

# Configure and Troubleshoot XMPP Federation on Expressway

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Step 1. Enable XMPP Federation on Expressway E](#)

[Verify the XMPP Configuration on Expressway](#)

[Troubleshoot XMPP Federation on Expressway C and Expressway E](#)

[Step 2. Configure Dialback secret](#)

[Verify the Dialback Secret](#)

[Step 3. Configure Security mode](#)

[Troubleshoot Security Mode](#)

[Common issues:](#)

[Symptom 1: One way messaging. Internet to external doesn't work. IM&P status is active](#)

[Symptom 2: Federation fails, XCP router on CUP is bouncing packets](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes the configuration steps for Extensible Messaging and Presence Protocol (XMPP) federation on Expressway.

## Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

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

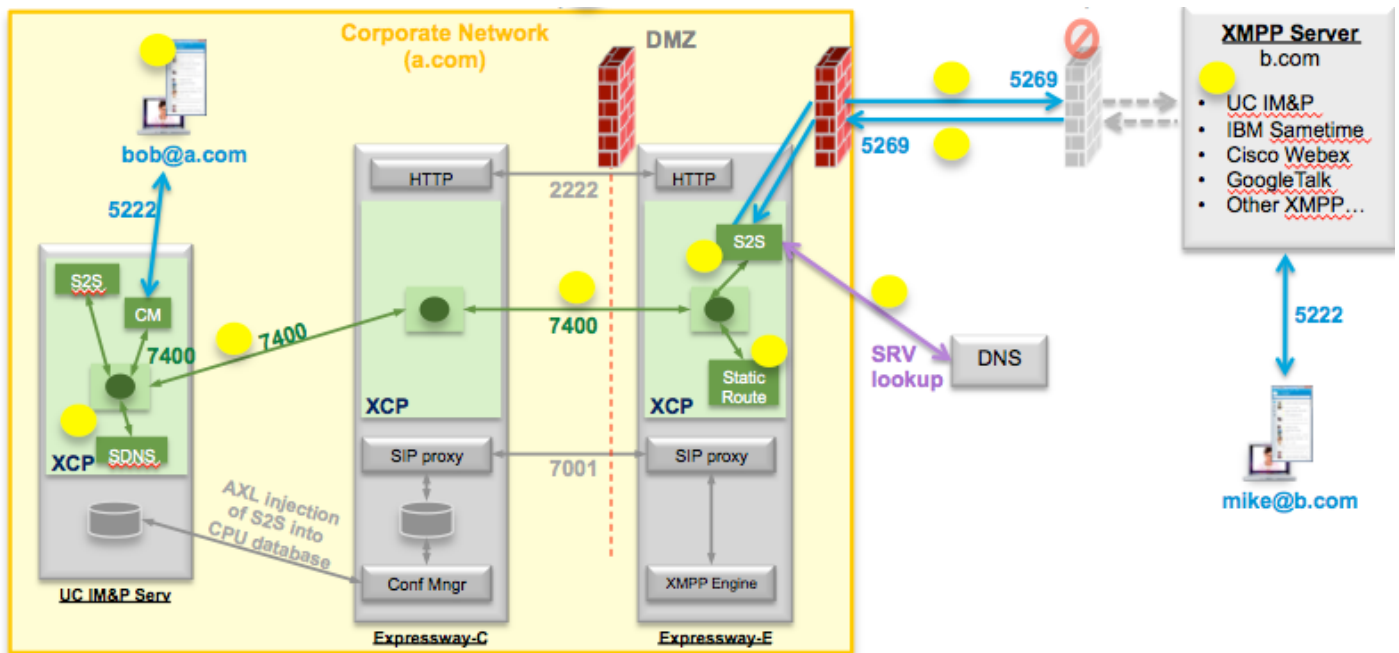
- Cisco Expressway X8.2 or later
- Unified Call Manager(CM) Instant Messenger (IM) and Presence Service 9.1.1 or later

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.

