Configure Proxy WebRTC With CMS over Expressway with Dual Domain

Contents

Introduction

This document describes an example configuration of the proxy Web Real-Time Communication (webRTC) for Cisco Meeting Server (CMS) through Expressway with different internal and external domain.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- CMS single combined deployment version 2.1.4 and above
- Expressway C and Expressway E version X8.9.2 and above
- Callbridge and webbridge configured on CMS
- Mobile and Remote Access (MRA) enabled on the Expressway pair
- Traversal Using Relay NAT (TURN) option key added to the Expressway-E

- External resolvable Domain Name Server (DNS) record for webbridge URL, for external domain
- Internal resolvable DNS record for CMS IP address from external to internal domain
- Extensible Messaging and Presence Protocol (XMPP) multi domain configured on CMS, for internal and external domain
- TCP Port 443 opened on Firewall from the Public internet to the Expressway-E's Public IP address
- TCP and UDP Port 3478 opened on Firewall from Public internet to the Expressway-E's Public IP address
- UDP port range 24000-29999 opened on Firewall to and from the Expressway-E's Public IP address

Components Used

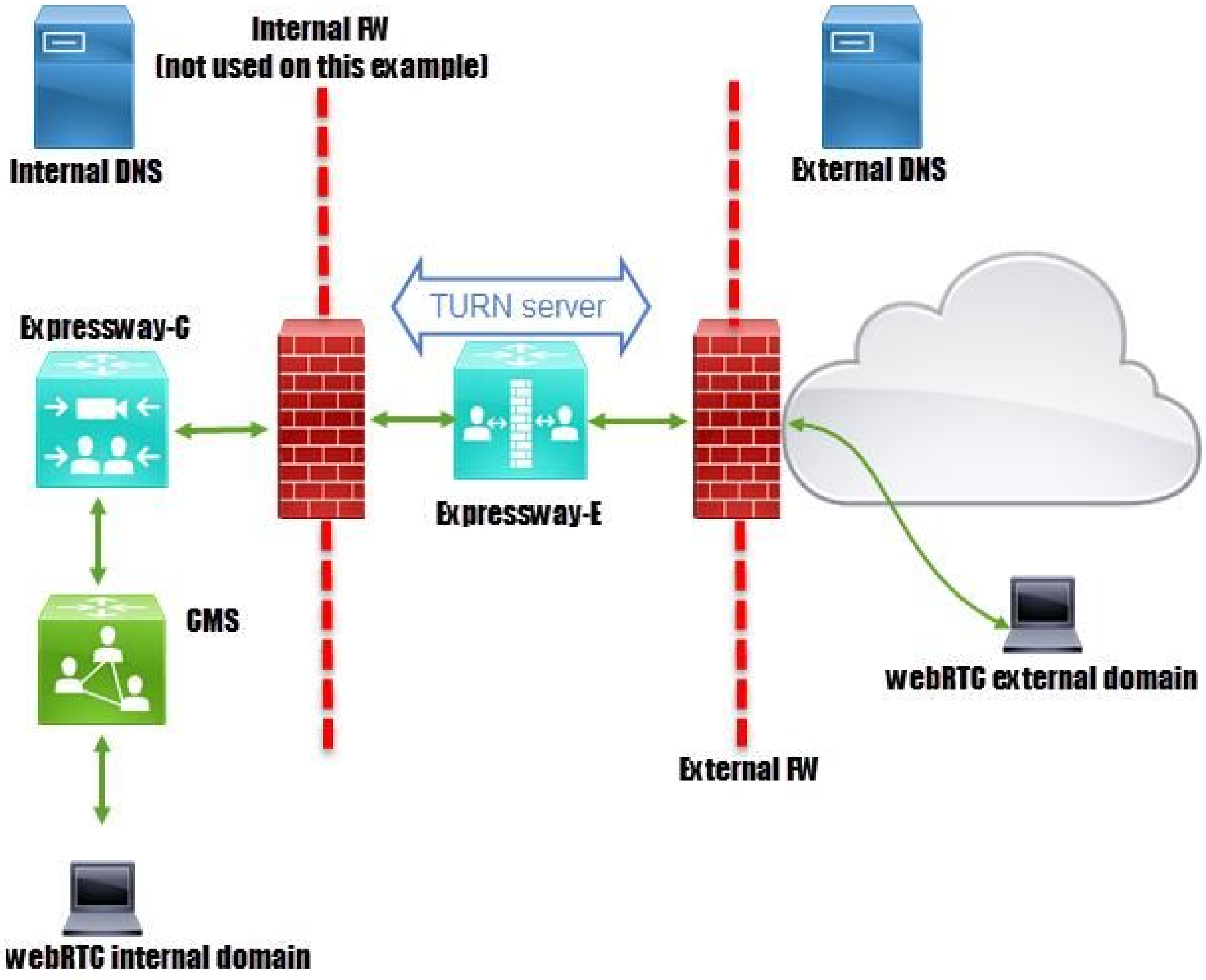
The information in this document is based on these software and hardware versions:

- CMS single combined deployment version 2.2.1
- Expressway-C and Expressway-E with dual Network Interface Card (NIC) and static Network Address Translation (NAT) Software version X8.9.2
- Postman

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, make sure that you understand the potential impact of any command.

Configure

Network Diagram

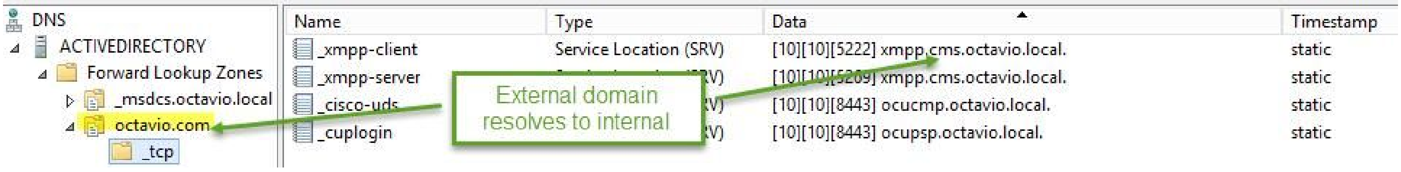


Technical Information

Internal domain	**cms.octavio.local**
External domain	**octavio.com**
CMS IP address	172.16.85.180
Expressway-C IP address	172.16.85.167
Expressway-E LAN1 IP address (internal)	172.16.85.168
Expressway-E LAN2 IP address (external)	192.168.245.61
Static NAT IP address	10.88.246.156

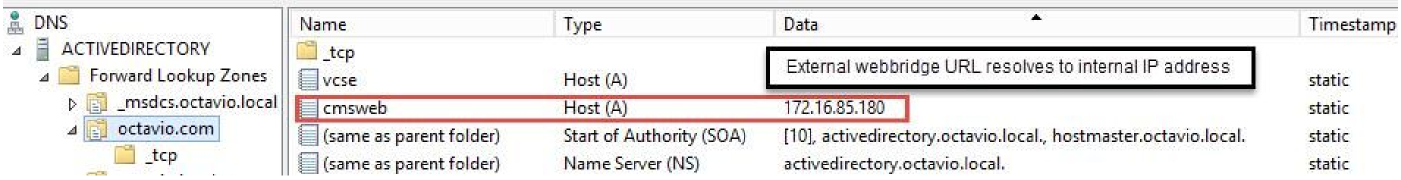
DNS Configuration

Internal DNS Configuration



Name	Type	Data	Timestamp
_xmpp-client	Service Location (SRV)	[10][10][5222] xmpp.cms.octavio.local.	static
_xmpp-server	Service Location (SRV)	[10][10][5269] xmpp.cms.octavio.local.	static
_cisco-uds	Service Location (SRV)	[10][10][8443] ocucmp.octavio.local.	static
_cuplogin	Service Location (SRV)	[10][10][8443] ocupsp.octavio.local.	static

External domain resolves to internal

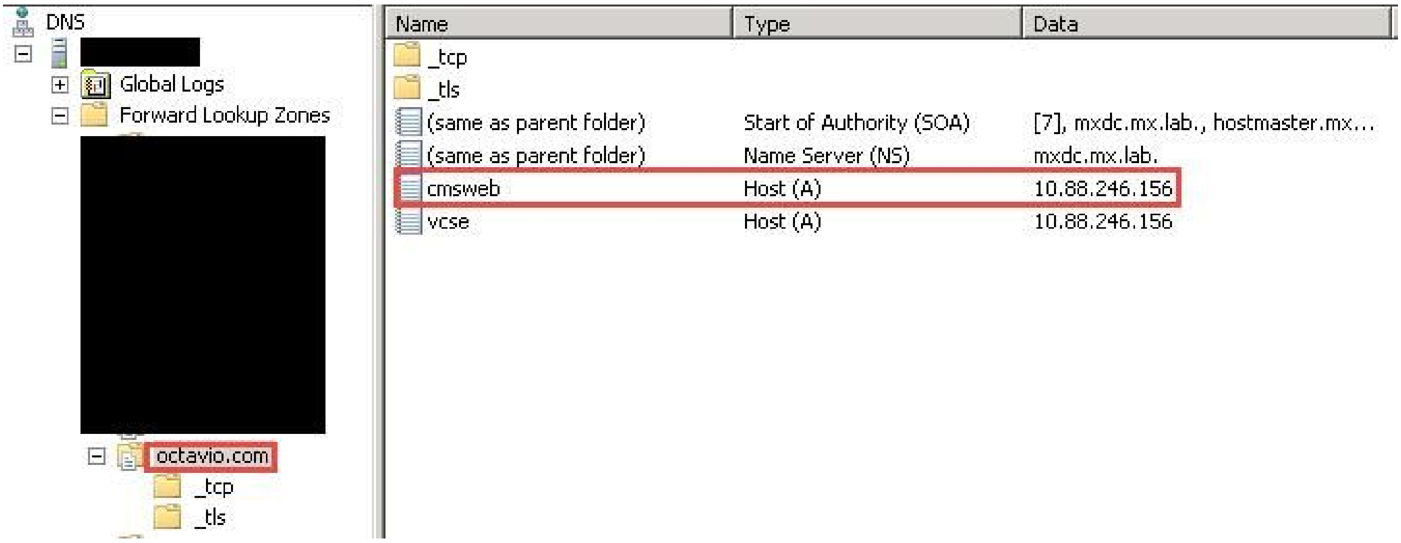


External webbridge URL resolves to internal IP address

Name	Type	Data	Timestamp
_tcp			
vcse	Host (A)		static
cmsweb	Host (A)	172.16.85.180	static
(same as parent folder)	Start of Authority (SOA)	[10], activedirectory.octavio.local., hostmaster.octavio.local.	static
(same as parent folder)	Name Server (NS)	activedirectory.octavio.local.	static

External DNS Configuration

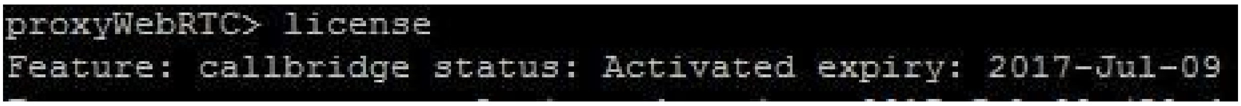
The external DNS must have the webbridge URL which resolves to the Static NAT IP address of the Expressway-E as shown in the image.



Name	Type	Data
_tcp		
_tls		
(same as parent folder)	Start of Authority (SOA)	[7], mxdc.mx.lab., hostmaster.mx...
(same as parent folder)	Name Server (NS)	mxdc.mx.lab.
cmsweb	Host (A)	10.88.246.156
vcse	Host (A)	10.88.246.156

CMS, Callbridge, Webbridge and XMPP Configuration

Step 1. You must have the callbridge license activated. The image shows a callbridge license that is active.

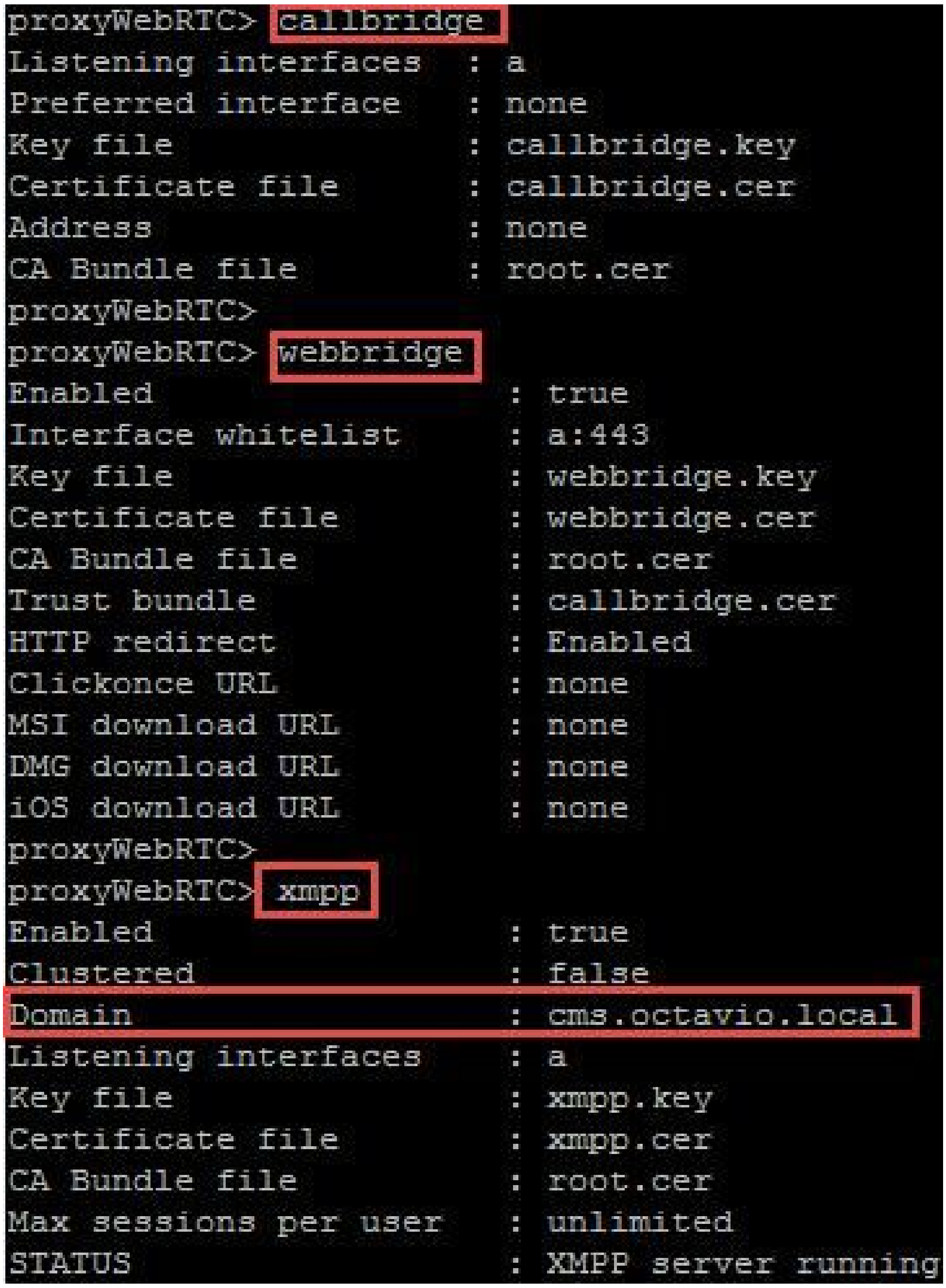


```
proxyWebRTC> license
Feature: callbridge status: Activated expiry: 2017-Jul-09
```

