

# Configure CMS WebRTC or Web App Proxy over Expressway

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configuration Steps](#)

[Step 1. Integrate CMS WB onto Expressway-C](#)

[Step 2. Enable TURN on the Expressway-E and Add the Authentication Credential to the Local Authentication Database](#)

[Step 3. Change the Administration Port of the Expressway-E](#)

[Step 4. Add the Expressway-E as TURN Server\(s\) for Media NAT Traversal onto the CMS Server](#)

[Verify](#)

[Step 1. On Expressway-C, Check that the WB is Correctly Integrated](#)

[Step 2. Verify that the TURN Server has been Added to the CMS Server](#)

[Step 3. Verify TURN Relay Usage during Ongoing call](#)

[Troubleshoot](#)

[External WebRTC Client Connects but no Media \(Due to ICE Failure\)](#)

[External WebRTC Client does not Get Join Call Option](#)

[External WebRTC Client Stuck \(on Loading media\) when Connecting to Cospace and then Gets Redirected to the WB Initial Page](#)

[External WebRTC Client unable to Join Cospace and Gets the Warning \(Unable to Connect - Try Again Later\)](#)

[Related Information](#)

## Introduction

This document describes the steps to configure and troubleshoot Cisco Meeting Server (CMS) WebRTC over Expressway.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Expressway X12.6.1 and later (x12.6.1 and later can only work with CMS 2.9.2 or later due to changes in Exp TURN behavior)
- CMS server 2.9.3 and later
- Network Address Translation (NAT)
- Traversal Using Relays (TURN) around NAT
- Session Traversal Utilities (STUN) for NAT
- Domain Name System (DNS)

## Configuration prerequisites:

- Basic Mobile and Remote Access (MRA) related settings (UC Traversal zone, SSH tunnels) must already be enabled and configured on the Expressway, [click here](#) for MRA guides.
- For CMS 2.9.x - WebBridge (WB), XMPP and CallBridge configured and enabled on CMS, see the [configuration guide](#)
- TURN option key installed on the Expressway-E.
- TCP Port 443 opened on Firewall from the public internet to the Expressway-E's public IP address.
- TCP and UDP Port 3478 (TURN requests) opened on Firewall from Public Internet to the Expressway-E's public IP address.
  - TCP 3478 only needed if 'turnservers' in CMS API has tcpPortNumberOverride set to 3478.
- UDP Port 3478 (TURN requests) opened on Firewall from CMS to the Expressway-E's private IP address (if you use Dual-NIC on the Expressway-E).
  - CMS 2.9.2 and earlier sends Binding Requests to the Exp E, while 2.9.3 onward sends Allocate Requests
- External DNS records for the Join URL for webbridge, resolvable to the Expressway-E's public-facing IP address.
- Internal DNS record for Join URL resolvable to the webbridge server's IP address.
- If running X12.5.2 or earlier, ensure NAT reflection allowed on external firewall for Expressway-E's Public IP address, [click here](#) for example configuration. As of X12.5.3, this is no longer needed for a standalone Expressway.
- When using port 443 for TURN, you still need to open UDP port 3478 for media on the external firewall.

---

**Caution:** When TCP port 443 is enabled, the Expressway can no longer respond on TCP port 3478.

---

**Note:** Expressway pair which is used for Jabber Guest services cannot be used for CMS WebRTC proxy services.

---

**Note:** If upgrading to 3.0 or later from previous versions, please refer to [Guidance for Smooth Upgrade from Cisco Meeting Server 2.9 to 3.0 \(and Onwards\)](#)

---

## Components Used

This document is not restricted to specific software and hardware versions, however, the minimum software version requirements must be met.

- CMS Application Program Interface (API)
- Expressway
- CMS Server

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

WebRTC proxy support has been added to Expressway from Version X8.9.2 which enables off-premise users to browse to a Cisco Meeting Server Web Bridge.

External clients and guests can manage or join spaces without the need of any software other than a

supported browser. [Click here](#) for a list of supported browsers.

