Configure CMS WebRTC Proxy over Expressway

Contents

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 X8.9.2 and later
- CMS server 2.1.4 and later

- Network Address Translation (NAT)
- Traversal Using Relays around NAT (TURN)
- Session Traversal Utilities for NAT (STUN)
- Domain Name System (DNS)

Configuration prerequisites:

- Basic Mobile and Remote Access (MRA) related settings (UC Traversal zone, SSH tunnels) must be already enabled and configured on the Expressway, click here for MRA guides
- WebBridge (WB), Extensible Messaging and Presence Protocol (XMPP) and CallBridge configured and enabled on CMS, click here for 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 and 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)
- External DNS records for the FQDN of the WebBridge, resolvable to the Expressway-E's public-facing IP address
- Internal DNS record WB FQDN resolvable to the CMS server's IP address
- NAT reflection allowed on external firewall for Expressway-E's Public IP address, click here for example configuration

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

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)
- Postman (API Client)
- 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.

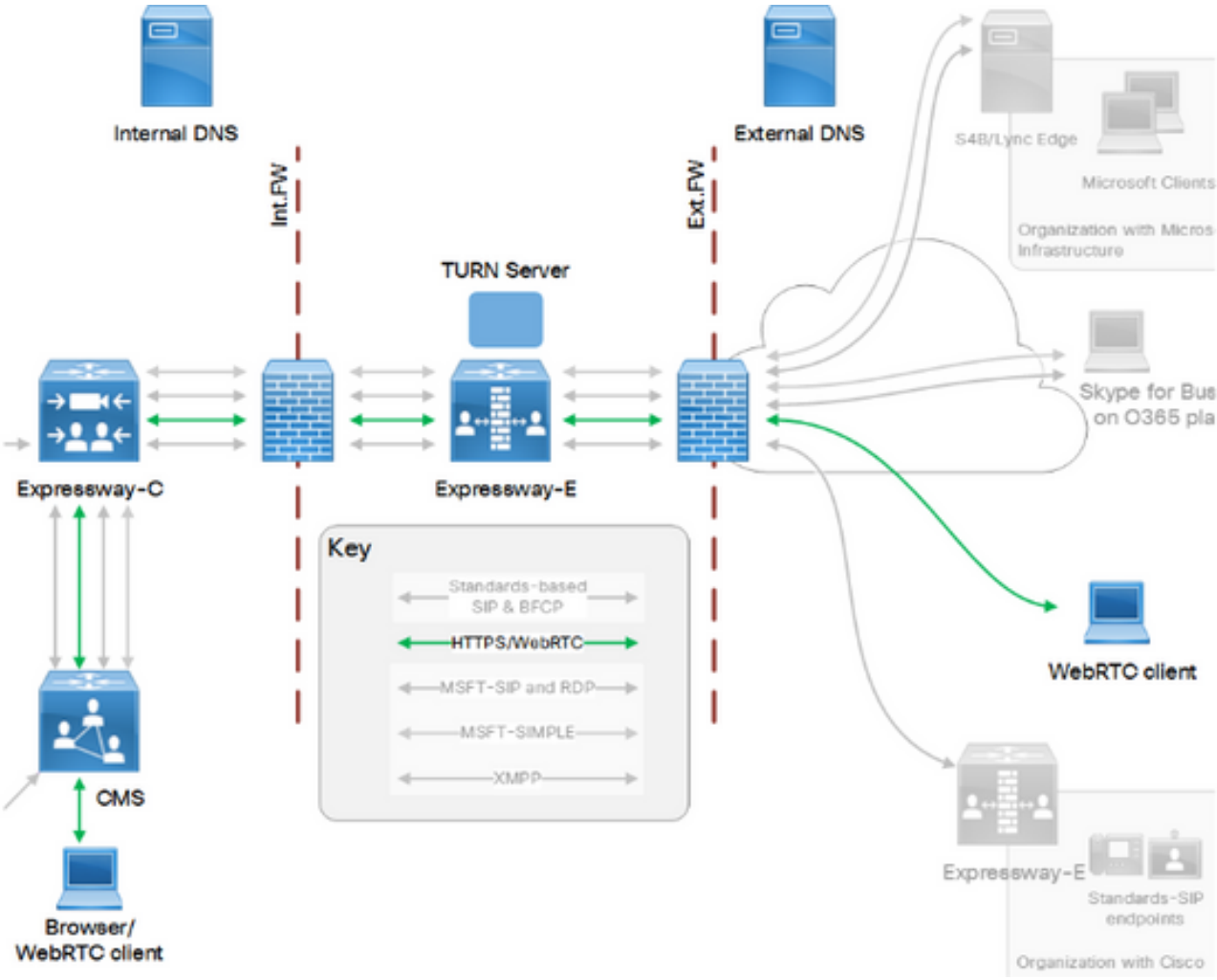
Background Information

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

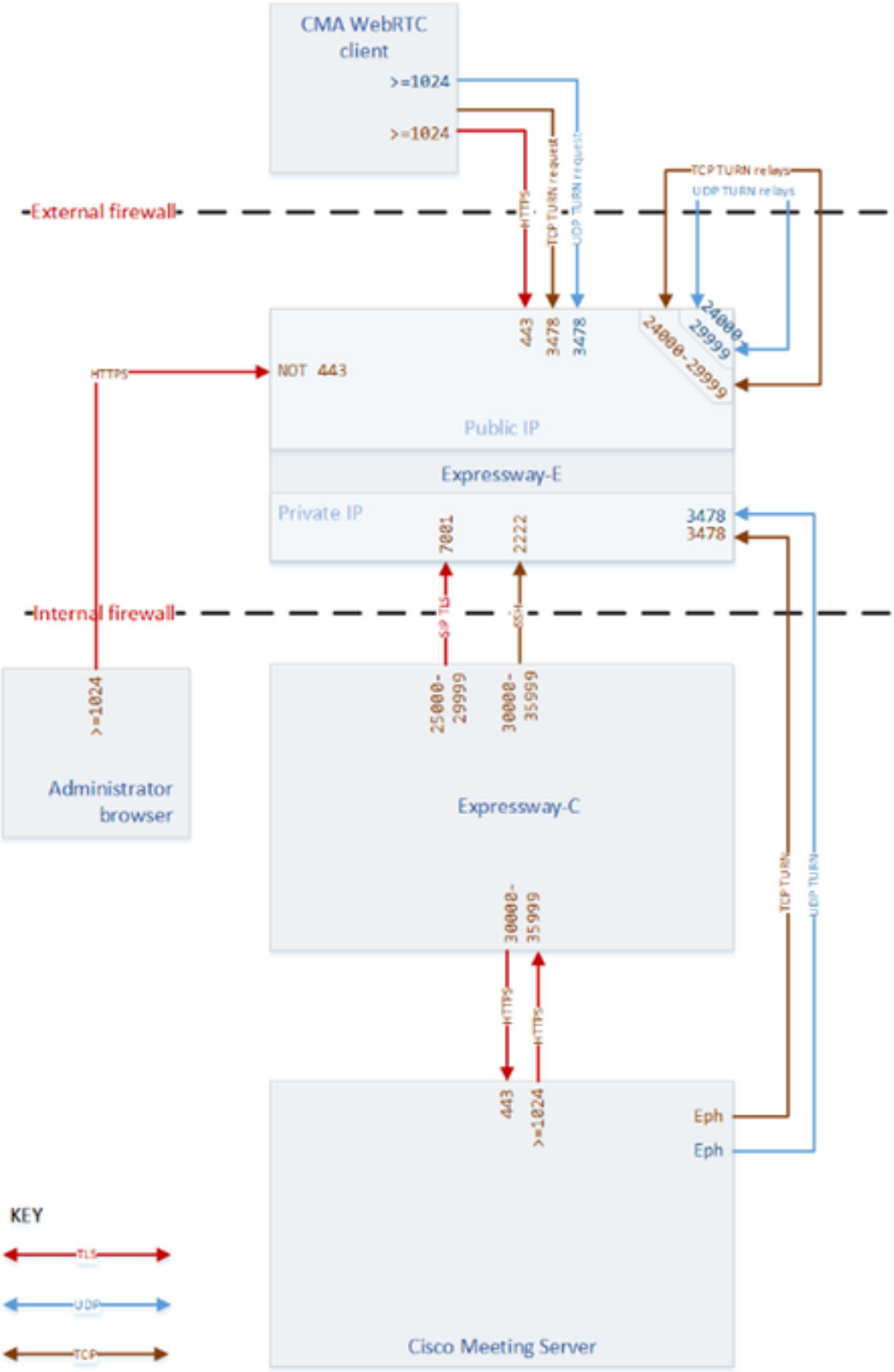
External clients and Guests can manage or join spaces without the need of any software other than a supported browser. Click here for a list of supported browsers.

