Resolve Collaboration Edge Most Common Issues

Contents

Introduction

This document describes how to troubleshoot the Collaboration Edge most common problems that you face during the deployment phase.

Background Information

Mobile & Remote Access (MRA) is a deployment solution for Virtual Private Network-less (VPN) Jabber capability. This solution allows end users to connect to internal enterprise resources from anywhere in the world. This guide has been written to give engineers who troubleshoot the Collaboration Edge solution the capability to quickly identify and resolve the most common problems you face during the deployment phrase.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM)
- Cisco Expressway Core
- Cisco Expressway Edge
- Cisco IM and Presence (IM&P)
- Cisco Jabber for Windows
- Cisco Jabber for MAC
- Cisco Jabber for Android
- Cisco Jabber for iOS®
- Security Certificates
- Domain Name System (DNS)

Components Used

The information in this document is based on these software and hardware versions:

- Expressway Version X8.1.1 or later
- CUCM Release 9.1(2)SU1 or later and IM&P Version 9.1(1) or later
- Cisco Jabber Version 9.7 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Log In Issues

Jabber Unable to Sign In Through MRA

This symptom can be caused by a wide range of issues, a few of which are outlined here.

1. Collaboration Edge Service Record (SRV) Not Created and/or Port 8443 Unreachable

For a Jabber client to be able to log in successfully with MRA, a specific collaboration edge SRV record must be created and accessible externally. When a Jabber client is initially started, it makes DNS SRV queries:

1. **_cisco-uds**: This SRV record is used in order to determine if a CUCM server is available.

2. **_cuplogin**: This SRV record is used in order to determine if an IM&P server is available.

3. **_collab-edge**: This SRV record is used in order to determine if MRA is available.

If the Jabber client is started and **does not** receive an SRV answer for **_cisco-uds** and **_cuplogin** and **does** receive an answer for **_collab-edge**, then it uses this answer to try to contact the Expressway-E listed in the SRV answer.

The **_collab-edge** SRV record points to the Fully Qualified Domain Name (FQDN) of Expressway-E with port **8443**. If the **_collab-edge** SRV is not created, or is not externally available, or if it is available, but port 8443 is not reachable, then the Jabber client fails to log in.

You can confirm if the **_collab-edge** SRV record is resolvable and TCP port 8443 reachable with the SRV Checker in Collaboration Solutions Analyzer (CSA).

If port 8443 is not reachable, this is possibly because a security device (Firewall) blocks the port or a misconfiguration of the Default Gateway (GW) or Static routes in the Exp-E.

2. Unacceptable or No Available Certificate on VCS Expressway

After the Jabber client has received an answer for **_collab-edge**, it then contacts Expressway with Transport Layer Security (TLS) over port 8443 to try to retrieve the certificate from Expressway to set up TLS for communication between the Jabber client and Expressway.

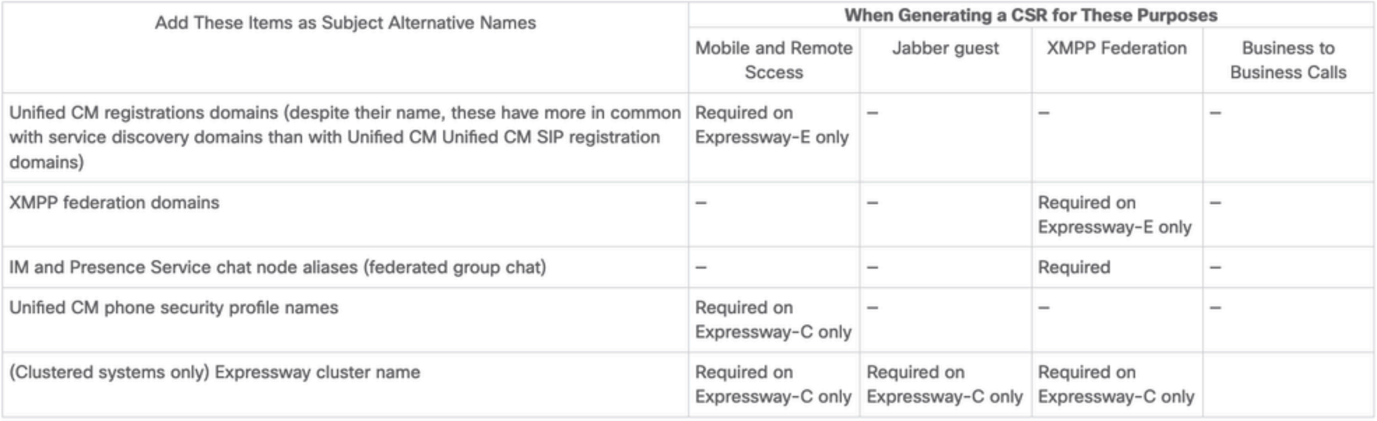
If Expressway does not have a valid signed certificate that contains either the FQDN or domain of Expressway, then this fails and the Jabber client fails to log in.