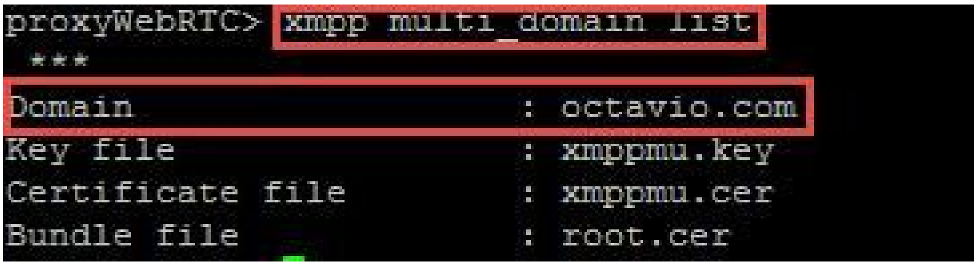
For more licensing information:

http://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-1/Cisco-Meeting-Server-2-1-Single-Combined-Server-Deployment.pdf#page=10

Step 2. Enable callbridge, webbridge and XMPP through MMP as shown in the image.



```
proxyWebRTC> callbridge
Listening interfaces    : a
Preferred interface     : none
Key file                : callbridge.key
Certificate file        : callbridge.cer
Address                 : none
CA Bundle file          : root.cer
proxyWebRTC>
proxyWebRTC> webbridge
Enabled                   : true
Interface whitelist       : a:443
Key file                  : webbridge.key
Certificate file          : webbridge.cer
CA Bundle file            : root.cer
Trust bundle              : callbridge.cer
HTTP redirect             : Enabled
Clickonce URL             : none
MSI download URL          : none
DMG download URL          : none
iOS download URL          : none
proxyWebRTC>
proxyWebRTC> xmpp
Enabled                   : true
Clustered                 : false
Domain                    : cms.octavio.local
Listening interfaces      : a
Key file                  : xmpp.key
Certificate file          : xmpp.cer
CA Bundle file            : root.cer
Max sessions per user     : unlimited
STATUS                    : XMPP server running
```



```
proxyWebRTC> xmpp multi_domain list
 ***
Domain                    : octavio.com
Key file                  : xmppmu.key
Certificate file          : xmppmu.cer
Bundle file               : root.cer
```

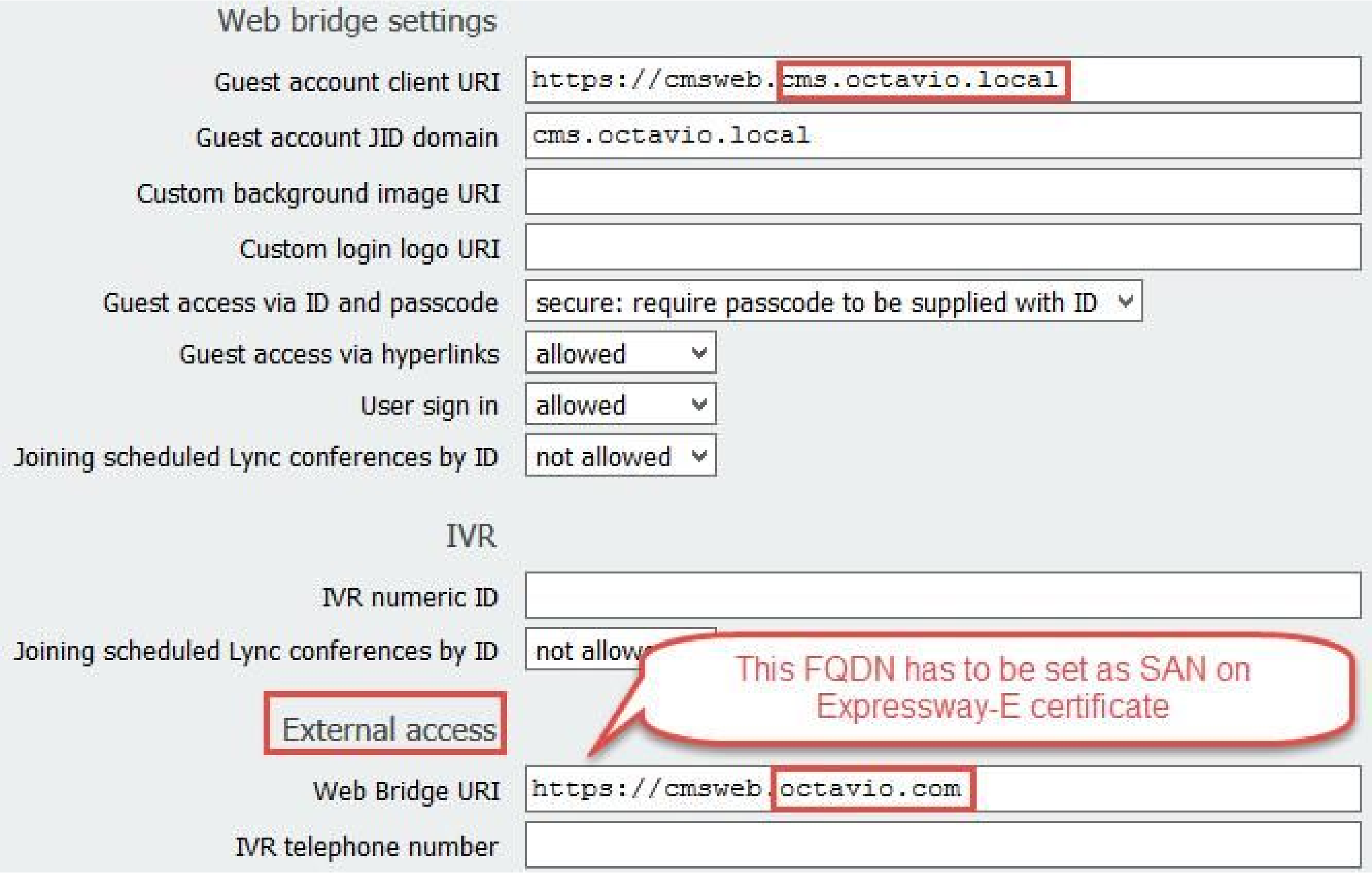
Follow this link for a detail process on how to enable them:

http://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-1/Cisco-Meeting-Server-2-1-Single-Combined-Server-Deployment.pdf

Follow this link for a detail process on how to create a certificate:

http://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-2/Certificate-Guidelines-Single-Combined-Server-Deployment-2-2.pdf

Step 3. Navigate to the CMS web page on **Configuration > General** and configure the internal and external URL for the webbridge as shown in the image.



Web bridge settings

Guest account client URI: https://cmsweb.cms.octavio.local

Guest account JID domain: cms.octavio.local

Custom background image URI:

Custom login logo URI:

Guest access via ID and passcode: secure: require passcode to be supplied with ID

Guest access via hyperlinks: allowed

User sign in: allowed

Joining scheduled Lync conferences by ID: not allowed

IVR

IVR numeric ID:

Joining scheduled Lync conferences by ID: not allowed

External access

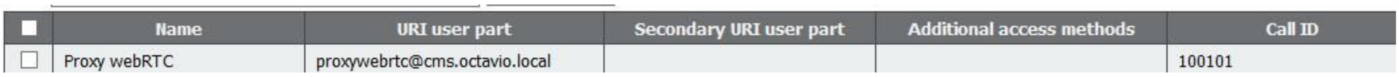
Web Bridge URI: https://cmsweb.octavio.com

IVR telephone number:

This FQDN has to be set as SAN on Expressway-E certificate

Note: The CMS must be configured with at least one Space.

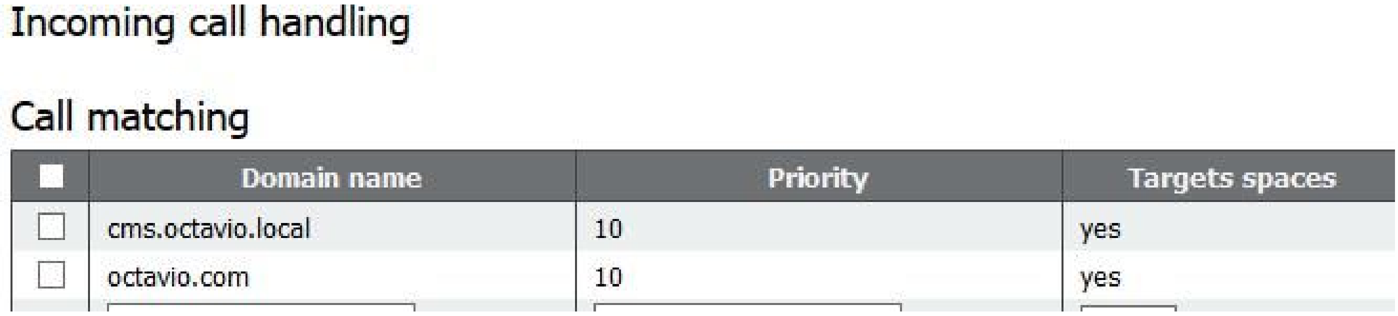
An example of a configured Space on CMS as shown in the image.



■	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
□	Proxy webRTC	proxywebrtc@cms.octavio.local			100101

Note: The incoming calls must be configured for the internal and external domains

An example of configured domains for incoming call handling is as shown in the image.



Incoming call handling

Call matching

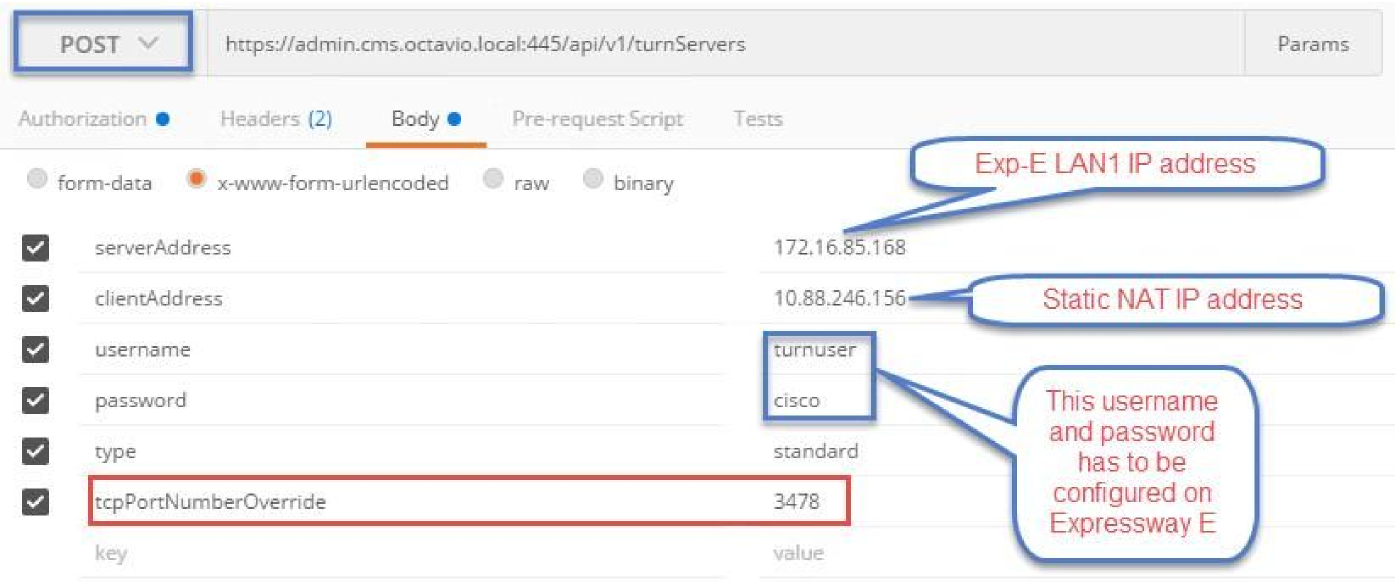
■	Domain name	Priority	Targets spaces
□	cms.octavio.local	10	yes
□	octavio.com	10	yes

TURN Configuration

Step 1. TURN must be configured by API through Postman. This command is used through all the configuration.

https://<cms_web_admin_address>:<web_admin_port>/api/v1/turnServers

Step 2. Use the POST method and navigate to **Body** either to view the TURN server parameters or edit them. The parameters configured to the TURN server are as shown in the image.



POST https://admin.cms.octavio.local:445/api/v1/turnServers

○ form-data ● x-www-form-urlencoded ○ raw ○ binary

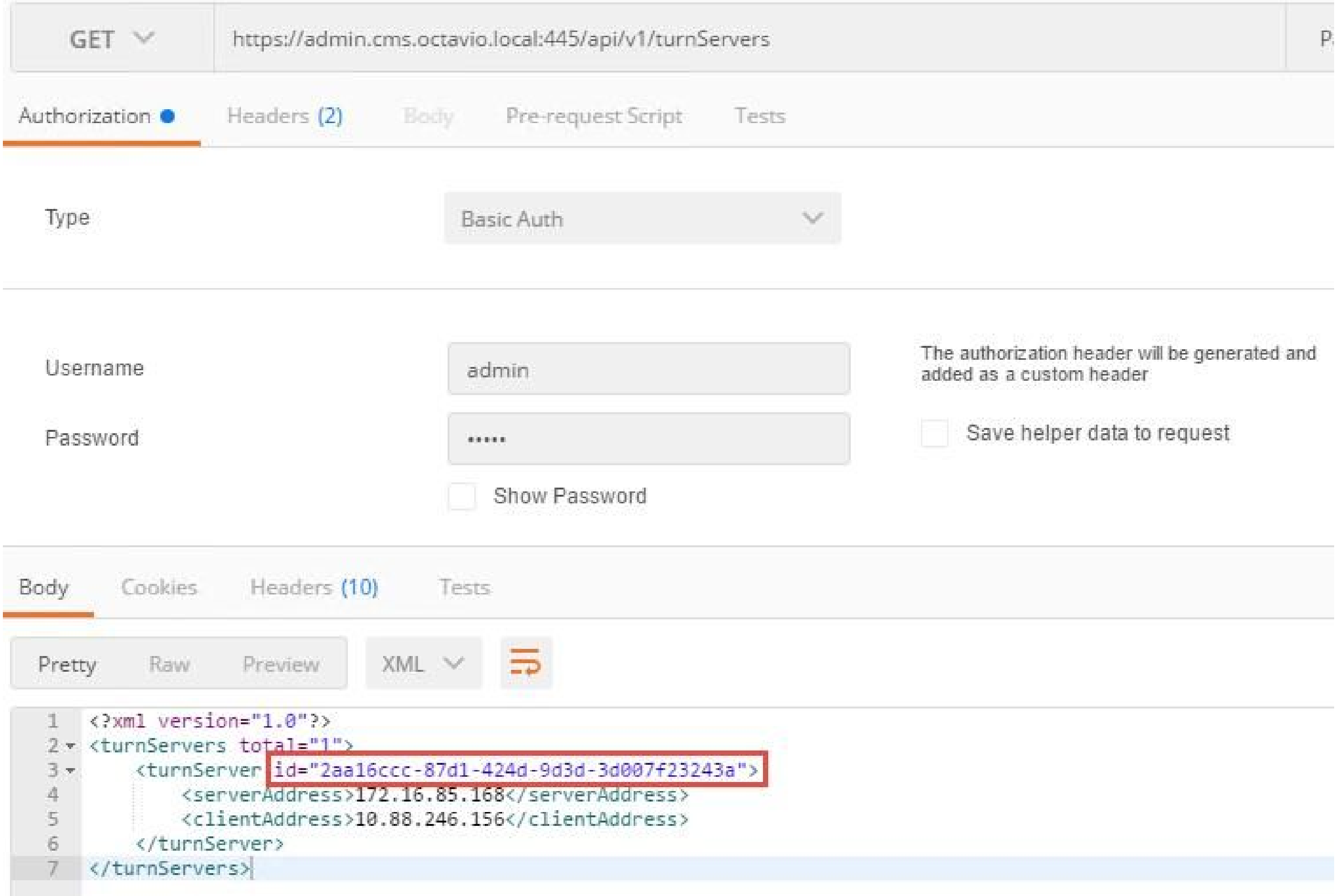
☑	serverAddress	172.16.85.168
☑	clientAddress	10.88.246.156
☑	username	turnuser
☑	password	cisco
☑	type	standard
☑	tcpPortNumberOverride	3478
	key	value

Exp-E LAN1 IP address

Static NAT IP address

This username and password has to be configured on Expressway E

Step 3. Check the status of the TURN server configuration by running the method GET and copy the server ID. The ID that must be copied is as shown in the image.



