

Configuración de Proxy WebRTC con CMS sobre Expressway con dominio doble

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Información técnica](#)

[Configuración de DNS](#)

[Configuración de DNS interno](#)

[Configuración de DNS externo](#)

[Configuración de CMS, Callbridge, Webbridge y XMPP](#)

[Configuración TURN](#)

[Configuración de Expressway-C y E](#)

[Configuración en Expressway-C](#)

[Configuración en Expressway-E](#)

[Verificación](#)

[Troubleshoot](#)

[No se muestra el botón Conectar a llamada](#)

[La página WebRTC muestra 'Solicitud incorrecta'](#)

[El cliente WebRTC muestra una conexión no segura](#)

[El cliente WebRTC se conecta pero nunca se conecta y luego se agota el tiempo de espera y se desconecta](#)

Introducción

Este documento describe una configuración de ejemplo de Web Real-Time Communication (WebRTC) proxy para Cisco Meeting Server (CMS) a través de Expressway con diferentes dominios internos y externos.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Versión 2.1.4 de implementación combinada única de CMS y posterior
- Expressway C y Expressway E versión X8.9.2 y posterior
- Callbridge y webbridge configurados en CMS
- Acceso remoto y móvil (MRA) habilitado en el par de Expressway

- Tecla de opción Traversal mediante NAT de retransmisión (TURN) agregada a Expressway-E
- Registro externo de servidor de nombres de dominio (DNS) resoluble para URL de webbridge, para dominio externo
- Registro DNS resoluble interno para la dirección IP de CMS del dominio externo al interno
- Varios dominios Extensible Messaging and Presence Protocol (XMPP) configurados en CMS para dominio interno y externo
- Puerto TCP 443 abierto en el servidor de seguridad de la Internet pública a dirección de (dirección) del Expressway-E
- El puerto TCP y UDP 3478 se abrió en el firewall desde la Internet pública a la dirección IP pública de Expressway-E
- El intervalo de puertos UDP 24000-29999 se abrió en el firewall hacia y desde la dirección IP pública de Expressway-E

