Troubleshooting Collaboration Edge Mobile and Remote Access

Philip Smeuninx
Technical Leader Services
Agenda

• Introduction
• Mobile and Remote Access Deployment
• Mobile and Remote Access Troubleshooting and Monitoring
• Mobile and Remote Access Tool - Demo
Cisco Spark

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

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

cs.co/ciscolivebot#BRKCOL-2021
Mobile and Remote Access Deployment
Topology

CUCM

Expressway-C

Expressway-E

Internet

IM&P
Mobile and Remote Access Deployment

- System configuration
- Certificate configuration and deployment
- Traversal zone configuration
- UC server discovery
- DNS and domain configuration/deployment
- MRA Access Control
Mobile and Remote access
System Configuration
System Configuration

• Set Unified Communications mode to ‘Mobile and remote access’ on E and C

Configuration > Unified Communications > Configuration

• Check the Administrator guide for more help on system configuration topics
System Configuration - NTP

• When NTP is not configured and synchronized on ExpressWay-C and ExpressWay-E, Jabber Telephony registration to CUCM may not succeed.

• Security mechanism based on SIP SERVICE messages.
  1. Expressway-E time-stamps a SERVICE message
  2. Expressway-E sends the SERVICE message to Expressway-C
  3. Expressway-C verifies the SERVICE is received within 60 secs error margin
System Configuration - DNS

- Expressway E must have forward and reverse DNS entries.
- Certificate CN validation through DNS reverse lookup.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.113</td>
<td>XMPP/XML</td>
<td>117</td>
<td>STARTTLS</td>
</tr>
<tr>
<td>10.48.55.113</td>
<td>10.48.55.94</td>
<td>XMPP/XML</td>
<td>116</td>
<td>PROCEED</td>
</tr>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.113</td>
<td>TLSv1.2</td>
<td>264</td>
<td>Client Hello</td>
</tr>
<tr>
<td>10.48.55.113</td>
<td>10.48.55.94</td>
<td>TLSv1.2</td>
<td>1700</td>
<td>Server Hello, Certificate, Server Hello Done</td>
</tr>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.107</td>
<td>DNS</td>
<td>85</td>
<td>Standard query 0xca34 PTR 113.55.48.10.in-addr.arpa</td>
</tr>
<tr>
<td>10.48.55.107</td>
<td>10.48.55.94</td>
<td>DNS</td>
<td>119</td>
<td>Standard query response 0xca34 PTR 113.55.48.10.in-addr.arpa</td>
</tr>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.113</td>
<td>TLSv1.2</td>
<td>356</td>
<td>Application Data</td>
</tr>
<tr>
<td>10.48.55.113</td>
<td>10.48.55.94</td>
<td>TLSv1.2</td>
<td>345</td>
<td>Application Data</td>
</tr>
</tbody>
</table>

```ruby
$ rdnSequence: 6 items
  | id-at-commonName=eft-xwye-a.coluc.com,
  | id-at-organizationalUnitName=TAC,
  | RDNSquence item: 1 item (id-at-countryName=BE)
  | RelativeDistinguishedName item (:)
    | Id: 2.5.4.6 (id-at-countryName CountryName: BE)
    | 113.55.48.10.in-addr.arpa: type PTR, class IN, eft-xwye-a.coluc.com
    | Name: 113.55.48.10.in-addr.arpa
    | Type: PTR (domain name PoinTeR) (12)
    | Class: IN (0x0001)
    | Time to live: 3600
    | Data length: 22
    | Domain Name: eft-xwye-a.coluc.com
```
## System Configuration - DNS

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.93</td>
<td>XMMP/XML</td>
<td>117</td>
<td>STARTTLS</td>
</tr>
<tr>
<td>10.48.55.93</td>
<td>10.48.55.94</td>
<td>XMMP/XML</td>
<td>116</td>
<td>PROCEED</td>
</tr>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.93</td>
<td>TLSv1.2</td>
<td>264</td>
<td>Client Hello</td>
</tr>
<tr>
<td>10.48.55.93</td>
<td>10.48.55.94</td>
<td>TLSv1.2</td>
<td>1700</td>
<td>Server Hello, Certificate, Server Hello Done</td>
</tr>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.107</td>
<td>DNS</td>
<td>84</td>
<td>Standard query 0x6382 PTR 93.55.48.10.in-addr.arpa</td>
</tr>
<tr>
<td>10.48.55.107</td>
<td>10.48.55.94</td>
<td>DNS</td>
<td>145</td>
<td>Standard query response 0x6382 No such name PTR 93.55.48.10.in-addr.arpa</td>
</tr>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.93</td>
<td>TLSv1.2</td>
<td>73</td>
<td>Alert (Level: Fatal, Description: Internal Error)</td>
</tr>
<tr>
<td>10.48.55.94</td>
<td>10.48.55.93</td>
<td>XMMP/XML</td>
<td>132</td>
<td>FAILURE</td>
</tr>
</tbody>
</table>

- **rdnSequence: 6 items** (id-at-commonName=eft-xwyee-a.coluc.com, id-at-organizationalUnitName=TAC,)
- **RDNSSequence item: 1 item** (id-at-countryName=BE)
  - RelativeDistinguishedName item (id-at-countryName=BE)
    - Id: 2.5.4.6 (id-at-countryName)
    - CountryName: BE

- **Flags: 0x8583** Standard query response, No such name
  - 1... ..... ..... ..... = Response: Message is a response
  - .000 0... ..... ..... = Opcode: Standard query (0)

---

2018-01-13T13:58:11.102-06:00 hostname XCP_JABBERD[20026]: UTCTime="2018-01-13 13:58:11,102" ThreadID="139882696623872" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:409" Detail="caught exception: exception in reverseDNSLookup: reverse DNS lookup failed for address=x.x.x.x"
Expressway Service Setup

Welcome to Cisco Collaboration services

Select Series
- Expressway series
- VCS series

Select Type
- Expressway-C
- Expressway-E

Select Services
- Cisco Spark Hybrid Services
- Mobile and Remote Access including Meeting Server Web Proxy
- Jabber Guest services
- Microsoft gateway service
- Registrar
- Collaboration Meeting Rooms (CMR) Cloud
- Business to business calls

After you select services, you get a simplified menu that is relevant to your selection.

If you proceed without selecting services, you will get the full menu.

Continue
Expressway Service Setup
Firewall

• What traffic does the firewall need to pass?
  • HTTPS proxy for secure provisioning of endpoints
  • SIP/TLS, RTP/SRTP for audio/video media
  • XCP/XMPP for IM&P
  • HTTPS Services
  • Traversal Connection between ExpressWay-C and E
  • SSH Tunnel: ClusterDB change notifications and HTTPS reverse proxy traffic
Firewall

Cisco Expressway IP Port Usage

Configuration Guide

Cisco Expressway IP Port Usage Configuration Guide

Mobile and Remote Access

MRA Connections
Firewall

- Local Inbound ports
- Local Outbound ports
- Remote listening ports
Expressway E – Demultiplexing media ports

- Small/medium deployment

- Configured Media Demultiplexing ports
  Default: 2776 (RTP) – 2777 (RTCP)
  or

- First 2 ports from Traversal Media port range
  Default: 36000 (RTP) – 36001 (RTCP)
Expressway E – Demultiplexing media ports

- For large systems new install

- First 12 ports from Traversal Media port range
  Default: 36000 (RTP) – 36011 (RTCP)
Mobile and Remote Access Certificates
DX650/70/80 and 88XX/78XX ‘Certificate Authority Trust List’

- Pre-installed CA Trust list
- CA-Trust-List.docx

Technical References

Cisco Unified IP Conference Phone 8831

Cisco Unified IP Conference Phone 8831 Accessibility Features

Accessibility Features for the Cisco IP Phone 8800 Series

Certificate Authority Trust List (DOCX - 366 KB)
TFTP encrypted configuration file

- Jabber, DX, 78XX/88XX Out-of-the-box enrolment over MRA not supported.
- Requires CAPF operation

INFO.. [csf.ecc] [csf::ecc::ConfigRetriever::secureProcessConfigFile] - Full config is encrypted.
ERROR.. [csf.ecc] [csf::ecc::ConfigRetriever::secureProcessConfigFile] Config file is encrypted, but we don't have a local certificate. Device must be put into enrolment mode to fix!
ERROR.. [csf.ecc.api] [csf::ecc::CallControlManagerImpl::doFetchSoftphoneConfig] - doFetchSoftphoneConfig() could not obtain config for CSFEFT2
... ERROR.. [csf.ecc] [csf::ecc::CallControlManagerImpl::doConnect] - doConnect() failed – eCapfEnrolmentRequired
... ERROR..[csf.ecc] [csf::ecc::ConfigRetriever::secureProcessConfigFile] - Need to perform CAPF, but this is not supported via edge
Expressway Certificates

- > Maintenance
- > Security Certificate
- > Server Certificate

Server certificate

Certificate signing request (CSR)

Upload new certificate

Select the server private key file
Select the server certificate file

Upload server certificate data
Expressway Certificates

- Maintenance > Security Certificate > Trusted CA Certificate

### Trusted CA certificate

<table>
<thead>
<tr>
<th>Type</th>
<th>Issuer</th>
<th>Subject</th>
<th>Expiration date</th>
<th>Validity</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>O=CISCO-TS, OU=TAC, CN=CAOS</td>
<td>Matches Issuer</td>
<td>Jan 03 2017</td>
<td>Valid</td>
<td>View (decoded)</td>
</tr>
<tr>
<td>Certificate</td>
<td>O=CISCO, OU=TAC, CN=CAOS</td>
<td>Matches Issuer</td>
<td>Jun 30 2024</td>
<td>Valid</td>
<td>View (decoded)</td>
</tr>
<tr>
<td>Certificate</td>
<td>O=CISCO, OU=TAC, CN=CATAAC</td>
<td>Matches Issuer</td>
<td>Feb 06 2026</td>
<td>Valid</td>
<td>View (decoded)</td>
</tr>
</tbody>
</table>

### Upload

Select the file containing trusted CA certificates

![Browse... No file selected.](image)
Expressway-C Certificate
Where is it used?

- CUCM
- IM&P
- Expressway-C
- Expressway-E
- Clustering
- SIP MTLS

Internet

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Expressway-C Certificate Requirements

Extended Key Usage
1. TLS Web Server Authentication
2. TLS Web Client Authentication

SAN elements configured with:
3. FQDN Expressway C
4. IM and Presence chat node alias
5. Unified CM Security Profile names
6. Cluster Name
Expressway-C Certificate
Additional Requirements

• Must be CA Signed -> Enterprise CA or Public CA

• CA Root which issued the certificate must be appended to “Trusted CA certificate” on both ExpressWay’s

• CA Root must be uploaded to Callmanager-trust store on every node in the cluster
ExpressWay-C Certificate Requirements

Generate CSR

Common name
- FQDN of Expressway: exp-c-1.dcloud.cisco.com

Alternative name
- Subject alternative names: conference-2-StandaloneCluster7545a.dcloud.cisco.com, conf
- Additional alternative names: cisco-secure.dcloud.com
- IM and Presence chat node aliases: conference-2-StandaloneCluster7545a.dcloud.cisco.com

Digest algorithm

Country
- BE

State or province
- BRABANT

Locality (town name)
- DIEGEM

Organization (company name)
- Cisco

Organizational unit
- TAC

Email address
- admin@dcloud.com

Generate CSR
Troubleshooting
CA Root not uploaded on ExpressWay E

• Traversal Zone State Failed

• Expressway-C Diagnostics logs (traversal client)
  .. Event="Outbound TLS Negotiation Error" Service="SIP"
  Src-ip="10.48.55.98" Src-port="25016" Dst-ip="10.48.55.113" Dst-port="7001"
  Detail="tlsv1 alert unknown ca" Protocol="TLS" Common-name="eft-xwyeb.coluc.com" ..