GET https://admin.cms.octavio.local:445/api/v1/turnServers

Type: Basic Auth

Username: admin

Password: •••••

□ Show Password

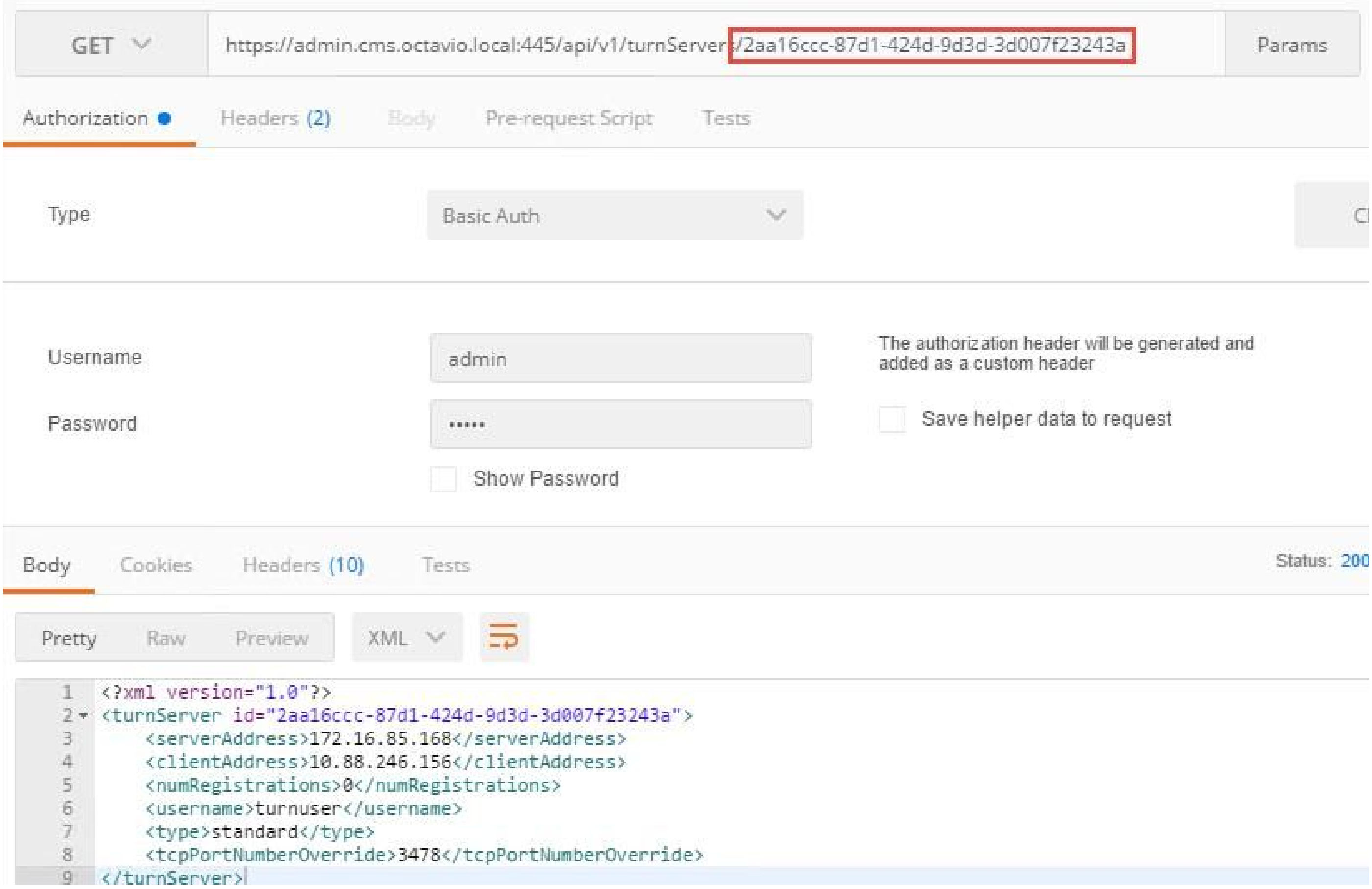
The authorization header will be generated and added as a custom header

□ Save helper data to request

```
<?xml version="1.0"?>
<turnServers total="1">
    <turnServer id="2aa16ccc-87d1-424d-9d3d-3d007f23243a">
        <serverAddress>172.16.85.168</serverAddress>
        <clientAddress>10.88.246.156</clientAddress>
    </turnServer>
</turnServers>
```

Step 4. Copy the ID at the end of the API command and use the GET method in order to see the TURN server information as shown in the image.

Note: The information won't show the server's password.



GET https://admin.cms.octavio.local:445/api/v1/turnServers/2aa16ccc-87d1-424d-9d3d-3d007f23243a

Type: Basic Auth

Username: admin

Password: •••••

□ Show Password

The authorization header will be generated and added as a custom header

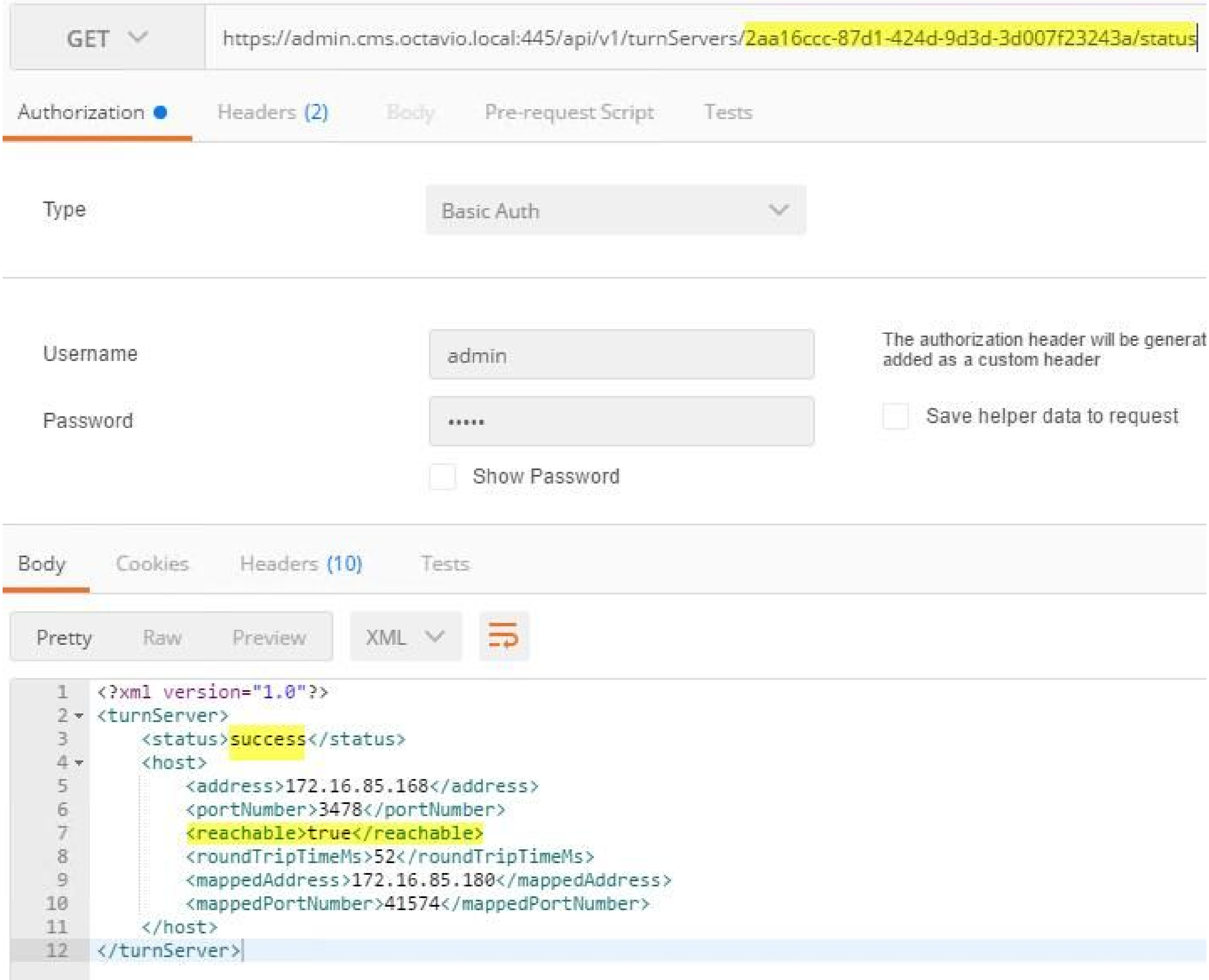
□ Save helper data to request

Status: 200

XML

```
<?xml version="1.0"?>
<turnServer id="2aa16ccc-87d1-424d-9d3d-3d007f23243a">
    <serverAddress>172.16.85.168</serverAddress>
    <clientAddress>10.88.246.156</clientAddress>
    <numRegistrations>0</numRegistrations>
    <username>turnuser</username>
    <type>standard</type>
    <tcpPortNumberOverride>3478</tcpPortNumberOverride>
</turnServer>
```

Step 5. Click **send** to get the server status. An example of a successful configuration as shown in the image.



GET https://admin.cms.octavio.local:445/api/v1/turnServers/2aa16ccc-87d1-424d-9d3d-3d007f23243a/status

Type: Basic Auth

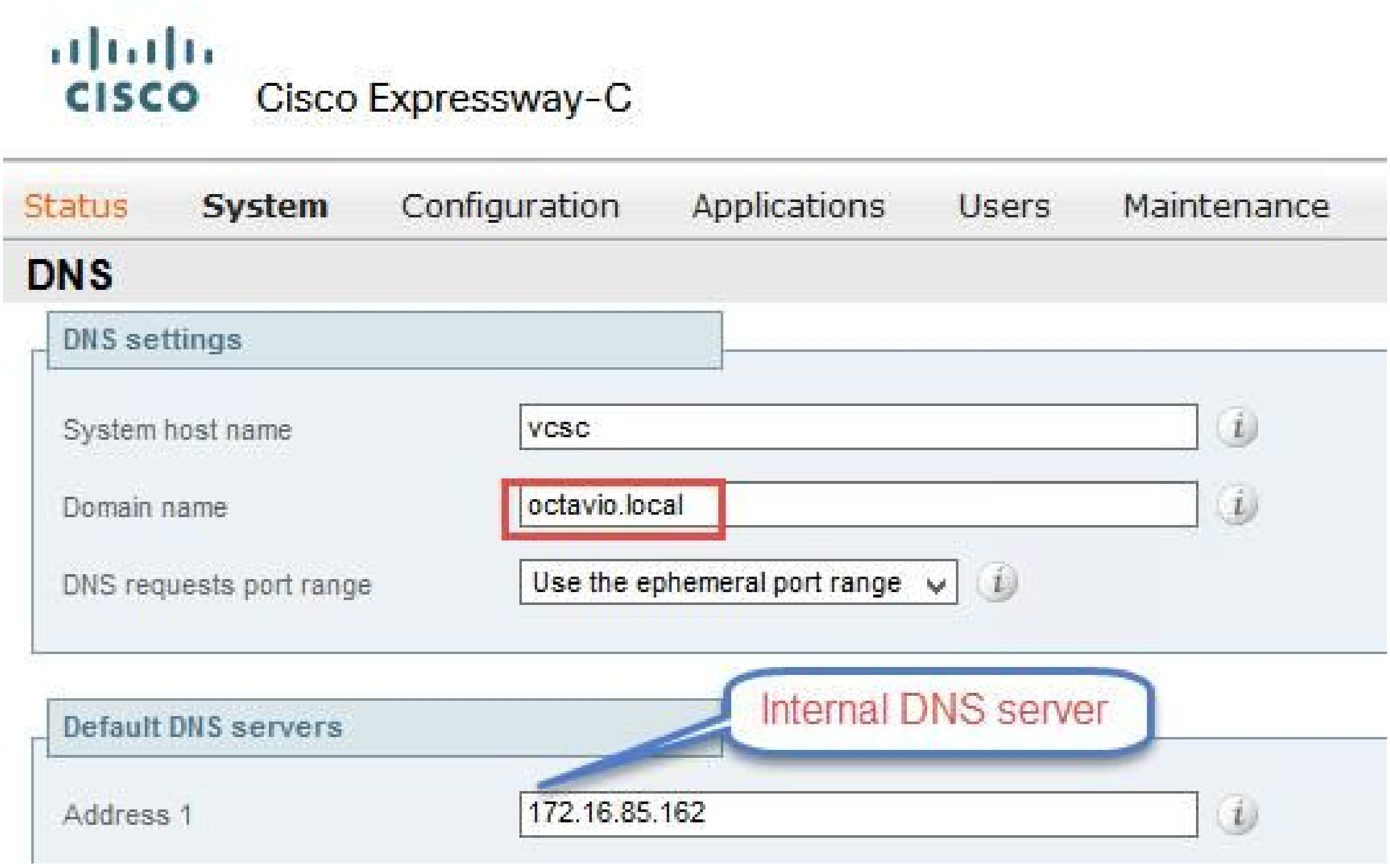
Username: admin

Password: •••••

```
<?xml version="1.0"?>
<turnServer>
    <status>success</status>
    <host>
        <address>172.16.85.168</address>
        <portNumber>3478</portNumber>
        <reachable>true</reachable>
        <roundTripTimeMs>52</roundTripTimeMs>
        <mappedAddress>172.16.85.180</mappedAddress>
        <mappedPortNumber>41574</mappedPortNumber>
    </host>
</turnServer>
```

Expressway-C and E Configuration

Step 1. The expressway-C must have the internal domain (octavio.local) and the Expressway-E must have the external domain (octavio.com) configured as shown in the image.



DNS

DNS settings

System host name: vcsc

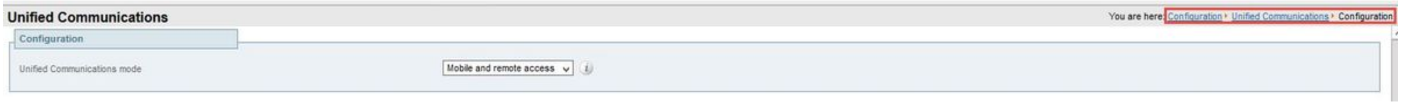
Domain name: octavio.local

DNS requests port range: Use the ephemeral port range

Default DNS servers

Address 1: 172.16.85.162

Step 2. MRA must be enabled on both Expressway C and E as shown in the image.