If this issue occurs, use the Certificate Signing Request (CSR) tool on Expressway, which automatically includes the FQDN of Expressway as a Subject Alternative Name (SAN).

Note: MRA requires secure communication between Expressway-C and Expressway-E, and between Expressway-E and external endpoints.

The next table with the Expressway certificate requirements by feature can be found in the MRA Deployment Guide:

Table 1. CSR Alternative Name Element and Unified Communications Features



Add These Items as Subject Alternative Names	When Generating a CSR for These Purposes			
	Mobile and Remote Sccess	Jabber guest	XMPP Federation	Business to Business Calls
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM Unified CM SIP registration domains)	Required on Expressway-E only	–	–	–
XMPP federation domains	–	–	Required on Expressway-E only	–
IM and Presence Service chat node aliases (federated group chat)	–	–	Required	–
Unified CM phone security profile names	Required on Expressway-C only	–	–	–
(Clustered systems only) Expressway cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C only	

3. No UDS Servers Found in Edge Configuration

After the Jabber client successfully establishes a secure connection with Expressway-E, it asks for its edge configuration (**get_edge_config**). This edge configuration contains the SRV records for **_cuplogin** and **_cisco-uds**. If the **_cisco-uds** SRV records are not returned in the edge configuration, then the Jabber client is not able to proceed with log in.

In order to fix this, make sure that **_cisco-uds** SRV records are created internally and resolvable by Expressway-C.

More information on the DNS SRV records can be found in the MRA Deployment Guide for X8.11.

This is also a common symptom if you are in a dual domain. If you run in a dual domain and find the Jabber client is not returned any User Data Service (UDS), you must confirm that the _cisco-uds SRV records are created in the internal DNS with the external domain.

> **Note**: After Expressway Version X12.5, it is no longer a requirement to add a _cisco-UDS SRV record to the internal DNS. For more information on this enhancement, see the Mobile and Remote Access Through Cisco Expressway Deployment Guide (X12.5).

4. Expressway-C Logs Show This Error: XCP_JABBERD Detail=Unable to connect to host '%IP%', port 7400:(111) Connection Refused

If Expressway-E Network Interface Controller (NIC) is incorrectly configured, this can cause the Extensible Communications Platform (XCP) server to not be updated. If Expressway-E meets these criteria, then you probably encounter this issue:

1. Uses a single NIC.
2. Advanced Networking Option Key is installed.
3. The Use Dual Network Interfaces option is set to **Yes**.

In order to correct this problem, change the Use Dual Network Interfaces option to **No**.

The reason this is a problem is because Expressway-E listens for the XCP session on the wrong network interface, which causes the connection to fail/timeout. Expressway-E listens on TCP port 7400 for the XCP session. You can verify this if you use the **netstat** command from the VCS as root.

5. Expressway-E Server Hostname/Domain Name Does Not Match What is Configured in the _collab-edge SRV

If the Expressway-E Server hostname/domain in the DNS page configuration does not match what was received in the **_collab-edge** SRV answer, the Jabber client is not able to communicate with Expressway-E. The Jabber client uses the xmppEdgeServer/Address element in the **get_edge_config** response to establish the XMPP connection to Expressway-E.

This is an example of what the xmppEdgeServer/Address looks like in the **get_edge_config** response from Expressway-E to the Jabber client:

```
<xmppEdgeServer>
<server>
<address>examplelab-vcse1.example URL</address>
<tlsPort>5222</tlsPort>
</server>
</xmppEdgeServer>
```

In order to avoid this, make sure that the **_collab-edge** SRV record matches the Expressway-E hostname/domain name. Cisco bug ID CSCuo83458 has been filed for this and partial support was added on Cisco bug ID CSCuo82526.