• Expressway-C Event logs

Results
2018-01-26T14:37:51.996+00:00 tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.94" Src-port="25012" Dst-ip="10.48.55.113" Dst-port="7001"
  Detail="tlsv1 alert unknown ca" Protocol="TLS" Common-name="eft-xwyeb.coluc.com" Level="1" UTCTime="2018-01-26 14:37:51.996"
Troubleshooting
Security Profile added as SAN (CUCM trace)

- SIPTcp - Connection Indication - Listen Port = 5061, Peer Port = 25002

SIPTcp - wait_SdlReadRsp: Incoming SIP TCP message from 10.48.55.98 on port 25002 index 10 with 2994 bytes:[53,NET]
REGISTER sip:COLCM9PUB SIP/2.0…

... //SIP/SIPHandler/ccbId=0/scbId=0/wait_SIPCertificateInd: could not find a trunk device using address or x509SubjectName calling findSIPStationInit
/SIP/SIPHandler/ccbId=0/scbId=0/findDeviceByX509Subject: x509Subject:xwayc.coluc.com, port:5061
/SIP/SIPHandler/ccbId=25/scbId=0/findDevicePID: Routed to SIPStationInit

... SIPStationInit: connId=10, CSFEWAYJ, 10.48.55.98:5061, Incoming register request received over TLS. Subject=[/C=BE/ST=BRABANT/L=DIEGEM/O=CISCO/OU=TAC/CN=xwayc.coluc.com]

... SIPStationD(9) - validTLSConnection:TLS InvalidX509NameInCertificate, Rcvd=xwayc.coluc.com, Expected=CSFEWAYJ. Will check SAN the next

... SIPStationD(9) - validTLSConnection: Found matching SAN, SAN Rcvd=xwayc.coluc.com;conference-2-ecup9.coluc.com;csf-secure, Expected=csf-secure
Troubleshooting

Security Profile not added as SAN (CUCM trace)

- SIPTcp - Connection Indication - Listen Port = 5061, Peer Port = 25004

  SIPTcp - wait_SdlReadRsp: Incoming SIP TCP message from 10.48.55.98 on port 25004 index 10 with 2994 bytes:[53,NET]
  REGISTER sip:COLCM9PUB SIP/2.0…
  ...
  //SIP/SIPHandler/ccbId=0/scbId=0/wait_SIPCertificateInd: could not find a trunk device using address or x509SubjectName calling findSIPStationInit
  //SIP/SIPHandler/ccbId=0/scbId=0/findDeviceByX509Subject: x509Subject:xwayc.coluc.com, port:5061
  //SIP/SIPHandler/ccbId=25/scbId=0/findDevicePID: Routed to SIPStationInit
  ...
  SIPStationInit: connId=10, CSFEWAYJ, 10.48.55.98:5061, Incoming register request received over TLS. Subject=/[C=BE/ST=BRABANT/L=DIEGEM/O=CISCO/OU=TAC/CN=xwayc.coluc.com]
  ...
  SIPStationD(3) - validTLSConnection:TLS InvalidX509NameInCertificate, Rcvd=xwayc.coluc.com, Expected=CSFEWAYJ. Will check SAN the next
  ...
  SIPStationD(3) - validTLSConnection:TLS InvalidX509NameInCertificate Error, did not find matching SAN either, Rcvd=xwayc.coluc.com;conference-2-ecup9.coluc.com, Expected=csf-secure
Expressway-E Certificate
Where is it used?
Expressway-E Certificate Requirements

Extended Key Usage
1. TLS Web Server Authentication
2. TLS Web Client Authentication

SAN elements configured with:
3. FQDN Expressway E
4. Public UC Domain
5. IM and Presence chat node alias
6. XMPP Federation Domains
Expressway-E Certificate
Additional Requirements

• Must be CA Signed
• Public CA
• CA Root which issued the certificate must be appended to “Trusted CA certificate” on both ExpressWay’s
ExpressWay-E Certificate Requirements

Expressway E

**Generate CSR**

- **Common name**
  - Common name: FQDN of Expressway
  - Common name as it will appear: ef-exway-a.coltuc.com

- **Alternative name**
  - Additional alternative names (comma separated):
    - coluc.com
    - coluc.com
    - conference-2-ecup9.coltuc.com
  - Alternative name as it will appear:
    - DNS: ef-exway-a.coltuc.com
    - DNS: coluc.com
    - DNS: conference-2-ecup9.coltuc.com

- **Additional information**
  - Key length (in bits): 4096
  - Country: BE
  - State or province: BRABANT
  - Locality (town name): DIEGEM
  - Organization (company name): CISCO
  - Organizational unit: TAC

---

**Expressway C**

**Domains**

- **Configuration**
  - Domain name: coluc.com

- **Supported services for this domain**
  - SIP registrations and provisioning on Unified CM: On
  - IM and Presence services on Unified CM: On
  - XMPP federation: On
Troubleshooting Certificates – Wireshark decode as

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>627</td>
<td>2016-05-27</td>
<td>14:28:11.740416000</td>
<td>10.149.4.185</td>
<td>TCP</td>
<td>5605-1-pcsync-https [SYN] seq=0 Wln=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1</td>
</tr>
<tr>
<td>633</td>
<td>2016-05-27</td>
<td>14:28:11.728520000</td>
<td>10.149.4.185</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>635</td>
<td>2016-05-27</td>
<td>14:28:11.725857000</td>
<td>10.149.4.185</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>636</td>
<td>2016-05-27</td>
<td>14:28:11.765988000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>637</td>
<td>2016-05-27</td>
<td>14:28:11.767369000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>638</td>
<td>2016-05-27</td>
<td>14:28:11.769193000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>639</td>
<td>2016-05-27</td>
<td>14:28:11.769285000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>641</td>
<td>2016-05-27</td>
<td>14:28:11.769832000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>650</td>
<td>2016-05-27</td>
<td>14:28:11.769693000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>652</td>
<td>2016-05-27</td>
<td>14:28:11.731878000</td>
<td>10.149.4.185</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>653</td>
<td>2016-05-27</td>
<td>14:28:11.732850000</td>
<td>10.149.4.185</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>655</td>
<td>2016-05-27</td>
<td>14:28:11.789835000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>656</td>
<td>2016-05-27</td>
<td>14:28:11.789999000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>674</td>
<td>2016-05-27</td>
<td>14:28:11.193087000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>675</td>
<td>2016-05-27</td>
<td>14:28:11.193342000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>676</td>
<td>2016-05-27</td>
<td>14:28:11.193474000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>677</td>
<td>2016-05-27</td>
<td>14:28:11.194229000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>678</td>
<td>2016-05-27</td>
<td>14:28:11.194529000</td>
<td>173.38.114.85</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
<tr>
<td>1801</td>
<td>2018-05-27</td>
<td>14:28:11.207030000</td>
<td>10.149.4.185</td>
<td>TCP</td>
<td>5605-1-pcsync-https [ACK] seq=0 Ack=0 Wln=0 Len=0</td>
</tr>
</tbody>
</table>

Frame 627: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, src: IntelCor_r47c79c6 (24:77:03:7f:ce:6c), dst: ciscoacirc.9f:01:00:00:0c:9f:0f:01
Internet Protocol Version 4, src: 10.149.4.191 (10.149.4.191), dst: 173.38.114.85 (173.38.114.85)
Transmission Control Protocol, src Port: 56079 (56079), dst Port: pscync-https (8443), Seq: 0, Len: 0
Troubleshooting Certificates – Wireshark decode as

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>027</td>
<td>2016-03-27 14:28:11.740610000</td>
<td>10.149.4.191</td>
<td>173.38.154.85</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>026</td>
<td>2016-03-27 14:28:11.724295000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>024</td>
<td>2016-03-27 14:28:11.736735000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>023</td>
<td>2016-03-27 14:28:11.738570000</td>
<td>10.149.4.191</td>
<td>173.38.154.85</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>022</td>
<td>2016-03-27 14:28:11.739999000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>021</td>
<td>2016-03-27 14:28:11.767960000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>020</td>
<td>2016-03-27 14:28:11.768939000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>019</td>
<td>2016-03-27 14:28:11.769462000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>018</td>
<td>2016-03-27 14:28:11.769285000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>017</td>
<td>2016-03-27 14:28:11.769285000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>016</td>
<td>2016-03-27 14:28:11.769462000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>015</td>
<td>2016-03-27 14:28:11.769285000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>014</td>
<td>2016-03-27 14:28:11.769285000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
<tr>
<td>013</td>
<td>2016-03-27 14:28:11.769285000</td>
<td>173.38.154.85</td>
<td>10.149.4.191</td>
<td>TCP</td>
<td>56075-pcsync-httpss</td>
</tr>
</tbody>
</table>

Wireshark Decode As

- Decode
- Do not decode

TCP [both (56075=8443)] port 8443
- STANAG 5066 37
- STANAG 5066 37
Troubleshooting Certificates – Wireshark

TLS Handshake failure

- Client Hello
- Server Hello, Server Certificate
- Client Certificate
- Server does not trust CA that signed client certificate
Troubleshooting Certificates – Wireshark Certificate Export
Troubleshooting Certificates – Wireshark Certificate Export

![Wireshark Export Raw Data](image)

- **Certificate Information**
  - **Issued for:** VeriSign Class 3 Public Primary Certification Authority - GS
  - **Issued by:** Class 3 Public Primary Certification Authority
  - **Valid from:** 8/1/2016 to 8/1/2021

Learn more about certificates.

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Mobile and Remote Access
Unified Communications Traversal Zone
Unified Communications Traversal Zone

- Expressway-E is traversal server in DMZ
- Expressway-C is traversal client inside the network
- Establish traversal link between both using traversal zone configuration
UC Traversal Zone
ExpressWay E – Traversal Server

Select Type: Unified Communications traversal

Configure username to be used by Traversal Client to authenticate with server

Port is default 7001, listening port for traversal client connection

Must match CN or SAN from Certificate presented by Traversal Client (ExpressWay C), here clustername

Advanced Encryption Cipher for encrypting/decrypting SRTP media
- Jabber 11.9 with EnableNGEPolicy
- 7800 and 8800 Series do not support over MRA
UC Traversal Zone
ExpressWay E – Traversal Server

- Traversal Zone Status
- Connection status with Traversal Client
UC Traversal Zone
ExpressWay C – Traversal Client

Select ‘Unified Communications Traversal’ as Type

Configure same username and password as added on the Traversal Server (Expressway E)

Destination port Traversal Server is listening on

Advanced Encryption Cipher for encrypting/decrypting SRTP media
- Jabber 11.9 with EnableNGEPolicy
- 7800 and 8800 Series do not support over MRA
UC Traversal Zone
ExpressWay C – Traversal Client

Must resolve to Public IP address Expressway E when single NIC deployment

- Must be FQDN (*)
- Must match CN or SAN from Certificate presented by Expressway E
UC Traversal Zone
ExpressWay C – Traversal Client

Peer Connectivity Status

Zone Status
UC Traversal Zone
ExpressWay – SSH Tunnel

• SSH Tunnel – From Status > Unified Communications

---

**Unified Communications SSH tunnels status**

<table>
<thead>
<tr>
<th>Target</th>
<th>Domain</th>
<th>Status</th>
<th>Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>eft-xwy-e.coluc.com</td>
<td>coluc.com</td>
<td>Active</td>
<td>eft-xwyc-b.coluc.com</td>
</tr>
<tr>
<td>eft-xwy-a.coluc.com</td>
<td>coluc.com</td>
<td>Active</td>
<td>eft-xwyc-a.coluc.com</td>
</tr>
<tr>
<td>eft-xwy-e.coluc.com</td>
<td>coluc.com</td>
<td>Active</td>
<td>eft-xwyc-b.coluc.com</td>
</tr>
<tr>
<td>eft-xwy-a.coluc.com</td>
<td>coluc.com</td>
<td>Active</td>
<td>eft-xwyc-a.coluc.com</td>
</tr>
</tbody>
</table>
Troubleshooting
Peer Address not matching CN

• Peer Address configured as IP address

<table>
<thead>
<tr>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer 1 address</td>
</tr>
<tr>
<td>Peer 2 address</td>
</tr>
</tbody>
</table>

• ExpressWay C diagnostic logs
  .. tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25697" Dst-ip="10.48.55.113" Dst-port="7001" Detail= "Peer’s TLS certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.55.113" Level="1" ..

• ExpressWay C Event logs

Troubleshooting
Peer Address not matching CN

- Peer Address/FQDN not matching CN

Secure traversal test
FQDN of Expressway-E: expe.external.com
TLS verify name of this Expressway-C (as it appears on the Expressway-E): eft-xwyc.coluc.com

Results
Description: The Expressway-E name 'expe.external.com' did not match any CN or SAN attributes in its certificate: 'eft-xwye.external.com, collab-edge.external.com, eft-xwye-a.external.com'
Action: Check that what you entered matches a valid CN or SAN identity in the Expressway-E's certificate. We recommend using the FQDN format. We discourage the use of hostname or IP address formats on public interfaces.
Troubleshooting
Password incorrect

• Traversal Client will show for this zone

<table>
<thead>
<tr>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer 1 address</td>
</tr>
<tr>
<td>Peer 2 address</td>
</tr>
</tbody>
</table>

• ExpressWay C diagnostic logs

Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="xwaye.coluc.com"
Type="A and AAAA"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to: ['IPv4"TCP"10.48.55.99']
(A/AAAA) Number of relevant records retrieved: 1"
Module="network.tcp" Level="DEBUG": Src-ip="10.48.55.98" Src-port="25723" Dst-ip="10.48.55.99"
Dst-port="7001" Detail="TCP Connecting"
Module="network.tcp" Level="DEBUG": Src-ip="10.48.55.98" Src-port="25723" Dst-ip="10.48.55.99"
Dst-port="7001" Detail="TCP Connection Established"
Password incorrect (contd.)