## Background Information

This diagram illustrates the high level communication:



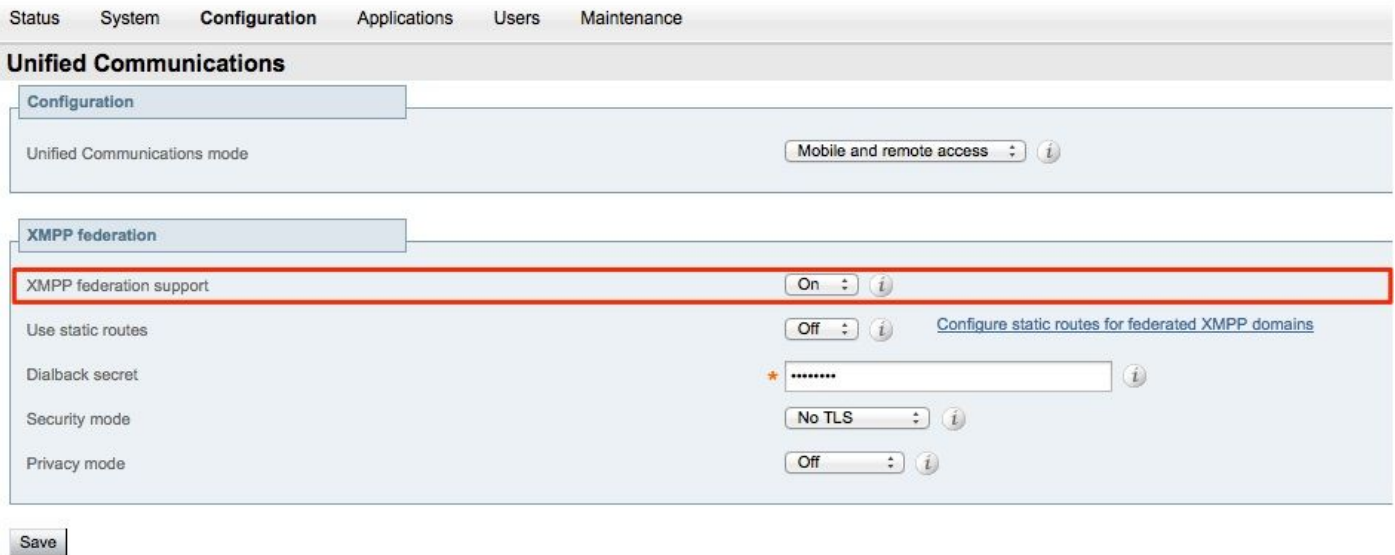
If you enable XMPP Federation on Expressway, the active Server to Server(S2S) moves from Cisco Unified Presence (CUP) to Expressway Edge (Expressway E). This component is manages all XMPP communications between the federated domains.

- S2S uses port 5269 to communicate with the federated domains
- Internal XMPP traffic between XCP routers on ExpresswayE, C and CUP runs on port 7400
- XMPP Provisioning information from Expressway E is send to Expressway C through the SSH tunnel on port 2222
- Expressway C updates CUP with the necessary routing information via AXL port 8443

## Configure

### Step 1. Enable XMPP Federation on Expressway E

Configuration > Unified Communication > XMPP federation support > On



After you enable XMPP federation this will be observed:

1. Expressway-E updates it's local configuration and replicates this setting with Expressway Core (Expressway C).

Expressway E logs will show: "Detail="xconfiguration xcpConfiguration is\_federation\_enabled - changed from: 0 to: 1"

2. Expressway-C updates the "xmpps2snodes" table on the CUP database with the realms of the Expressway E S2S component.

Expressway C logs will show: "Module="network.axl" Level="INFO" Action="Send" URL="<https://cups.ciscotac.net:8443/axl/>" Function="executeSQLQuery"

3. Ensure that the Public DNS is updated with the XMPP server SRV records for all domains with which federation is needed.