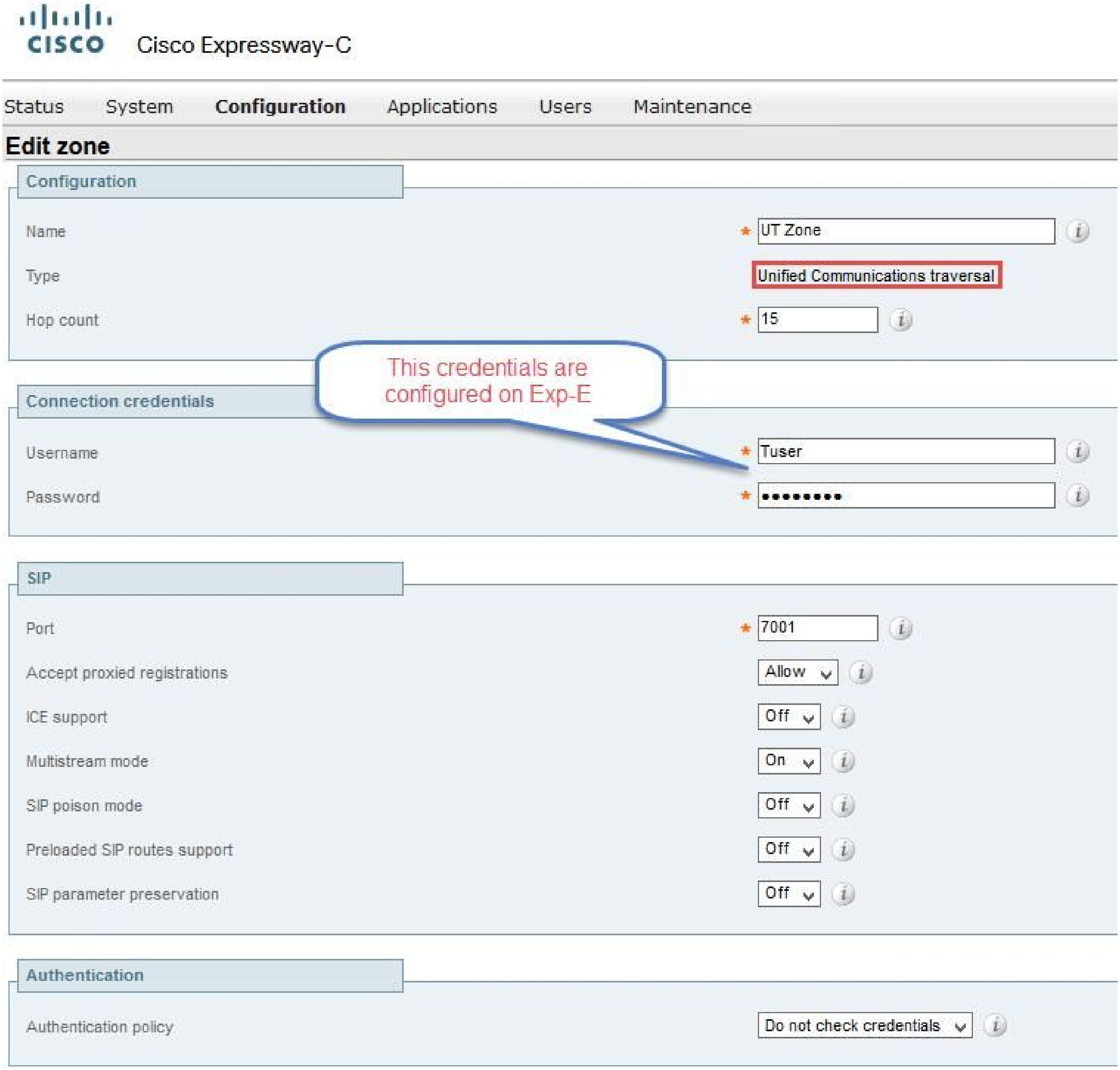

Unified Communications

You are here: Configuration › Unified Communications › Configuration

Configuration

Unified Communications mode: Mobile and remote access

Step 3. Create a Unified Communication traversal zone between the Expressway-C and E as shown in the image.



Cisco Expressway-C

Edit zone

Configuration

Name * UT Zone

Type Unified Communications traversal

Hop count * 15

This credentials are configured on Exp-E

Connection credentials

Username * Tuser

Password * •••••••••

SIP

Port * 7001

Accept proxied registrations Allow

ICE support Off

Multistream mode On

SIP poison mode Off

Preloaded SIP routes support Off

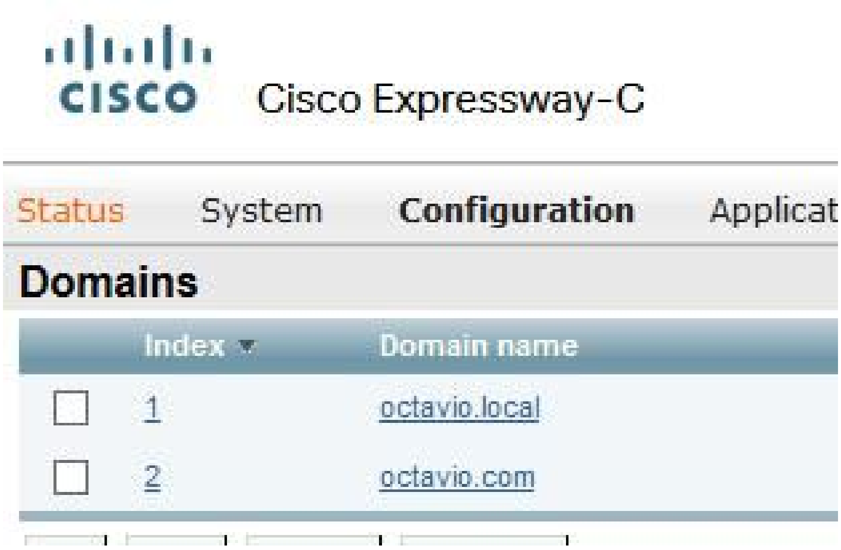
SIP parameter preservation Off

Authentication

Authentication policy Do not check credentials

Configuration on Expressway-C

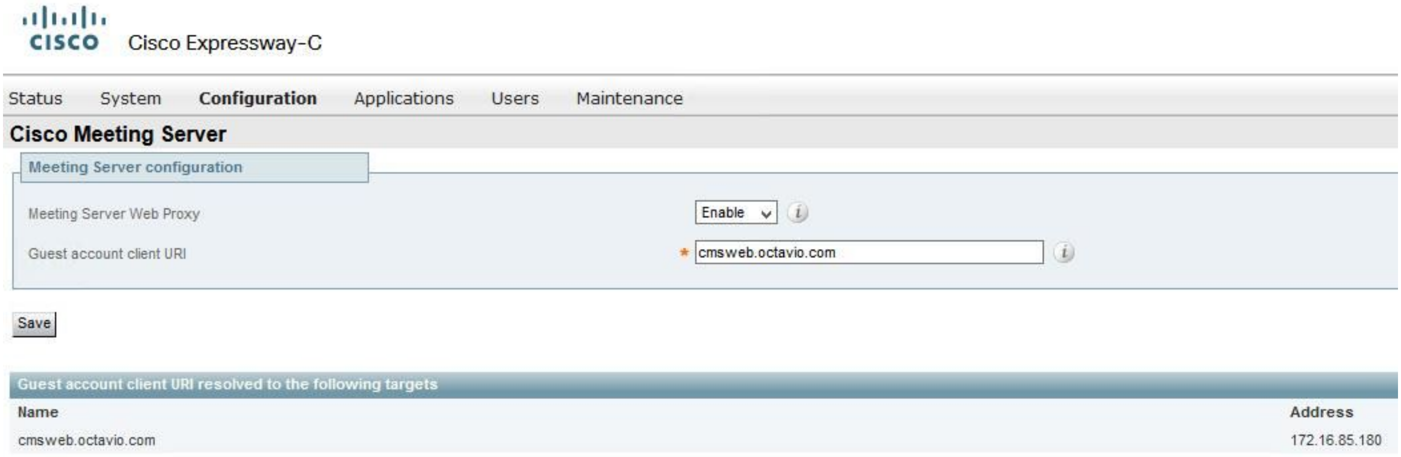
Step 1. Configure the internal and external domain on the Expressway-C as shown in the image.



Domains

	Index	Domain name
□	1	octavio.local
□	2	octavio.com

Step 2. Enable the Cisco Meeting configuration. Navigate to **Configuration > Unified Communications > Cisco Meeting Server**. Configure the external webbridge URL on the Guest account client URI field as shown in the image.



Cisco Meeting Server

Meeting Server configuration

Meeting Server Web Proxy: Enable

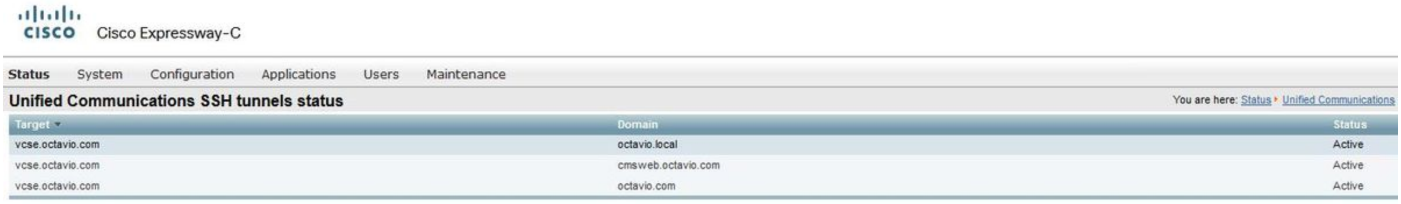
Guest account client URI: * cmsweb.octavio.com

Guest account client URI resolved to the following targets

Name	Address
cmsweb.octavio.com	172.16.85.180

Note: The internal DNS should resolve the external webbridge URL (cmsweb.octavio.com) to the internal CMS webbridge IP address. In this example case the IP is 172.16.85.180.

The Secure Shell (SSH) tunnels on the Expressway-C must become active after some seconds as shown in the image.



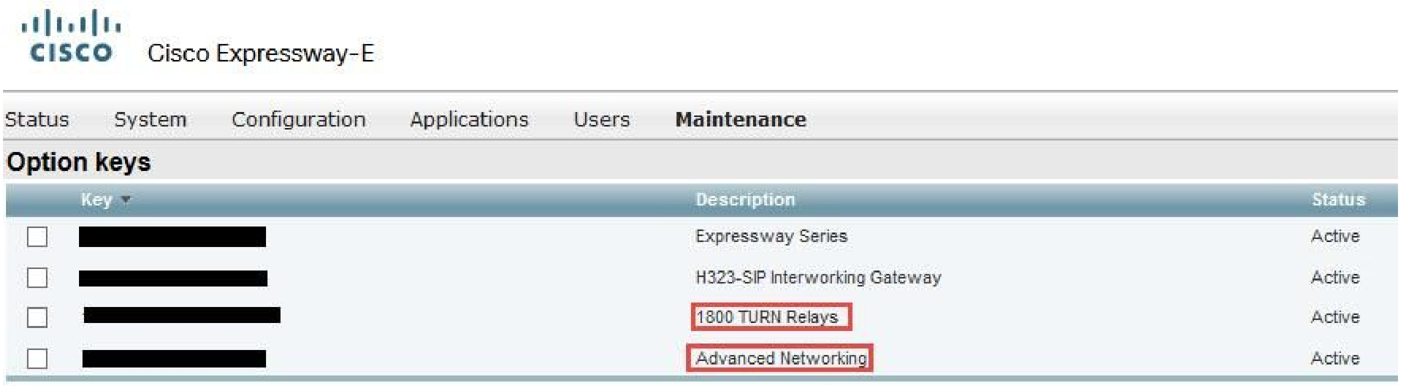
Unified Communications SSH tunnels status

Target	Domain	Status
vcse.octavio.com	octavio.local	Active
vcse.octavio.com	cmsweb.octavio.com	Active
vcse.octavio.com	octavio.com	Active

Note:The server must have a server certificate and a CA certificate.

Configuration on Expressway-E

Step 1. The expressway-E must have a TURN license as shown in the image.

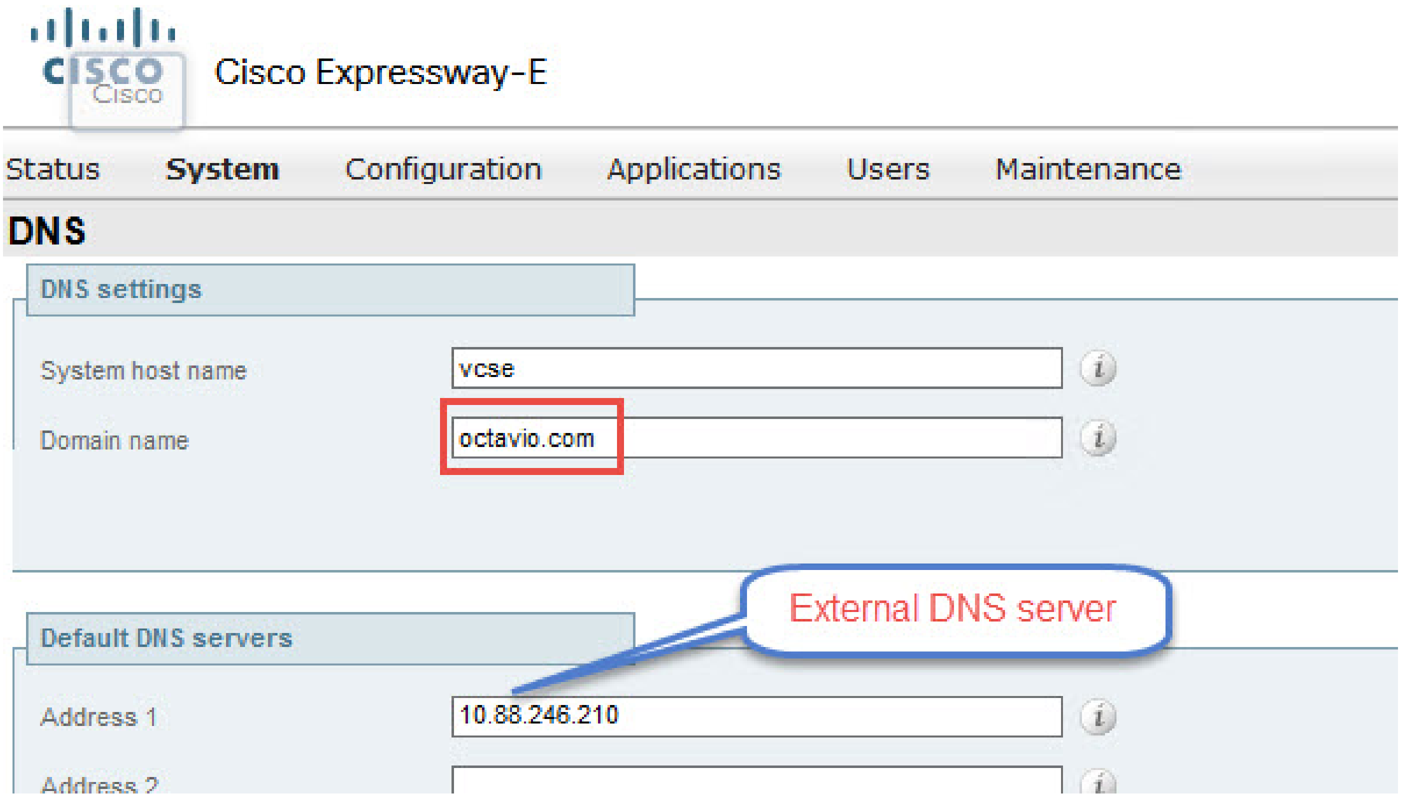


Cisco Expressway-E

Option keys

	Key	Description	Status
□	[redacted]	Expressway Series	Active
□	[redacted]	H323-SIP Interworking Gateway	Active
□	[redacted]	1800 TURN Relays	Active
□	[redacted]	Advanced Networking	Active

Step 2. The Expressway-E must be configured with the external domain as shown in the image.