- ExpressWay C diagnostics logs

```
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="10.48.55.98" Local-port="25723" Dst-ip="10.48.55.99" Dst-port="7001"
SIPMSG:
|OPTIONS sip:10.48.55.99:7001;transport=tls SIP/2.0
....
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="10.48.55.98" Local-port="25723" Src-ip="10.48.55.99" Src-port="7001"
SIPMSG:
|SIP/2.0 401 Unauthorised
...
WWW-Authenticate: Digest realm="TraversalZone", nonce="527e7f2a24ff1c54e3e4cd5025f674967e81d2aa9b214fda98cef27f3f82", opaque="AQAAAPet....
....
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="10.48.55.98" Local-port="25723" Dst-ip="10.48.55.99" Dst-port="7001"
SIPMSG:
|OPTIONS sip:10.48.55.99:7001;transport=tls SIP/2.0
....
Authorization: Digest nonce="527e7f2a24ff1c54e3e4cd5025f674967e81d2aa9b214fda98cef27f3f82", realm="TraversalZone", opaque="AQAAAPet+0JJTq4cyuB34opHePwV7bkk", algorithm=MD5, uri="sip:10.48.55.99:7001;transport=tls", username="xway", response="...
....
Module="network.sip" Level="DEBUG": Action="Received"
SIPMSG:
|SIP/2.0 401 Unauthorised
....
Event="External Server Communications Failure" Reason="gatekeeper timed out" Service="NeighbourGatekeeper" Dst-ip="10.48.55.99" Dst-port="7001" Detail="name:xwayne.coluc.com" Protocol="TCP" Level="1"
```
Troubleshooting
Password incorrect

• ExpressWay E diagnostic logs

Module="network.ldap" Level="INFO": Detail="Authentication credential found in directory for identity: xway"

... Module="developer.nomodule" Level="WARN" CodeLocation="ppcmain/sip/sipproxy/SipProxyAuthentication.cpp(686)"
Method="SipProxyAuthentication::checkDigestSAResponse" Thread="0x7f2485cb0700":
calculated response does not match supplied response,
calculatedResponse=769c8f488f71ebdf28b61ab1dc9f5e9,
response=319a0bb365decf98c1bb7b3ce350f6ec

... Event="Authentication Failed" Service="SIP" Src-ip="10.48.55.98" Src-port="25723"
Detail="Incorrect authentication credential for user" Protocol="TLS" Method="OPTIONS" Level="1"
Mobile and Remote Access
UC Server Discovery
# UC Server Discovery

## Unified Communications

You are here: Configuration > Unified Communications > Configuration

### Configuration

**Unified Communications mode**

- **Mobile and remote access**

### Single Sign-On

**Single Sign-On support**

- **Off**
  - Configure identity providers (IdP)
  - Export SAML data

### IM and Presence Service nodes, Unified CM servers and Unity Connection servers

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence Service nodes</td>
<td>1</td>
</tr>
<tr>
<td>Unified CM servers</td>
<td>0</td>
</tr>
<tr>
<td>Unity Connection servers</td>
<td>0</td>
</tr>
</tbody>
</table>

---

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
CUCM Server Discovery

- Discovers hostname (processnodetable)
- Discovers version
- Discovers Cluster Security mode (Transport Protocols)
## CUCM Server Discovery – TLS verify mode

### TLS verify mode = On

<table>
<thead>
<tr>
<th>Unified CM server lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified CM publisher address</strong></td>
</tr>
<tr>
<td><strong>Username</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>TLS verify mode</strong></td>
</tr>
<tr>
<td><strong>AES GCM support</strong></td>
</tr>
</tbody>
</table>

### Certificate Settings

- **Locally Uploaded**: 03/07/14
- **File Name**: tomcat.pem
- **Certificate Purpose**: tomcat
- **Certificate Type**: certs
- **Certificate Group**: product-cpi
- **Description (friendly name)**: Certificate Signed by CAOS

### Certificate File Data

```json
{
  "Version": "V3",
  "Serial Number": 74,
  "Signature Algorithm": "SHA1withRSA (1.2.840.113549.1.1.5)"
}
```

- **Issuer Name**: EMAILADDRESS=CAOS@CAOS.COM, CN=CAOS, OU=TAC, O=CISCO, L=Diegem, ST=Brabant, C=BE
- **Validity From**: Thu Jul 03 15:23:49 CEST 2014
- **Validity To**: Sun Jun 30 15:23:49 CEST 2024
- **Subject Name**: CN=CUCM10P.coluc.com, OU=tac, O=cisco, L=Diegem, ST=Brabant, C=BE

**Publisher address = FQDN, MUST match CN TOMCAT Certificate Publisher (*)**
### CUCM Server Discovery – TLS verify mode

**TLS verify mode = On**

<table>
<thead>
<tr>
<th>Unified CM server lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified CM publisher address</strong></td>
</tr>
<tr>
<td><strong>Username</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>TLS verify mode</strong></td>
</tr>
<tr>
<td><strong>AES GCM support</strong></td>
</tr>
</tbody>
</table>

**Certification Settings**

<table>
<thead>
<tr>
<th>Locally Uploaded</th>
<th>03/07/14</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Name</strong></td>
<td>tomcat.pem</td>
</tr>
<tr>
<td><strong>Certificate Purpose</strong></td>
<td>tomcat</td>
</tr>
<tr>
<td><strong>Certificate Type</strong></td>
<td>certs</td>
</tr>
<tr>
<td><strong>Certificate Group</strong></td>
<td>product-cpi</td>
</tr>
<tr>
<td><strong>Description</strong> (friendly name)</td>
<td>Certificate Signed by CAOS</td>
</tr>
</tbody>
</table>

**Certificate File Data**

```json
[
  {
    "Extension": "SubjectAltName (OID.2.5.29.17)"
  },
  {
    "Critical": false,
    "altNames": 2 names,
    "1): coluc.com (dNSName)"
  },
  {
    "2): CUCM10P.coluc.com (dNSName)"
  }
]
```

**Publisher address = FQDN MUST match SAN TOMCAT Certificate Publisher**

(*) Only valid statement RFC 6125
CUCM Server Discovery – TLS verify mode

TLS verify mode = On

CA Certificate must be uploaded
‘Trusted CA certificate’ list Expressway C
CUCM Server Discovery – TLS verify mode

TLS verify mode = Off

No requirements for TOMCAT Certificate Publisher
CUCM Server Discovery – Zone Configuration

• Auto-Zone Configuration per node and per transport protocol
• Syntax: ‘CEtcp-<UCMName>’ and ‘CEtls-<UCMName>’
# CUCM Server Discovery – Zone Configuration

<table>
<thead>
<tr>
<th>Publisher address</th>
<th>Username</th>
<th>TLS verify mode</th>
<th>Nodes discovered by this lookup</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUCM10P.coluc.com</td>
<td>ccmadmin</td>
<td>On</td>
<td>cucm10s1.coluc.com, cucm10p.coluc.com</td>
<td>View/Edit</td>
</tr>
</tbody>
</table>

**TLS verify mode = On**

- ‘TLS verify mode’ Discovery
- ‘TLS verify mode’ Zone
CUCM Server Discovery – Zone Configuration

- **TLS verify mode = On**

- ‘CEtlS-<UCMName>’ Zone:
  - TLS Verify mode = On
  - Peer Address must match CN or SAN from Callmanager certificate
CUCM Server Discovery – Zone Configuration

- CA or Expressway C certificate must be uploaded to Callmanager-trust store
- Verifies SIP TLS during discovery

The Unified CM cannot verify the CA 'CATAc', which signed the Expressway-C's certificate: Check that this CA is listed as a CallManager-trust in the Unified CM's truststore.

Unified CM server lookup

Unified CM publisher address: CUCM10P.coluc.com

Username: ccmadmin
Password: ********

TLS verify mode = On

AES GCM support: On

TLS verify mode = On
CUCM Server Discovery – Zone Configuration

<table>
<thead>
<tr>
<th>Publisher address</th>
<th>Username</th>
<th>TLS verify mode</th>
<th>Nodes discovered by this lookup</th>
<th>AES GCM support</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUCM10P.coluc.com</td>
<td>ccmadmin</td>
<td>Off</td>
<td>10.48.79.105, 10.48.55.100</td>
<td>On</td>
<td>View/Edit</td>
</tr>
</tbody>
</table>

- TLS verify mode = Off
- ‘TLS verify mode’ configuration Discovery
- ‘TLS verify mode’ configuration Zone
CUCM Server Discovery – Zone Configuration

<table>
<thead>
<tr>
<th>Publisher address</th>
<th>Username</th>
<th>TLS verify mode</th>
<th>Nodes discovered by this lookup</th>
<th>AES GCM support</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>cucm10p.coluc.com</td>
<td>ccmadmin</td>
<td>On</td>
<td>10.48.79.105, 10.48.55.100</td>
<td>On</td>
<td>View/Edit</td>
</tr>
</tbody>
</table>

- ‘AES GCM’ configuration Discovery
- ‘AES GCM’ configuration Zone
CUCM Server Discovery – Search Rule Configuration

- 1 Search Rule per node per transport protocol
- Pattern matching for header

<table>
<thead>
<tr>
<th>Priority</th>
<th>Rule name</th>
<th>Protocol</th>
<th>Source</th>
<th>Authentication required</th>
<th>Mode</th>
<th>Pattern type</th>
<th>Pattern string</th>
<th>Pattern behavior</th>
<th>On match</th>
<th>Target</th>
<th>State</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>CEscp-cucm10p.coluc.com</td>
<td>SIP</td>
<td>Any</td>
<td>No</td>
<td>Alias pattern match</td>
<td>Prefix</td>
<td>cucm10p.coluc.com;transport=TCP</td>
<td>Leave</td>
<td>Stop</td>
<td>Enabled</td>
<td>View</td>
<td>Clone</td>
</tr>
<tr>
<td>45</td>
<td>CEscp-cucm10s1.coluc.com</td>
<td>SIP</td>
<td>Any</td>
<td>No</td>
<td>Alias pattern match</td>
<td>Prefix</td>
<td>cucm10s1.coluc.com;transport=TCP</td>
<td>Leave</td>
<td>Stop</td>
<td>Enabled</td>
<td>View</td>
<td>Clone</td>
</tr>
<tr>
<td>45</td>
<td>CEls-cucm10p.coluc.com</td>
<td>SIP</td>
<td>Any</td>
<td>No</td>
<td>Alias pattern match</td>
<td>Prefix</td>
<td>cucm10p.coluc.com;transport=TLS</td>
<td>Leave</td>
<td>Stop</td>
<td>Enabled</td>
<td>View</td>
<td>Clone</td>
</tr>
<tr>
<td>45</td>
<td>CEls-cucm10s1.coluc.com</td>
<td>SIP</td>
<td>Any</td>
<td>No</td>
<td>Alias pattern match</td>
<td>Prefix</td>
<td>cucm10s1.coluc.com;transport=TLS</td>
<td>Leave</td>
<td>Stop</td>
<td>Enabled</td>
<td>View</td>
<td>Clone</td>
</tr>
</tbody>
</table>
Troubleshooting - Search Rule matching for Edge/MRA calls

```
INVITE sip:2000@cucm10p.coluc.com;user=phone SIP/2.0
Via: SIP/2.0/TLS 10.48.55.93:7001;egress-zone=TraversalUC;branch=…
Via: SIP/2.0/TLS 10.48.55.106:52008;branch=z9hG4bK000073dc;received=10.48.55.106;ingress-zone=CollaborationEdgeZone
Call-ID: 0050568a-003a0004-0000592c-00003095@10.48.55.106
CSeq: 101 INVITE
Remote-Party-ID: "5445" <sip:5445@cucm10p.coluc.com>-party=calling:id-type=subscriber;privacy=off;screen=yes
Contact: <sip:1622b86e-bc3b-fa8c-66d3-2d7a96c892bf@10.48.55.106;transport=tls;video;bfcp
From: "5445" <sip:5445@cucm10p.coluc.com>;tag=0050568a003a000800006fdd-00006fed;
To: <sip:2000@cucm10p.coluc.com>
Max-Forwards: 10
```

Set by client based on:
- Device Pool
- Device Security mode

![Table of search rules](image)

You are here: Configuration > Dial plan > Search rules
Troubleshooting - Self Signed Certificates

• TLS verify + Self Signed CCM/Tomcat certificate
  
  When Tomcat cert is uploaded first -> discovery will succeed
  When CCM cert is uploaded first -> discovery will fail

• TLS verify + Self Signed CCM/Tomcat certificate + Encryption
  
  Either discovery will fail or TLS connections with CUCM will fail

With self-signed certificates use ‘TLS verify mode’ = ‘Off’
Mobile and Remote Access
DNS and Domain
Domain Configuration
DNS Configuration

• System > DNS
Domain Configuration
ExpressWay C – Domain Configuration

• Configurations > Domains
Mobile and Remote Access
Dual Domain Deployment

• Dual Domain
  - Mixed domain structure
  - Expressway servers : domain2.com
  - UC and CUP servers : domain1.com
  - IM&P domain : domain1.com (internal)
Question: How do I login?

Answer:
- With `<userid>@domain1.com` (*)
- ‘voicesservicesdomain’ set to domain2.com
Question: How is my external DNS configured?

Answer:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Resolves to</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV record '_collab-edge._tls.domain2.com'</td>
<td>xwayE.domain2.com port 8443</td>
</tr>
<tr>
<td>A record 'xwayE.domain2.com'</td>
<td>External IP address ExpressWay E</td>
</tr>
</tbody>
</table>

Mobile and Remote Access Dual Domain Deployment
Question: How is my ExpressWay E configured?
Answer:
> System > DNS >
- System host name ‘xwayE’
- Domain name ‘domain2.com’
VoiceservicesDomain is embedded as UCM Registration

Expressway E

HTTPMSG:

|GET https://ZG9tYWluMi5jb20=|get_edge_config?service_name=_cisco-uds&service_name=_cuplogin HTTP/1.1
Host: eft-xwye-b.external.com:8443
Authorization: xxxxx
Accept: */*
User-Agent: Jabber-Win-462

Decodes to domain2.com
Question: How is my ExpressWay C configured?

Answer:

> System > DNS >
  - System host name ‘xwayC’
  - Domain name ‘domain2.com’

> Configuration > Domains >
  - Domain ‘domain1.com’ enabled for ‘UCM registrations’ and ‘IM and Presence’
  - Domain ‘domain2.com’ enabled for ‘UCM registrations’ and ‘IM and Presence’
**Mobile and Remote Access**
**Dual Domain Deployment**

Question: How is my Internal DNS configured?