`_xmpp-server._tcp.domain.com` on port 5269

### Verify the XMPP Configuration on Expressway

Step 1. Verify if the database changes were succesfully accepted by the IM&P server by running this query from CUP Command Line Interface (CLI) :

```
admin:run sql select * from xmpps2snodes
pkid                cp_id
=====
055c13d9-943d-459d-a3c6-af1d1176936d cm-2_s2scp-1.eft-xwye-a-coluc-com
admin:
```

Step 2. Verify that XMPP federation is off on IM&P server:

**Presence > Inter-Domain Federation > XMPP Federation > Settings > XMPP Federation**

**Node Status > Off**

## **Troubleshoot XMPP Federation on Expressway C and Expressway E**

Step 1. .Enable the DEBUG level log:

On Expressway-E:

**Maintanance > Diagnostics > Advanced > Support Log configuration > developer.clusterdb.restapi**

On Expressway-C:

**Maintanance > Diagnostics > Advanced > Support Log configuration > developer.clusterdb.restapi**

**Maintanance > Diagnostics > Advanced > Network Log configuration > network.axl**

Step 2. Start diagnostic log and TCP dumps on Expressway-C and Expressway-E:

If network issue is suspected perform packet capture on IM&P side from CLI:

```
"utils network capture eth0 file axl_inject.pcap count 1000000 size all"
```

Step 3. Enable the XMPP Federation on Expressway-E

Wait 30sec and next go through the steps described under "Verify the XMPP Configuration on Expressway"

## **Step 2. Configure Dialback secret**

**Configuration > Unified Communication > Dialback Secret**

Status System **Configuration** Applications Users Maintenance ? Help Logout

**Unified Communications** You are here: Configuration > Unified Communications > Configuration

**Success: Saved**

**Configuration**

Unified Communications mode Mobile and remote access ⓘ

**XMPP federation**

XMPP federation support On ⓘ

Use static routes Off ⓘ [Configure static routes for federated XMPP domains](#)

**Dialback secret** \*  ⓘ

Security mode No TLS ⓘ

Privacy mode Off ⓘ

**Save**

---

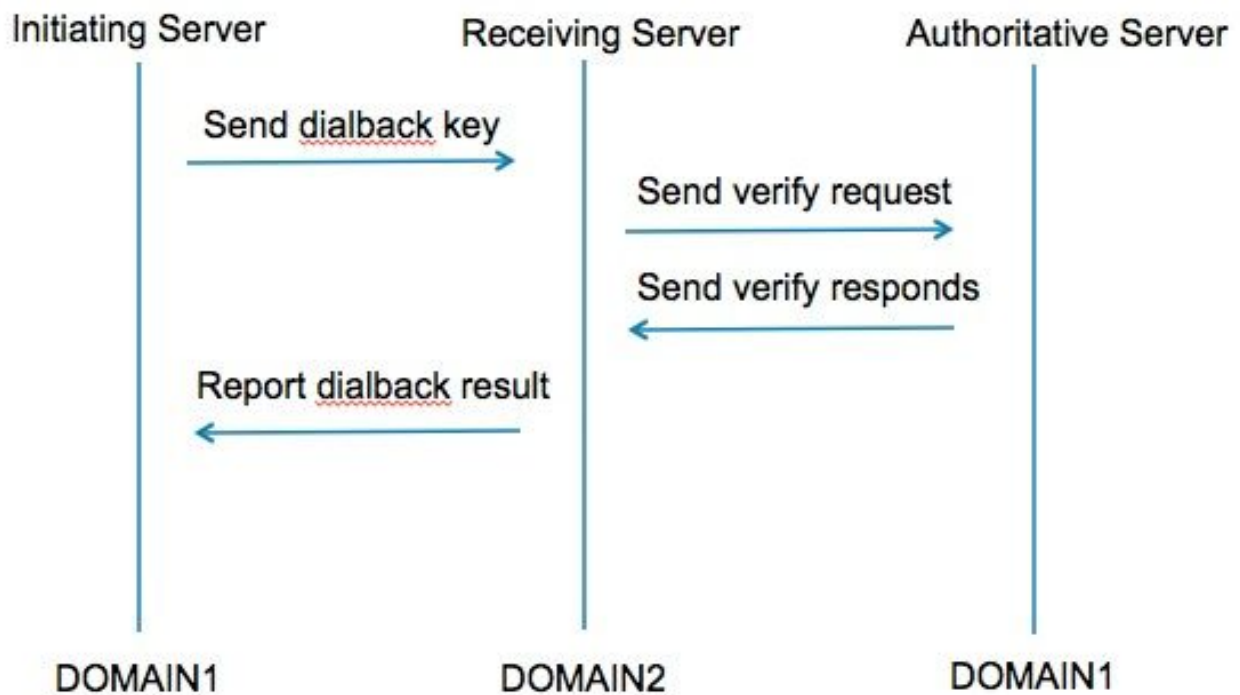
**Unified Communications service configuration status**

