<th>Presence Gateway Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Save" />, <img src="image" alt="Delete" />, <img src="image" alt="Add New" /></td>
</tr>
</tbody>
</table>

**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 push information (e.g., phone on/off hook status).

<table>
<thead>
<tr>
<th>Presence Gateway Type*</th>
<th>CUCM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description*</td>
<td>CUCM</td>
</tr>
<tr>
<td>Presence Gateway*</td>
<td>10.1.5.15</td>
</tr>
</tbody>
</table>

**Presence Gateway IP Address of CUCM**
d) Configure Client Settings

- TFTP Servers
  - Primary TFTP Server: 10.1.5.15
  - Backup TFTP Server
  - Backup TFTP Server

- Phone Control
e) Restart All Proxy Services
f) Check System Dashboard
f) System Configuration Troubleshooter

Troubleshooting GUI for:
- System
- Sync Agent
- Presence Engine
- Sip Proxy
- Topology
- Cisco Jabber
- XCP
- User
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
a) Basic Configuration - DNS

Corporate DNS

Public DNS
a) Basic Configuration - SIP

![Cisco Expressway-C SIP Configuration](image1)

![Cisco Expressway-E SIP Configuration](image2)
b) Configure Domains and Supported Services on Expressway-C
Enable MRA

Enable Mobile and Remote Access
d) Configure Unified CM Servers on Expressway-C

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
f) Check Status of Servers on Expressway-C

Publisher & Subscriber nodes

IM and Presence node
g) Check Search Rules

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

  X.509v3 Extended Key Usage:
  TLS Web Client Authentication
  TLS Web Server Authentication

- Public CA signed certificates allow Jabber clients and endpoints to validate the server certificate without a CTL
- Jabber clients with a CTL will not use the CTL to validate Expressway certificate - no requirement to include Expressway certs in CTL
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)
### Subject Alternative Name (SAN) Requirements

Expressway-E Server Certificate

```c
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
k) Generate CSR: Expressway-E
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

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
- Currently loaded certificate expires on Dec 20 2015

Upload new certificate

- Select the server private key file
- Select the server certificate file
  - Choose File: certnew.pem

Upload server certificate data
n) Upload CA Certificate to Expressway-C and Expressway-E

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

Type  Issuer
Certificate  O=Temporary CA d634b5d8-7f89-11e3-af0c-005056b41ed3, OU=Temporary CA d634b5d8-7f89-005056b41ed3
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
Choose File  No file chosen

Append CA certificate  Reset to default CA certificate
```
Configure Traversal Client on Expressway-C

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Hop count</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connection credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Accept proxied registrations</td>
</tr>
<tr>
<td>ICE support</td>
</tr>
</tbody>
</table>

Create Zone
Unified Communications Traversal
p) Configure Traversal Client on Expressway-C

![Diagram showing configuration of Traversal Client on Expressway-C]
q) Configure Traversal Server on Expressway-E

Transport TLS
SSH Tunnel only supports TLS
r) Verify Traversal Zone Status

Configuration > Zones
Check traversal zone status to Expressway-E
Verify SSH Tunnel Status
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

![Cisco Jabber login screen]

- Enter username and password:
  - Username: jdoe@collab10x.cisco.com
  - Password: ********

- Click on "Sign In" button.

![Connection Status]

- Softphone: Connected
- Protocol: SIP
- Address: 10.1.5.15 (CCMCP - Expressway)
- Device: /dev/ciscojabber
- Line: 2001

- Presence: Connected
- Address: expressway-E.collab10x.cisco.com
- Protocol: XMPP
- Port: 5222

- Outlook address book: Last connection successful
- Protocol: IMAP
- Address: Outlook

- Directory: Last connection successful
- Address: 10.1.5.15
- Protocol: UDS (HTTPS)
s) Verification: Check Status on Expressway-C

Status > Unified Communications
View provisioning
Sessions
s) Verification: Check Status in Cisco Unified Communications Manager

![Cisco Unified Communications Manager screenshot](image)

**Device > Phone**

Cisco Jabber shows IP address of Expressway-C
s) Verification: Check Call Status

### Call status

<table>
<thead>
<tr>
<th>Start time</th>
<th>Duration</th>
<th>Source</th>
<th>Destination</th>
<th>Type</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-12-21 15:32:25</td>
<td>1 minute 12 seconds</td>
<td>sip2001@10.1.5.15</td>
<td>sip:3001@10.1.5.15</td>
<td>Traversal</td>
<td>Multiple components</td>
</tr>
</tbody>
</table>

*Traversal Call*

```
Model: Traversal Call
```

### Call status

<table>
<thead>
<tr>
<th>Start time</th>
<th>Duration</th>
<th>Source</th>
<th>Destination</th>
<th>Type</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-12-21 15:32:25</td>
<td>4 minutes 23 seconds</td>
<td>sip:2001@10.1.5.15</td>
<td>sip:3001@10.1.5.15</td>
<td>Traversal</td>
<td>SIP &lt;-&gt; SIP</td>
</tr>
</tbody>
</table>