Answer:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Resolves to</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV record '_cisco-uds._tcp.domain2.com'</td>
<td>cucm.domain1.com port 8443</td>
</tr>
<tr>
<td>A record 'cucm.domain1.com'</td>
<td>IP address CUCM</td>
</tr>
</tbody>
</table>
Question: How is my CUCM configured?
Answer:
> CCMADMIN > System > Server
  - Server with hostname ‘cucm’
> CLI ‘set network domain ‘domain1.com’
Question: How is my CUP configured?
Answer:
> CUPAdmin > Clustertopology
  - Node configuration with ‘cup.domain1.com’
  - IM and Presence Domain with ‘domain1.com’
Mobile and Remote Access Dual Domain Deployment

Expressway E certificate with SAN ‘domain2.com’ or ‘collab-edge.domain2.com’

[cifar::http::CurlHttpUtils::configureEasyRequest] - ---- Configuring request #2 GET https://xwaye.domain2:8443/ZG9tYWluMi5jb20=/get_edge_config...
[cifar::cert::BaseCertVerifier::checkIdentity] - About to check for an Identity Match.
[cifar::cert::CertVerifier::checkIdentity] - Verifying identity 'xwaye.domain2.com'
[cifar::cert::utils::AltNameParserImpl::verify] - Match for 'xwaye.domain2.com' found in dnsNames index: 0
[cifar::cert::BaseCertVerifier::checkIdentifiers] - Verification of identity succeeded. Matched identifier : 'xwaye.domain2.com'
[cifar::cert::CertVerifier::checkIdentity] - Verifying identity 'domain2.com'
[cifar::cert::utils::AltNameParserImpl::verify] - No Match Found for 'domain2.com'
[cifar::cert::CertVerifier::checkIdentity] - Verifying identity 'collab-edge.domain2.com'
[cifar::cert::utils::AltNameParserImpl::verify] - Match for 'collab-edge.domain2.com' found in dnsNames index: 2
[cifar::cert::BaseCertVerifier::checkIdentifiers] - Verification of identity succeeded. Matched identifier : 'collab-edge.domain2.com'
Mobile and Remote Access
Dual Domain Deployment

Expressway E certificate without SAN 'domain2.com' or 'collab-edge.domain2.com'

[csf.httpclient] [csf::http:CurlHttpUtils::configureEasyRequest] - "-----" Configuring request #2 GET https://xwaye.domain2.com:8443/ZG9tYWluMi5jb20=/get_edge_config?
[csf.cert] [csf::cert::BaseCertVerifier::checkIdentity] - About to check for an Identity Match.
[csf.cert] [csf::cert::CertVerifier::checkIdentity] - Verifying identity 'xwaye.domain2.com'
[csf.cert.util] [csf::cert::AltNameParserImpl::verify] - Match for 'xwaye.domain2.com' found in dnsNames index: 0
[csf.cert] [csf::cert::BaseCertVerifier::checkIdentifiers] - Verification of identity succeeded. Matched identifier : 'xwaye.domain2.com'
[csf.cert] [csf::cert::CertVerifier::checkIdentity] - Verifying identity 'domain2.com'
[csf.cert.util] [csf::cert::AltNameParserImpl::verify] - No Match Found for 'domain2.com'
[csf.cert] [csf::cert::CertVerifier::checkIdentity] - Verifying identity 'collab-edge.domain2.com'
[csf.cert.util] [csf::cert::AltNameParserImpl::verify] - No Match Found for 'collab-edge.domain2.com'
[csf.cert] [csf::cert::BaseCertVerifier::checkIdentifiers] - Verification of identity: 'domain2.com' 'collab-edge.domain2.com' failed.

Prompt user
XMPP Identity based on DN-ID

[csf.cert] [csf::cert::BaseCertVerifier::checkIdentity] - About to check for an Identity Match.
[csf.cert.xmpp] [csf::cert::XmppCertVerifier::checkIdentifier] - 
Verifying XMPP identity 'domain1.com'
[csf.cert.xmpp] [csf::cert::XmppCertVerifier::checkIdentifier] - 
Verifying XMPP identity 'xwaye.domain2.com'
[csf.cert.xmpp] [csf::cert::XmppCertVerifier::checkIdentifier] - 
Xmpp match was not found for: 'domain1.com'
[csf.cert.xmpp] [csf::cert::XmppCertVerifier::checkIdentifier] - 
No Match Found for 'domain1.com'
[csf.cert.xmpp] [csf::cert::XmppCertVerifier::checkIdentifier] - 
Match for 'xwaye.domain2.com' found in dnsNames index: 0
[csf.cert.] [csf::cert::BaseCertVerifier::checkIdentifiers] - Verification of identity succeeded. Matched identifier : 'xwaye.domain2.com'
Domain Considerations

- Expressway E domain = cookie domain in HTTP responds

Target URL Jabber must match or be a subdomain of the cookie domain returned by HTTP server (Expressway E)

Examples

https://expresswaye.cisco.com:8443/Y29sdWMuY29t/get_edge_config
-> Cookie domain : cisco.com

https://expresswaye.edge.cisco.com:8443/Y29sdWMuY29t/get_edge_config
-> Cookie domain : cisco.com

https://expresswaye.cisco.com:8443/Y29sdWMuY29t/get_edge_config
-> Cookie domain : ms.com
## Certificate Consideration – Multi Tenant Support

### Server Name Identification (SNI)

### Without SNI Support

<table>
<thead>
<tr>
<th>Service Domain</th>
<th>IP Phone (78/88XX)</th>
<th>Phone 1</th>
<th>Phone 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>User enters “Domain” in login window</td>
<td>‘dcloud.com’</td>
<td>‘cisco.com’</td>
<td></td>
</tr>
<tr>
<td>DNS Domain Check</td>
<td>Service domain and DNS SRV hostname must have at lease same root domain</td>
<td>SRV A ‘exp.dcloud.com’</td>
<td>SRV A ‘exp.dcloud.com’</td>
</tr>
<tr>
<td>DNS Check or Certificate Service Identification fails?</td>
<td>Reject connection</td>
<td>Connect</td>
<td>Reject Connection</td>
</tr>
</tbody>
</table>
Certificate Consideration – Multi Tenant Support
Server Name Identification (SNI)

With SNI Support

<table>
<thead>
<tr>
<th>Service Domain</th>
<th>User enters “Domain” in login window</th>
<th>'dcloud.com'</th>
<th>'cisco.com'</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Domain Check</td>
<td>Service domain and DNS SRV hostname may have different root domain</td>
<td>SRV A ‘exp.dcloud.com’</td>
<td>SRV A ‘exp.dcloud.com’</td>
</tr>
<tr>
<td>Certificate Service Identification fails?</td>
<td>Reject connection</td>
<td>Connect</td>
<td>Connect</td>
</tr>
</tbody>
</table>

- Phone builds TLS Client Hello with SNI Field = <Host SRV A record + Service Domain> = ‘exp.cisco.com’
- Expressway returns ‘exp.cisco.com’ Domain Certificate

Expressway X8.10
Phone 12.0(1)

Current only HCS
Access Control
Access Control

• “Authorize by user credentials” – Default
• “Authorize by OAuth token” – SSO/Idp
• “Authorize by OAuth token with refresh” – Recommended Deployment
Login Scenario 1
“Authorize by user credentials”

Expressway-C > Configuration > Unified Communications > Configuration

MRA Access Control

- Authentication path: UCM/LDAP basic authentication
- Authorize by OAuth token with refresh: Off
- Authorize by user credential: On
Login Scenario 1
“Authorize by user credentials”

GET https://ZGNsb3VkLmNpc2NvLmNvbQ/get_edge_sso

200 OK

<?xml version='1.0' encoding='UTF-8'?><SSOResult version="1.0"><Response><SingleSignOn><Status enabled="false"/><Token reuse="false"/></SingleSignOn></Response></SSOResult>
Login Scenario 1  
“Authorize by user credentials”

![Diagram showing Jabber Client, Expressway E, Expressway C, CUCM Home UDS, and IM&P Server]
Login Scenario 1
“Authorize by user credentials”

GET https://ZGNsb3VkLmNpc2NvLmNvbQ/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin
Host: exp-e-1.dcloud.cisco.com:8443
Authorization:<CONCEALED>
Accept: */*
User-Agent: Jabber-Win-30

GET //ucm-sub1.dcloud.cisco.com:8443/cucm-uds/user/cholland/devices
Authorization: <CONCEALED>
HTTP/1.1 200 OK
Strict-Transport-Security: ['max-age=31536000; includeSubdomains']
Set-Cookie: <CONCEALED>

Detail="Authenticated user successfully"
Login Scenario 1
“Authorize by user credentials”

REGISTER sip:ucm-sub1.dcloud.cisco.com SIP/2.0

SIP/2.0 407 Proxy Authentication Required

REGISTER sip:ucm-sub1.dcloud.cisco.com SIP/2.0

Proxy-Authentication: Digest username="cholland", realm="exp-e-1.dcloud.cisco.com",
url="sip:ucm-sub1.dcloud.cisco.com", response="415001bc54092b7c6a8a7d9d54cac89a" …

SERVICE sip:serviceserver@ucm-sub1.dcloud.cisco.com

<?xml version="1.0" encoding="utf-8"?> <methodCall><params><username>cholland</username><realm>..</params>

Detail="Calculated response matches supplied response"

SIP/2.0 200 OK
Login Scenario 2
“Authorize by OAuth token with refresh”

<table>
<thead>
<tr>
<th>Device</th>
<th>Minimum Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expressway</td>
<td>X8.10.1</td>
</tr>
<tr>
<td>UCM</td>
<td>11.5(1)SU3 or 12.0(1)</td>
</tr>
<tr>
<td>IMP</td>
<td>11.5(1)SU3 or 12.0(1)</td>
</tr>
<tr>
<td>Unity</td>
<td>11.5(1)SU3 or 12.0(1)</td>
</tr>
<tr>
<td>Jabber client</td>
<td>11.9(0)</td>
</tr>
</tbody>
</table>
Login Scenario 2
“Authorize by OAuth token with refresh”

Expressway-C > Configuration > Unified Communications > Configuration

MRA Access Control

- Authentication path
- Authorize by OAuth token with refresh
- Authorize by user credential
- Allow Jabber iOS clients to use embedded Safari browser
- Check for internal authentication availability

UCM/LDAP basic authentication
On
No
Yes
Login Scenario 2
“Authorize by OAuth token with refresh”

CUCM/IM&P Administration > System > Enterprise Parameters

<table>
<thead>
<tr>
<th>SSO and OAuth Configuration</th>
<th>Value 1</th>
<th>Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAuth Token Expiry Timer (minutes) *</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>OAuth Refresh Token Expiry Timer (days) *</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Redirect URIs for Third Party SSO Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO Login Behavior for iOS *</td>
<td>Use embedded browser (WebView)</td>
<td>Use embedded browser (WebView)</td>
</tr>
<tr>
<td>OAuth with Refresh Login Flow *</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use SSO for RTMT *</td>
<td>False</td>
<td>True</td>
</tr>
</tbody>
</table>

![Diagram showing Jabber Client, Expressway E, Expressway C, CUCM Home UDS, IM&P Server]
Login Scenario 2
“Authorize by OAuth token with refresh”