Componentes Utilizados

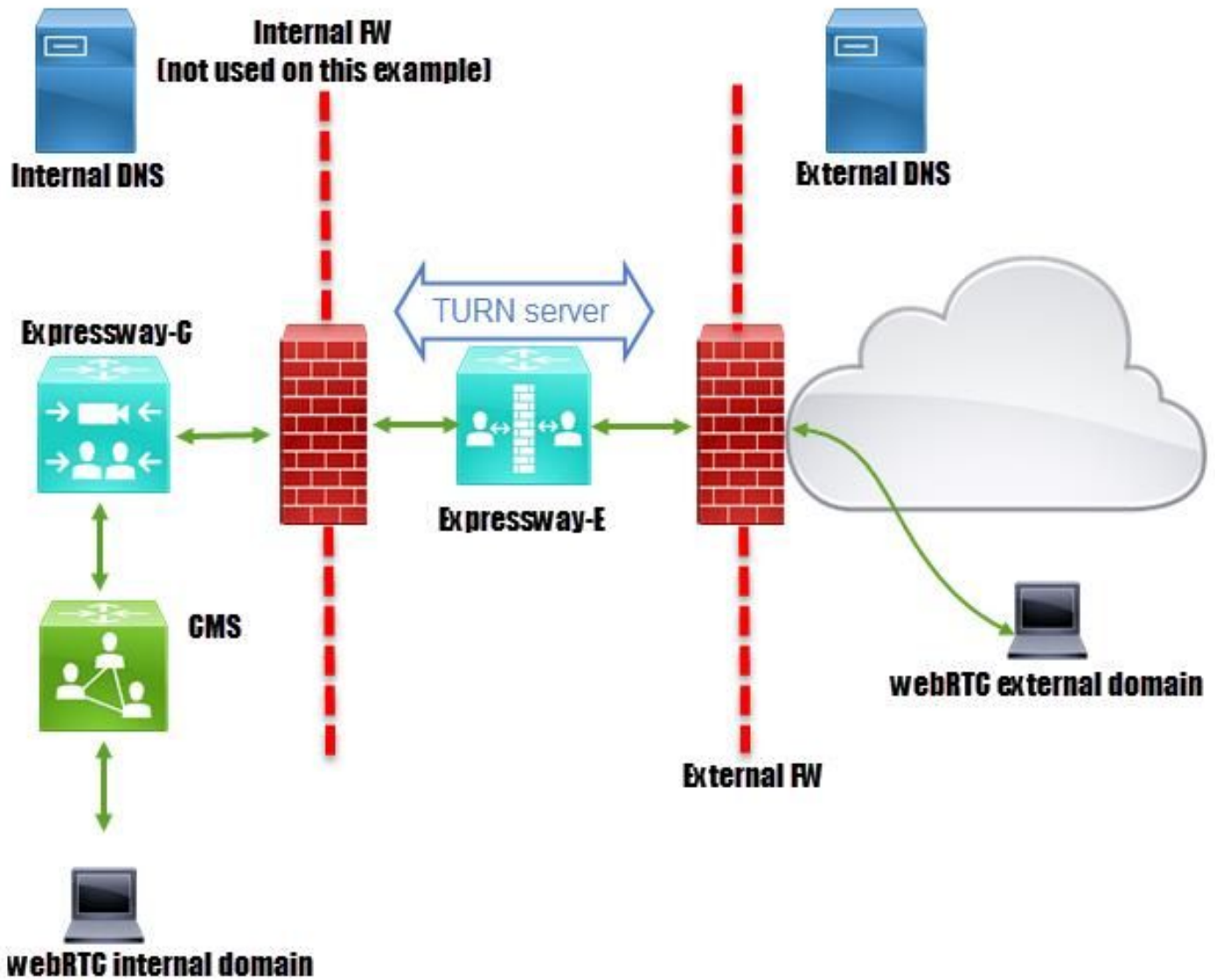
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 2.2.1 de implementación combinada única de CMS
- Expressway-C y Expressway-E con tarjeta de interfaz de red (NIC) dual y software de traducción de direcciones de red (NAT) estática versión 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.

Configurar

Diagrama de la red



Información técnica

Dominio interno	cms.octavio.local
Dominio externo	octavio.com
Dirección IP de CMS	172.16.85.180
Dirección IP de Expressway-C	172.16.85.167
Dirección IP LAN1 de Expressway-E (interna)	172.16.85.168
Dirección IP LAN2 de Expressway-E (externa)	192.168.245.61
Dirección IP NAT estática	10.88.246.156

Configuración de DNS

Configuración de DNS interno

Name	Type	Data	Timestamp
ACTIVEDIRECTORY			
Forward Lookup Zones			
_msdcs.octavio.local			
octavio.com			
_tcp			
_xmpp-client	Service Location (SRV)	[10][10][5222] xmpp.cms.octavio.local.	static
_xmpp-server	Service Location (SRV)	[10][10][5209] 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

Name	Type	Data	Timestamp
vcse	Host (A)	External webbridge URL resolves to internal IP address	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

Configuración de DNS externo

El DNS externo debe tener la URL de webbridge que se resuelve a la dirección IP NAT estática de Expressway-E, como se muestra en la imagen.

Name	Type	Data
(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

Configuración de CMS, Callbridge, Webbridge y XMPP

Paso 1. Debe tener activada la licencia de callbridge. La imagen muestra una licencia de callbridge activa.

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

Para obtener más información sobre licencias:

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

Paso 2. Habilite callbridge, webbridge y XMPP a través de MMP como se muestra en la imagen.

```
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
```

Siga este enlace para ver un proceso detallado sobre cómo habilitarlos:

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

Siga este enlace para ver un proceso detallado sobre cómo crear un certificado:

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

Paso 3. Navegue hasta la página web de CMS en **Configuration > General** y configure la URL interna y externa para el webbridge como se muestra en la imagen.