Configure

Network Diagram



This image provides an example of connections flow of Web Proxy for CMS WebRTC:



Note: 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).

Configuration Steps

Step 1. Integrate CMS WB onto Expressway-C

a. Navigate to **Configuration > Unified Communication > Cisco Meeting Server**

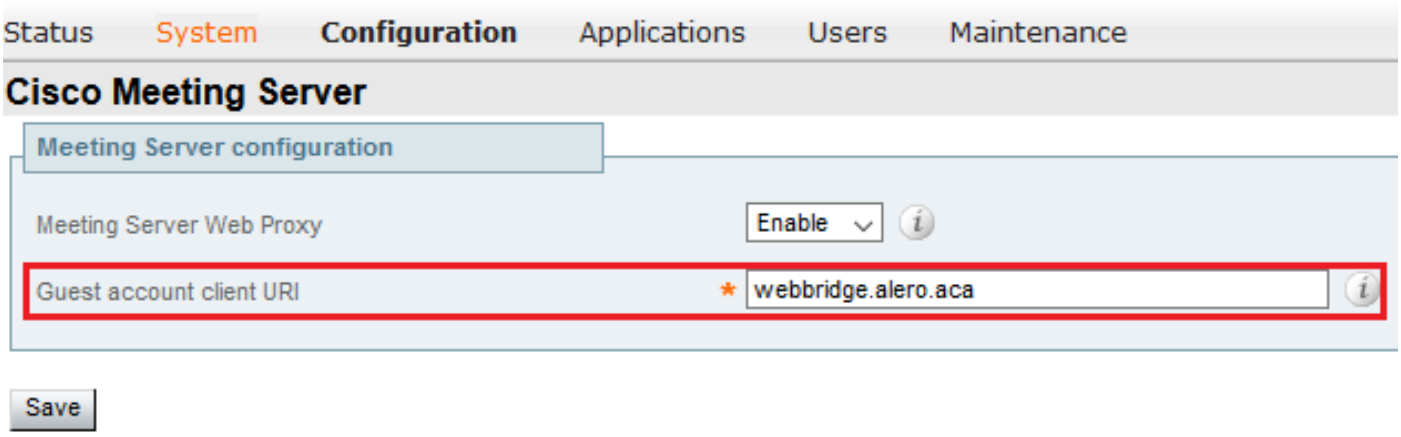
b. Enable **Meeting Server Web Proxy**

c. Enter the FQDN of the WB in the **Guest account client URI** field

d. Click on **Save**

e. Add the FQDN of the WB onto the Expressway-E server certificate as a Subject Alternative Name (SAN), click here for the Expressway certificate guide.

> **Note**: **The Guest account client URI** must be as configured on the CMS server WebAdmin (Web GUI Interface) without the **https://** prefix.



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. Select **Configure TURN client credentials on local database** and add the credentials (username and password)

> **Note**: If you have a cluster of Expressway-E and they're all to be used as TURN servers, then ensure to 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).

Step 3. Change the administration port of the Expressway-E (optional)

a. Navigate to **System > Administration**

b. Under **Web server configuration**, change the **Web administrator port** to **445** from the drop-down options, then select **Save**

c. Repeat steps **3a** to **3b** on all Expressway-E 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

a. Download and install Postman from here.