GET `https://ZGNsb3VkLmNpc2NvLmNvbQ/get_edge_sso`

200 OK

GET `//ucm-pub.dcloud.cisco.com:8443/ssosp/ws/public/singleSignOn`

200 OK

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SSOResult version="1.0">
  <Response>
    <SingleSignOn version="11.5.1.13902-2">
      <Status enabled="false"/>
      <Token reuse="true"/>
      <Uri>https://ucm-pub.dcloud.cisco.com:8443/ssosp/oauth/authorize</Uri>
      <allowEmbeddedSafari>false</allowEmbeddedSafari>
    </SingleSignOn>
  </Response>
</SSOResult>
```
Login Scenario 2
“Authorize by OAuth token with refresh”
Login Scenario 2
“Authorize by OAuth token with refresh”

POST https://ZGNsb3VkLmNpc2NvLmNvbQ/localauthentication

302 FOUND

GET https://oauthcb

200 OK

POST //ucm-pub.dcloud.cisco.com:8443/ssosp/token/authorize_proxy

200 OK

{"redirect_uri":"https://ucm-pub:8443/ssosp/public/oauthcb#code=<CONCEALED>&expires_in=300&realm=local&state=1807704808"}
Login Scenario 2
“Authorize by OAuth token with refresh”

POST https:///ZGNsb3VkLmNpc2NvLmNvbQ/access_token

POST //ucm-pub.dcloud.cisco.com:8443/ssosp/token/access_token

200 OK

{ "expires_in":300,
"token_type":"Bearer",
"refresh_token":"eyJhbGci...9qkn8hHhQUA",
"refresh_token_expires_in":86400,
"access_token":"eyJhbGciOiJSUzI1NiIsInR5c...ajRyLaxWSEQ" }

200 OK
Login Scenario 2
“Authorize by OAuth token with refresh”

GET https:///ZGNsb3VkLmNpc2NvLmNvbQ/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin
Host: exp-e-1.dcloud.cisco.com:8443
Authorization:<CONCEALED>
Accept: */*
User-Agent: Jabber-Win-30

Access Token Validated by Expressway-C
Login Scenario 2
“Authorize by OAuth token with refresh”

Access Token Validation by Expressway-C

Detail="Process request" Method="POST" URI="/oauthvalidator"
Detail="Inspecting Access Token"
**Detail="Matched AuthZ key" Issuer="ucm-pub.dcloud.cisco.com"**
Detail="Validating Access Token payload"
Detail="Access Token OK" Subject="cholland" Expiry="1516799325" Scope="[u'im & presence'; u'voice'; u'video']"
Issuer="ucm-pub.dcloud.cisco.com" Issuertype="cucm" Deployment="1"
Detail="Token validation successful"
Login Scenario 2
“Authorize by OAuth token with refresh”

REGISTER sip:ucm-sub1.dcloud.cisco.com SIP/2.0

SIP/2.0 407 Proxy Authentication Required

REGISTER sip:ucm-sub1.dcloud.cisco.com SIP/2.0

Proxy-Authorization: Bearer token="eyJhbGciOiJSUzI1NiIsInR5c... ajRyLaxWSEQ"

Access Token Validated by Expressway-C
Dropped in subsequent SIP Messages
“Authorize by OAuth token with refresh”
Recommended Deployment

• Token Refresh
• Fast Login
• Off-Line Login
• Access Policy Support
• Roaming Support
“Authorize by OAuth token with refresh”
Refresh CUCM & IM&P Registration

...Action="Received" Request-url="https://ucm-pub.dcloud.cisco.com:8443/ssosp/token/access_token"

HTTPMSG:
| HTTP/1.1 200 OK |
| "expires_in":3600, |
| "token_type":"Bearer", |
| "refresh_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzdXBhYmFzZSIsImllbWJlbnRzIjoiYWJvdXQifQ", |
| "refresh_token_expires_in":5184000, |
| "access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzdXBhYmFzZSIsImllbWJlbnRzIjoiYWJvdXQifQ", |

...Detail="Token Validation failed" Type="Access Token" Response="401"
...Detail="Validation failed" Error="No key available to validate." Status="401" Type="Access Token" …
"Authorize by OAuth token with refresh"
Refresh CUCM & IM&P Registration

...Action="Send" Method="GET" URL="https://ucm-pub.dcloud.cisco.com:8443/ssosp/token/keys" Function="token/keys"

...Action="Received" URL="https://ucm-pub.dcloud.cisco.com:8443/ssosp/token/keys" Function="token/keys" Status="200" Content="

{ "keys": [ 
{ "purpose":"Verify",
"id":"f827...bc1",
"value":"MIIBIjANBg...
pqwIDAQAB"},
{ "purpose":"Decrypt",
"id":"f827...6a4",
"value":"nqJm...6dU="}]
}"

Jabber Client  Expressway E  Expressway C  CUCM Home UDS  IM&P Server
“Authorize by OAuth token with refresh”

- CUCM/IM&P
  - Enable OAuth Service - Enterprise Parameters
- Unity
  - Add AuthZ Servers (= CUCM)
  - Enable OAuth Service - Enterprise Parameters
- Expressway – Add/Synch CUCM Servers
“Authorize by OAuth token with refresh”
Check for internal authentication availability disabled
“Authorize by OAuth token with refresh”
Check for internal authentication availability disabled

Authentication fails

From Client
HTTPMSG:
|POST https:///ZGNsb3VkLmNpc2NvLmNvbQ/localauthentication HTTP/1.1

Responds from Expressway

… Event="Edge OAuth/SSO" Detail="Forbidden at authorization server"
Remote-reason="Invalid credentials" …

|HTTP/1.1 200 OK
X-Local-Auth-Failed: fail
Content-Type: text/html
Content-Length: 1837
Server: CE_C ECS
“Authorize by OAuth token with refresh”
Refresh CUCM & IM&P Registration

• Regenerate Tokens
  • Encryption Key - CLI
    set key regen authz encryption
  • Signing Key – CLI and OS Administration
    set key regen authz signing

• Re-voke Tokens
  curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>

• You MUST refresh on Expressway-C the CUCM/IM&P servers!!
Mobile and Remote Access
Troubleshooting and Monitoring
# Unified Communications Status – Expressway E

## Unified Communications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unified CM registrations</td>
<td>Configured</td>
</tr>
<tr>
<td>IM and Presence Service</td>
<td>Configured</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>
<tr>
<td>OAuth token with refresh</td>
<td>Configured</td>
</tr>
</tbody>
</table>

### Activity

<table>
<thead>
<tr>
<th>Activity</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM calls: Current video</td>
<td>0</td>
</tr>
<tr>
<td>Unified CM calls: Current audio (SIP)</td>
<td>0</td>
</tr>
</tbody>
</table>

### Domains

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

### Zones

<table>
<thead>
<tr>
<th>Name</th>
<th>SIP status</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCTraversal (eft-xwyc.coluc.com)</td>
<td>Active</td>
</tr>
</tbody>
</table>

---

**Advanced status information**

- View ssh tunnel status
## Unified Communications Status – Expressway C

### Unified Communications (last updated: 21:44:56 UTC)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unified CM registrations</td>
<td>Configured</td>
</tr>
<tr>
<td>IM and Presence Service</td>
<td>Configured</td>
</tr>
<tr>
<td>XMPP Federation</td>
<td>Not configured</td>
</tr>
<tr>
<td>Single Sign-On support</td>
<td>Not configured</td>
</tr>
<tr>
<td>OAuth token with refresh</td>
<td>Configured</td>
</tr>
</tbody>
</table>

### Activity

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

- [View detailed MRA authentication statistics](#)
- [View and manage OAuth token holders](#)

### Domains

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

### Zones

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

### Servers

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence Service nodes</td>
<td>1</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>
Unified Communications Status – Expressway C
“Authorize by user credentials”

<table>
<thead>
<tr>
<th>Activity</th>
<th>Requests</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM calls: Current video</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified CM calls: Current audio (SIP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current UCM/LDAP basic authenticated sessions</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Total UCM/LDAP basic authenticated sessions</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Total provisioning requests since last restart</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

View detailed MRA authentication statistics
View and manage OAuth token holders

<table>
<thead>
<tr>
<th>MRA authentication statistics</th>
<th>Requests</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Sent</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>200</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SSO Availability checks
| Sent SSO Not Enabled response                      | 3        |           |

OAuth Availability checks
| Sent OAuth Not Enabled response                    | 3        |           |

Requests for Unified Communications Services
| Successfully redirected for authentication          | 0        |           |
| IdP responses received from clients                | 0        |           |

Unified CM Proxy Authorization
| Successful                                         | 0        |           |

Unity Connection Server Proxy Authorization
| Successful                                         | 0        |           |

UCM/LDAP basic authentication
| Requests                                           | 0        |           |

SAML SSO authenticated sessions
| Requests                                           | 0        |           |
Unified Communications Status – Expressway C

“Authorize by user credentials”

Advanced status information

View sessions authorized by user credential
View ssh tunnel status

Unified Communications proxy requests

Records: 1

<table>
<thead>
<tr>
<th>Username</th>
<th>Device</th>
<th>User agent</th>
<th>Unified CM server</th>
<th>Expire time</th>
</tr>
</thead>
<tbody>
<tr>
<td>cholland</td>
<td>198.18.2.37</td>
<td>Jabber-Win-883</td>
<td>ucm-pub.dccloud.cisco.com</td>
<td>2018-01-23 23:33:52</td>
</tr>
</tbody>
</table>

Clear all MRA authentications

Advanced

HTTP server allow list
Configure HTTP server allow list

SIP Path headers

See automatic inbound rules

Credentials refresh interval (minutes) 480
Credentials cleanup interval (minutes) 720
Maximum authorizations per period 8
Rate control period (seconds) 300
Unified Communications Status – Expressway C
“Authorize by OAuth token with refresh”

<table>
<thead>
<tr>
<th>Unified Communications (last updated: 16:27:23 UTC)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unified CM registrations</td>
<td>Configured</td>
</tr>
<tr>
<td>IM and Presence Service</td>
<td>Configured</td>
</tr>
<tr>
<td>XMPP Federation</td>
<td>Configured</td>
</tr>
<tr>
<td>Single Sign-On support</td>
<td>Not configured (Enable on the Unified Communications page)</td>
</tr>
</tbody>
</table>

| OAuth token with refresh | Configured |

| Activity |
|-----------------------------------------------|---|
| Unified CM calls: Current video | 0 |
| Unified CM calls: Current audio (SIP) | 0 |
| Current UCM/LDAP basic authenticated sessions | 0 |
| Total UCM/LDAP basic authenticated sessions | 0 |
| Total provisioning requests since last restart | 1 |

| View detailed MRA authentication statistics |  |
| View and manage OAuth token holders |  |

<table>
<thead>
<tr>
<th>MRA authentication statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requests</strong></td>
<td></td>
</tr>
<tr>
<td>Received</td>
<td>3</td>
</tr>
<tr>
<td><strong>Responses</strong></td>
<td></td>
</tr>
<tr>
<td>Sent</td>
<td>4</td>
</tr>
<tr>
<td>200</td>
<td>3</td>
</tr>
<tr>
<td>302</td>
<td>1</td>
</tr>
<tr>
<td><strong>SSO Availability checks</strong></td>
<td></td>
</tr>
<tr>
<td>Sent SSO Not Enabled response</td>
<td>1</td>
</tr>
<tr>
<td><strong>OAuth Availability checks</strong></td>
<td></td>
</tr>
<tr>
<td>Sent OAuth Enabled response</td>
<td>1</td>
</tr>
<tr>
<td><strong>Requests for Unified Communications Services</strong></td>
<td></td>
</tr>
<tr>
<td>Successfully redirected for authentication</td>
<td>0</td>
</tr>
<tr>
<td>IdP responses received from clients</td>
<td>0</td>
</tr>
<tr>
<td>Accepted</td>
<td>0</td>
</tr>
<tr>
<td><strong>Unified CM Proxy Authorization</strong></td>
<td></td>
</tr>
<tr>
<td>Successful</td>
<td>1</td>
</tr>
<tr>
<td><strong>Unity Connection Server Proxy Authorization</strong></td>
<td></td>
</tr>
<tr>
<td>Successful</td>
<td>0</td>
</tr>
<tr>
<td><strong>UCM/LDAP basic authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Requests</td>
<td>1</td>
</tr>
<tr>
<td><strong>SAML SSO authenticated sessions</strong></td>
<td></td>
</tr>
<tr>
<td>Requests</td>
<td>1</td>
</tr>
</tbody>
</table>
How to validate the registration on CUCM?

<table>
<thead>
<tr>
<th>Status</th>
<th>Phone Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status: Ready</td>
<td>Phone Type: Cisco Unified Client Services Framework</td>
</tr>
</tbody>
</table>

**Association**
- Line [1] - +1.1972555018 in DN

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

**Real-time Device Status**
- Registration: Registered with Cisco Unified Communications Manager ucm-sub1.dcloud.cisco.com
- IPv4 Address: 198.18.133.152
- Active Load ID: Jabber_for_Windows-10.6.2
- Download Status: None

Show Expressway C as source IP address
SIP Registration – SIP Path Headers Support

- Expressway X8.9
- CUCM 11.5(1)SU2
- Provides feature support for:
  - Shared line features 78XX and 88XX
- Check release notes for more details
SSH Tunnels Status

Advanced status information

View sessions authorized by user credential

View ssh tunnel status

---

Unified Communications SSH tunnels status

<table>
<thead>
<tr>
<th>Target</th>
<th>Domain</th>
<th>Status</th>