*Traversal Call*

```
Model: Traversal Call
```
Registering Remote Cisco Jabber to Cisco Unified Communications Manager

Unified CM - Local DNS - CM IM & Presence - Expressway-C - Inside Firewall - Expressway-E - Outside Firewall - Public DNS - Cisco Jabber

DNS SRV Lookup: _cisco-uds._tcp.domain
Not found

DNS SRV Lookup: _collab-edge._tls.domain

Expressway-E address

TLS Handshake, Trusted certificate authentication

get_edge_config?service_name=_cisco-uds&service_name=_cuplogin HTTP/1.1
Registering Remote Cisco Jabber to Cisco Unified Communications Manager

GET /cucm-uds/servers HTTP/1.1
GET /cucm-uds/user/jdoe HTTP/1.1
GET /cucm-uds/user/jdoo/devices HTTP/1.1
GET /global-settings.xml HTTP/1.1
GET /jabber-config.xml HTTP/1.1
POST /EPASSoap/service/v105 HTTP/1.1

Sending Request Method=REGISTER, CSeq=690, To=sip:2001@10.1.5.5
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
Tools: Expressway Series

Search History

• Status > Search History
• Search details of call
• View call information
• View all events for the call
Tools: Cisco Jabber

Network Log

- `%user_profile%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`
Scenario 1: Cannot Find Services

✓ Does Cisco Jabber register locally?
✓ Is_cisco-uds SRV request blocked?
X Do we get a response to _collab-edge.tls SRV request?
Scenario 1: Cannot Find Services

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?

X Is the SSH Tunnel OK?
Scenario 2: Cannot Communicate with Server

<table>
<thead>
<tr>
<th>Unified Communications (last updated: 03:33:30 UTC)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unified CM registrations</td>
<td>Domain configured but no active zone connection</td>
</tr>
<tr>
<td>IM and Presence Service</td>
<td>Domain configured but no active zone connection</td>
</tr>
<tr>
<td>XMPP Federation</td>
<td>Not configured (Configure a domain on Expressway-C)</td>
</tr>
<tr>
<td>Single Sign-On support</td>
<td>Not configured (Enable on the Unified Communications page)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Domains</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>cscnhb10x.cisco.com</td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>Unified CM registrations, IM and Presence Service</td>
</tr>
<tr>
<td>Associated zones</td>
<td>TraverseToExpressway-E</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zones</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>TraverseToExpressway-E</td>
</tr>
<tr>
<td>SIP status</td>
<td>Failed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Servers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence Service nodes</td>
<td>1 (XMPP: router: inactive)</td>
</tr>
<tr>
<td>Unified CM servers</td>
<td>2</td>
</tr>
<tr>
<td>Unity Connection servers</td>
<td>There are no Unity Connection servers configured</td>
</tr>
</tbody>
</table>
### Scenario 2: Cannot Communicate with Server

#### Unified Communications

<table>
<thead>
<tr>
<th>Unified Communications status</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM registrations</td>
<td>Not configured (Configure a domain on Expressway-C)</td>
</tr>
<tr>
<td>IM and Presence Service</td>
<td>Not configured (Configure a domain on Expressway-C)</td>
</tr>
<tr>
<td>XMPP Federation</td>
<td>Not configured (Enable federation on Unified Communications page)</td>
</tr>
<tr>
<td>Single Sign-On support</td>
<td>Not configured (Enable on the Unified Communications page)</td>
</tr>
</tbody>
</table>

#### Activity

| Unified CM calls: Current video | 0 |
| Unified CM calls: Current audio (SP) | 0 |

#### Domains

No domain configuration has been received from the Expressway-C. Check zone connection activity on the Expressway-C.

#### Zones

<table>
<thead>
<tr>
<th>Name</th>
<th>SIP status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TraversalToExpressway-C (expressway-C.collab10x.cisco.com)</td>
<td>On (no active connections)</td>
</tr>
</tbody>
</table>
Scenario 2: Cannot Communicate with Server

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

-government-config OK?

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

Enter your username and password for Phone Services.

jdoe@collab10x.cisco.com

Sign me in when Cisco Jabber starts

Sign In
Scenario 3: Cannot Communicate with Server

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
Scenario 3: Cannot Communicate with Server

Expressway-E DNS

DNS name cisco.com does not match name requested by Cisco Jabber
Scenario 4: Username/Password Not Valid

✓ Does Cisco Jabber register locally?
✓ ls_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?
Scenario 4: Username/Password Not Valid

X get_edge_config OK?

```cpp
[\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 [0x000006ea0] [scoery\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-p="127.0.0.1" Local-port="22111" Det-ip="127.0.0.1" Det-port="34955" Code="503" HTTP/1.1 503 Service Unavailable Server: [CE-6-503]
```

Scenario 4: Username/Password Not Valid

Cisco Jabber 10.6.3

- Your username or password is not correct.
- Enter your username and password for Phone Services:
  - jdoe@collab10x.cisco.com
  - ********
- Sign in when Cisco Jabber starts
- Advanced settings

Mismatched Service Domain
Scenario 5: Cannot Place Calls

CM IM & Presence

HQ

Expressway-C

Inside Firewall

Expressway-E

Outside Firewall

Internet

Cisco Jabber Ext. 2001

XMPP HTTPS SIP

BR1

Ext. 3001

Ext. 2001

Cisco Public
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?