Cisco Expressway-E

DNS

DNS settings

System host name: vcse

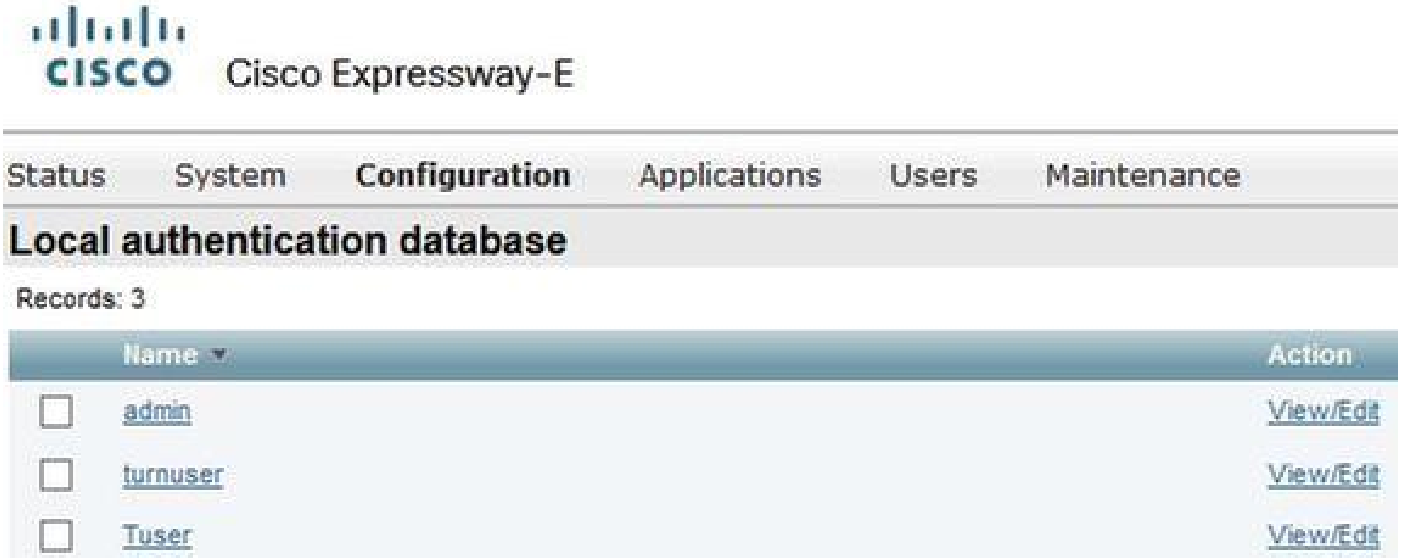
Domain name: octavio.com

Default DNS servers

Address 1: 10.88.246.210

Address 2:

Step 3. Create users for the TURN server and for the Unified Communication traversal zone as shown in the image.



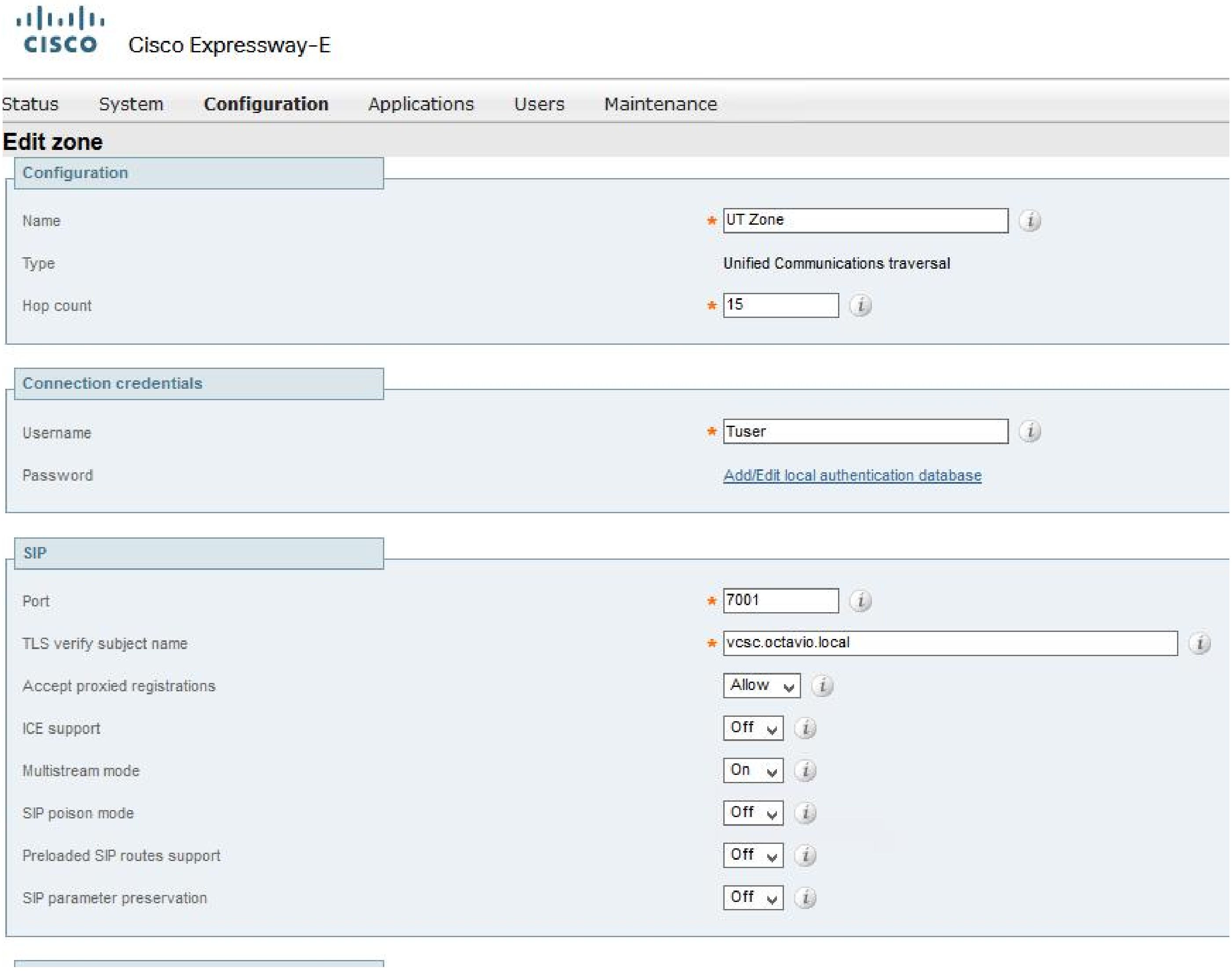
Cisco Expressway-E

Local authentication database

Records: 3

	Name	Action
□	admin	View/Edit
□	turnuser	View/Edit
□	Tuser	View/Edit

Step 4. Create a Unified Communication traversal zone as shown in the image.



Cisco Expressway-E

Edit zone

Configuration

Name	* UT Zone
Type	Unified Communications traversal
Hop count	* 15

Connection credentials

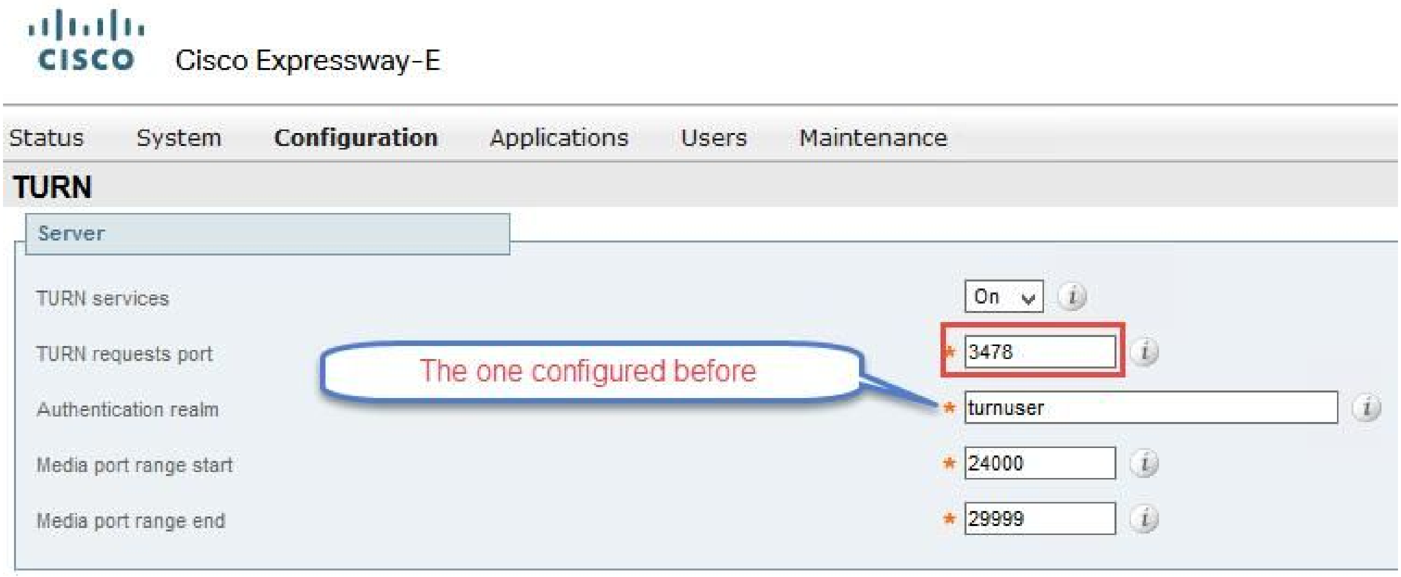
Username	* Tuser
Password	Add/Edit local authentication database

SIP

Port	* 7001
TLS verify subject name	* vcsc.octavio.local
Accept proxied registrations	Allow
ICE support	Off
Multistream mode	On
SIP poison mode	Off
Preloaded SIP routes support	Off
SIP parameter preservation	Off

Step 5. Configure the TURN server. Navigate to **Configuration > Traversal > TURN** as shown in the image.

> **Note**: The TURN request must be to the port 3478 as it is the port where the web client requests the TURN connection.

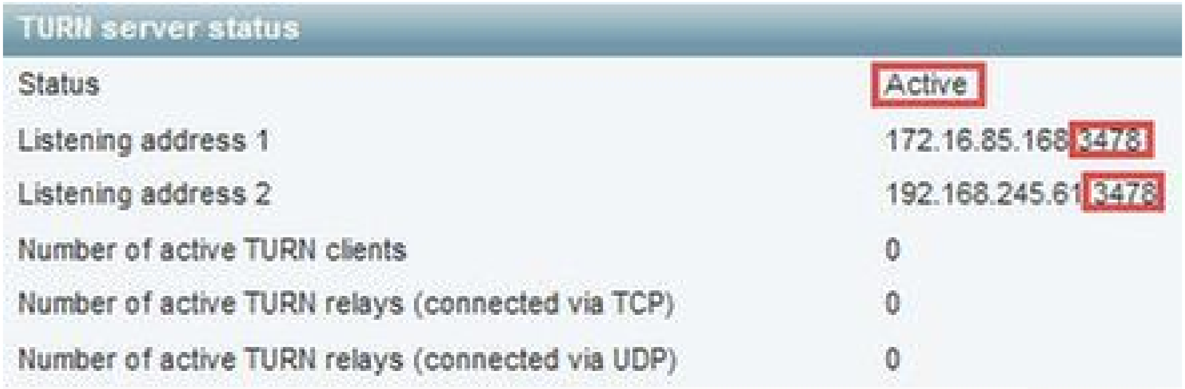


TURN

Server

TURN services	On
TURN requests port	* 3478
Authentication realm	* turnuser
Media port range start	* 24000
Media port range end	* 29999

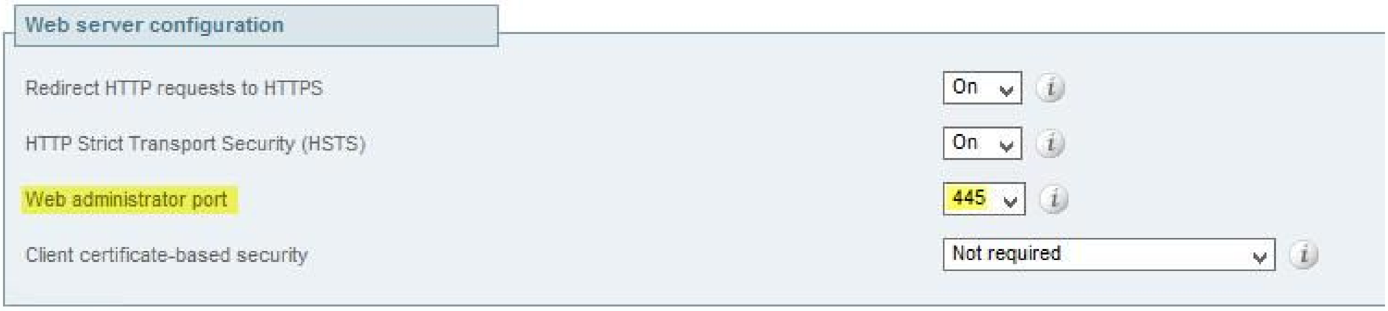
Once the Turn come up, the status shows Active as shown in the image.



TURN server status

Status	Active
Listening address 1	172.16.85.168 3478
Listening address 2	192.168.245.61 3478
Number of active TURN clients	0
Number of active TURN relays (connected via TCP)	0
Number of active TURN relays (connected via UDP)	0

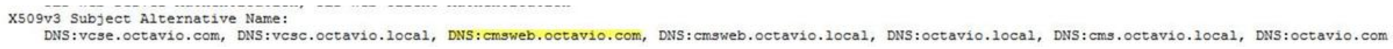
Step 6. Navigate to **System > Administration.** The webRTC client request access on port 443, for this reason the administration port of the Expressway-E must be changed to a different one, in this example case it is changed to 445 as shown in the image.



Web server configuration

Redirect HTTP requests to HTTPS	On
HTTP Strict Transport Security (HSTS)	On
Web administrator port	445
Client certificate-based security	Not required

Step 7. Certificate creation for the Expressway-E: the webbridge URL must be added as a SAN on the server certificate as shown in the image.