SIP registrations and provisioning on Unified CM	Configured ( <a href="#">See Unified Communications status</a> )
IM and Presence services on Unified CM	Configured ( <a href="#">See Unified Communications status</a> )
XMPP federation	Configured ( <a href="#">See Unified Communications status</a> )

**Related tasks**

[View XMPP federation activity in the event log](#)

How does dialback work?



Step 1. The initiating server computes based on the secret configured its dialback result and sends to receiving server.

Step 2. The receiving server will validate this results with the authoritative server from the initiating

domain.

Step 3. As the authoritative server shares the same dialback secret it will be able to validate the result.

Step 4. Once validated the receiving server will accept XMPP from the initiating server.

Step 5. The initiating server performs a lookup against `_xmpp-server._tcp.<target domain>` to find receiving server

Step 6. The receiving server performs a lookup against `_xmpp-server._tcp.<originating domain>` to find the authoritative server

Step 7. The authoritative server can be the same as the initiating server

## Verify the Dialback Secret

### Expressway shows this debug when it is the initiating server:

```
XCP_CM2[12122]:.. Level="INFO " CodeLocation="stanza.component.out"
Detail="xcoder=34A9B60C8 sending:: <db:result from='coluc.com'
to='vngtp.lab'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:result>"
```

```
XCP_CM2[12122]:.. Level="DEBUG" CodeLocation="stream.out" Detail="(00000000-0000-0000-
0000-000000000000, coluc.com:vngtp.lab, OUT) xcoder=34A9B60C8 Scheduling dialback
timeout in 30 secs."
```

```
XCP_CM2[12122]:.. Level="INFO " CodeLocation="ConnInfoHistory" Detail="Connection state
change: PENDING->CONNECTED: ..."
```

### Expressway shows this debug when it is the receiving server:

```
XCP_CM2[22992]:.. Level="VBOSE" CodeLocation="stanza.component.in"
Detail="xcoder=05E295A2B received::
<db:result from='coluc.com'
to='vngtp.lab'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:result>"
```

```
XCP_CM2[22992]:.. Level="INFO " CodeLocation="Resolver.cpp:128" Detail=
"Starting resolver lookup for 'coluc.com:puny=coluc.com:service=_xmpp-server._tcp:default=0"
```

```
XCP_CM2[22992]:.. Level="INFO " CodeLocation="debug" Detail="(e5b18d01-fe24-4290-bba1-
a57788a76468, vngtp.lab:coluc.com, IN)
resolved dialback address for host=coluc.com method=SRV dns-timings=(TOTAL:0.003157
SRV:0.002885)"
```

```
XCP_CM2[22992]:.. Level="INFO " CodeLocation="DBVerify.cpp:270" Detail="(e5b18d01-fe24-
4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN)
DBVerify stream is open. Sending db:verify packet: <db:verify from='vngtp.lab' id='05E295A2B'
to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>"
```

```
XCP_CM2[22992]:.. Level="INFO " CodeLocation="DBVerify.cpp:282" Detail="(e5b18d01-fe24-
4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN)
```

DBVerify Packet Received <db:verify from='coluc.com' id='05E295A2B' to='vngtp.lab' type='valid'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>