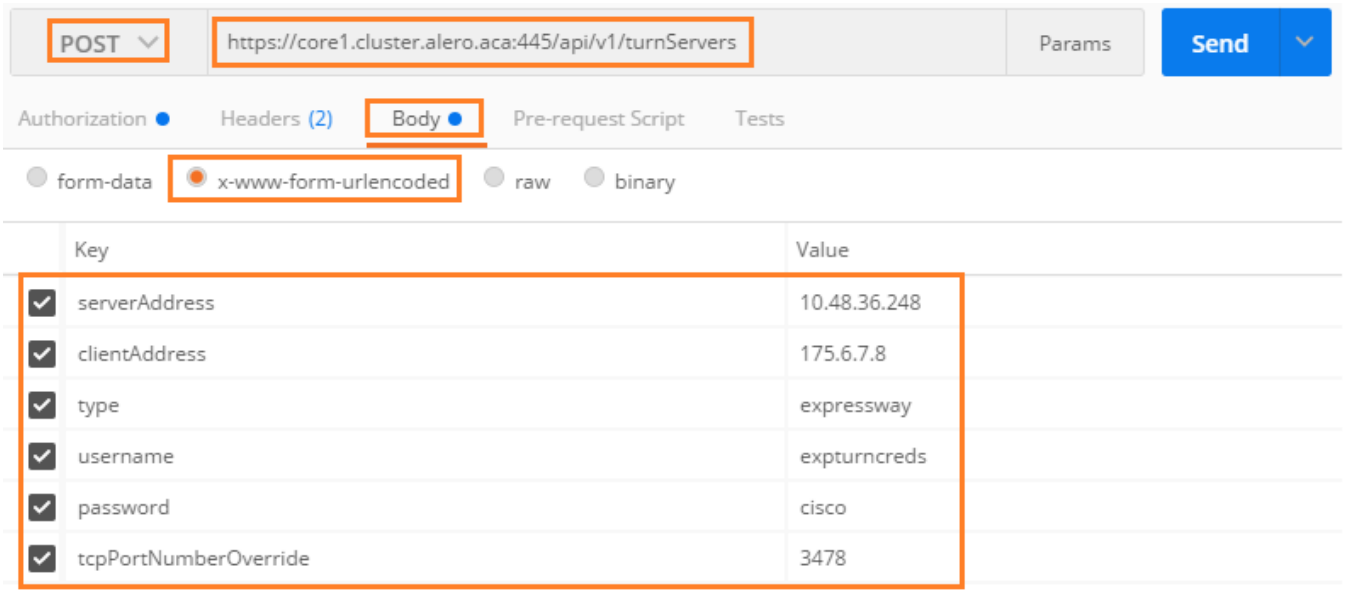
b. Enter the API access URL in the address bar, for example; **https://<Callbridge_fqdn>:445/api/v1/<entity>**

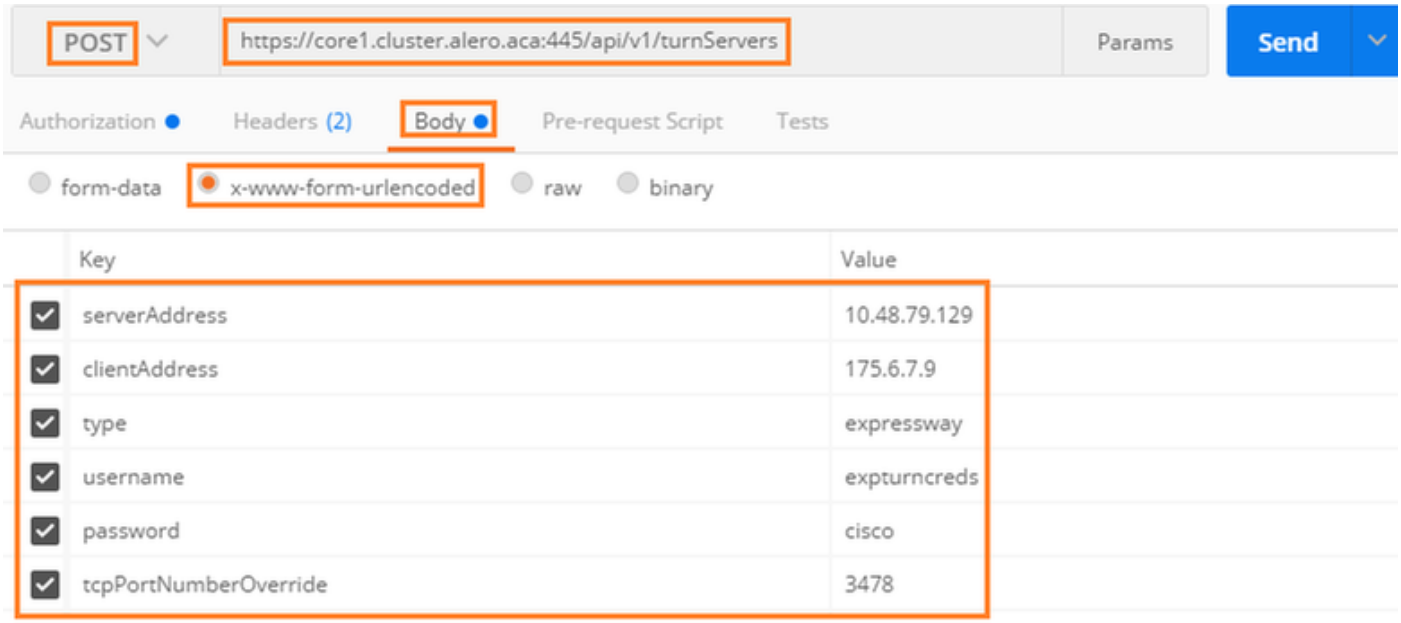
c. Send a POST with https://<Callbridge_fqdn>:445/api/v1/turnservers**,** after you add these fields in the Body:

- **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

These images provide examples of the configurational steps:



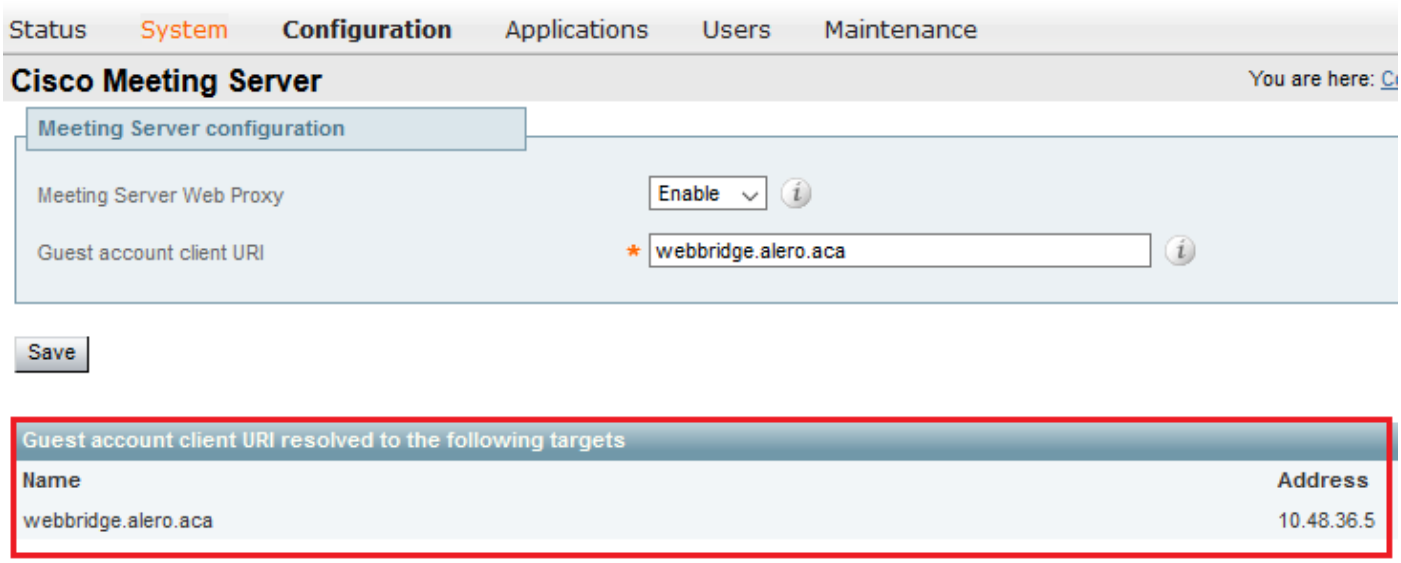


Verify

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,** and you must see the IP address of the WB:



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 the 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:

Step 2. Verify that the TURN server has been added to the CMS server

a. On the WebUI, if you use a Single Expressway Server, navigate to **Logs > Event logs**, the output shows the TURN server IP address, as in the example:

```
2017-04-1509:37:26.864Info TURN server 7: starting up "10.48.36.248" (configured object 6508065f-298f-4146-8697-4b7087279de3)
```

b. If you use multiple Expressway TURN servers, send a **GET** request with an API client with this command:

https://<Callbridge_IP>:445/api/v1/turnservers

Note: This command can also be used if you have a single Expressway TURN server.