<th>Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>eft-xwyc-a</td>
<td>coluc.com</td>
<td>Active</td>
<td>eft-xwyb.coluc.com</td>
</tr>
<tr>
<td>eft-xwyc-a</td>
<td>coluc.com</td>
<td>Active</td>
<td>eft-xwyb.coluc.com</td>
</tr>
<tr>
<td>eft-xwyc-b</td>
<td>coluc.com</td>
<td>Active</td>
<td>eft-xwyb.coluc.com</td>
</tr>
<tr>
<td>eft-xwyc-b</td>
<td>coluc.com</td>
<td>Active</td>
<td>eft-xwyb.coluc.com</td>
</tr>
</tbody>
</table>
Unified Communications Status – Event, Network, Config Logs

Event Log

Filter

Contains all of the words: failure

More options

Configure log settings | Download this page

Go to page | Go

Results

2018-01-27T20:27:52.081+00:00

tvcs: Event="External Server Communications Failure" Reason="gatekeeper timed out" Service="NeighbourGatekeeper" Dst-ip="10.48.55.93" Dst-port="7000" Detail="name:ef-xwye-b.coluc.com" Protocol="TCP" Level="1" UTCTime="2018-01-27 20:27:52.081"

2018-01-27T20:27:52.071+00:00

tvcs: Event="External Server Communications Failure" Reason="gatekeeper timed out" Service="NeighbourGatekeeper" Dst-ip="10.48.55.113" Dst-port="7000" Detail="name:ef-xwye-a.coluc.com" Protocol="TCP" Level="1" UTCTime="2018-01-27 20:27:52.071"
Unified Communications Status – Event, Network, Config Logs

Network Log

Filter

Contains all of the words: 21:54:51

Configure log settings | Download this page

Results

2018-01-27T21:54:51.927+00:00 tvcs: UTCTime="2018-01-27 21:54:51.926" Module="network.sip" Level="INFO": Action="Received" Local-ip="10.48.55.94" Local-port="25048" Src-ip="10.48.55.93" Src-port="7001" Detail="Receive Response Code=401, Method=OPTIONS, CSeq=3096, To-sip:10.48.55.93:7001, Call-ID=38b910954552dfc0@10.48.55.94, From-Tag=0f740e3254f4da3, To-Tag=9e552e5e77912b68, Msg-Hash=3994237476532063355, Local-SessionID=, Remote-SessionID="
Unified Communications Status – Event, Network, Config Logs

<table>
<thead>
<tr>
<th>Name</th>
<th>Level</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>DEBUG</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.auth</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.cdr</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.cdr4</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.cdrg</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.cdrh</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.db</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.dialplan</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.dnsp</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.dns</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.dnssec</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.ldap</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.mediarouting</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.rpc</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.rpcnologon</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.search</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.sip</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
<tr>
<td>network.sourceforge</td>
<td>INFO</td>
<td>View/Edit</td>
</tr>
</tbody>
</table>

Configure log settings | Download this page

Reset to info | Set to debug | Select all | Unselect all
Unified Communications Status – Event, Network, Config Logs

Network Log

2018-01-27T21:57:31.923+00:00

Module: network.sql
Level: DEBUG
Action: Received
Local ip: 10.48.55.94
Local port: 25047
Src ip: 10.48.55.113
Src port: 7001
Msg Hash: 623333416812130204
SIP MSG:
SIP/2.0 401 Unauthorized
Via: SIP/2.0:TLS 10.48.55.94:5061;branch=z9hG4bK4A95bf6e34127aa2d433205a8411af77487;received=10.48.55.94;port:25047
Call ID: c2a42da47a5c5323@10.48.55.94
CSeq: 55508 OPTIONS
From: <sip:10.48.55.94;tag=c5e1b5462174147>
To: <sip:10.48.55.113;7001;tag=c8406868327806ce>
Server: TANDBERG/4135 (X.10.4)
WWW-Authenticate: Digest realm="UCTraversals", nonce="e89ea219349735625724121b2e06d2ee6ddcbb54ac0e23ea8f73e70387", opaque="AgAAAGGXXHb+qVqKsV+RGw1UxCGm6V7", sstate=FA, algorithm=MD5, qop="auth"
Content-Length: 0

2018-01-27T21:57:31.920+00:00

Module: network.sql
Level: DEBUG
Action: Sent
Local ip: 10.48.55.94
Local port: 25047
Dst ip: 10.48.55.93
Dst port: 7001
Msg Hash: 9139525146788214109
SIP MSG:
OPTIONS sip:10.48.55.93:7001;transport=tls SIP/2.0
Via: SIP/2.0:TLS 10.48.55.94:5061;branch=z9hG4bK4A95bf6e34127aa2d433205a8411af77487;received=10.48.55.94
CSeq: 11861 OPTIONS
From: <sip:10.48.55.94;tag=9d52b9a5f5bf68d>
To: <sip:10.48.55.93:7001>
Max-Forwards: 0
User-Agent: TANDBERG/4135 (X.10.4)
Authorization: Digest nonce="c8d3d2e07f8a0690424a56885c61034577d058eac476256e0f30659077b", realm="UCTraversals", opaque="AQAAGGXXH4/X2wqJvF7/tzrZrXsElKpYzq", algorithm=MD5, url="sip:10.48.55.93:7001;transport=tls", username="traversalus", response="2edef5b02af3570b64e780748bc253", qop=auth, cnonce="06cf3d102G277d782d826db7875c1234059092e0d806ed5151a0455339ea", nc=00000001
Supported: com.tandberg.vcs.resourceusage
Content-Type: text/xml
Content-Length: 801

<xml version="1.0" encoding="utf-8"?>
<stuff resourceusageinfo="traversalscallsavailable"="300" traversalscallsavailable="false" traversalscallsavailable="true" traversalscallsavailable="false" traversalscallsavailable="false">
</stuff>
Unified Communications Status – Event, Network, Config Logs
### Alarms

#### Alarm Description

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
<th>State</th>
<th>Severity</th>
<th>Peer</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRKCOL</td>
<td>One or more modules of the Network Log or Support Log are set to a level of Debug or Trace.</td>
<td>Raised</td>
<td>Warning</td>
<td></td>
<td>Network Log and Support Log modules should be set to a level of Info, unless advised otherwise by your Cisco support representative. If diagnostic logging is in progress they will be reset automatically when diagnostic logging is stopped.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>First raised</th>
<th>Last raised</th>
<th>ID</th>
</tr>
</thead>
</table>

#### Acknowledge | Select all | Unselect all
DNS Lookup

DNS lookup

Host: coluc.com
Query type: All

DNS lookup

Host: coluc.com
Query type: All

Query type | Name | TTL | Class | Type | Response
---|---|---|---|---|---
A | coluc.com. | 600 | IN | A | 10.48.83.51
SRV | _sips_tcp.coluc.com. | 3600 | IN | SRV | 0 0 5061 colcm9pub.coluc.com.
SRV | _sip_tcp.coluc.com. | 3600 | IN | SRV | 0 0 5080 colcm9pub.coluc.com.
Expressway Diagnostic Logs

- Diagnostics logs

![Diagnostic logging interface](image-url)
How to validate Calls? Expressway

<table>
<thead>
<tr>
<th>Status</th>
<th>System</th>
<th>Configuration</th>
<th>Applications</th>
<th>Users</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Call status**

<table>
<thead>
<tr>
<th>Start time</th>
<th>Duration</th>
<th>Source</th>
<th>Destination</th>
<th>Type</th>
<th>Protocol</th>
<th>Peer</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-04-22 07:21:02</td>
<td>26 seconds</td>
<td>sip: <a href="mailto:+19725556018@ocm1.dcloud.cisco.com">+19725556018@ocm1.dcloud.cisco.com</a></td>
<td>sip: <a href="mailto:aperoz@dcloud.cisco.com">aperoz@dcloud.cisco.com</a></td>
<td>Traversal</td>
<td>SIP &lt;-&gt; SIP</td>
<td>This system</td>
<td>View</td>
</tr>
</tbody>
</table>

See Next Slide
How to validate Calls? Expressway

Generic Call Info
- Call Type

Bandwidth Allocated
- Zones route

Calling Party – Leg 1

Called Party – Leg 2

SIP Session State

Media Stats
- See Next Slide
How to validate Calls? Expressway

**Call Stats SIP Session 5 Channels**

- **Channel 1:** Audio, DTMF
- **Channel 2:** Video (main)
- **Channel 3:** Video (content)
- **Channel 4:** BFCP
- **Channel 5:** FarEnd

---

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
How to validate Calls? Expressway

- Event Logs

### Call history

<table>
<thead>
<tr>
<th>Start time</th>
<th>End time</th>
<th>Duration</th>
<th>Source</th>
<th>Destination</th>
<th>Type</th>
<th>Protocol</th>
<th>SIP variant</th>
<th>Status</th>
<th>Peer</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-02-20 10:54:52</td>
<td>2017-02-20 10:54:57</td>
<td>5 seconds</td>
<td>sip:6000@10.48.79.105</td>
<td>sip:5010@10.48.79.105</td>
<td>Traversal</td>
<td>SIP &lt;-&gt; SIP</td>
<td>Standards-based</td>
<td>487 Request Terminated</td>
<td>1</td>
<td>View</td>
</tr>
<tr>
<td>2017-02-20 10:51:56</td>
<td>2017-02-20 10:52:05</td>
<td>9 seconds</td>
<td>sip:6000@10.48.79.105</td>
<td>sip:5010@10.48.79.105</td>
<td>Traversal</td>
<td>SIP &lt;-&gt; SIP</td>
<td>Standards-based</td>
<td>487 Request Terminated</td>
<td>1</td>
<td>View</td>
</tr>
</tbody>
</table>

### Call history

<table>
<thead>
<tr>
<th>Status</th>
<th>Tag</th>
<th>Box-unique call serial number</th>
<th>Source alias</th>
<th>Destination alias</th>
<th>Start time</th>
<th>End time</th>
<th>Disconnect reason</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnected</td>
<td>a30569a5-0a88-4a14-85a3-3732d3a3bf2</td>
<td>e18a3089-8b45-4b83-9b1b-3481a8f3b43</td>
<td>sip:6000@10.48.79.105</td>
<td>sip:5010@10.48.79.105</td>
<td>2017-02-20 10:54:52</td>
<td>2017-02-20 10:54:57</td>
<td>487 Request Terminated</td>
<td>5 seconds</td>
</tr>
</tbody>
</table>

### Call components

<table>
<thead>
<tr>
<th>Local call serial number</th>
<th>Source alias</th>
<th>Destination alias</th>
<th>Protocol</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>cda8580-5333-4eb9-a755-57c0c250d03e</td>
<td>sip:6000@10.48.79.105</td>
<td>sip:5010@10.48.79.105</td>
<td>SIP &lt;-&gt; SIP</td>
<td>487 Request Terminated</td>
<td>Expressway</td>
</tr>
</tbody>
</table>

**Related tasks**

View all events associated with this call
How to validate Calls? Expressway

Event Log

Filter

Contains all the words: a30569ad-0a98-4e14-85a0-2732d3a3bdf2

Filter  Reset

Configure log settings | Download this page

Results

2017-02-20T10:54:57.408+01:00  tvcs: Event="Call Rejected" Service="SIP" Src-ip="10.48.55.108" Src-port="52602" Src-alias-type="SIP" Src-alias="sip:6000@10.48.79.105" Dst-alias-type="SIP" Dst-alias="sip:5010@10.48.79.105;user=phone" Call-serial-number="cda85808-53a3-4eb9-a7f8-07cab250d03e" Tag="a30569ad-0a98-4e14-85a0-2732d3a3bdf2" Detail="Request Terminated" Protocol="TLS" Response-code="487" Level="1" UTCTime="2017-02-20 09:54:57.406"

2017-02-20T10:54:57.408+01:00  tvcs: Event="Search Cancelled" Service="SIP" Dst-alias-type="SIP" Dst-alias="sip:5010@10.48.79.105;user=phone" Call-serial-number="cda85808-53a3-4eb9-a7f8-07cab250d03e" Tag="a30569ad-0a98-4e14-85a0-2732d3a3bdf2" Detail="searchtype:INVITE" Level="1" UTCTime="2017-02-20 09:54:57.406"

2017-02-20T10:54:52.821+01:00  tvcs: Event="Call Attempted" Service="SIP" Src-ip="10.48.55.108" Src-port="52602" Src-alias-type="SIP" Src-alias="sip:6000@10.48.79.105" Dst-alias-type="SIP" Dst-alias="sip:5010@10.48.79.105;user=phone" Call-serial-number="cda85808-53a3-4eb9-a7f8-07cab250d03e" Tag="a30569ad-0a98-4e14-85a0-2732d3a3bdf2" Protocol="TLS" Auth="YES" Level="1" UTCTime="2017-02-20 09:54:52.809"

2017-02-20T10:54:52.821+01:00  tvcs: Event="Search Attempted" Service="SIP" Dst-alias-type="SIP" Dst-alias="sip:5010@10.48.79.105;user=phone" Call-serial-number="cda85808-53a3-4eb9-a7f8-07cab250d03e" Tag="a30569ad-0a98-4e14-85a0-2732d3a3bdf2" Detail="searchtype:INVITE" Level="1" UTCTime="2017-02-20 09:54:52.809"
Jabber Diagnostics – shift+crtl+d

**Discovery**

- Discovery Outcome: Success: Cisco IM & Presence
- Domain Controller: \ad1.dcloud.cisco.com
- Edge Configuration: [https://esp-e-1.dcloud.cisco.com:8443/ZGNsb3VkImNpc2NvM2F1bQ/get_edge_config?service_name= Cisco-uds&service_name= cuplogin](https://esp-e-1.dcloud.cisco.com:8443/ZGNsb3VkImNpc2NvM2F1bQ/get_edge_config?service_name= Cisco-uds&service_name= cuplogin)
- Edge Domain: dcloud.cisco.com
- Edge Required: Yes
- Edge Visibility: Visible
- Excluded Services: None
- Internal Visibility: Not Visible
- JID created from: username + presence domain
- Jabber ID: cholland@dcloud.cisco.com
- Services Domain: dcloud.cisco.com
- Services Domain Source: Windows User Principal Name (UPN)
- UPN: Enabled: cholland@dcloud.cisco.com
- User Image: [http://ad1.dcloud.cisco.com/directory/cholland.jpg](http://ad1.dcloud.cisco.com/directory/cholland.jpg)
- Virtual environment: VDI is ON but without VXME.
- Voice Services Domain: dcloud.cisco.com

**UCM Summary**

- Device Configuration: [https://ucm-pub.dcloud.cisco.com:6972/cholland.cnf.xml](https://ucm-pub.dcloud.cisco.com:6972/cholland.cnf.xml)
- Home UDS: [https://ucm-sub1.dcloud.cisco.com:8443/ucm-uds/user/cholland](https://ucm-sub1.dcloud.cisco.com:8443/ucm-uds/user/cholland)
- SSO Login: [https://ucm-sub1.dcloud.cisco.com:8443/ssosp/oauth/authorize](https://ucm-sub1.dcloud.cisco.com:8443/ssosp/oauth/authorize)
- Service Profile Configuration: [https://ucm-pub.dcloud.cisco.com:6972/SPDefault.cnf.xml](https://ucm-pub.dcloud.cisco.com:6972/SPDefault.cnf.xml)
- Supports SSO: True
- UCM Version: 11.5.1
Jabber Diagnostics – shift+crtl+d
Jabber Diagnostics – shift+crtl+d