Web bridge settings

Guest account client URI:

Guest account JID domain:

Custom background image URI:

Custom login logo URI:

Guest access via ID and passcode:

Guest access via hyperlinks:

User sign in:

Joining scheduled Lync conferences by ID:

IVR

IVR numeric ID:

Joining scheduled Lync conferences by ID:

External access

Web Bridge URI:

IVR telephone number:

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

Nota: El CMS debe configurarse con al menos un espacio.

Ejemplo de un espacio configurado en CMS como se muestra en la imagen.

<input type="checkbox"/>	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
<input type="checkbox"/>	Proxy webRTC	proxywebrtc@cms.octavio.local			100101

Nota: Las llamadas entrantes deben configurarse para los dominios internos y externos

Un ejemplo de dominios configurados para el manejo de llamadas entrantes es como se muestra en la imagen.

Incoming call handling

Call matching

<input type="checkbox"/>	Domain name	Priority	Targets spaces
<input type="checkbox"/>	cms.octavio.local	10	yes
<input type="checkbox"/>	octavio.com	10	yes

Configuración TURN

Paso 1. La función TURN se debe configurar mediante API a través de Postman. Este comando

se utiliza en toda la configuración.

<https://>

Paso 2. Utilice el método POST y navegue hasta **Body** para ver los parámetros del servidor TURN o editarlos. Los parámetros configurados para el servidor TURN son como se muestra en la imagen.

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

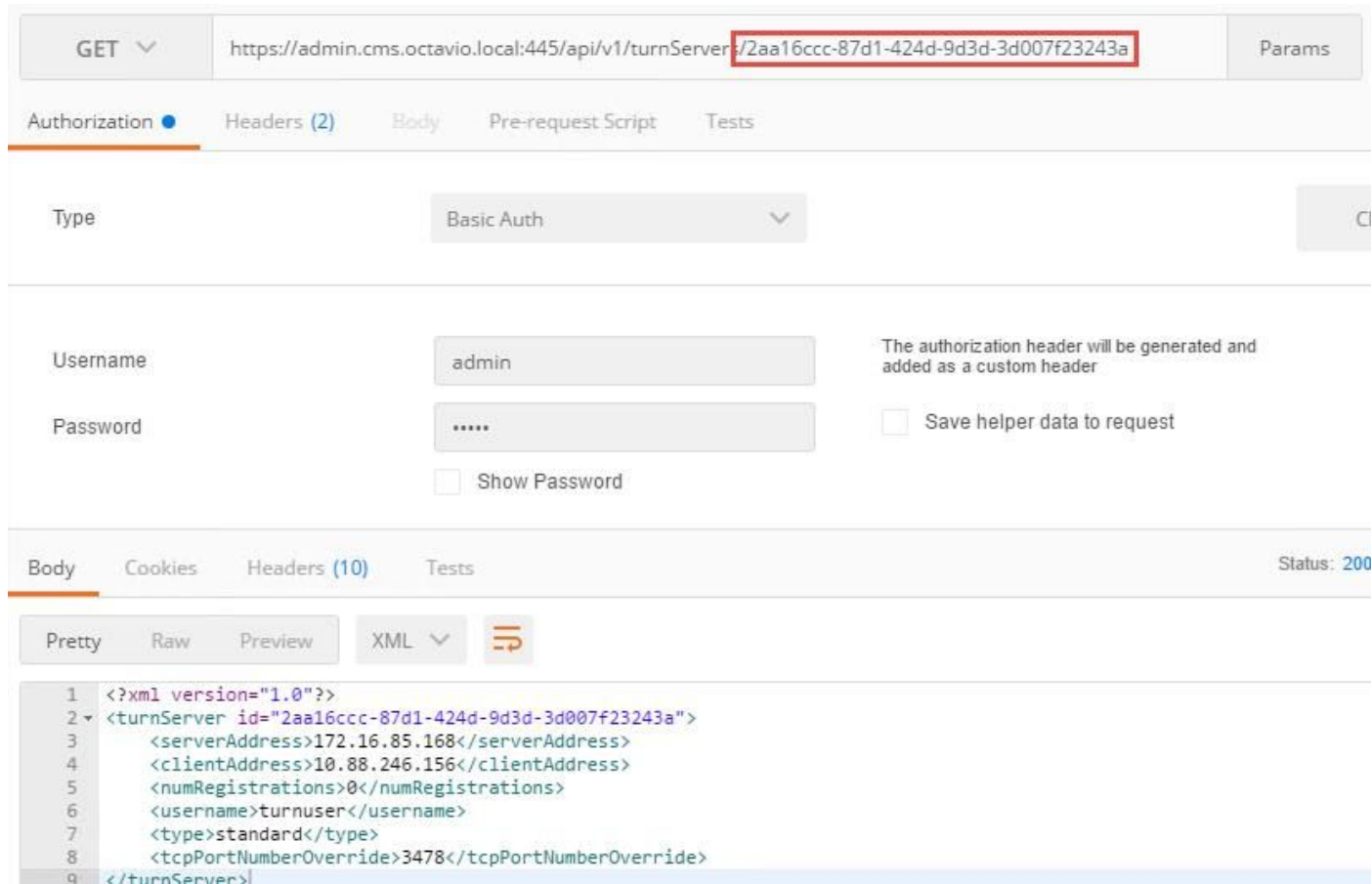
Paso 3. Verifique el estado de la configuración del servidor TURN ejecutando el método GET y copie el ID del servidor. El ID que se debe copiar es como se muestra en la imagen.

```
<?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>
```