As of February 5, 2021, these are the supported browsers for CMS 3.1.1:

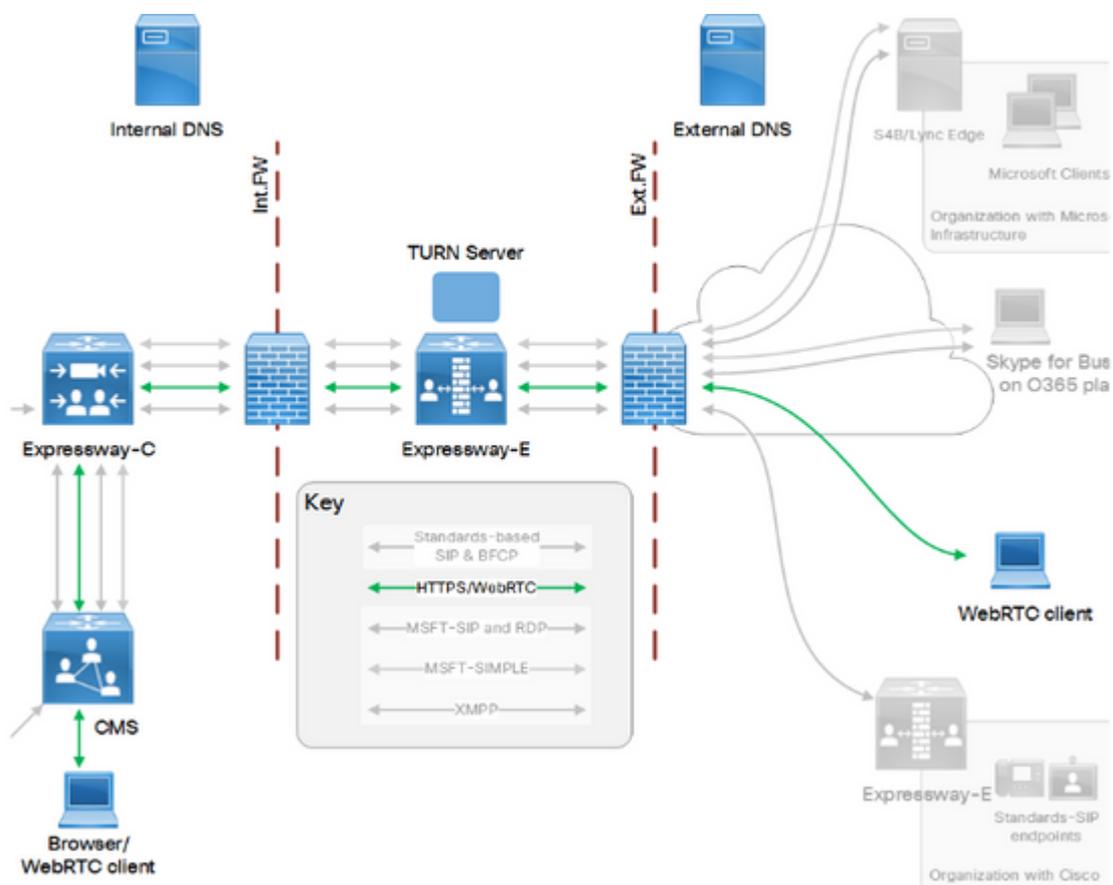
Browsers	Versions
Google Chrome (Windows, macOS and Android)	85
Microsoft Edge (Windows)	82
Chromium-based Microsoft Edge (Windows)	88
Apple Safari for macOS	13.1 and 14.0
Apple Safari for iOS	iOS versions: 13.x and 14.0
Yandex (Windows)	20.8 and 20.11

Note: Web app is not supported on the legacy Microsoft Edge.

Note: Web app is not supported on virtual machines (VMs) running these supported browsers.