[Diagram showing network setup with Cisco Jabber and Expressway-C/E nodes inside and outside the firewall.]
Scenario 5: Cannot Place Calls

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

[Diagram showing network topology with nodes labeled CM IM & Presence, HQ, BR1, Expressway-C, Expressway-E, Cisco Jabber, and Subsearch details.]
Scenario 5: Cannot Place Calls

Is the Expressway-C forwarding the Invite to HQ Unified Communications Manager through the CEtcp-@ neighbour zone?
Scenario 5: Cannot Place Calls

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

Diagram:

- CM IM & Presence
- HQ 10.1.5.15
- Expressway-C 10.1.5.19
- Inside Firewall
- Expressway-E
- Outside Firewall
- Internet
- Cisco Jabber Ext. 2001
- [Cisco.Jabber] 10.1.5.19
- [1] INVITE
- [2]: 100 Trying
- [3]: INVITE
- [4]: 100 Trying
- [5]: 404 Not Found
- [6]: ACK
- [7]: 183 Session Progress
- [8]: ACK
- BR1
- Ext. 3001
- 10.1.5.19
- 10.1.5.19
- [10]: 741.7.45
- [10]: 741.7.45
Scenario 5: Cannot Place Calls

✓ Is the Invite received by Unified Communications Server at BR1?
Scenario 5: Cannot Place Calls

X Can BR1 reach device at 3001?

HQ

CM IM & Presence

Expressway-C

Expressway-E

Outside Firewall

Internet

Cisco Jabber Ext. 2001

[1] INVITE

[2]: 100 Trying

[3]: INVITE

[4]: 100 Trying

[5]: 404 Not Found

[6]: ACK

[7]: 103 Session Progress

[8]: ACK

[9]: 404 Not Found

BR1 unable to reach Ext. 3001

BR1

404 Not Found

Ext. 3001

Inside Firewall

Inside Firewall

404 Not Found

Ext. 3001
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.
Appendix A
Certificates
Request a Certificate using Microsoft CA

Microsoft Active Directory Certificate Services -- V360-V360-SERVER-CA

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
Submit an Advanced Certificate Request

Select the certificate type:
- Web Browser Certificate
- E-Mail Protection Certificate

Or, submit an advanced certificate request.
Submit a Certificate Request

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

Microsoft Active Directory Certificate Services

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:

Additional Attributes:
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 -- V360-V360-SERVER-CA

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

The certificate you requested was issued to you.

- DER encoded
- Base 64 encoded

Download certificate
Download certificate chain
Check Certificate

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer
- Proves your identity to a remote computer

Issued to: expressway-c.collab10x.cisco.com

Issued by: v360-V360-SERVER-CA

Valid from 12/20/2014 to 12/20/2015

Learn more about [certificates]
Download CA Certificate

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

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 360-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
  - GET https://edge.com:8443/#(domain)/get_edge_sso?email=EMAIL
  - GET https://edge.com:8443/#(domain)/get_edge_sso?useridentifier=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 userid` - 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=CLI\n  ENT-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=CLI\n  ENT-ID&realm=local&device_id=DEVICE-\n  ID&service= #(domain/protocol/address/port)&username=USER-NAME
EDGE SSO - Call Flow Sequence

**Jabber**

1. GET /oauthcb

**Expressways Service**

2. GET /get_edge_sso

3. GET /authorise

4. 302 Found  Location: https://ad01.eft.cisco.com/adfs/ls

**CUCM: Auth & Resource**

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

6. 200 OK [Login Form]

7. POST [Credentials]

8. 200 OK + Post[SAML Assertion] +IDP Cookie

**Simplified Call-Flow.**

- More details in previous slides /get_edge_sso and /authorise.

- Detects VCS version.

**Request Authorization - OAUTH**

- Jabber: Browser

- Expressways Service

- CUCM: Auth & Service

- iDP
The Services reuses the Assertion to get an `access_token` for the end user. The Service generates the **SAML Bearer Grant API**.

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

**Simplified Call-Flow**
EDGE SSO - Call Flow Sequence

Once VCS has authorised the user, it caches the oauth token, generates the SIP token – not for unity and gives it to Jabber.

200 OK [access_token]

Jabber Signs (Oauth, Identity)

Simplified Call-Flow
Edge SSO Tokens

• Jabber receives three tokens 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 OAuth Token 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]