Paso 4. Copie el ID al final del comando API y utilice el método GET para ver la información del

servidor TURN como se muestra en la imagen.

Nota: La información no mostrará la contraseña del servidor.



Paso 5. Haga clic en **send** para obtener el estado del servidor. Un ejemplo de una configuración exitosa como se muestra en la imagen.

The screenshot shows a REST client interface with the following details:

- Method:** GET
- URL:** `https://admin.cms.octavio.local:445/api/v1/turnServers/2aa16ccc-87d1-424d-9d3d-3d007f23243a/status`
- Authorization:** Basic Auth
- Username:** admin
- Password:** [Redacted]
- Body:** XML response

```
1 <?xml version="1.0"?>
2 <turnServer>
3   <status>success</status>
4   <host>
5     <address>172.16.85.168</address>
6     <portNumber>3478</portNumber>
7     <reachable>true</reachable>
8     <roundTripTimeMs>52</roundTripTimeMs>
9     <mappedAddress>172.16.85.180</mappedAddress>
10    <mappedPortNumber>41574</mappedPortNumber>
11  </host>
12 </turnServer>
```

Configuración de Expressway-C y E

Paso 1. Expressway-C debe tener el dominio interno (octavio.local) y Expressway-E debe tener el dominio externo (octavio.com) configurado como se muestra en la imagen.



DNS

DNS settings

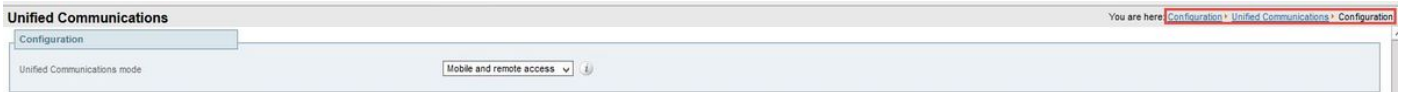
System host name	<input type="text" value="vcsc"/>	
Domain name	<input type="text" value="octavio.local"/>	
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>	

Default DNS servers

Address 1	<input type="text" value="172.16.85.162"/>	
-----------	--	--

Internal DNS server

Paso 2. MRA debe estar habilitado en Expressway C y E como se muestra en la imagen.