6. Unable to Log In Because of a Current WebEx Connect Subscription

Jabber for Windows logs show this:

```
2014-11-22 19:55:39,122 INFO  [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)]
[service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs
Available] - makeCasLookupForDomain result is  'Code: IS_WEBEX_CUSTOMER; Server:
http://URL server;
Url: http://example URL server';;;.2014-11-22
19:55:39,122 INFO  [0x00002808] [overy\WebexCasLookupDirectorImpl.cpp(67)]
[service-discovery] [WebexCasLookupDirectorImpl::determineIsWebexCustomer] -
Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122
DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)]
[service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_
lookup_url : http://example URL server2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://example URL server/cas/FederatedSSO?org=example URL]2014-11-22
19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)]
[TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist
Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStore
Manager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url]
skipLocal : [0]  value: [http://website URL/cas/FederatedSSO?org=example URL]
success: [true] configStoreName: [LocalFileConfigStore]
```

The log in attempts are directed to WebEx Connect.

For a permanent resolution, you must contact WebEx in order to have the site decommissioned.

Workaround

In the short term, you can utilize one of these options to exclude it from the lookup.

- Add this parameter to the jabber-config.xml. Then upload the jabber-config.xml file to the TFTP server on CUCM. It requires that the client logs in internally first.

  ```
  <?xml version="1.0" encoding="utf-8"?>
  <config version="1.0">
  <Policies>
  <ServiceDiscoveryExcludedServices>WEBEX<
  /ServiceDiscoveryExcludedServices>
  </Policies>
  </config>
  ```

- From an application perspective, run this:
  msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX

Note: The second option does not work for mobile devices.

- Create a clickable URL that excludes the WEBEX service: **ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX**

You can find more details about the UC service discovery and how to exclude some services in On-Premises Deployment for Cisco Jabber 12.8.

7. The Expressway-C Server Displays the Error Message: "Configured but with errors. Provisioning server: Waiting for traversal server info."

If you navigate to **Status > Unified Communications** and see the error message, **"Configured but with errors. Provisioning server: Waiting for traversal server info."** for Unified CM registrations and IM&P Service, the internal DNS server(s) configured on the Expressway-C have two DNS A records for the Expressway-E. The reason behind multiple DNS A records for the Expressway-E could be that the affected user moved from single NIC with static NAT enabled on the Expressway-E to dual-NIC with static NAT enabled, or vice versa, and forgot to delete the appropriate DNS A record in the internal DNS server(s). Therefore, when you use the DNS lookup utility in the Expressway-C and resolve the Expressway-E FQDN, you notice two DNS A records.

Solution

If the Expressway-E NIC is configured for a single NIC with static NAT:

1. Delete the DNS A record for the Expressway-E internal IP address in the DNS server(s) configured in the Expressway-C.
2. Flush the DNS cache in the Expressway-C and the user PC via CMD (**ipconfig /flushdns)**.
3. Reboot the Expressway-C server.

If the Expressway-E NIC is configured for dual NIC with static NAT enabled:

1. Delete the DNS A record for the Expressway-E *external* IP address in the DNS server(s) configured in the Expressway-C.
2. Flush the DNS cache in the Expressway-C and user PC via CMD (**ipconfig /flushdns**).
3. Reboot the Expressway-C server.,

8. Microsoft DirectAccess Installed

If you use Microsoft DirectAccess on the same PC as the Jabber Client, when you attempt to log in remotely, this can break MRA. DirectAccess forces DNS queries to be tunnelled in to the internal network as though the PC used a VPN.

Note: Microsoft DirectAccess is not supported with Jabber over MRA. Any troubleshooting is best effort. Configuration of DirectAccess is the responsibility of the network administrator.

Some times you can successfully block all DNS records in the Microsoft DirectAccess Name Resolution Policy Table. These records are not processed by DirectAccess (Jabber needs to be able to resolve these via public DNS with MRA):

- SRV record for _cisco-uds
- SRV record for _cuplogin
- SRV record for _collab-edge

- A record for all Expressway Es

9. Expressway Reverse DNS Lookups Fails

Beginning in Version X8.8, Expressway/VCS requires forward and reverse DNS entries to be created for ExpE, ExpC, and all CUCM nodes.

For full requirements, see Prerequisites and Software Dependencies in the x8.8 Release Notes and DNS Records for Mobile and Remote Access.