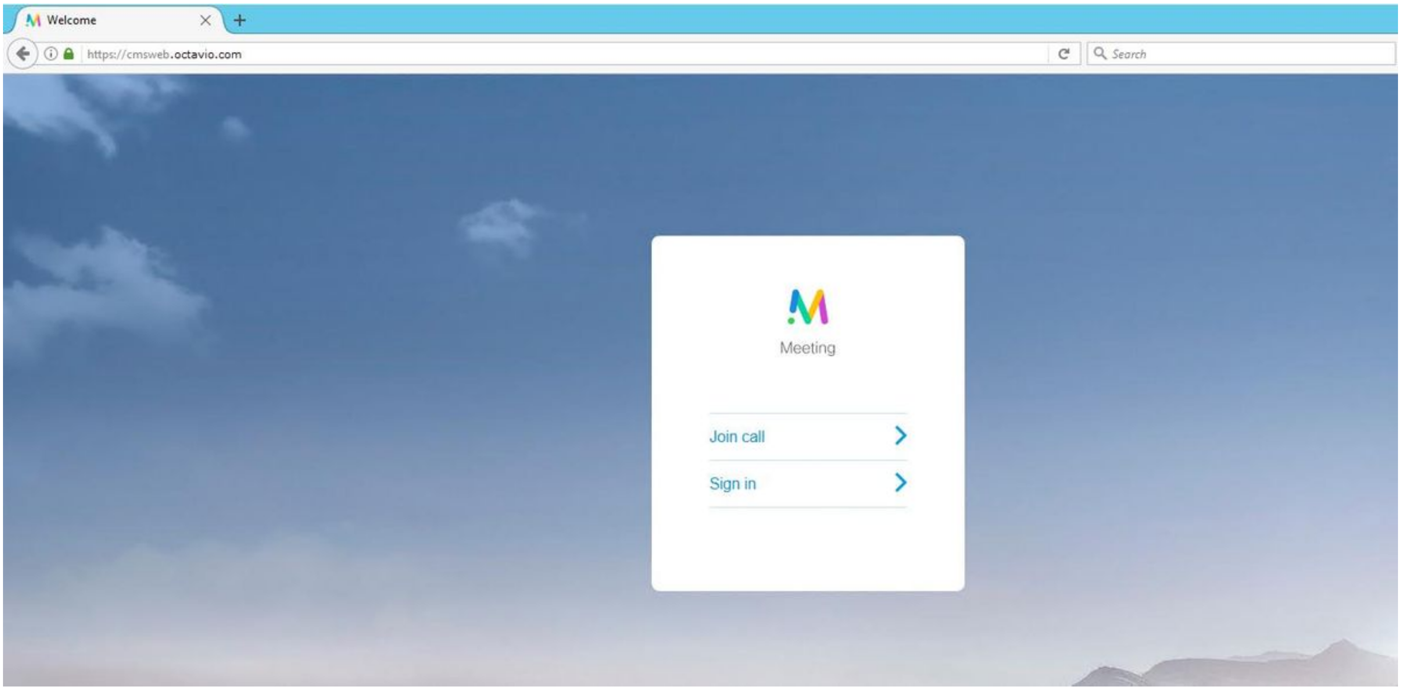
```
X509v3 Subject Alternative Name:
    DNS:vcse.octavio.com, DNS:vcsc.octavio.local, DNS:cmsweb.octavio.com, DNS:cmsweb.octavio.local, DNS:octavio.local, DNS:cms.octavio.local, DNS:octavio.com
```

Verify

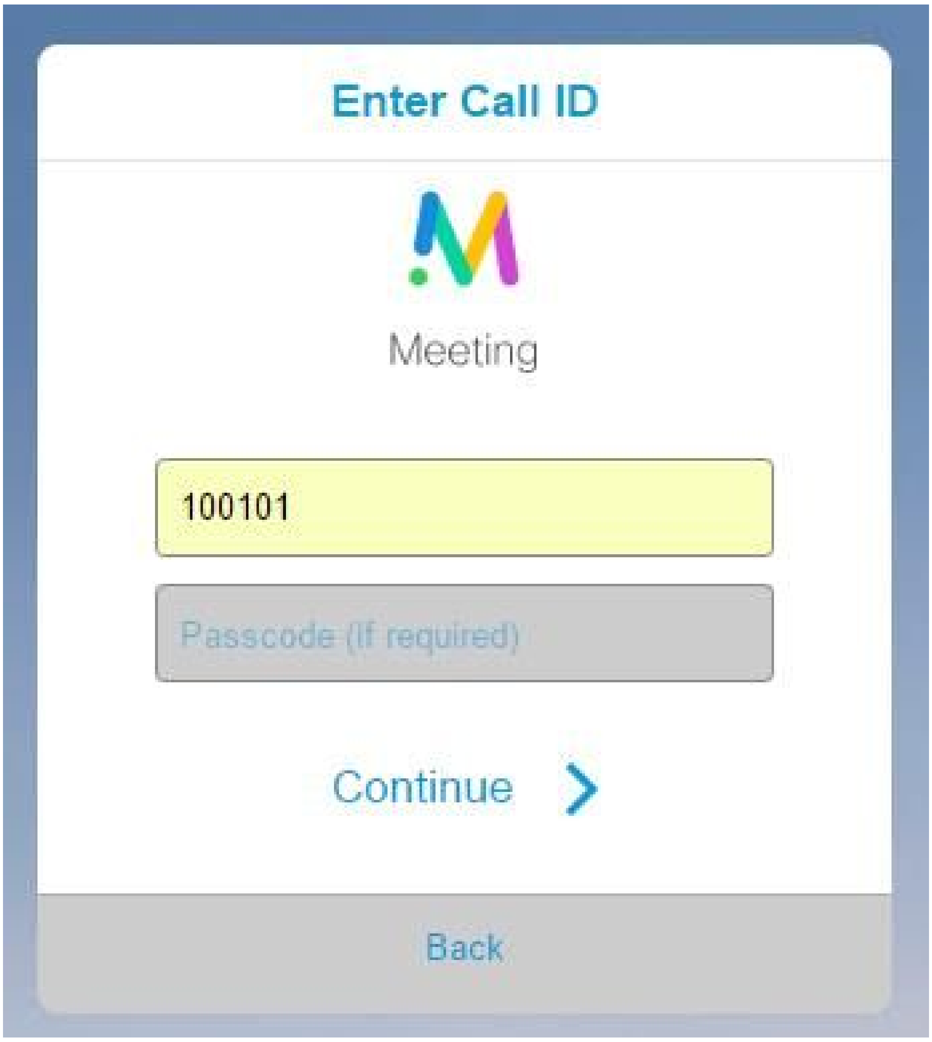
Use this section to confirm that your configuration works properly.

Step 1. Select a supported web browser and enter the external webbridge URL, you must see the next screen as shown in the image.

Note: You can find a list of supported browsers and versions on the link: https://kb.acano.com/content/2/4/en/what-versions-of-browsers-do-we-support-for-webrtc.html?highlight=html%5C-5%20compliant%20browsers#content



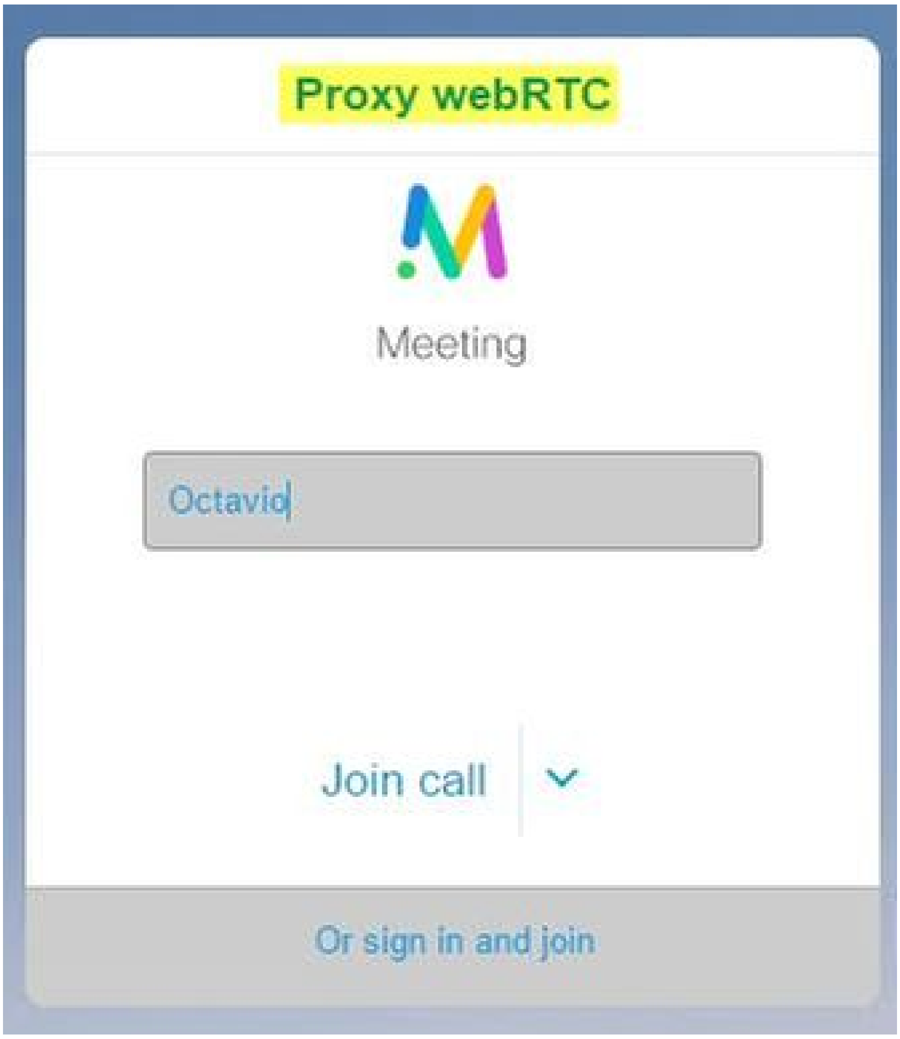
Step 2. Select **Join call** and enter the Space ID previously configured as shown in the image.



Enter Call ID

100101

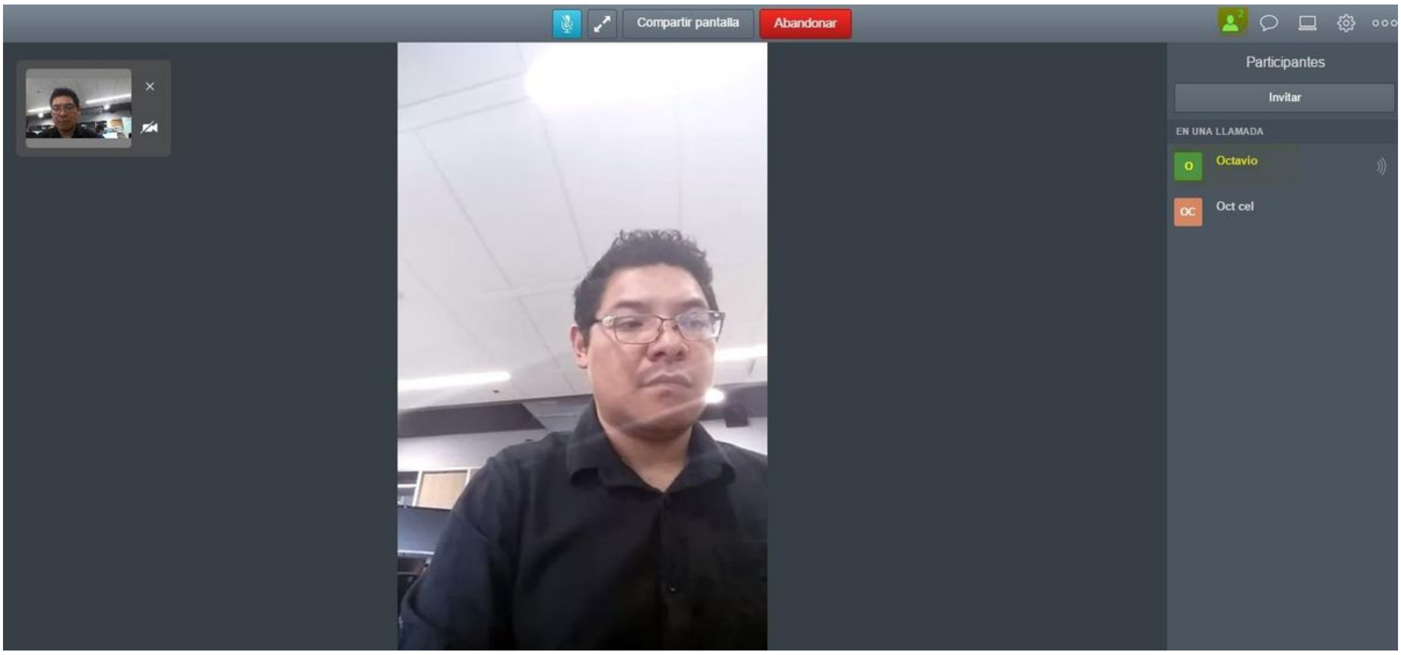
Step 3. Click **continue** and enter your name, at this point you must see the name of the space you’re going to join, in this case the space name is Proxy webRTC**.** Click **Join call** as shown in the image.



Proxy webRTC

Octavio

Step 4. Join with another device and you must see both devices connected in the conference as shown in the image.

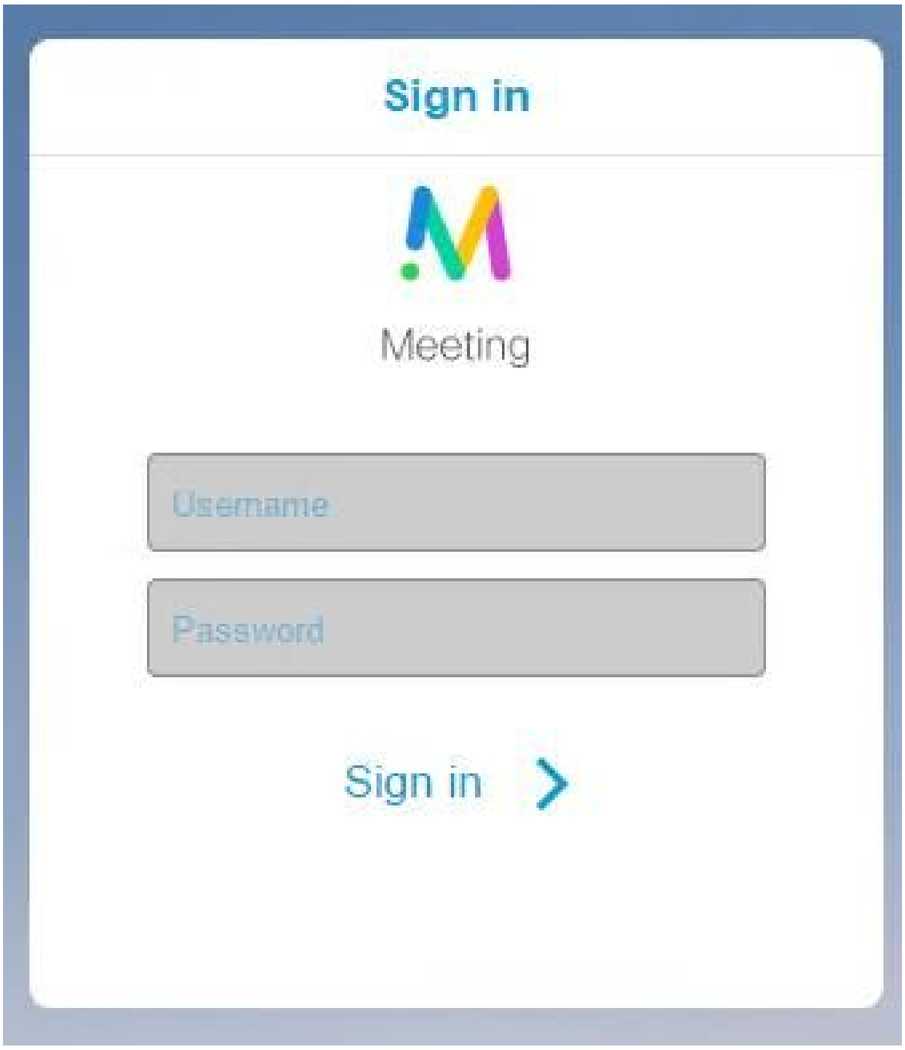


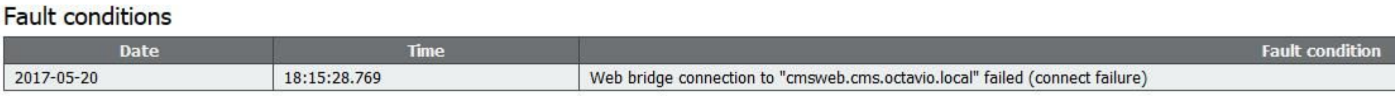
Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Join Call Button is Not Shown

The **Join call** button is not shown when you open the webbridge page and you see the error shown in the second image when you enter to the CMS web page as shown in the image.