Paso 3. Cree una zona transversal de Unified Communication entre Expressway-C y E como se muestra en la imagen.



Edit zone

Configuration	
Name	<input type="text" value="UT Zone"/> ⓘ
Type	<input type="text" value="Unified Communications traversal"/>
Hop count	<input type="text" value="15"/> ⓘ

Connection credentials	
Username	<input type="text" value="Tuser"/> ⓘ
Password	<input type="password" value="....."/> ⓘ

SIP	
Port	<input type="text" value="7001"/> ⓘ
Accept proxied registrations	<input type="text" value="Allow"/> ⓘ
ICE support	<input type="text" value="Off"/> ⓘ
Multistream mode	<input type="text" value="On"/> ⓘ
SIP poison mode	<input type="text" value="Off"/> ⓘ
Preloaded SIP routes support	<input type="text" value="Off"/> ⓘ
SIP parameter preservation	<input type="text" value="Off"/> ⓘ

Authentication	
Authentication policy	<input type="text" value="Do not check credentials"/> ⓘ

This credentials are configured on Exp-E

Configuración en Expressway-C

Paso 1. Configure el dominio interno y externo en Expressway-C como se muestra en la imagen.



Status System **Configuration** Application

Domains

Index	Domain name
<input type="checkbox"/> 1	octavio.local
<input type="checkbox"/> 2	octavio.com

Paso 2. Habilite la configuración de Cisco Meeting. Vaya a **Configuration > Unified Communications > Cisco Meeting Server** (Configuración > Comunicaciones unificadas > Cisco Meeting Server). Configure la URL de webbridge externa en el campo URI del cliente de cuenta de invitado como se muestra en la imagen.



Status System **Configuration** Applications Users Maintenance

Cisco Meeting Server

Meeting Server configuration

Meeting Server Web Proxy Enable *i*

Guest account client URI *i*

Guest account client URI resolved to the following targets

Name	Address
cmsweb.octavio.com	172.16.85.180

Nota: El DNS interno debe resolver la URL de webbridge externa (cmsweb.octavio.com) a la dirección IP de webbridge CMS interna. En este caso de ejemplo, la IP es 172.16.85.180.

Los túneles Secure Shell (SSH) de Expressway-C deben activarse después de unos segundos como se muestra en la imagen.



Status System Configuration Applications Users Maintenance

Unified Communications SSH tunnels status

You are here: Status > Unified Communications

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

Nota: El servidor debe tener un certificado de servidor y un certificado de CA.

Configuración en Expressway-E


Paso 1. Expressway-E debe tener una licencia de activación como se muestra en la imagen.

Status System Configuration Applications Users **Maintenance**

Option keys

Key	Description	Status
<input type="checkbox"/> ██████████	Expressway Series	Active
<input type="checkbox"/> ██████████	H323-SIP Interworking Gateway	Active
<input type="checkbox"/> ██████████	1800 TURN Relays	Active
<input type="checkbox"/> ██████████	Advanced Networking	Active

Paso 2. Expressway-E debe configurarse con el dominio externo como se muestra en la imagen.

 Cisco Expressway-E

Status **System** Configuration Applications Users Maintenance

DNS

DNS settings

System host name ⓘ

Domain name ⓘ


Default DNS servers

Address 1 ⓘ

Address 2 ⓘ

External DNS server

Paso 3. Cree usuarios para el servidor TURN y para la zona transversal de Unified Communication como se muestra en la imagen.

 Cisco Expressway-E

Status System **Configuration** Applications Users Maintenance



Local authentication database


Records: 3









Name	Action
<input type="checkbox"/> admin	View/Edit
<input type="checkbox"/> turnuser	View/Edit
<input type="checkbox"/> Tuser	View/Edit

Paso 4. Cree una zona transversal de Unified Communication como se muestra en la imagen.