```xml
<edgeConfig>
  - <sipEdgeServer>
    <server>
      <address>exp-e-1.dcloud.cisco.com</address>
      <tlsPort>5061</tlsPort>
    </server>
  </sipEdgeServer>
  - <sipRequest>
    <route><sip:198.18.133.152:5061;transport=tls;zone-id=1;directed;lr></route>
  </sipRequest>
  - <xmppEdgeServer>
    <server>
      <address>exp-e-1.dcloud.cisco.com</address>
      <tlsPort>5222</tlsPort>
    </server>
  </xmppEdgeServer>
  - <httpEdgeServer>
    <server>
      <address>exp-e-1.dcloud.cisco.com</address>
      <tlsPort>8443</tlsPort>
    </server>
  </httpEdgeServer>
  - <userUdsServer>
    <server>
      <address>198.18.133.3</address>
      <tlsPort>8443</tlsPort>
    </server>
  </userUdsServer>
</edgeConfig>
```

Generate Problem Report
Jabber Diagnostics – shift+crtl+d
Mobile and Remote Access Tool Demo

cs.co/csa
Conclusion
Conclusion

• Mobile and Remote Access Deployment
• Mobile and Remote Access Monitoring
• Collaboration Solutions Analyzer
• Mobile and Remote Access Registration and Call Flow
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

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

cs.co/ciscolivebot#BRKCOL-2021
• Please complete your Online Session Evaluations after each session

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

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

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscobtive.com/global/on-demand-library/.
Thank you
Have a safe journey
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
Thank you
Reference
Jabber Registration & Call Flow
Which Expressway? Which CUCM? Which IM&P?

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expressway</td>
<td>DNS SRV_collab-edge_tls.coluc.com</td>
</tr>
<tr>
<td>CUCM</td>
<td>Device XML Configuration File (*.cnf.xml)</td>
</tr>
<tr>
<td>IM&amp;P</td>
<td>User Service Profile (*.cnf.xml)</td>
</tr>
<tr>
<td>CUC</td>
<td>User Service Profile (*.cnf.xml)</td>
</tr>
</tbody>
</table>
REGISTER sip:ucm-sub1.dcloud.cisco.com SIP/2.0
Via: SIP/2.0/TLS 198.18.2.37:51172;branch=z9hG4bK00001055
Call-ID: 005056b8-21130003-000062b1-000035fd@198.18.2.37
CSeq: 102 REGISTER
Contact: <sip:509764ed-5917-eb59-0bca-413a773223c9@198.18.2.37:51172;transport=tls>;+sip.instance="urn:uuid:00000000-0000-0000-0000-005056b82113">;+u.sip!devicename.cisco.com=colland;+u.sip!model.cisco.com= 503;video
From: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=005056b82113000200001174-0000712a
To: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>
Max-Forwards: 70
Route: <sip:exp-e-1.dcloud.cisco.com;transport=tls;lr>,<sip:198.18.133.152:5061;transport=tls;zone-id=1;directed;lr>,<sip:ucm-sub1.dcloud.cisco.com;transport=tcp;lr>
User-Agent: Cisco-CSF
Expires: 3600
Date: Wed, 20 Apr 2016 10:00:24 GMT
response="d8ad62d5f7555cd9441464bd56f2a869", nonce="bc9fde6c224d6617f6dc4a6f8ae59a369c5f9ebeecb20220091bf27ea75", 
opaque="AGQQAEEd65TRpiTDUddWMttJLzZ2uOd", qop="000065", qop_auth_no=00000001, algorithm_MD5
Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,...
Reason: SIP ;cause=200;text="cisco-alarm:25 Name=cholland ActiveLoad=Jabber_for_Windows-10.6.2 InactiveLoad=Jabber_for_Windows-10.6.2 Last=initialized"
Mime-Version: 1.0
Content-Type: multipart/mixed;boundary=uniqueBoundary
Content-Length: 1271
Module="network.search" Level="DEBUG": Detail="Search rule 'LocalZoneMatch' ignored due to system generated search rule filtering"
Module="network.search" Level="DEBUG": Detail="Search rule 'CEtcp-ucm-sub1.dcloud.cisco.com' did not match destination alias 'ucm-sub1.dcloud.cisco.com;transport=tcp;lr'"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B-to-external' ignored due to system generated search rule filtering"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B-from-external' did not match destination alias 'ucm-sub1.dcloud.cisco.com;transport=tcp;lr'"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'CEtcp-ucm-sub1.dcloud.cisco.com' towards target 'CEtcp-ucm-sub1.dcloud.cisco.com' at priority '45' with alias 'ucm-sub1.dcloud.cisco.com;transport=tcp;lr'"

Route: <sip:ucm-sub1.dcloud.cisco.com;transport=tcp;lr>

Route header matches search rule on Expressway C
REGISTER sip:ucm-sub1.dcloud.cisco.com SIP/2.0
Via: SIP/2.0/TCP 198.18.133.152:5060;egress-zone=CEtcpucmsub1dcloudciscocom;branch=z9hG4bK4c0a69b71818676b4f9b1843da21359561537.11271e07df1c8857e73858d689a16fb9;proxy-call-id=d1b5a0d4-a227-4636-a9f9-2c1db44f750a;rport
Via: SIP/2.0/TLS 198.18.1.152:7001;egress-zone=TraversalServerMRA;branch=z9hG4bK2722c2f1e37e8551419dfb274557c6111.62f36d33d1c49546b9ec07f652ee345b;proxy-call-id=abb45b93-a6b5-4c2a-a06e-bc829293b12e;received=198.18.1.152;rport=7001;ingress-zone=TraversalClientMRA
Via: SIP/2.0/TLS 198.18.2.37:51172;branch=z9hG4bK00001055;received=198.18.2.37;ingress-zone=CollaborationEdgeZone
Call-ID: 005056b8-21130003-000062b1-000035fd@198.18.2.37
CSeq: 102 REGISTER
Contact: <sip:509764ed-5917-eb59-0bca-413a773223c9@198.18.133.152:5060;transport=tcp;orig-hostport=198.18.2.37:51172>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-005056b82113>";+sip.defaultdevice.ccm.cisco.com="cholland";+sip.model.ccm.cisco.com="503";video
From: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=005056b82113000200001174-0000712a
To: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>
Max-Forwards: 14
Route: <sip:ucm-sub1.dcloud.cisco.com;transport=tcp;lr>
User-Agent: Cisco-CSF
Expires: 3600
Date: Wed, 20 Apr 2016 10:00:24 GMT
Supported: replaces,join,sdp-anat,norefersub,resource-priority,…
P-Asserted-Identity: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>
X-TAATag: bd6ccf07-6713-4003-9f89-7d8d0c73777c
Reason: SIP ;cause=200;text="cisco-alarm:25 Name=cholland ActiveLoad=Jabber_for_Windows-10.6.2 InactiveLoad=Jabber_for_Windows-10.6.2 Last=initialized"…
## SIP TLS – Exp C cert includes Security Profile

<table>
<thead>
<tr>
<th>SIPTcp - Connection Indication</th>
<th><strong>Listen Port</strong> = 5061, Peer Port = 25002</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIPTcp - wait_SdlReadRsp: Incoming SIP TCP message from 198.18.133.152 on port 25002 index 10 with 2994 bytes:[53,NET]</td>
<td><strong>REGISTER sip:ucm-sub1.dcloud.cisco.com SIP/2.0</strong></td>
</tr>
<tr>
<td>...</td>
<td><strong>Route: <a href="">sip:ucm-sub1.dcloud.cisco.com;transport=tls;lR</a></strong></td>
</tr>
<tr>
<td>...</td>
<td>//SIP/SIPHandler/ccbId=0/scbId=0/wait_SIPCertificatElnd: could not find a trunk device using address or x509SubjectName calling findSIPStationInit</td>
</tr>
<tr>
<td>...</td>
<td>//SIP/SIPHandler/ccbId=0/scbId=0/findDeviceByX509Subject: x509Subject:exp-c-1.dcloud.cisco.com, port:5061</td>
</tr>
<tr>
<td>...</td>
<td>//SIP/SIPHandler/ccbId=25/scbId=0/findDevicePID: Routed to SIPStationInit</td>
</tr>
<tr>
<td>...</td>
<td>SIPStationInit: connId=10, <strong>CSFEWAYJ</strong>, 10.48.55.98:5061, Incoming register request received over TLS. Subject=[/C=BE/ST=BRABANT/L=DIEGEM/O=CISCO/OU=TAC/CN=exp-c-1.dcloud.cisco.com]</td>
</tr>
<tr>
<td>...</td>
<td>SIPStationD(9) - validTLSConnection: <strong>TLS InvalidX509NameInCertificate</strong>, Rcvd=exp-c-1.dcloud.cisco.com, Expected=CSFEWAYJ. Will check SAN the next</td>
</tr>
<tr>
<td>...</td>
<td>SIPStationD(9) - validTLSConnection: <strong>Found matching SAN</strong>, SAN Rcvd=exp-c-1.dcloud.cisco.com;conference-2-cup.dcloud.cisco.com;csf-secure, Expected=csf-secure</td>
</tr>
</tbody>
</table>
SIP/2.0 200 OK

Via: SIP/2.0/TCP 198.18.133.152:5060;egress-zone=CEtcpucmsub1dcloudciscocom;branch=z9hG4bK4c0a69b71818676b4f9b1843da21359561537....proxy-call-id=d1b5a0d4-a227----;rport,
SIP/2.0/TLS 198.18.1.152:7001;egress-zone=TraversalServerMRA;branch=z9hG4bK272c22f12e37e8551419ddf2b74557....proxy-call-id=abb45b93-a6b5----;received=198.18.1.152;proxy-call-id=abb45b93-a6b5----;received=198.18.1.152;ingress-zone=TraversalClientMRA,
SIP/2.0/TLS 198.18.2.37:51172;branch=z9hG4bK00001055;received=198.18.2.37;ingress-zone=CollaborationEdgeZone

Call-ID: 005056b8-21130003-000062b1-000035fd@198.18.2.37
CSeq: 102 REGISTER
Contact: <sip:509764ed-5917-eb59-0bca-413a773223c9@198.18.133.152:5060;transport=tcp;orig-hostport=198.18.2.37:51172>;+sip.instance=":urn:uuid:00000000-0000-0000-0000-005056b82113";+u.sip!devicename.ccm.cisco.com="cholland";+u.sip!model.ccm.cisco.com="503";video;x-cisco-newreg
From: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=005056b82113000200001174-0000712a
To: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=1883801707
Server: Cisco-CUCM10.5
Expires: 120
Date: Wed, 20 Apr 2016 10:00:25 GMT
Supported: X-cisco-srtp-fallback,X-cisco-sis-7.1.1
Content-Type: application/x-cisco-remotecc-response+xml
Content-Length: 381
SIP/2.0 200 OK
Via: SIP/2.0/TLS 198.18.1.152:7001;egress-zone=TraversalServerMRA;branch=z9hG4bK272c22f12e37e8551419dd12b74557....;proxy-call-id=abb45b93-a6b5-....;received=198.18.1.152;rport=7001;ingress-zone=TraversalClientMRA,
SIP/2.0/TLS 198.18.2.37:51172;branch=z9hG4bK00001055;received=198.18.2.37;ingress-zone=CollaborationEdgeZone
Call-ID: 005056b8-21130003-000062b1-000035fd@198.18.2.37
CSeq: 102 REGISTER

Contact: <sip:509764ed-5917-eb59-0bca-413a773223c9@198.18.133.152:5060;transport=tcp;orig-hostport=198.18.2.37:51172>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-005056b82113">";+u.sip!devicename.ccm.cisco.com="cholland";+u.sip!model.ccm.cisco.com="503";video;x-cisco-newreg

From: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=005056b82113000200001174-0000712a
To: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=1883801707
Server: Cisco-CUCM10.5
Expires: 120
Date: Wed, 20 Apr 2016 10:00:25 GMT
Supported: X-cisco-srtp-fallback,X-cisco-sis-7.1.1
Content-Type: application/x-cisco-remotecc-response+xml
Content-Length: 381
SIP/2.0 200 OK
Via: SIP/2.0/TLS 198.18.2.37:51172;branch=z9hG4bK00001055;received=198.18.2.37;ingress-zone=CollaborationEdgeZone
Call-ID: 005056b8-21130003-000062b1-000035fd@198.18.2.37
CSeq: 102 REGISTER
Contact: <sip:509764ed-eb59-5917-0bca-413a773223c9@198.18.133.152:5060;transport=tcp;orig-hostport=198.18.2.37:51172>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-005056b82113">";+u.sip!devicename.ccm.cisco.com="cholland";+u.sip!model.ccm.cisco.com="503";video;x-cisco-newreg
From: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=005056b82113000200001174-0000712a
To: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=1883801707
Server: Cisco-CUCM10.5
Expires: 120
Date: Wed, 20 Apr 2016 10:00:25 GMT
Supported: X-cisco-srtp-fallback,X-cisco-sis-7.1.1
Content-Type: application/x-cisco-remotecc-response+xml
Content-Length: 381
<table>
<thead>
<tr>
<th>REGISTER sip:ucm-sub1.dcloud.cisco.com SIP/2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Via: SIP/2.0/TCP 198.18.133.152:5060;egress-zone=CEtcpucmsub1dcloudciscocom;branch=z9hG4bK4c0a69b71818676b4f9b1843da21359561537.1f271e07df1c8857e738586d89a16fb9;proxy-call-id=d1b5a0d4-a227-4636-a9f9-2c1db44f750a;rport</td>