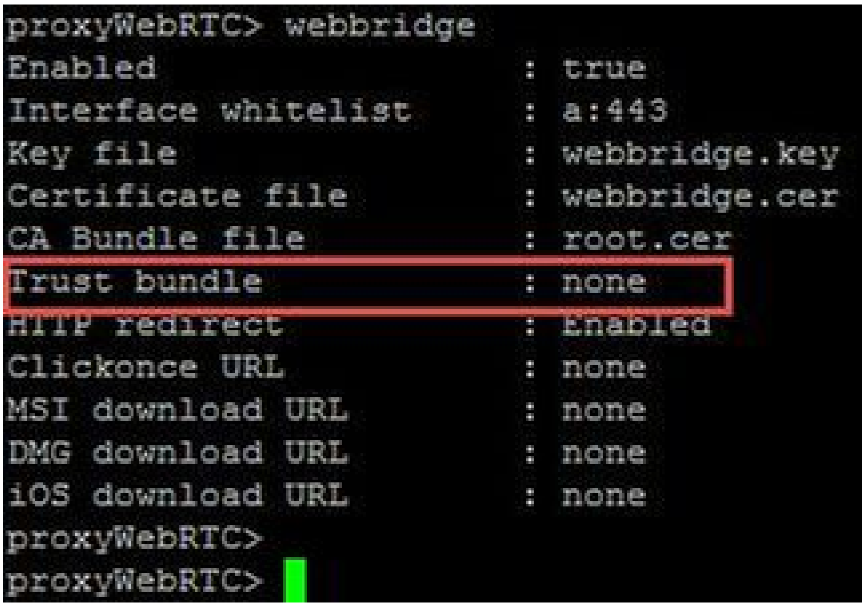
Fault conditions

Date	Time	Fault condition
2017-05-20	18:15:28.769	Web bridge connection to "cmsweb.cms.octavio.local" failed (connect failure)

The problem happens when the webbridge does not communicate correctly with the call bridge.

Solution

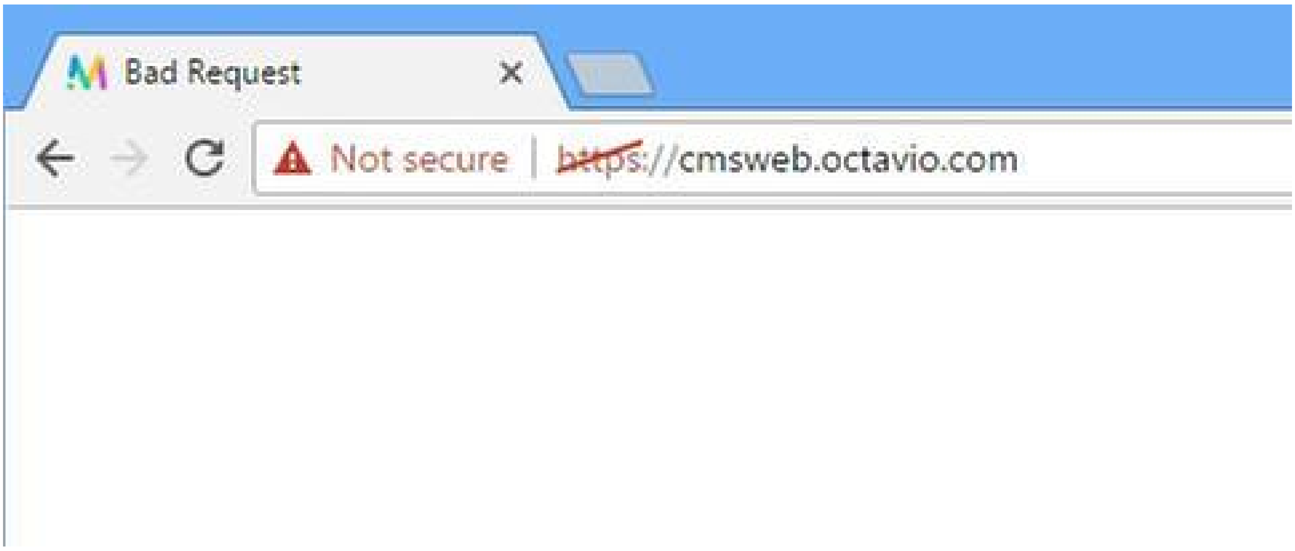
- Check the webbridge URL is correctly configured on the CMS admin webpage. Navigate to **Configuration > General** for this purpose.
- The webbridge and callbridge must trust each other, check the trust bundle is added to the webbridge configuration as shown in the images:



```
proxyWebRTC> webbridge
Enabled                   : true
Interface whitelist       : a:443
Key file                  : webbridge.key
Certificate file          : webbridge.cer
CA Bundle file            : root.cer
Trust bundle              : none
HTTP redirect             : Enabled
Clickonce URL             : none
MSI download URL          : none
DMG download URL          : none
iOS download URL          : none
proxyWebRTC>
proxyWebRTC>
```

Note: The trust bundle is the call bridge certificate.

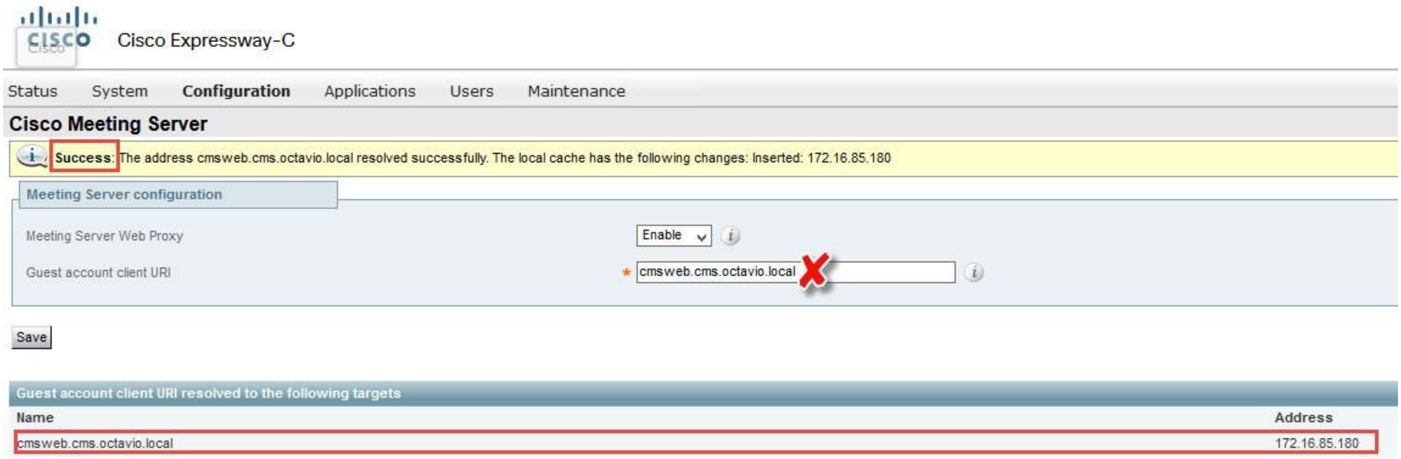
WebRTC Page Shows 'Bad Request'



Solution

- Check the correct Guest account client URI is configured on Expressway-C. Navigate to **Configuration > Unified Communication > Cisco Meeting Server** for this purpose.

If the internal URL is configured in the Guest account client URL, the Expressway-C will resolve it since there is a record created on the DNS server, but this can cause the "bad request" error message in the web browser. In this example case, the internal URL is configured in order to show the error as shown in the image.



Cisco Meeting Server

Success: The address cmsweb.cms.octavio.local resolved successfully. The local cache has the following changes: Inserted: 172.16.85.180

Meeting Server configuration

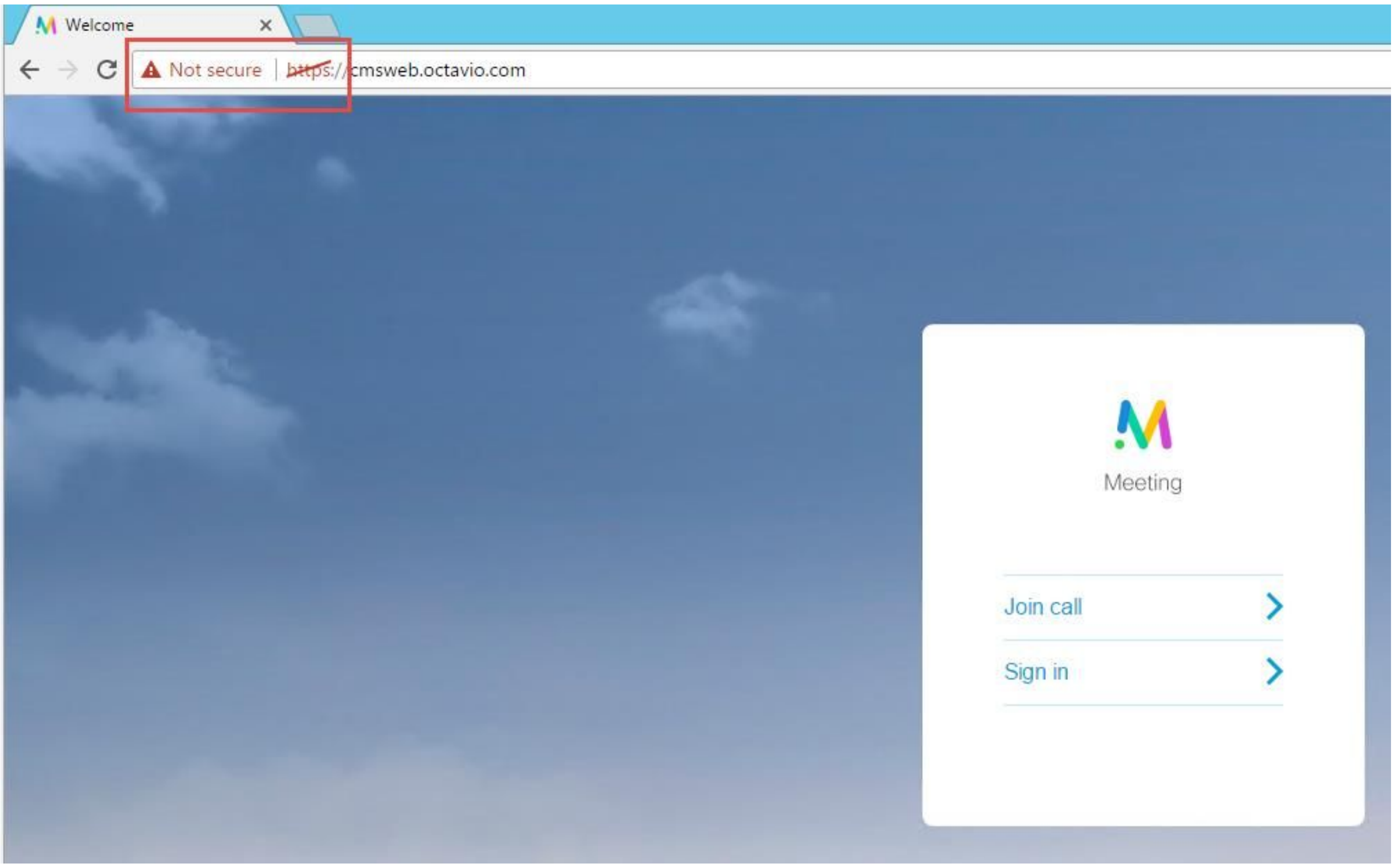
Meeting Server Web Proxy: Enable

Guest account client URI: cmsweb.cms.octavio.local

Guest account client URI resolved to the following targets

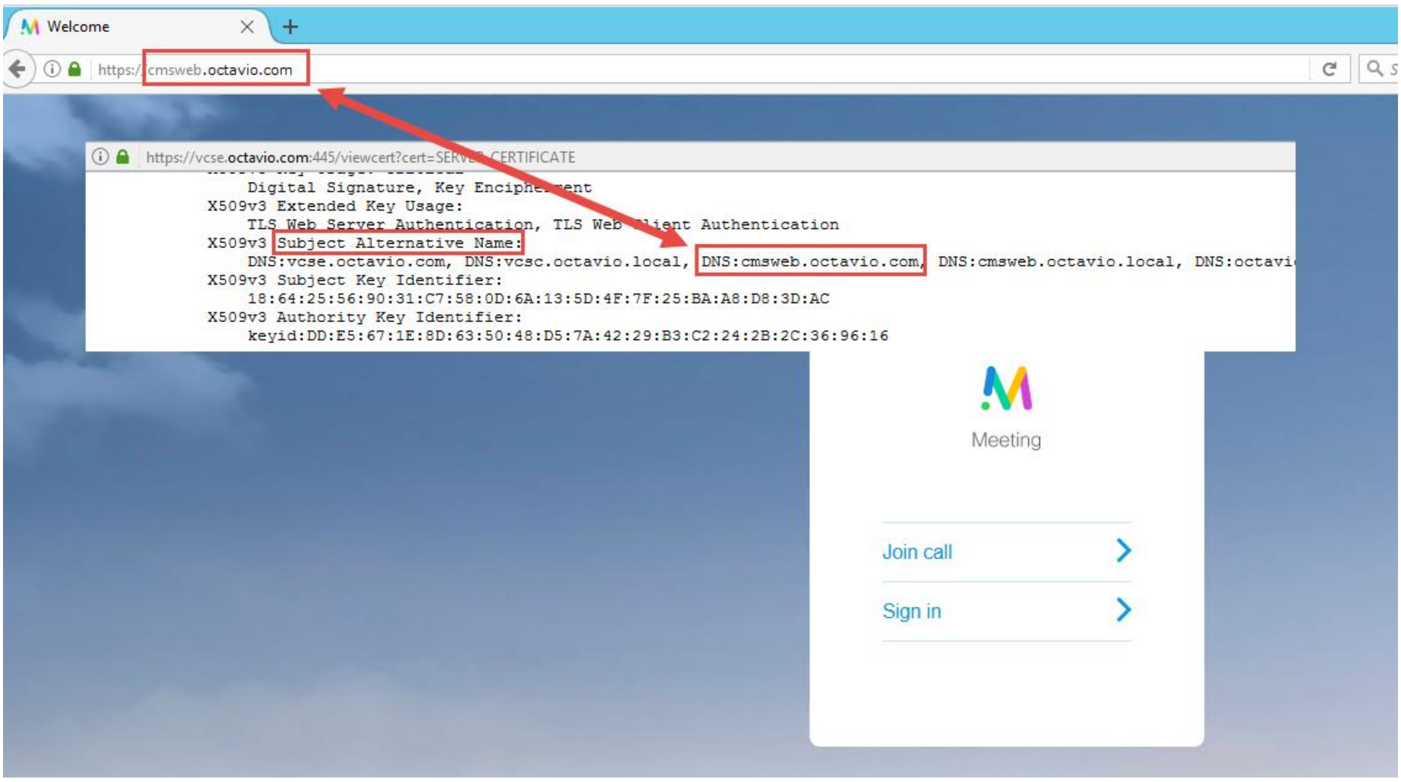
Name	Address
cmsweb.cms.octavio.local	172.16.85.180