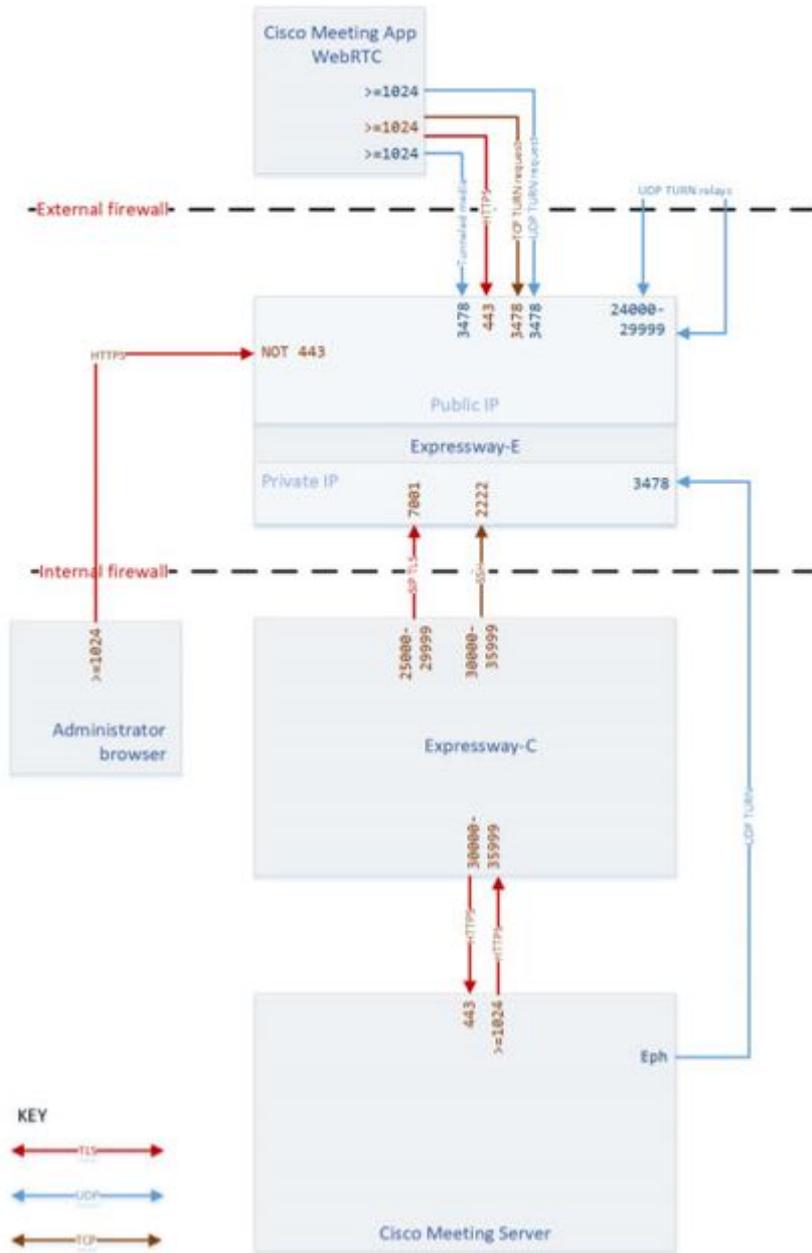
## Configure

### Network Diagram



This image provides an example of connections flow of Web Proxy for CMS WebRTC: (from Exp IP port Usage [configuration guide](#)).

## Web Proxy for Cisco Meeting Server Connections



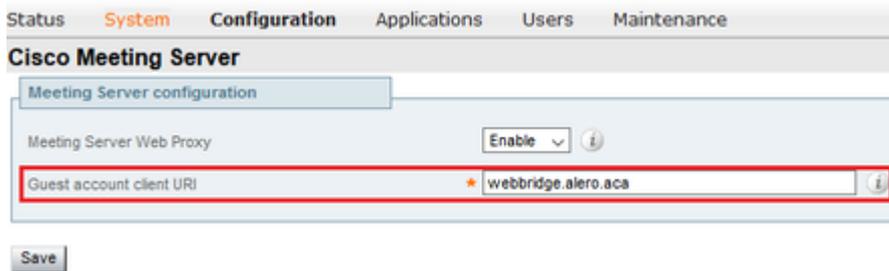
**Note:** When running X12.5.2 or earlier, you must configure your external firewall to allow NAT reflection for the Expressway-E& public IP address (firewalls typically mistrust packets which have the same source and destination IP address). As of X12.5.3, this is no longer needed for a standalone Expressway.