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 

Paso 5. Configure el servidor de activación. Vaya a **Configuration > Traversal > TURN** como se muestra en la imagen.

Nota: La solicitud TURN debe estar en el puerto 3478 ya que es el puerto donde el cliente web solicita la conexión TURN.



TURN

Server

TURN services On *i*

TURN requests port * *i*

Authentication realm * *i*

Media port range start * *i*

Media port range end * *i*

The one configured before

Una vez que se activa la ventana, el estado muestra Active como se muestra en la imagen.

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

Paso 6. Vaya a **Sistema > Administración**. El cliente webRTC solicita acceso en el puerto 443, por esta razón el puerto de administración de Expressway-E debe cambiarse a otro, en este caso se cambia a 445 como se muestra en la imagen.

Web server configuration

Redirect HTTP requests to HTTPS On *i*

HTTP Strict Transport Security (HSTS) On *i*

Web administrator port *i*

Client certificate-based security *i*

Paso 7. Creación de certificados para Expressway-E: la URL de webbridge se debe agregar como una SAN en el certificado del servidor como se muestra en la imagen.

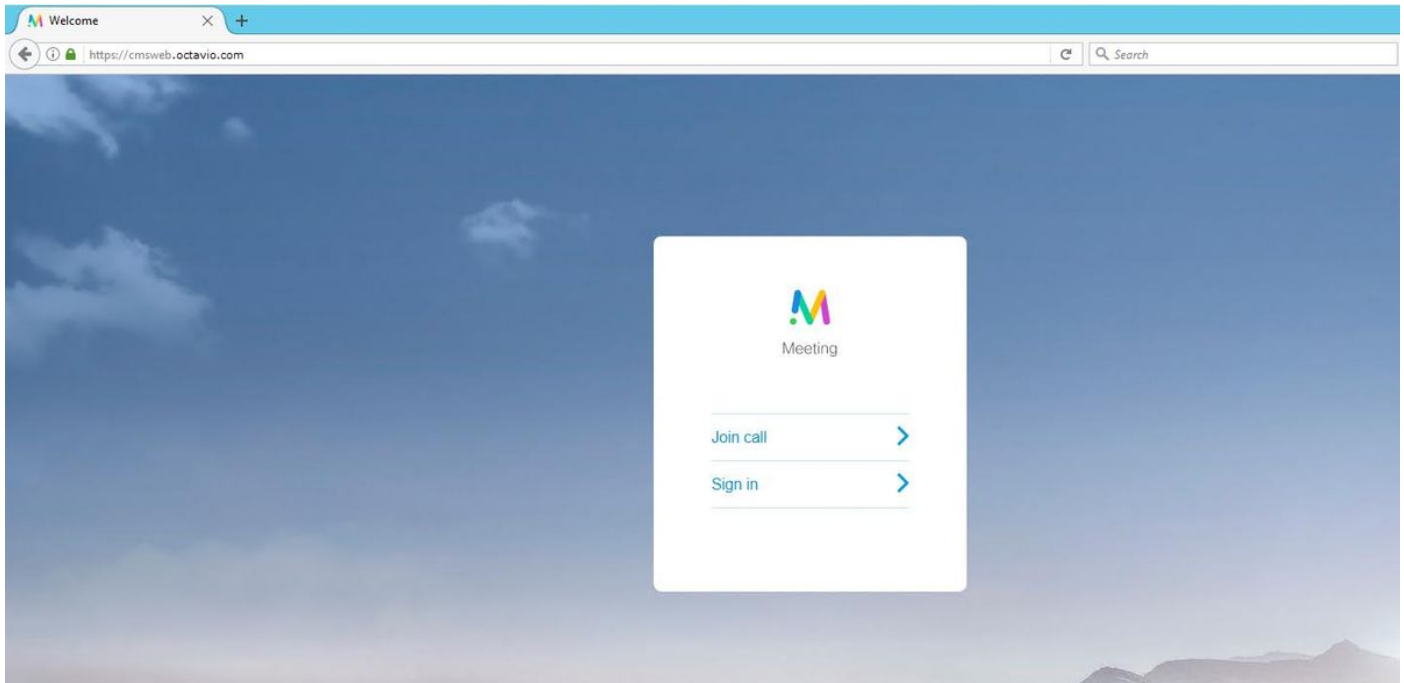
X509v3 Subject Alternative Name:
DNS:vcse.octavio.com, DNS:vcse.octavio.local, **DNS:cmsweb.octavio.com**, DNS:cmsweb.octavio.local, DNS:octavio.local, DNS:cms.octavio.local, DNS:octavio.com