If internal DNS records are not present, there is a possible error in Expressway logs that refer to reverseDNSLookup:

```
2016-07-30T13:58:11.102-06:00 hostname XCP_JABBERD[20026]: UTCTime="2016-07-30 19:58:11,102" 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-C only receives one FQDN when querying the PTR record for the Expressway-E IP. If it receives an incorrect FQDN from DNS, it shows this line in the logs and fail:

```
2020-04-03T17:48:43.685-04:00 hostname XCP_JABBERD[10043]: UTCTime="2020-04-03 21:48:43,685" ThreadID="140028119959296"
Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:601" Detail="Certificate verification failed for host=xx.xx.xx.xx, additional
info: Invalid Hostname"
```

Registration Issues

Softphone is Not Able to Register, SIP/2.0 405 Method Not Allowed

A diagnostic log from Expressway-C shows a **SIP/2.0 405 Method Not Allowed** message in response to the Registration request sent by the Jabber client. This is likely due to a current Session Initiation Protocol (SIP) trunk between Expressway-C and CUCM with port 5060/5061.

<#root>

```
SIP/2.0 405 Method Not Allowed


Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1
ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-
80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=Traversal
Zone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d35
27fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=
7001;ingress-zone=TraversalZone,SIP/2.0/TLS
192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;
ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER

Warning: 399 collabzone "SIP trunk disallows REGISTER"

Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

In order to correct this issue, change the SIP port on the SIP Trunk Security Profile that is applied to the current SIP trunk configured in CUCM and the Expressway-C neighbor zone for CUCM to a different port such as 5065. This is explained further in this video. Here is a configuration summary:

CUCM

1. Create a new SIP Trunk security profile with a listening port other than 5060 (5065).
2. Create a SIP Trunk associated to the SIP Trunk Security Profile and destination set to the Expressway-C IP address, port 5060.

Expressway-C

1. Create a neighbor zone to CUCM(s) with a target port other than 5060 (5065) to match the CUCM configuration.
2. In Expressway-C **Settings** > **Protocols** > **SIP**, make sure Expressway-C still listens on 5060 for SIP.

Softphone is Not Able to Register, Reason="Unknown domain"

A diagnostic log from Expressway-C shows Event=**"Registration Rejected" Reason="Unknown domain"** Service="SIP" Src-ip="XXX.XXX.XXX.XXX" Src-port="51601" Protocol="TCP" AOR="sip:XXX.XXX.XXX.XXX".

In order to correct this issue, check these points:

- Does the Jabber client use a **Secure Device Security Profile** in CUCM when the intention is not to use a non-secure Device Security Profile?
- If the Jabber clients use a secured Device Security Profile, is the name of the security profile in FQDN format and is that FQDN name configured on the Expressway-C certificate as a SAN?
- If the Jabber clients use a secured Device Security Profile, navigate to **System** > **Enterprise Parameters** > **Security Parameters** > **Cluster Security Mode** and check that the Cluster Security Mode is set to 1 in order to verify that the CUCM cluster has been secured. If the value is **0**, the administrator must go through the documented procedure to secure the cluster.

Softphone is Not Able to Register, Reason "Idle countdown expired"

When you review the Expressway-E logs during the timeframe that the Jabber client sends in a REGISTER message, look for an "**Idle countdown expired"** error as indicated in the code snippet here.

<#root>

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG":  Src-ip="

JabberPubIP

" Src-port="4211"
Dst-ip="

VCS-E_IP

" Dst-port="

5061
```

```
" Detail="

TCP Connecting

"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG":  Src-ip="

JabberPubIP

" Src-port="4211" Dst-ip=
"

VCS-E_IP

" Dst-port="

5061

" Detail="

TCP Connection Established

"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG":  Src-port="4211" Dst-ip=
"

VCS-E_IP

" Dst-port="

5061

" Detail="

TCP Connection Closed

" Reason="

Idle
countdown expired

"
```

This snippet indicates that the firewall does have port 5061 open; however, there is no application-layer traffic that is passed over in a sufficent amount of time so the TCP connection closes.

If you encounter this situation, there is a high degree of probability that the firewall in front of Expressway-E has SIP Inspection/Application Layer Gateway (ALG) functionality turned on. In order to remediate this issue, you must diable this functionality. If you are unsure of how to do this, refer to your firewall vendor product documentation.

For more information on SIP Inspection/ALG, you can reference Appendix 4 of the Cisco Expressway-E and Expressway-C-Basic Configuration DeploymentGuide.

MRA Fails Because of Phone Proxy Configured in Firmware

A diagnostic log from the Expressway-E shows a TLS Negotiation Failure in port 5061, however the SSL handshake succeeded in port 8443.

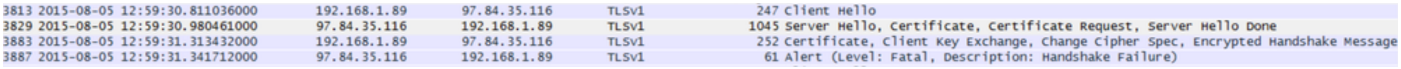
```
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-port="24646"
```