## Configuration Steps

### Step 1. Integrate CMS WB onto Expressway-C

- Navigate to **Configuration > Unified Communication > Cisco Meeting Server**.
- Enable **Meeting Server Web Proxy**.

- c. Enter the Join URL in the **Guest account client URI** field.
- d. Click **Save**.
- e. Add the CMS Join URL onto the Expressway-E server certificate as a Subject Alternative Name (SAN). See the [Cisco VCS Certificate Creation and Use Deployment Guide](#).



## Step 2. Enable TURN on the Expressway-E and Add the Authentication Credential to the Local Authentication Database

- a. Navigate to **Configuration > Traversal > TURN**.
- b. Enable **TURN services**, from **off** to **on**.
- c. Choose **Configure TURN client credentials on local database** and add the credentials (username and password).

---

**Note:** If you have a cluster of Expressway-Es and they are all to be used as TURN servers, then ensure that you enable it on all the nodes. You must configure two separate turnServer instances over API, and point them to each of the Expressway-E servers in the cluster (as per the configurational process shown in Step 4, which shows the process for one Expressway-E server; the second turnServer's configuration would be similar, only using the respective IP addresses and turn credentials for the other Expressway-E server).

---

**Note:** You can use a network load balancer in front of your expressways for TCP/HTTPS traffic, but TURN media must still go from client to TURN servers public IP. TURN media must not pass through the network load balancer

---

## Step 3. Change the Administration Port of the Expressway-E

This step is required since webrtc connections come in on TCP 443, but Exp 12.7 introduced a new Dedicated Management Interface (DMI) that can be used for 443.

- a. Navigate to **System > Administration**.
- b. Under **Web server configuration**, change the **Web administrator port** to **445** from the drop-down options, then click **Save**.
- c. Repeat steps 3a to 3b on all Expressway-Es used for WebRTC proxy services.

---

**Note:** Cisco recommends the administration port be changed because WebRTC clients use 443. If the WebRTC browser tries to access port 80, the Expressway-E redirects the connection to 443.

---

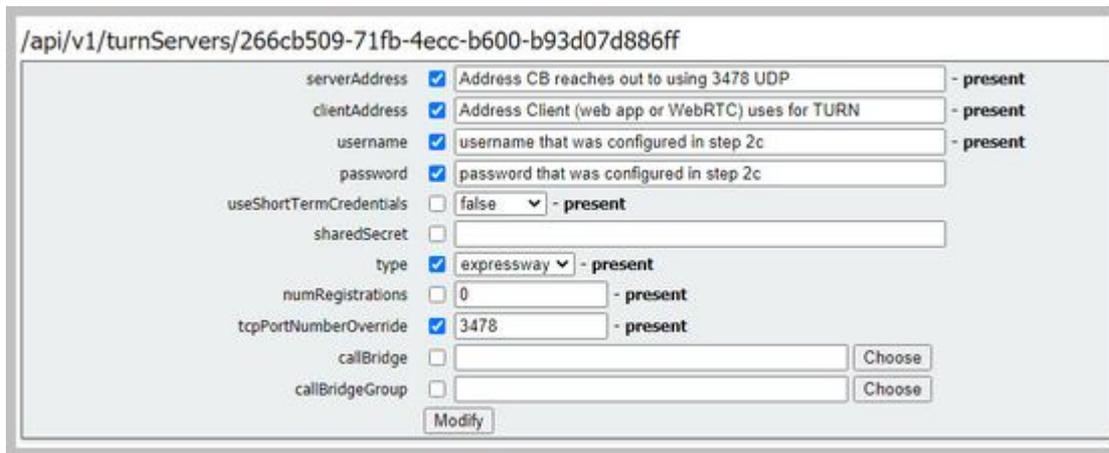
## Step 4. Add the Expressway-E as TURN Server(s) for Media NAT Traversal onto the CMS Server

In CMS 2.9.x onward, use the **Configuration --> API** menu to add turn servers:

- serverAddress: (Private IP address of Expressway)
- clientAddress: (Public IP address of Expressway)
- type: (expressway)
- username: (as configured in step 2c)
- password: (as configured in step 2c)
- tcpPortNumberOverride: 3478

d. Repeat step 4c for every Expressway-E server to be used for TURN

This image provides an example of the configurational steps:



The screenshot shows the configuration page for a TURN server, titled `/api/v1/turnServers/266cb509-71fb-4ecc-b600-b93d07d886ff`. The page contains several configuration fields, each with a checkbox and a text input field. The fields are:

- `serverAddress`:  Address CB reaches out to using 3478 UDP - present
- `clientAddress`:  Address Client (web app or WebRTC) uses for TURN - present
- `username`:  username that was configured in step 2c - present
- `password`:  password that was configured in step 2c
- `useShortTermCredentials`:  false - present
- `sharedSecret`:
- `type`:  expressway - present
- `numRegistrations`:  0 - present
- `tcpPortNumberOverride`:  3478 - present
- `callBridge`:  Choose
- `callBridgeGroup`:  Choose

At the bottom of the form, there is a `Modify` button.

## Verify

Use this section in order to confirm that your configuration works properly.

### Step 1. On Expressway-C, Check that the WB is Correctly Integrated

a. Navigate to **Configuration > Unified Communication > Cisco Meeting Server**. You must see the IP address of the WB:

**Cisco Meeting Server** You are here: [C](#)

Meeting Server configuration

Meeting Server Web Proxy Enable

Guest account client URI \*

Guest account client URI resolved to the following targets	
Name	Address
webbridge.alero.aca	10.48.36.5

b. Navigate to **Configuration > Unified Communication > HTTP allow list > Automatically added rules**. Check that this has been added to the rules:

Meeting Server web bridges	https	443	Prefix	/	GET, POST, PUT, HEAD, DELETE
Meeting Server web bridges	wss	443	Prefix	/	GET, POST, PUT, HEAD, DELETE

**Note:** It is not expected to find the WB in the Discovered nodes because the rules are simply to allow for the proxy of HTTPS traffic to the WB, and not necessarily for unified communication.

c. Check that the Secure Shell (SSH) tunnel for the WB FQDN has been built on Expressway-C to the Expressway-E, and that it is active. Navigate to **Status > Unified Communications > Unified Communications SSH tunnels status**. You must see the FQDN of the WB, and the target must be the Expressway-E.

Status System Configuration Applications Users Maintenance

**Unified Communications SSH tunnels status** You are here: [Status](#) > [Unified Communications](#)

Target	Domain	Status
vcs-e.alero.local	webbridge.alero.aca	Active
vcs-e.alero.local	alero.lab	Active
vcs-e.alero.local	alero.local	Active
vcs-e2.alero.local	alero.lab	Active
vcs-e2.alero.local	webbridge.alero.aca	Active
vcs-e2.alero.local	alero.local	Active

**Step 2. Verify that the TURN Server has been Added to the CMS Server**

In the CMS API menu, look up the turn servers, and click on each one. Within each object, there is a link to check the status:

Related objects: [/api/v1/turnServers](#)  
[/api/v1/turnServers/266cb509-71fb-4ecc-b600-b93d07d886ff/status](#)

Table view XML view

Object configuration	
serverAddress	10.0.0.36
clientAddress	175.12.5.1
numRegistrations	0
username	cmsturn
useShortTermCredentials	false
type	expressway
tcpPortNumberOverride	3478

The output displays information which includes the Round-trip time (RTT) in milliseconds (Ms) associated the TURN server. This information is important to the CB selection of the best TURN server to use.

### Step 3. Verify TURN Relay Usage during Ongoing call

At the time that a live call that is made with the use of the WebRTC client, you can view the TURN media Relay status on the Expressway. Navigate to **Status > TURN relay usage**, then choose **view**.