Verificación

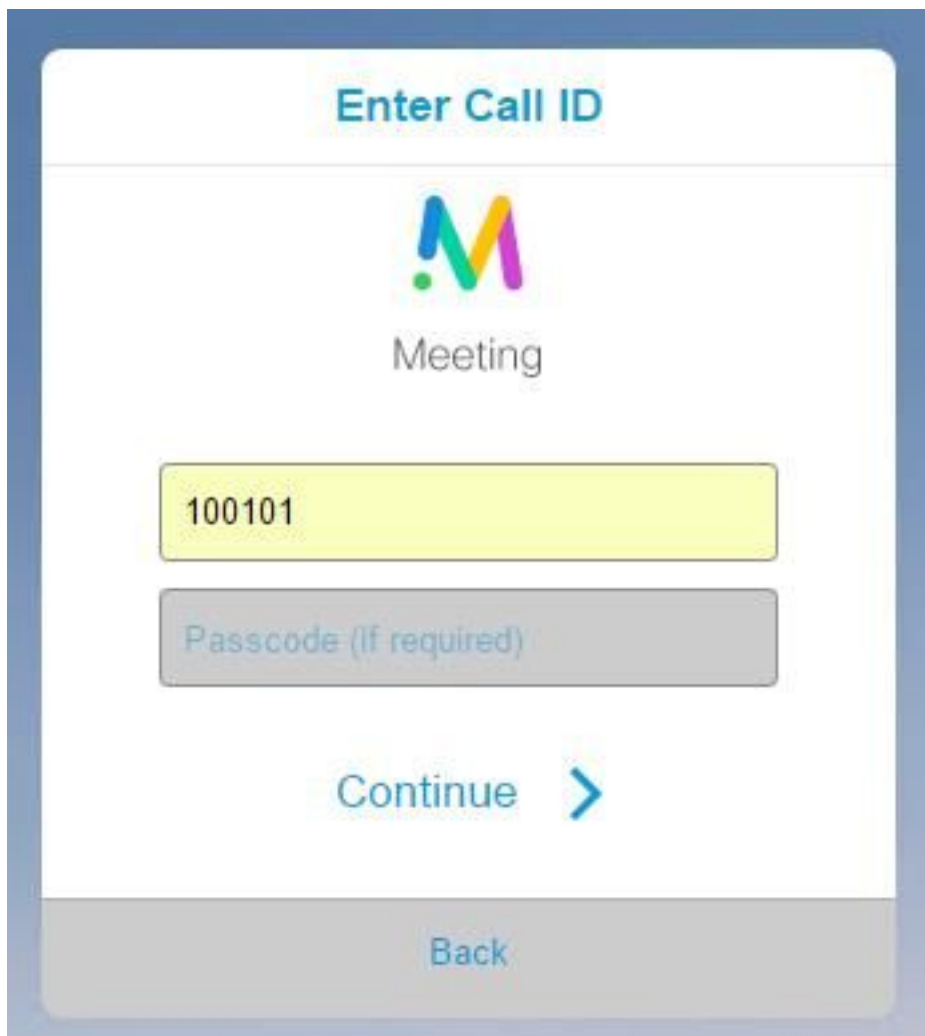
Use esta sección para confirmar que su configuración funciona correctamente.