</tr>
<tr>
<td>Via: SIP/2.0/TLS 198.18.1.152:7001;egress-zone=TraversalServerMRA;branch=z9hG4bK272c22f12e37e8551419d2f774557c6111.62f3633cd1c49546b99ec07f652ee345b;proxy-call-id=abb45b93-a6b5-4c2a-a06e-bc829293b12e;received=198.18.1.152;rport=7001;ingress-zone=TraversalClientMRA</td>
</tr>
<tr>
<td>Via: SIP/2.0/TLS 198.18.2.37:51172;branch=z9hG4bK00001055;received=198.18.2.37;ingress-zone=CollaborationEdgeZone</td>
</tr>
<tr>
<td>Call-ID: 005056b8-21130003-000062b1-000035fd@198.18.2.37</td>
</tr>
<tr>
<td>CSeq: 102 REGISTER</td>
</tr>
<tr>
<td>Contact: <a href="">sip:509764ed-5917-eb59-0bca-413a773223c9@198.18.2.37:51172;transport=tcp;orig-hostport=198.18.2.37:51172</a>;+sip.instance=&quot;<a href="">urn:uuid:00000000-0000-0000-0000-000000000000”</a>;+u.sip!devicename.ccm.cisco.com=&quot;cholland”};+u.sip!model.ccm.cisco.com=&quot;503”;video</td>
</tr>
<tr>
<td>From: <a href="">sip:+19725555018@ucm-sub1.dcloud.cisco.com</a>;tag=005056b82113000200001174-0000712a</td>
</tr>
<tr>
<td>To: <a href="">sip:+19725555018@ucm-sub1.dcloud.cisco.com</a></td>
</tr>
<tr>
<td>Max-Forwards: 14</td>
</tr>
<tr>
<td>Route: <a href="">sip:ucm-sub1.dcloud.cisco.com;transport=tcp;l</a></td>
</tr>
<tr>
<td>Path: <a href="">sip:198.18.133.152:5060;transport=tls;l</a></td>
</tr>
<tr>
<td>Path: <a href="">sip:198.18.1.152:7001;transport=tls;l</a></td>
</tr>
<tr>
<td>Path: <a href="">sip:198.18.2.37:51172;transport=tls;apparent;ds;l</a></td>
</tr>
<tr>
<td>User-Agent: Cisco-CSF</td>
</tr>
</tbody>
</table>

Path Headers included

Contact = Jabber
SIP/2.0 200 OK
Via: SIP/2.0/TCP 198.18.133.152:5060; egress-zone=CEtpucmsub1dcloudciscocom;branch=z9hG4bK4c0a69b71818676b4f9b1843da21359561537;+proxy-call-id=d1b5a0d4-a227-……;rport,
SIP/2.0/TLS 198.18.1.152:7001; egress-zone=TraversalServerMRA;branch=z9hG4bK272c22f12e37e8551419ddf2b74557;+proxy-call-id=abb45b93-a6b5-……;received=198.18.1.152;port=7001;ingress-zone=TraversalClientMRA,
SIP/2.0/TLS 198.18.2.37:51172;branch=z9hG4bK00001055;received=198.18.2.37;ingress-zone=CollaborationEdgeZone
Call-ID: 005056b8-21130003-000062b1-000035fd@198.18.2.37
CSeq: 102 REGISTER
Contact: <sip:509764ed-5917-eb59-0bca-413a773223c9@198.18.2.37:51172;transport=tcp;orig-hostport=198.18.2.37:51172>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-000000000000>";+u.sip!devicename.ccm.cisco.com="cholland";+u.sip!model.ccm.cisco.com="503";video;x-cisco-newreg
From: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=005056b82113000200001174-0000712a
To: <sip:+19725555018@ucm-sub1.dcloud.cisco.com>;tag=1883801707
Path: <sip:198.18.133.152:5060;transport=tls;lr>,<sip:198.18.1.152:7001;transport=tls;lr>,<sip:198.18.2.37:51172;transport=tls;apparent;ds;lr>

Path Headers included
I want to call aperez@dcloud.cisco.com

Single NIC Deployment

NAT Reflection

What is my Signaling Path?
What is my Media Path?
INVITE sip:aperez@dcloud.cisco.com SIP/2.0
Via: SIP/2.0/TLS 173.38.222.35:7001;egress-zone=VCSCforMRA;
branch=z9hG4bKa12e006856e66fc93ef9cbb7daa4d8b530.d920a4b98b9097f733cb0754c497dc37;proxy-call-id=a4988096-cec7-4ce5-97dd-16aad174117a;rport
Via: SIP/2.0/TLS 144.254.9.156:51989;branch=z9hG4bK085ff1e9;received=144.254.9.156;ingress-zone=CollaborationEdgeZone
Call-ID: a0999b00-a8fb000b-1f0dd3b5-44c62000@144.254.9.156
CSeq: 101 INVITE
Remote-Party-ID: "Charles Holland" <sip:+19725556018@cucm1.dcloud.cisco.com>;party=calling;id-type=subscriber;privacy=off;screen=yes
Contact: <sip:55ba4346-24fd-1091-40ae-66ae6b683a13@144.254.9.156:51989;transport=tls>;+u.sip!devicename.ccm.cisco.com="csfcholland";video;bfcp
From: "Charles Holland" <sip:+19725556018@cucm1.dcloud.cisco.com>;tag=a0999b00a8fb005f2b5f0346-6acffee8
To: <sip:aperez@dcloud.cisco.com>

Route: <sip:cucm1.dcloud.cisco.com;transport=tcp;lr>
Record-Route: <sip:proxy-call-id=a4988096-cec7-4ce5-97dd-16aad174117a@173.38.222.35:7001;transport=tls;lr;zone-id=2>
Record-Route: <sip:proxy-call-id=a4988096-cec7-4ce5-97dd-16aad174117a@173.38.222.35:5061;transport=tls;lr>

Session-Expires: 1800
Accept: application/sdp
P-Asserted-Identity: "Charles Holland" <sip:+19725556018@cucm1.dcloud.cisco.com>

Session-ID: 0000174b00105000a00005056b87f95;remote=0000000000000000000000000000000000000000
SIP INVITE

exp-e.collabedge.com
173.38.222.35 (external)

exp-c.dcloud.cisco.com
198.18.133.152

Module="network.search" Level="DEBUG": Detail="Search rule 'LocalZoneMatch' ignored due to system generated search rule filtering"
Module="network.search" Level="DEBUG": Detail="Search rule 'External IP address search rule' did not match destination alias 'cucm1.dcloud.cisco.com;transport=tcp;lr'"
Module="network.search" Level="DEBUG": Detail="Search rule 'Traversal zone search rule BIS' ignored due to system generated search rule filtering"
Module="network.search" Level="DEBUG": Detail="Search rule 'Route to CUCM URI Dialling' did not match destination alias 'cucm1.dcloud.cisco.com;transport=tcp;lr'"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'CEtcp-cucm1.dcloud.cisco.com' towards target 'CEtcp-cucm1.dcloud.cisco.com' at priority '45' with alias 'cucm1.dcloud.cisco.com;transport=tcp;lr'"

Route: <sip:cucm1.dcloud.cisco.com;transport=tcp;lr>

Route header matches search rule on Expressway C
SIP/2.0 200 OK

Via: SIP/2.0/TCP 198.18.133.152:5060;egress-zone=CEtcpcucm1dcloudciscocom;branch=…
SIP/2.0/TLS 198.18.133.152:5073;branch=…
SIP/2.0/TLS 198.18.133.152:5061;egress-zone=DefaultZone;branch=…
SIP/2.0/TLS 173.38.222.35:7001;egress-zone=VCSCforMRA;branch=…
SIP/2.0/TLS 144.254.9.156:51989;branch=z9hG4bK085ff1e9;received=144.254.9.156;ingress-zone=CollaborationEdgeZone

Call-ID: a0999b00-a8fb000b-1f0dd3b5-44c62000@144.254.9.156
CSeq: 101 INVITE

Record-Route: <sip:proxy-call-id=eda462ac-5076-4b9b-8b2f-94c25898c136@198.18.133.152:5060;transport=tcp;lr>,<sip:proxy-call-id=eda462ac-5076-4b9b-8b2f-94c25898c136@198.18.133.152:5061;transport=tls;lr>

Session-ID: 0000174b00105000a00005056b87f95;remote=00000000000000000000000000000000000000
BYE sip:198.18.133.152:5071;transport=tlsv2/2.0
Via: SIP/2.0/TLS 144.254.9.156:51989;branch=z9hG4bK6383a3a8
Call-ID: a0999b00-a8fb000b-1f0dd3b5-44c62000@144.254.9.156
CSeq: 102 BYE
From: "Charles Holland" <sip:+19725556018@cucm1.dcloud.cisco.com>;tag=a0999b00a8fb005f2b5f0346-6acffee8
To: <sip:aperez@dcloud.cisco.com>;tag=6c0aec964f8d37fb
Max-Forwards: 70

Route:
<sip:proxy-call-id=a4988096-cc7-4ce5-97dd-16aad174117a@173.38.222.35:5061;transport=tlsv2/2.0;lr>,
<sip:proxy-call-id=a4988096-cc7-4ce5-97dd-16aad174117a@173.38.222.35:7001;transport=tlsv2/2.0;lr;zone-id=2>,
<sip:proxy-call-id=33b7eae5-ca1c-4b2a-bd2f-5251f6e2672e@198.18.133.152:5061;transport=tlsv2/2.0;lr>,
<sip:proxy-call-id=33b7eae5-ca1c-4b2a-bd2f-5251f6e2672e@198.18.133.152:5061;transport=tlsv2/2.0;lr>

User-Agent: Cisco-CSF
Date: Fri, 22 Apr 2016 09:28:57 GMT
Proxy-Authorization: Digest username="cholland", realm="vcse.collabedge-170.dc-03.com", uri="sip:198.18.133.152:5071;transport=tlsv2/2.0", response="017516040f281b9956a916b0f00ef9c9", nonce="f17caea9836d78c72df4489fd29666909db875758d7fcd3c186b63e5f", opaque="AQAAAlpwsYAHX4/T3fOownYK/kuYoF", cnonce="576d9da2", qop=auth, nc=0000000a, algorithm=MD5
Session-ID: 2fd842dd00105000a000a0999b00a8fb;remote=00000000000000000000000000000000
Content-Length: 0
What happened with the media? SDP Offer (EO)

From UAC – Jabber
Content-Type: application/sdp
Content-Length: 4865
v=0
o=Cisco-SIPUA 25755 0 IN IP4 144.254.9.156
s=SIP Call
b=AS:2048
t=0 0
m=audio 24600 RTP/SAVP 114 9 104 105 0 8 18 101
  c=IN IP4 144.254.9.156
  a=rtpmap:114 opus/48000/2
  a=rtpmap:101 telephone-event/8000
  ...
  m=video 14200 RTP/SAVP 126 97
  c=IN IP4 144.254.9.156
  a=rtpmap:126 H264/90000
  a=content:main
  ...
  m=application 5686 UDP/BFCP *
  c=IN IP4 144.254.9.156
  ...
  m=application 38964 RTP/SAVP 125
  c=IN IP4 144.254.9.156
  a=rtpmap:125 H224/4800

Channel1: Audio
Channel2: Video (main)
Channel3: Video (content)
Channel4: BFCP
Channel5: FarEnd

From UAC – exp-e.collabedge.com
Content-Type: application/sdp
Content-Length: 4890
v=0
o=Cisco-SIPUA 25755 0 IN IP4 144.254.9.156
s=SIP Call
c=IN IP4 173.38.222.35
b=AS:2048
t=0 0
m=audio 36000 RTP/SAVP 114 9 104 105 0 8 18 101
  c=IN IP4 173.38.222.35
  a=rtpmap:114 opus/48000/2
  a=rtpmap:101 telephone-event/8000
  ...
  m=video 36000 RTP/SAVP 126 97
  c=IN IP4 173.38.222.35
  a=rtpmap:126 H264/90000
  a=content:main
  ...
  m=video 36000 RTP/SAVP 126 97
  a=rtpmap:126 H264/90000
  a=content:slides
  ...
  m=application 36000 UDP/BFCP *
  c=IN IP4 144.254.9.156
  ...
  m=application 36000 RTP/SAVP 125
  c=IN IP4 144.254.9.156
  a=rtpmap:125 H224/4800

From UAC – exp-c.dcloud.cisco.com
Content-Type: application/sdp
Content-Length: 1480
v=0
o=tandberg 0 1 IN IP4 198.18.133.152
s=
c=IN IP4 198.18.133.152
b=AS:2048
t=0 0
m=audio 48010 RTP/AVP 96 97 98 99 0 8 18 101
  a=rtpmap:114 opus/48000/2
  a=rtpmap:101 telephone-event/8000
  ...
  m=video 48012 RTP/AVP 96 97
  a=rtpmap:126 H264/90000
  a=content:main
  ...
  m=video 48014 RTP/AVP 96 97
  a=rtpmap:126 H264/90000
  a=content:slides
  ...
  m=application 48016 UDP/BFCP *
  ...
  m=application 48018 RTP/AVP 96
  c=IN IP4 144.254.9.156
  a=rtpmap:125 H224/4800

Channel1:
Audio DTMF
Channel2:
Video (main)
Channel3:
Video (content)
Channel4:
BFCP
Channel5:
FarEnd

Multiplex
What happened with the media? SDP Answer

Channel 1: Audio
Channel 2: Video (main)
Channel 3: Video (content)
Channel 4: BFCP
Channel 5: FarEnd

From UAS – exp-e.collabedge.com
Content-Type: application/sdp
Content-Length: 1291
v=0
o=tandberg 0 1 IN IP4 198.18.133.152
s=:
c=IN IP4 173.38.222.35...
m=audio 36022 RTP/SAVP 114 101
a=rtpmap:114 opus/48000/2
a=rtpmap:101 telephone-event/8000...
m=video 36024 RTP/SAVP 126
a=rtpmap:126 H264/90000
a=content:main...
m=video 36026 RTP/SAVP 126
a=rtpmap:126 H264/90000
a=content:slides...
m=application 36028 UDP/BFCP *
...
m=application 36030 RTP/SAVP 125
a=rtpmap:125 H224/4800
...

RTP

From UAS – exp-c.dcloud.cisco.com
Content-Type: application/sdp
Content-Length: 1296
v=0
o=tandberg 0 1 IN IP4 198.18.133.152
s=:
c=IN IP4 198.18.133.152...
m=audio 48000 RTP/SAVP 114 101
a=rtpmap:114 opus/48000/2
a=rtpmap:101 telephone-event/8000...
m=video 48002 RTP/SAVP 126
a=rtpmap:126 H264/90000
a=content:main...
m=video 48004 RTP/SAVP 126
a=rtpmap:126 H264/90000
a=content:slides...
m=application 48006 UDP/BFCP *
...
m=application 48008 RTP/SAVP 125
a=rtpmap:125 H224/4800
...

RTP

From UAS – ccm1.dcloud.cisco.com
Content-Length: 820
v=0
o=CiscoSystemsCCM-SIP 19369 1 IN IP4 198.18.133.3
s=SIP Call
c=IN IP4 198.18.18.37
b=AS:4000
l=0 0
m=audio 24632 RTP/AVP 114 101
a=rtpmap:114 opus/48000/2
a=rtpmap:101 telephone-event/8000...
m=video 14120 RTP/AVP 126
a=rtpmap:126 H264/90000
a=content:main...
m=video 14136 RTP/AVP 126
a=rtpmap:126 H264/90000
a=content:slides...
m=application 5786 UDP/BFCP *
...
m=application 32716 RTP/AVP 125
a=rtpmap:125 H224/4800
...

RTP

RTP