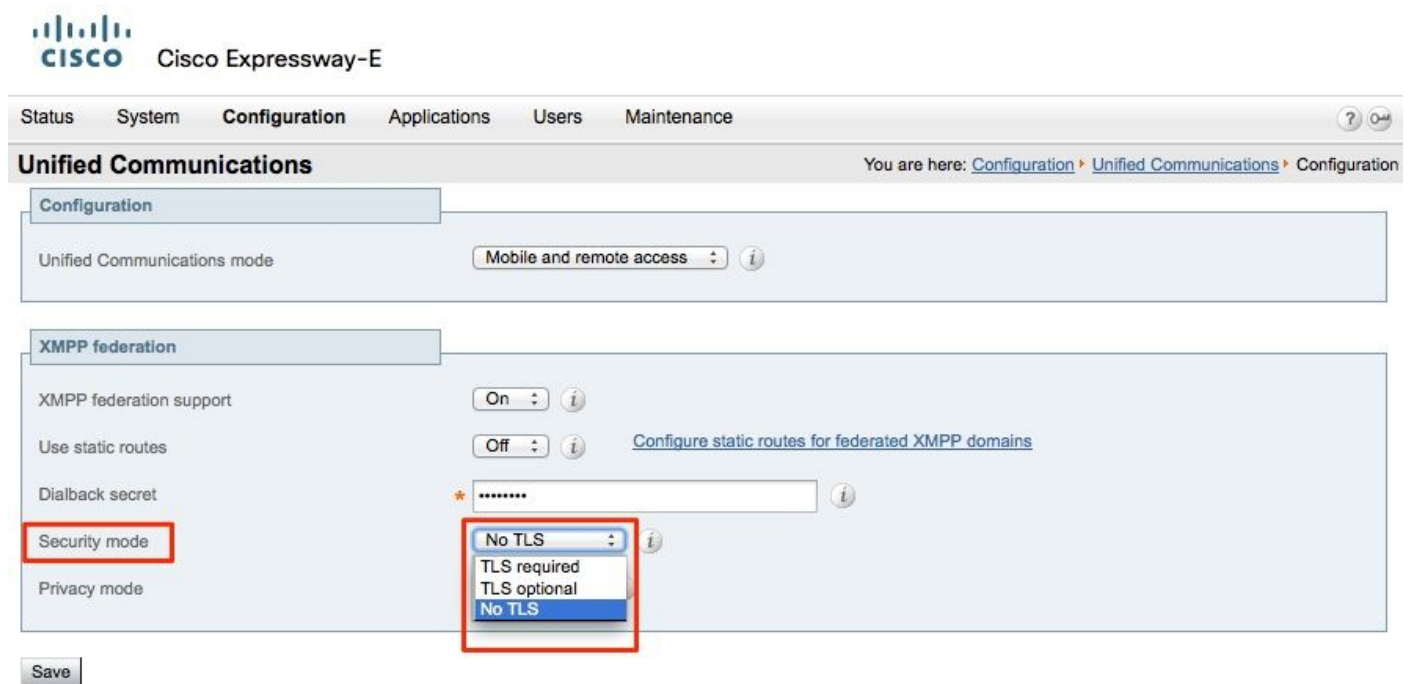
### Expressway shows this debug when it is the authoritative server

XCP\_CM2[5164]:...Level="INFO " CodeLocation="debug" Detail="xcoder=94A9B60C8 onStreamOpen::  
<stream:stream from='vngtp.lab' id='1327B794B' to='coluc.com' version='1.0' xml:lang='en-US.UTF-8' xmlns='jabber:server' xmlns:db='jabber:server:dialback' xmlns:stream='http://etherx.jabber.org/streams'/>"

XCP\_CM2[5164]:...Level="VBOSE" CodeLocation="stanza.component.in" Detail="xcoder=94A9B60C8 received::  
<db:verify from='vngtp.lab' id='05E295A2B' to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>"

XCP\_CM2[5164]:...Level="INFO " CodeLocation="stream.in" Detail="xcoder=94A9B60C8 closing stream used for dialback only"

### Step 3. Configure Security mode



### Troubleshoot Security Mode

- Wireshark can be used to troubleshoot
- Features will show if Transport Layer Security (TLS) is required, OPTIONAL or No TLS

This packet capture excerpt shows an example of when TLS is required:

Source	Destination	Protocol	Length	Info
10.48.36.171	10.48.55.113	TCP	74	30353 > xmpp-server [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1119103043 TSecr=0
10.48.55.113	10.48.36.171	TCP	74	xmpp-server > 30353 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=1119100129 TSecr=1119100129
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1119103043 TSecr=1119100129
10.48.55.113	10.48.36.171	TCP	66	xmpp-server > 30353 [ACK] Seq=1 Ack=204 Win=30080 Len=0 TSval=1119100130 TSecr=1119103044
10.48.55.113	10.48.36.171	XMPP/XML	254	STREAM < coluc.com
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=189 Win=30336 Len=0 TSval=1119103044 TSecr=1119100130
10.48.55.113	10.48.36.171	XMPP/XML	173	FEATURES
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=296 Win=30336 Len=0 TSval=1119103046 TSecr=1119100131
10.48.36.171	10.48.55.113	XMPP/XML	117	STARTTLS
10.48.55.113	10.48.36.171	XMPP/XML	116	PROCEED
10.48.36.171	10.48.55.113	TCP	298	[TCP segment of a reassembled PDU]
10.48.55.113	10.48.36.171	TCP	1434	[TCP segment of a reassembled PDU]
10.48.55.113	10.48.36.171	TCP	1369	[TCP segment of a reassembled PDU]
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=464 Ack=3017 Win=36096 Len=0 TSval=1119103049 TSecr=1119100134
10.48.36.171	10.48.55.113	TCP	640	[TCP segment of a reassembled PDU]
10.48.55.113	10.48.36.171	TCP	292	[TCP segment of a reassembled PDU]
10.48.36.171	10.48.55.113	TCP	298	[TCP segment of a reassembled PDU]
10.48.55.113	10.48.36.171	TCP	113	Application Data
10.48.36.171	10.48.55.113	XMPP Protocol		PROCEED [xmlns="urn:iETF:params:xml:ns:xmpp-tls"] xmlns:urn:iETF:params:xml:ns:xmpp-tls

```

XMPP Protocol
  FEATURES(stream) []
    STARTTLS [xmlns="urn:iETF:params:xml:ns:xmpp-tls"]
      xmlns:urn:iETF:params:xml:ns:xmpp-tls
      REQUIRED
  
```

```

XMPP Protocol
  STARTTLS [xmlns="urn:iETF:params:xml:ns:xmpp-tls"]
    xmlns:urn:iETF:params:xml:ns:xmpp-tls
  
```

When you debug as SSL you see the TLS handshake

Source	Destination	Protocol	Length	Info
10.48.36.171	10.48.55.113	TCP	74	30353 > xmpp-server [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1119103043 TSecr=0
10.48.55.113	10.48.36.171	TCP	74	xmpp-server > 30353 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=1119100129 TSecr=1119100129
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1119103043 TSecr=1119100129
10.48.55.113	10.48.36.171	TCP	66	xmpp-server > 30353 [ACK] Seq=1 Ack=204 Win=30080 Len=0 TSval=1119100130 TSecr=1119103044
10.48.55.113	10.48.36.171	TLSv1.2	254	Continuation Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=189 Win=30336 Len=0 TSval=1119103044 TSecr=1119100130
10.48.55.113	10.48.36.171	TLSv1.2	173	Continuation Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=296 Win=30336 Len=0 TSval=1119103046 TSecr=1119100131
10.48.36.171	10.48.55.113	TLSv1.2	117	Continuation Data
10.48.55.113	10.48.36.171	TLSv1.2	116	Continuation Data
10.48.36.171	10.48.55.113	TLSv1.2	275	Client Hello
10.48.55.113	10.48.36.171	TLSv1.2	1434	Server Hello
10.48.55.113	10.48.36.171	TLSv1.2	1369	Certificate, Server Hello Done
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=464 Ack=3017 Win=36096 Len=0 TSval=1119103049 TSecr=1119100134
10.48.36.171	10.48.55.113	TLSv1.2	640	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10.48.55.113	10.48.36.171	TLSv1.2	292	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
10.48.36.171	10.48.55.113	TLSv1.2	298	Application Data
10.48.55.113	10.48.36.171	TLSv1.2	283	Application Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1270 Ack=3460 Win=41600 Len=0 TSval=1119103110 TSecr=1119100156
10.48.55.113	10.48.36.171	TLSv1.2	113	Application Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1270 Ack=3507 Win=41600 Len=0 TSval=1119103110 TSecr=1119100195
10.48.36.171	10.48.55.113	TLSv1.2	190	Application Data
10.48.55.113	10.48.36.171	TCP	66	xmpp-server > 30353 [ACK] Seq=3507 Ack=1394 Win=33408 Len=0 TSval=1119100236 TSecr=1119103110
10.48.55.113	10.48.36.171	TLSv1.2	218	Application Data