```
Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-port="24646"
Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Established"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="developer.ssl" Level="ERROR"
CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(67)" Method="::TTSSLErrorOutput" Thread="0x7fae4ddb1700":
TTSSL_continueHandshake: Failed to establish SSL connection
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="network.tcp" Level="DEBUG":  Src-port="24646"
Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Closed" Reason="Got EOF on socket"
2015-08-04T10:14:23-05:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP"  Src-port="24646" Dst-ip="10.2.0.2" Dst-
port="5061" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2015-08-04 15:14:23,535"
```

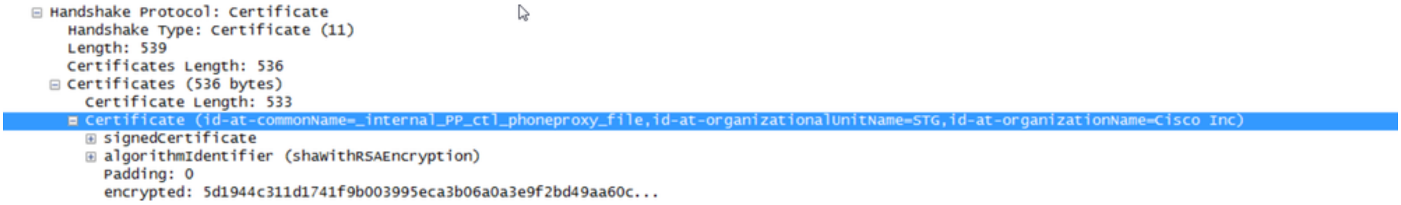
Logs from Jabber:

```
-- 2015-08-04 10:48:04.775 ERROR [ad95000] - [csf.cert.][checkIdentifiers] Verification of identity: 'URL address' failed.
-- 2015-08-04 10:48:04.777 INFO [ad95000] - [csf.cert][handlePlatformVerificationResultSynchronously] Verification result : FAILURE
reason : [CN_NO_MATCH UNKNOWN]
-- 2015-08-04 10:48:05.284 WARNING [ad95000] - [csf.ecc.handyiron][ssl_state_callback] SSL alert read:fatal:handshake failure
type=eSIP, isRelevant=true, server=URL server name:5061, connectionState=eFailed, isEncrypted=true, failureReason=eTLSFailure,
SSLErrorCode=336151568
type=eSIP, isRelevant=true, server=192.168.102.253:5060, connectionState=eFailed, isEncrypted=false, failureReason=eFailedToConnect,
serverType=ePrimary, role=eNone
-- 2015-08-04 10:48:05.287 ERROR [ad95000] - [csf.ecc.handyiron][secSSLIsConnected] SSL_do_handshake() returned : SSL_ERROR_SSL.
```

The packet capture from Jabber shows a SSL negotiation with the Expressway E IP; however the certificate sent does not come from this server:



```
3813 2015-08-05 12:59:30.811036000     192.168.1.89     97.84.35.116     TLSv1        247 Client Hello
3829 2015-08-05 12:59:30.980461000     97.84.35.116     192.168.1.89     TLSv1       1045 Server Hello, Certificate, Certificate Request, Server Hello Done
3883 2015-08-05 12:59:31.313432000     192.168.1.89     97.84.35.116     TLSv1        252 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3887 2015-08-05 12:59:31.341712000     97.84.35.116     192.168.1.89     TLSv1         61 Alert (Level: Fatal, Description: Handshake Failure)
```



```
⊟ Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 539
    Certificates Length: 536
  ⊟ Certificates (536 bytes)
      Certificate Length: 533
    ⊟ Certificate (id-at-commonName=_internal_PP_ctl_phoneproxy_file,id-at-organizationalUnitName=STG,id-at-organizationName=Cisco Inc)
      ⊞ signedCertificate
      ⊞ algorithmIdentifier (shaWithRSAEncryption)
        Padding: 0
        encrypted: 5d1944c311d1741f9b003995eca3b06a0a3e9f2bd49aa60c...
```

The FW has Phone Proxy configured.

Solution:

Confirm that the FW runs Phone Proxy. In order to check that, enter the **show run policy-map** command and it shows you something similar to:

```
class sec_sip
inspect sip phone-proxy ASA-phone-proxy
```

Disable Phone Proxy for phone services to connect successfully.

Call-Related Issues

No Media When You Call Through MRA

These are some of the absentand incorrect configurations that can cause this problem in Single and Dual NIC deployments:

- Static NAT is not configured in the Expressway-E under **System** > **Network Interfaces** > **IP**. NAT at the network layer still needs to be done in the firewall, but this setting translates the IP at the application layer.
- TCP/UDP ports are not open in the firewall. For a list of ports refer to the Cisco Expressway IP Port Usage Configuration Guide.

Single NIC with static NAT deployments are not recommended. Here are some considerations to prevent media issues:

- In the UC traversal zone, Expressway-C needs to point to the public IP address configured in the Expressway-E.
- Media must "hairpin" or reflect in the external firewall. A configuration example with a Cisco ASA Firewall can be found in Configure NAT Reflection On The ASA For The VCS Expressway TelePresence Devices.

More information on this can be found in Appendix 4 of the Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide.

No Ringback When Call Over MRA to PSTN

This issue is due to a limitation on Expressways prior to Version X8.5. Cisco bug ID CSCua72781 describes how Expressway-C does not forward early media in 183 Session Progress or 180 Ringing across the traversal zone. If you run Versions X8.1.x or X8.2.x, you can upgrade to Version X8.5 or alternatively perform the workaround listed here.

It is possible to use a workaround on the Cisco Unified Border Element (CUBE) if you make a SIP profile that turns the 183 into a 180 and applies it on the incoming dial-peer. For example:

```
voice class sip-profiles 11
response 183 sip-header SIP-StatusLine modify "SIP/2.0 183 Session Progress"
"SIP/2.0 180 Ringing"
```

Afterwards they would disable 180 Early Media on either the SIP profile of the **CUCM** > **CUBE** or the CUBE itself within sip-ua configuration mode.