WebRTC Client Shows Unsecure Connection



Solution

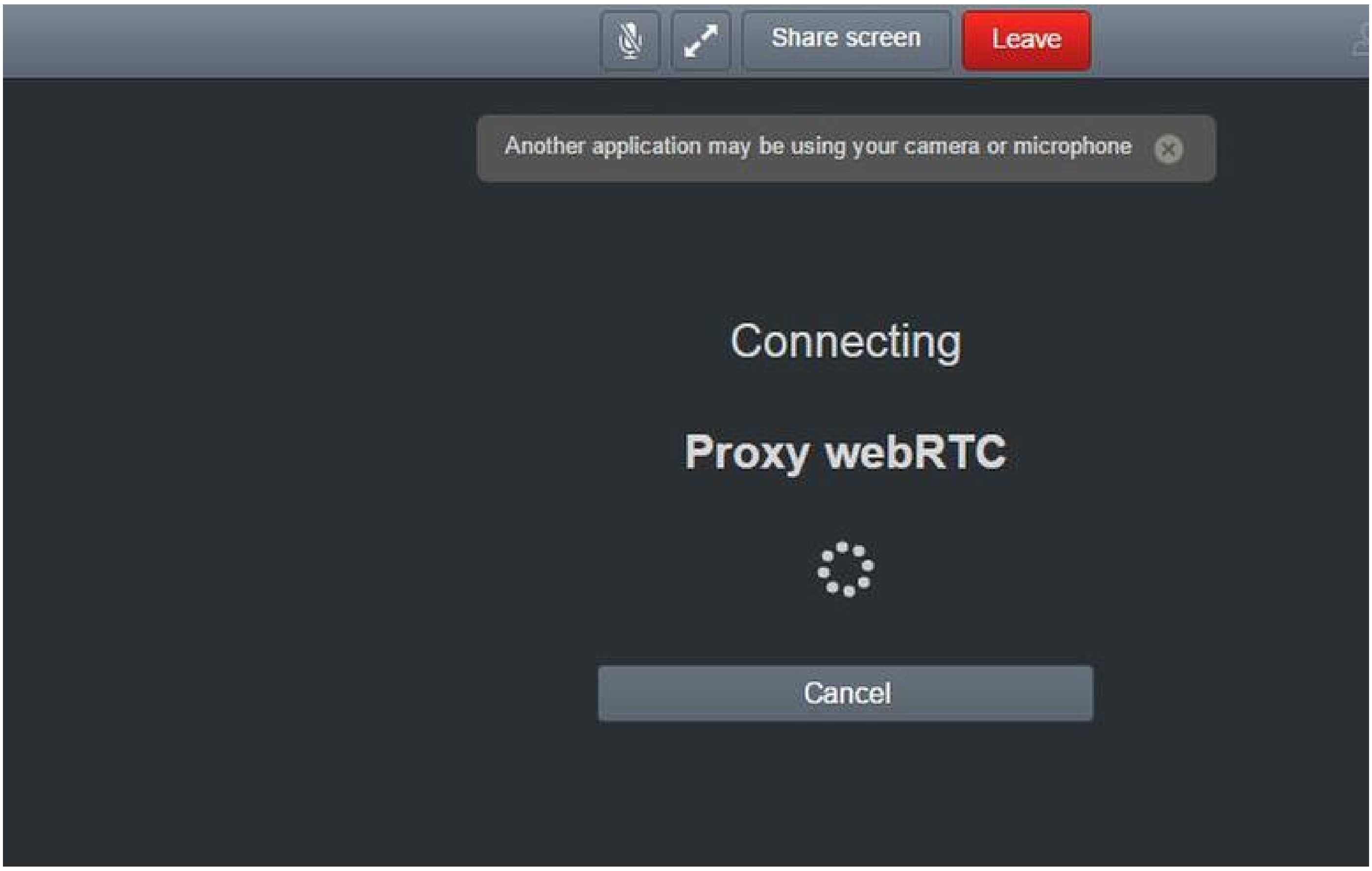
- The certificate is self-signed which causes the server to not trust the source. Change the certificate on the Expressway-E to a supported third party certificate authority.
- Check the external webbridge URL is added as a SAN on the Expressway-E server certificate as shown in the image.



https://vcse.octavio.com:445/viewcert?cert=SERVER_CERTIFICATE

```
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Subject Alternative Name:
        DNS:vcse.octavio.com, DNS:vcsc.octavio.local, DNS:cmsweb.octavio.com, DNS:cmsweb.octavio.local, DNS:octavi
    X509v3 Subject Key Identifier:
        18:64:25:56:90:31:C7:58:0D:6A:13:5D:4F:7F:25:BA:A8:D8:3D:AC
    X509v3 Authority Key Identifier:
        keyid:DD:E5:67:1E:8D:63:50:48:D5:7A:42:29:B3:C2:24:2B:2C:36:96:16
```

WebRTC Client Connects but Never Gets Connected and Then it Timed Out And Disconnects

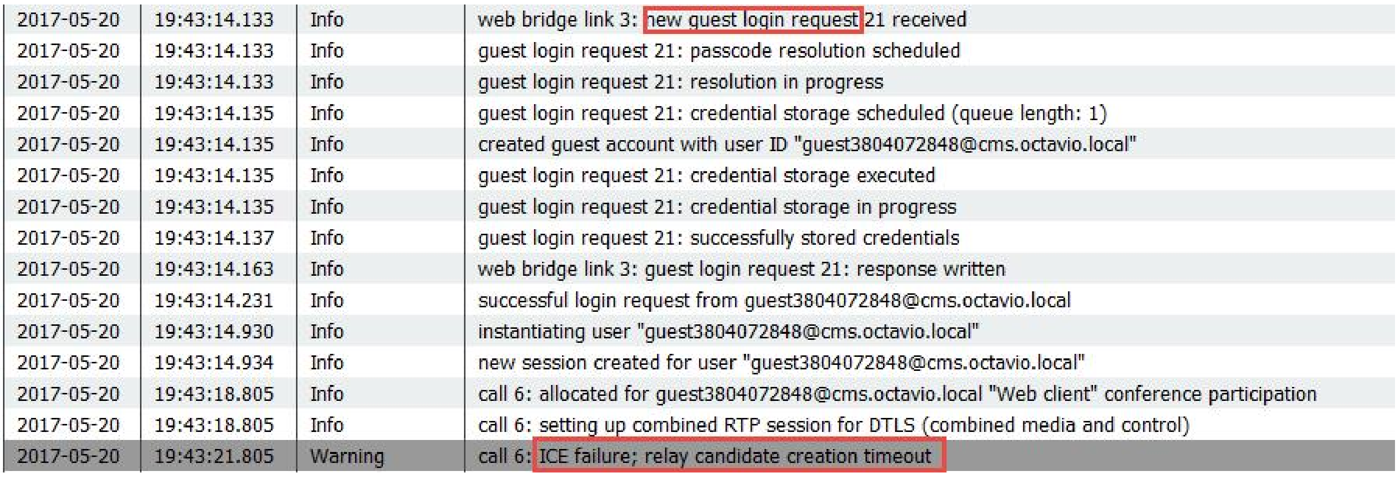


Another application may be using your camera or microphone

Connecting

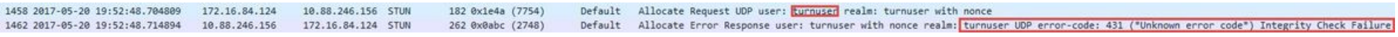
Proxy webRTC

The TURN server username or password are incorrectly configured either on the expressway-E or in the CMS via API. The logs contains the errors shown in the image.



```
2017-05-20   19:43:14.133   Info      web bridge link 3: new guest login request 21 received
2017-05-20   19:43:14.133   Info      guest login request 21: passcode resolution scheduled
2017-05-20   19:43:14.133   Info      guest login request 21: resolution in progress
2017-05-20   19:43:14.135   Info      guest login request 21: credential storage scheduled (queue length: 1)
2017-05-20   19:43:14.135   Info      created guest account with user ID "guest3804072848@cms.octavio.local"
2017-05-20   19:43:14.135   Info      guest login request 21: credential storage executed
2017-05-20   19:43:14.135   Info      guest login request 21: credential storage in progress
2017-05-20   19:43:14.137   Info      guest login request 21: successfully stored credentials
2017-05-20   19:43:14.163   Info      web bridge link 3: guest login request 21: response written
2017-05-20   19:43:14.231   Info      successful login request from guest3804072848@cms.octavio.local
2017-05-20   19:43:14.930   Info      instantiating user "guest3804072848@cms.octavio.local"
2017-05-20   19:43:14.934   Info      new session created for user "guest3804072848@cms.octavio.local"
2017-05-20   19:43:18.805   Info      call 6: allocated for guest3804072848@cms.octavio.local "Web client" conference participation
2017-05-20   19:43:18.805   Info      call 6: setting up combined RTP session for DTLS (combined media and control)
2017-05-20   19:43:21.805   Warning   call 6: ICE failure; relay candidate creation timeout
```

The error can be confirmed with a packet capture too. Run Wireshark on the PC where the webRTC client runs. Once you have the packet capture, filter the packets by STUN. You must see the errors shown in the image.

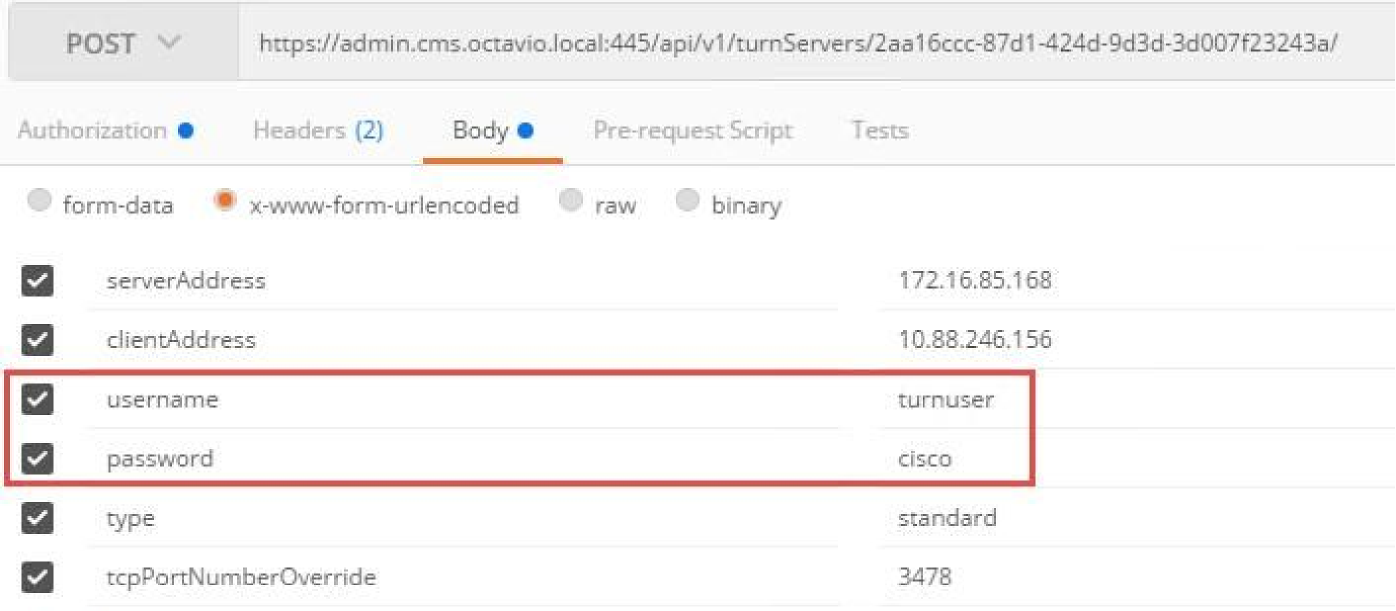


```
1458 2017-05-20 19:52:48.704809   172.16.84.124   10.88.246.156  STUN   182 0x1e4a (7754)   Default   Allocate Request UDP user: turnuser realm: turnuser with nonce
1462 2017-05-20 19:52:48.714894   10.88.246.156   172.16.84.124  STUN   262 0x0abc (2748)   Default   Allocate Error Response user: turnuser with nonce realm: turnuser UDP error-code: 431 ("Unknown error code") Integrity Check Failure
```

The PC sends an Allocate Request and the Expresssway NAT address answers with 'Integrity check failure' message.

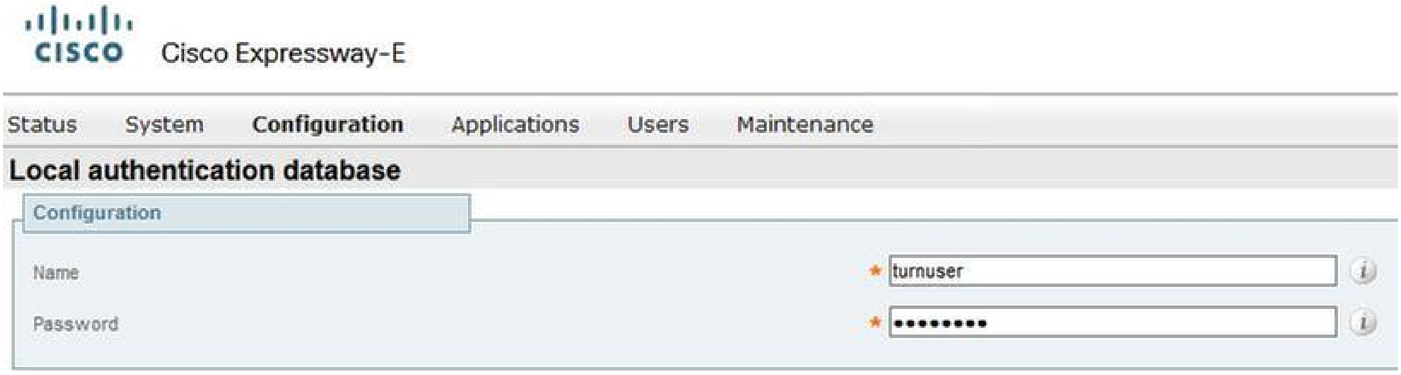
Solution

In order to fix the error, review the username and password. They must be correctly configured on the TURN server parameters as shown in the images.



POST https://admin.cms.octavio.local:445/api/v1/turnServers/2aa16ccc-87d1-424d-9d3d-3d007f23243a/

☑	serverAddress	172.16.85.168
☑	clientAddress	10.88.246.156
☑	username	turnuser
☑	password	cisco
☑	type	standard
☑	tcpPortNumberOverride	3478



Local authentication database

Configuration

Name * turnuser

Password * ••••••••