**Common issues:**

**Symptom 1: One way messaging. Internet to external doesn't work. IM&P status is active**

On Expressway-C logs:

"Function="executeSQLQuery" Status="401" Reason="None"

**Cause 1:** Wrong credentials for the IM&P user on Expressway-C side.

This can also be verified by running this URL and login with the credentials as configured on Expressway C

**Configuration > Unified Communications > IM and Presence Servers**

[https://cups\\_address.domain.com:8443/axl](https://cups_address.domain.com:8443/axl)

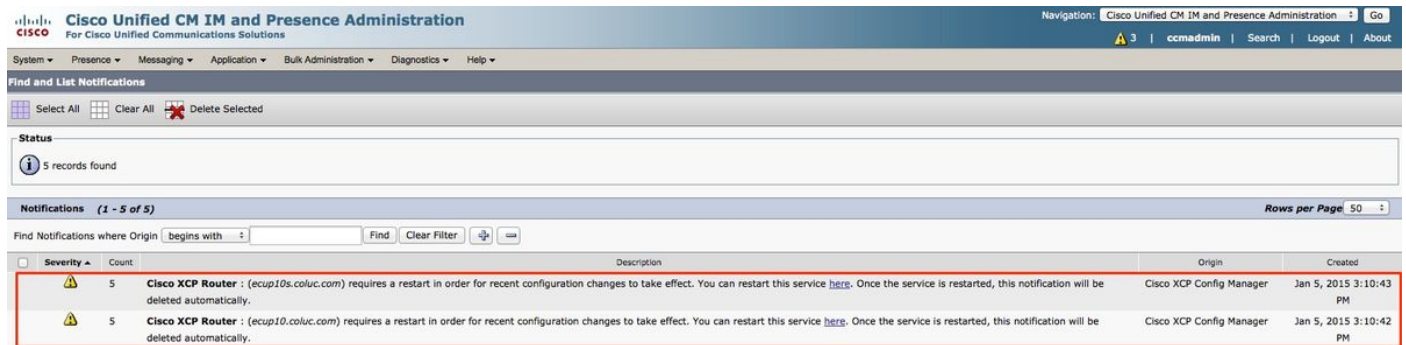


**Solution 1** : Update password, refresh CUP server discovery

## Symptom 2: Federation fails, XCP router on CUP is bouncing packets

**Cause 2** : XCP Router on CUP has not been restarted

This can be verified on CUP **Administration** under the **Notifications** page.



The screenshot shows the Cisco Unified CM IM and Presence Administration interface. The top navigation bar includes "System", "Presence", "Messaging", "Application", "Bulk Administration", "Diagnostics", and "Help". The main content area is titled "Find and List Notifications" and shows a status of "5 records found". Below this, there is a search bar and a table of notifications. The table has columns for "Severity", "Count", "Description", "Origin", and "Created". Two notifications are listed, both with a severity of 5 and a count of 5. The description for both notifications is: "Cisco XCP Router : (ecup10s.coluc.com) requires a restart in order for recent configuration changes to take effect. You can restart this service [here](#). Once the service is restarted, this notification will be deleted automatically." The origin for both is "Cisco XCP Config Manager" and the creation time is "Jan 5, 2015 3:10:42 PM".

Severity	Count	Description	Origin	Created
5	5	Cisco XCP Router : (ecup10s.coluc.com) requires a restart in order for recent configuration changes to take effect. You can restart this service <a href="#">here</a> . Once the service is restarted, this notification will be deleted automatically.	Cisco XCP Config Manager	Jan 5, 2015 3:10:42 PM
5	5	Cisco XCP Router : (ecup10s.coluc.com) requires a restart in order for recent configuration changes to take effect. You can restart this service <a href="#">here</a> . Once the service is restarted, this notification will be deleted automatically.	Cisco XCP Config Manager	Jan 5, 2015 3:10:42 PM

**Solution 2** : Restart XCP router on CUP

Sometimes there will be no notification, but the XCP Router log on CUP is still bouncing packets. If restarting the XCP Router service does not resolve this, rebooting the IM&P Cluster does.

## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)