The output, in the case of multiple Expressway TURN servers, is similar to that in this example:

```
<?xml version="1.0"?>
<turnServers total="2">
    <turnServer id="7eecf3eb-49f2-4963-bf67-2bac98355ca1">
        <serverAddress>10.48.79.129</serverAddress>
        <clientAddress>175.6.7.9</clientAddress>
    </turnServer>
    <turnServer id="eef94a2b-3bfa-40f7-b83c-ece8df424e15">
        <serverAddress>10.48.36.248</serverAddress>
        <clientAddress>175.6.7.8</clientAddress>
    </turnServer>
</turnServers>
```

c. To check the status of each TURN server do the following:

- Copy the **turnServer id** from step 2b
- Send a **GET** request with the API client with this command:
  https://<Callbridge_IP>:445/api/v1/turnservers/<turnServer id>/status

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.

The output below shows the status for the TURN server with ID **7eecf3eb-49f2-4963-bf67-2bac98355ca1**:

```
<?xml version="1.0"?>
<turnServer>
   <status>success</status>
   <host>
       <address>10.48.36.248</address>
       <portNumber>3478</portNumber>
       <reachable>true</reachable>
       <roundTripTimeMs>37</roundTripTimeMs>
       <mappedAddress>10.48.36.5</mappedAddress>
       <mappedPortNumber>44920</mappedPortNumber>
   </host>
</turnServer>
```

The output below shows the status for the TURN server with ID **eef94a2b-3bfa-40f7-b83c-ece8df424e15**:

```
<?xml version="1.0"?>
<turnServer>
   <status>success</status>
   <host>
       <address>10.48.79.129</address>
       <portNumber>3478</portNumber>
       <reachable>true</reachable>
       <roundTripTimeMs>48</roundTripTimeMs>
       <mappedAddress>10.48.36.5</mappedAddress>
       <mappedPortNumber>44920</mappedPortNumber>
   </host>
```

Step 3. Verify TURN relay usage an during ongoing call

At the time of 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 select **view.**

Troubleshoot

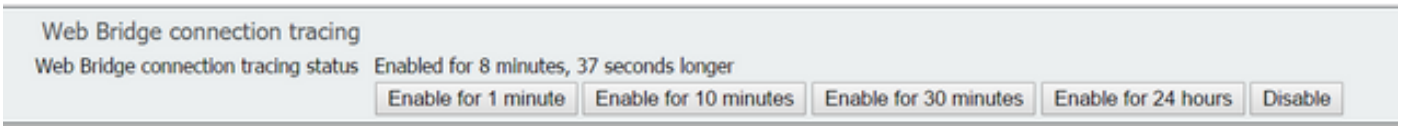
This section provides information you can use to troubleshoot your configuration, some typical WebRTC issues and possible failures.

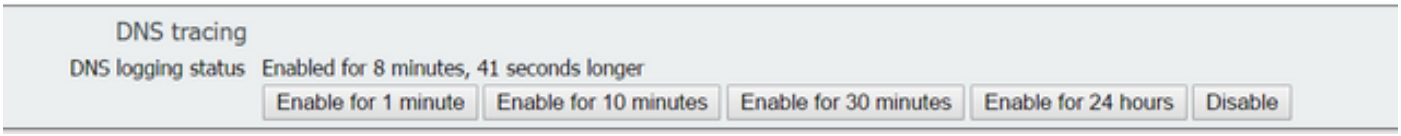
Logs for the WB connections and DNS tracing can be enabled on the WebAdmin of the CMS server:

a. Connect to the **WebAdmin**

b. Navigate to **Logs > Detailed Tracing**

c. Enable **Web Bridge connection tracing** and **DNS tracing** for the desired duration:





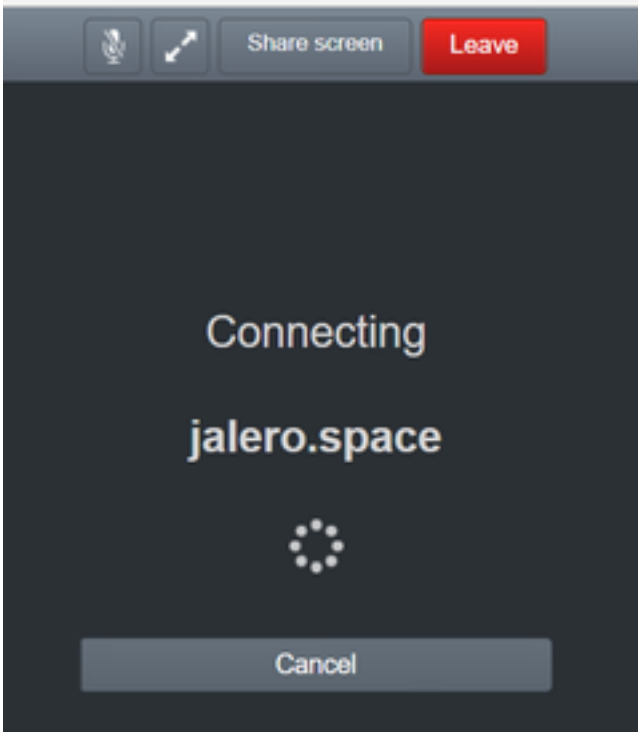
Chrome and Firefox console debug logging can be used to troubleshoot WebRTC client connection failures, such as issues with media and connectivity to the WB. This can be made visible with the use of the keyboard combination **Ctrl+Shift+C.**

On Chrome, use **chrome://webrtc-internals/** or **about:webrtc** on Firefox, on a separate tab at the time of a live call to display the advanced diagnostics, which is useful to troubleshoot media issues with WebRTC.

Whireshark packet capture on the WebRTC client also provide some useful information about the media relay with the TURN server.

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 on the image below:

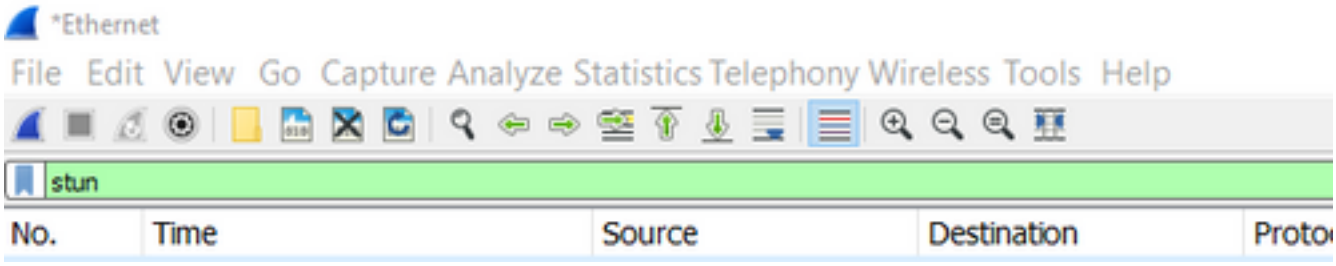


After about 30 seconds, it is redirected to the initial WB page.

To troubleshoot, do the following:

- Start wireshark on the RTC client when you attempt a call and when the failure occur, 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 example below:



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
```

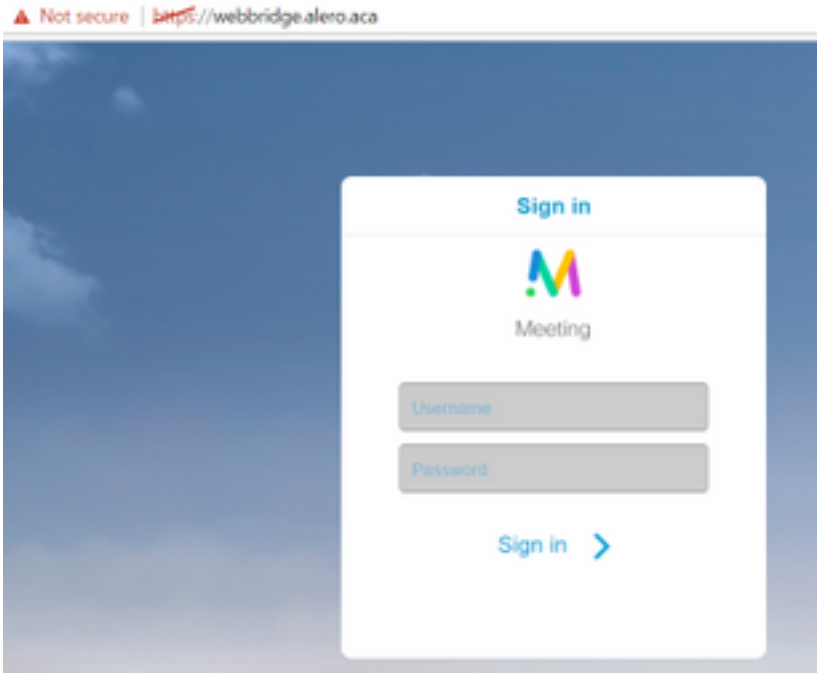
In the CMS logs, the log message below is shown:

```
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
```

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:

```
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
```

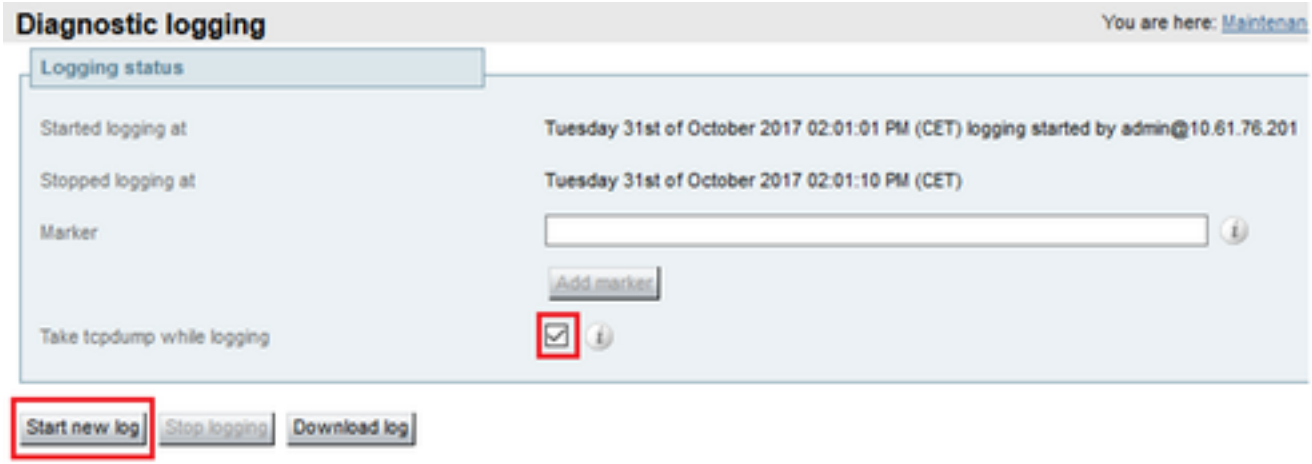
Solution:

- Ensure that the Callbridge can resolve the WB FQDN to the internal IP address (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 **_xmpp-client** SRV record on the internal network for the CB domain
- Collect 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 on the image below, before you select **Start new log**:

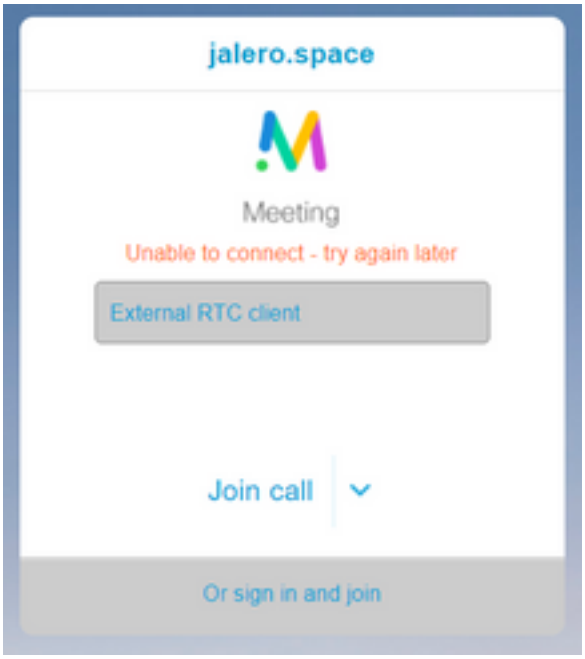


Note: Ensure that the Wireshark capture on the client's device and the logging on the Expressway-E are started before reproducing the failing call. When the failing call has been reproduced, stop and download the logging on the Expressway-E and the capture on the client.

- Extract/unzip the log bundle dowloaded 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 above are not blocked
- If the Expressway-E is deployed with a Dual Network Interface Controller (DUAL-NIC) with static NAT mode enabled, then ensure that NAT reflection is supported and configured on your External FW

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**