```
disable-early-media 180
```

CUCM and IM&P Issues

ASCII Error That Prevents Addition of CUCM

When you add CUCM to Expressway-C, you encounter an ASCII error that prevents the addition of CUCM.

When Expressway-C adds CUCM to its database, it runs through a series of AXL queries that relate to get and list functions. Examples of these include **getCallManager**, **listCallManager**, **listProcessNode**, **listProcessNodeService**, and **getCCMVersion**. After the **getCallManager** process is run, it is succeeded by an **ExecuteSQLQuery** set to retrieve all CUCM Call Manager-trust or tomcat-trusts.

Once CUCM receives the query and executes on it, CUCM then reports back all of its certificates. If one of the certificates contains a non-ASCII character, Expressway generates an error in the web interface similar to **"ascii codec cannot decode byte 0xc3 in position 42487: ordinal not in range(128)"**.

This issue is tracked with Cisco bug ID CSCuo54489 and is resolved in Version X8.2.

Outbound TLS Failures on 5061 from Expressway-C to CUCM in Secure Deployments

This issue occurs when you use self-signed certificates on CUCM and Tomcat.pem/CallManager.pem have the same subject. The issue is addressed with Cisco bug ID CSCun30200. The workaround to correct the issue is to delete the tomcat.pem and disable TLS Verify from the CUCM configuration on Expressway-C.

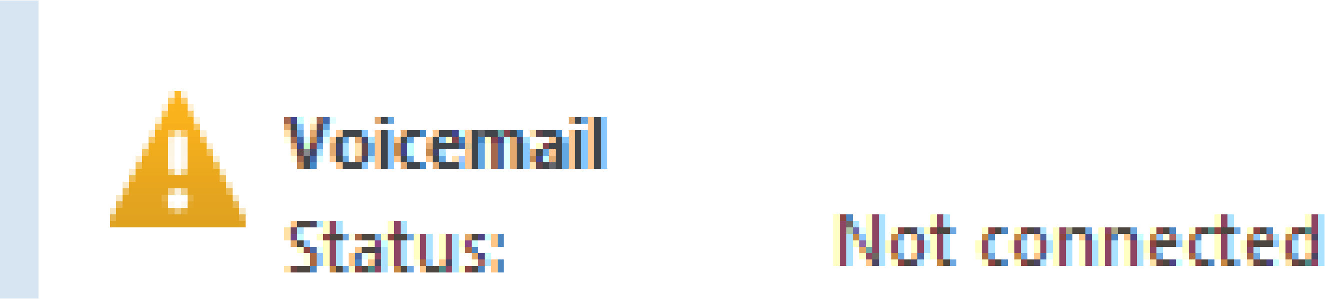
IM&P Server Not Added and Errors Encountered

When you add an IM&P Server, Expressway-C reports "This server is not an IM and Presence Server" or "Unable to communicate with .AXL query HTTP error "HTTPError:500"", which results in the IM&P Server to not be added.

As part of the addition of an IM&P server, Expressway-C uses an AXL query to look for the IM&P certificates in an explicit directory. Due to Cisco bug ID CSCul05131, the certificates are not in that store; therefore, you encounter the false error.

Miscellaneous Issues

Voicemail Status on Jabber Client Shows “Not connected”



Voicemail Status: Not connected

In order to make the Jabber client Voicemail status successfully connect, you must configure the Cisco Unity Connection IP address or hostname within the HTTP allow list on Expressway-C.

In order to complete this from Expressway-C, perform the relevant procedure:

Procedure for Versions X8.1 and X8.2

1. Click **Configuration** > **Unified Communications** > **Configuration** > **Configure HTTP server allow list**.
2. Click **New** > **Enter IP/Hostname** > **Create entry**.
3. Log out of the Jabber client, and then log back in.

Procedure for Version X8.5

1. Click **Configuration > Unified Communications > Unity Connection Servers**.
2. Click **New > Enter IP/Hostname, User account credentials > Add Address**.
3. Log out of the Jabber client, and then log back in.

Contact Photos Do Not Appear on Jabber Clients Through Expressways

The Mobile & Remote Access solution only utilizes UDS for Contact Photo resolution. This requires that you have a web server available to store the photos. The configuration itself is two-fold.