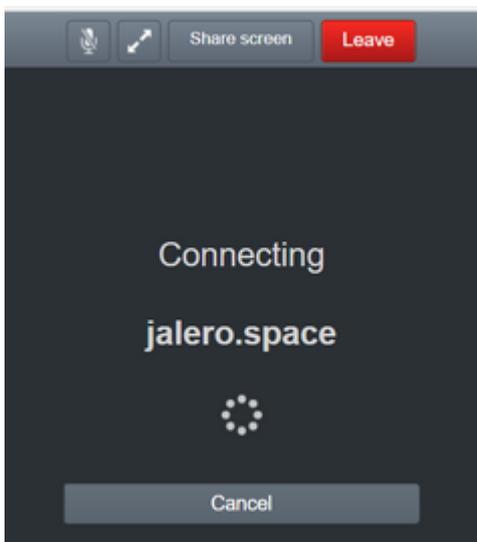
## Troubleshoot

Useful tools:

- HAR file from browsers ([How to generate a HAR file in Chrome or Firefox](#))
- WebRTC internals dump from browser - chrome://webrtc-internals or edge://webrtc-internals - Create dump as soon as Join is attempted.
- Browser console logs can be helpful too.
- Wireshark capture from the client, Exp E, Exp C and CMS.
- Exp E network.http.trafficserver debugs help with websocket troubleshooting.

### External WebRTC Client Connects but no Media (Due to ICE Failure)

In this scenario, the RTC client is able to resolve the Call ID to jalero.space, but when you enter your name and select **Join call**, the client displays **Connecting**, as shown in this image:



After about 30 seconds, it is redirected to the initial WB page.

In order to troubleshoot, complete these steps:

- Start Wireshark on the RTC client when you attempt a call and when the failure occurs, stop the capture.
- After the issue occurs, check the CMS Event logs:

Navigate to **Logs > Event logs** on the CMS WebAdmin.

- Filter the Wireshark traces with stun. See this example:



In the Wireshark traces, you see that the client sends **Allocate Request** with the credentials configured, to the Expressway-E TURN server on port 3478:

```
1329    2017-04-15 10:26:42.108282    10.55.157.229    10.48.36.248    STUN    186
    Allocate Request UDP user: expturncreds realm: TANDBERG with nonce
```

The server replies with **Allocate Error**:

```
1363    2017-04-15 10:26:42.214119    10.48.36.248    10.55.157.229    STUN    254
    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 431
    (*Unknown error code*) Integrity Check Failure
```

or

```
3965    2017-04-15 10:34:54.277477    10.48.36.248    10.55.157.229    STUN    218
    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 401
    (Unauthorized) Unauthorized
```

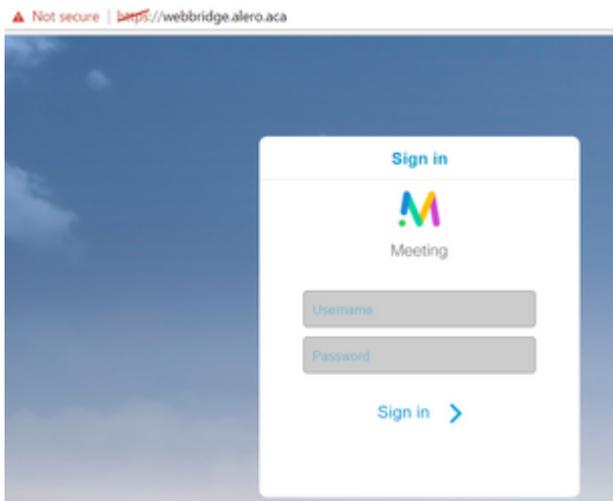
In the CMS logs, this log message is shown:

```
2017-04-15    10:34:56.536    Warning    call 7: ICE failure 4 (unauthorized - check credentials)
```

**Solution:**

Check the TURN credentials configured on the CMS, and ensure that it matches that which is configured on the Expressway-E local authentication database.

**External WebRTC Client does not Get Join Call Option**



On the Callbridge **Status > General** page, this is displayed:

```

2017-04-15 12:09:06.647 Web bridge connection to "webbridge.alero.aca" failed (DNS failure)
2017-04-15 12:10:11.634 Warning web bridge link 2: name resolution for "webbridge.alero.aca" fa
2017-04-15 11:55:50.835 Info failed to establish connection to web bridge link 2 (unknown error

```

Solution:

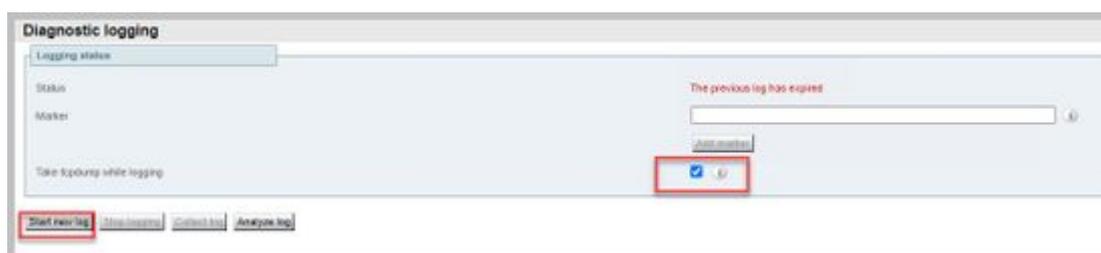
- Ensure that the Callbridge can resolve the Join URL to the webbridge FQDN (the Callbridge must not resolve this to the Expressway-E's IP address).
- Flush the DNS cache on the Callbridge, via Command line interface (CLI), with the command **dns flush**.
- Ensure that the WB trusts the Callbridge server certificate (not the issuer).

### External WebRTC Client Stuck (on Loading media) when Connecting to Cospace and then Gets Redirected to the WB Initial Page

Solution:

- Ensure that CMS can resolve the \_xmpp-client SRV record on the internal network for the CB domain, and make sure that WebRTC connections work internally.
- Collect a Wireshark capture on the client and Diagnostic logging including tcpdump on the Expressway-E while attempting to connect with the External client:

Navigate to **Maintenance > Diagnostics > Diagnostic logging** and ensure that **Take tcpdump while logging** is checked, as shown in this image, prior to you selecting **Start new log**:




---

**Note:** Ensure that the Wireshark capture on the client's device and the logging on the Expressway-E

---

---

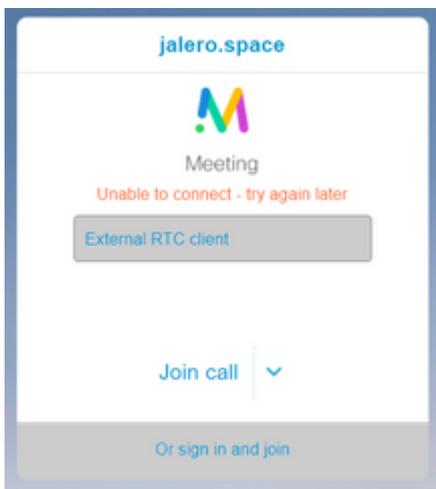
are started before reproducing the failing call. When the failing call has been reproduced, stop and download the logging on the Expressway-E and the capture on the client.

---

- Extract/unzip the log bundle downloaded from the Expressway-E and open the .pcap file taken on the Public-facing interface.
- Filter on both packet captures with stun:
  - Then look for the binding request from the External client to the Expressway-E Public IP address, right-click and select **Follow > UDP Stream**.
  - Usually the destination port of the Binding request from the client would be in the range of 24000-29999, which is the TURN relays port range on the Expressway-E.
- If no response to the Binding requests is received on the client's side, check on the Expressway-E's capture if the requests are arriving.
- If the requests are arriving and the Expressway-E is replying to the client, check if the External FW is allowing the outbound UDP traffic.
- If the requests are not arriving, check the FW to ensure that the port range previously listed is not blocked.
- If the Expressway-E is deployed with a Dual Network Interface Controller (DUAL-NIC) with static NAT mode enabled and is X12.5.2 or earlier, then ensure that NAT reflection is supported and configured on your External FW. As of X12.5.3 this is no longer needed for a standalone Expressway.

### External WebRTC Client unable to Join Cospace and Gets the Warning (Unable to Connect - Try Again Later)

In this scenario, the RTC client is able to resolve the Call ID to jalero.space, but when you enter your name and select **Join call**, the warning **Unable to connect - try again later** is displayed immediately:



Solution:

Check that CMS, on the internal network, is able to always resolve the \_xmpp-client SRV record for the CB domain.

## Related Information

- [VCS/Expressway IP Port Usage Guide](#)
- [Technical Support & Documentation - Cisco Systems](#)