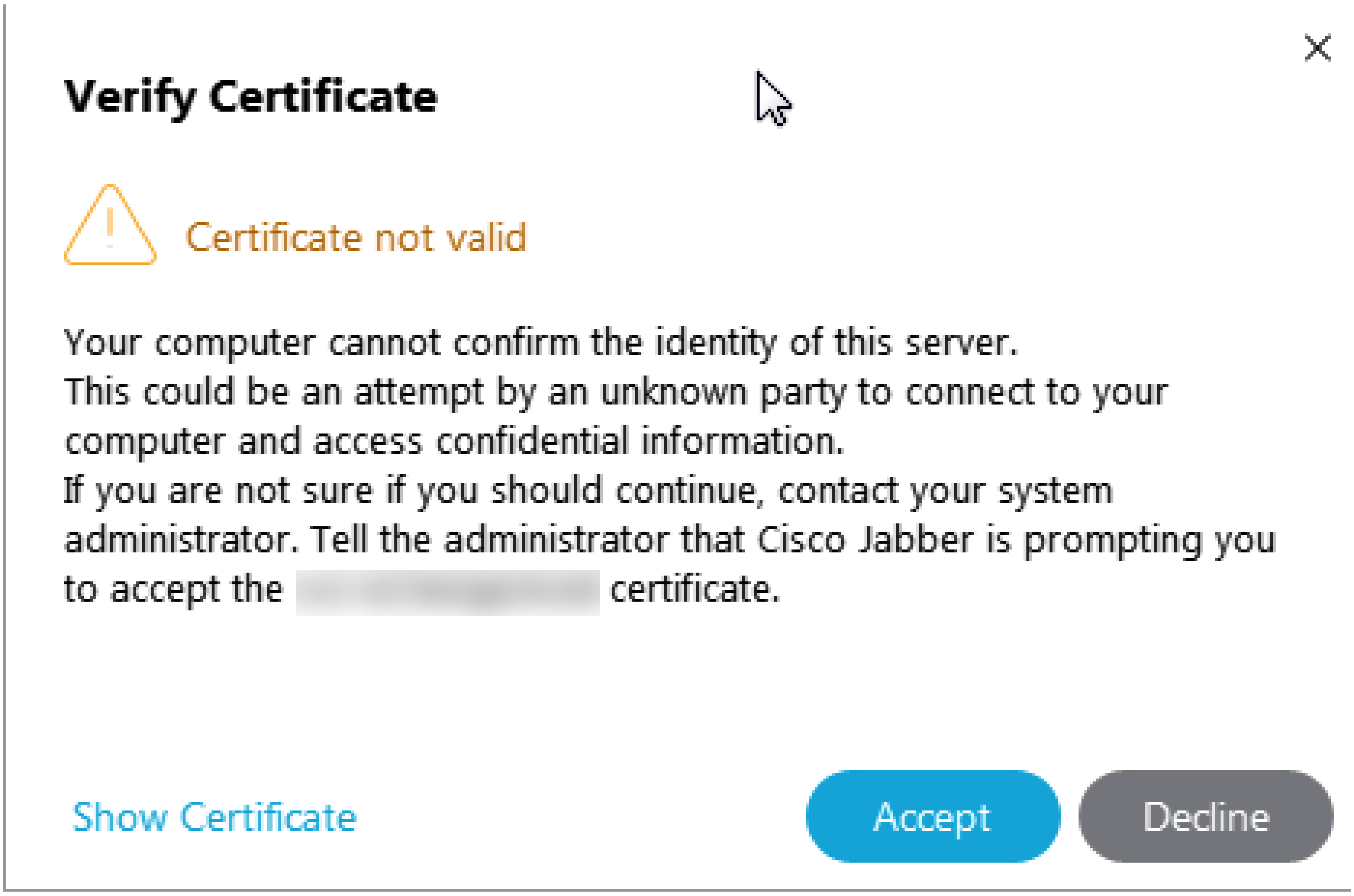
1. The jabber-config.xml file must be modified to direct the clients to the web server for Contact Photo resolution. The configuration here achieves this.

   ```
   <Directory>
   <DirectoryServerType>UDS</DirectoryServerType>
   <PhotoUriWithToken>http://%IP/Hostname%/photo%%uid%%.jpg<
   /PhotoUriWithToken>
   <UdsServer>%IP%</UdsServer>
   <MinimumCharacterQuery>3</MinimumCharacterQuery>
   </Directory>
   ```

2.
   1. Click **Configuration > Unified Communications > Configuration > Configure HTTP server allow list**.
   2. Click **New > Enter IP/Hostname > Create entry**.
   3. Log out of the Jabber client, and then log back in.Expressway-C must have the web server listed within the HTTP Server Allow List.

   Note: For more information on UDS Contact Photo resolution, refer to the Jabber Contact Photo Documentation.

Jabber Clients Are Prompted to Accept the Expressway-E Certificate During Login



Verify Certificate

Certificate not valid

Your computer cannot confirm the identity of this server.
This could be an attempt by an unknown party to connect to your computer and access confidential information.
If you are not sure if you should continue, contact your system administrator. Tell the administrator that Cisco Jabber is prompting you to accept the [redacted] certificate.

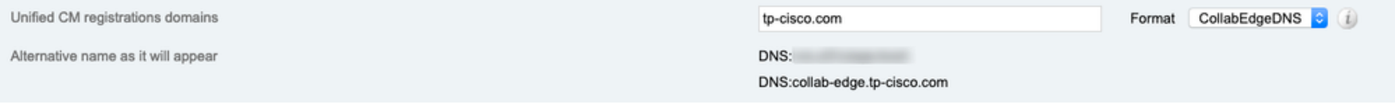
This error message can be related with the Expressway Edge certificate not signed by a public CA that is trusted by the client device or that the domain is absent as a SAN in the server certificate.

In order to stop the Jabber client from the Expressway certificate acceptance prompt, you must meet the two criteria listed below:

- The device/machine that runs the Jabber client must have the signer of the Expressway-E certificate listed within its certificate trust store.

  Note: This is easily accomplished if you use a public certificate authority because mobile devices contain a large certificate trust store.

- The Unified CM registration domain used for the collab-edge record must be present within the SAN of the Expressway-E certificate. CSR tool in the Expressway server gives you the option to add the Unified CM registration domain as a SAN, it is preloaded if the domain is configured for MRA. If the CA that signs the certificate does not accept a domain as a SAN, you can also use the "CollabEdgeDNS" option, which adds the prefix "collab-edge" to the domain:



Unified CM registrations domains: tp-cisco.com Format: CollabEdgeDNS

Alternative name as it will appear: DNS:[redacted]
DNS:collab-edge.tp-cisco.com

Related Information

- [Mobile & Remote Access guide over Expressways](#)

- **Cisco Expressway Certificate Creation and Use Deployment Guide**
- **Cisco TelePresence Video Communication Server (Cisco VCS) IP Port Usage for Firewall Traversal**
- **Deployment and Installation Guide for Cisco Jabber**
- **Technical Support & Documentation - Cisco Systems**