Paso 1. Seleccione un navegador web admitido e ingrese la URL de webbridge externa, debe ver la siguiente pantalla como se muestra en la imagen.

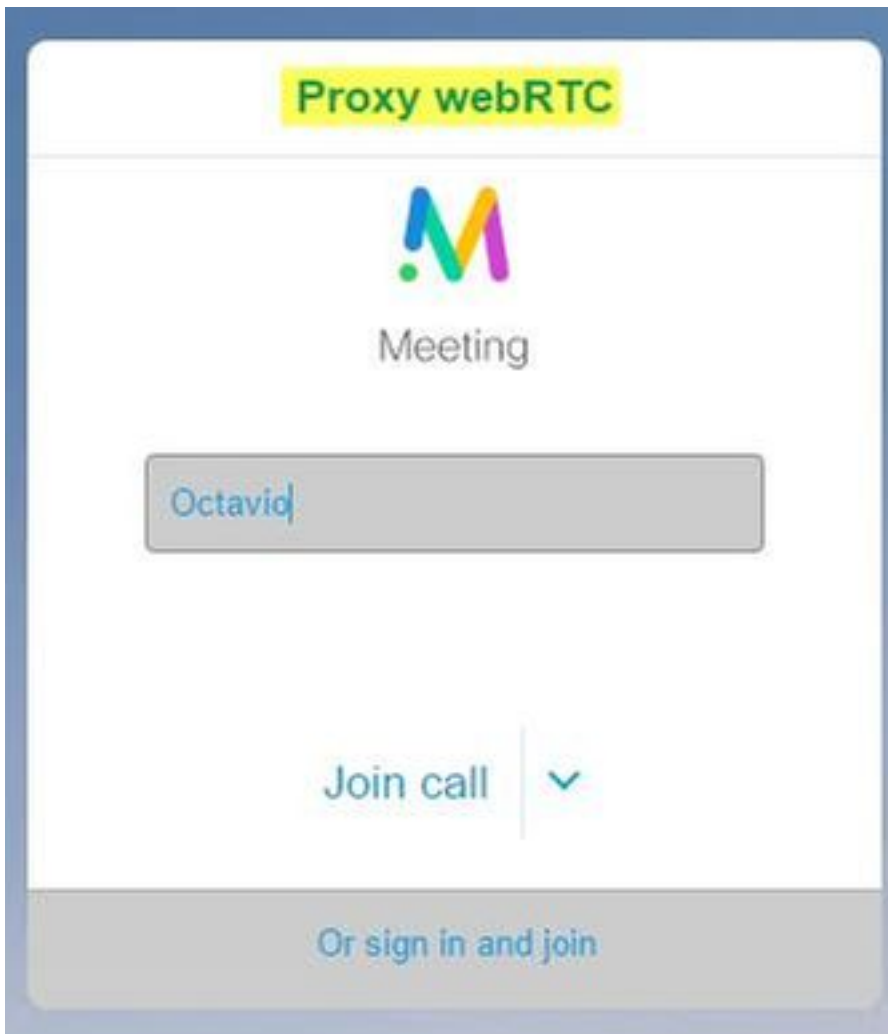
Nota: Puede encontrar una lista de los navegadores y versiones compatibles en el enlace: <https://kb.acano.com/content/2/4/en/what-versions-of-browsers-do-we-support-for-webrtc.html?highlight=html%5C-5%20compliant%20browsers#content>



Paso 2. Seleccione **Join call** e introduzca la ID de espacio configurada previamente como se muestra en la imagen.



Paso 3. Haga clic en **continue** e introduzca su nombre, en este punto debe ver el nombre del espacio al que se va a unir, en este caso el nombre del espacio es Proxy webRTC. Haga clic en **Unir llamada** como se muestra en la imagen.



Paso 4. Únase a otro dispositivo y deberá ver ambos dispositivos conectados en la conferencia como se muestra en la imagen.

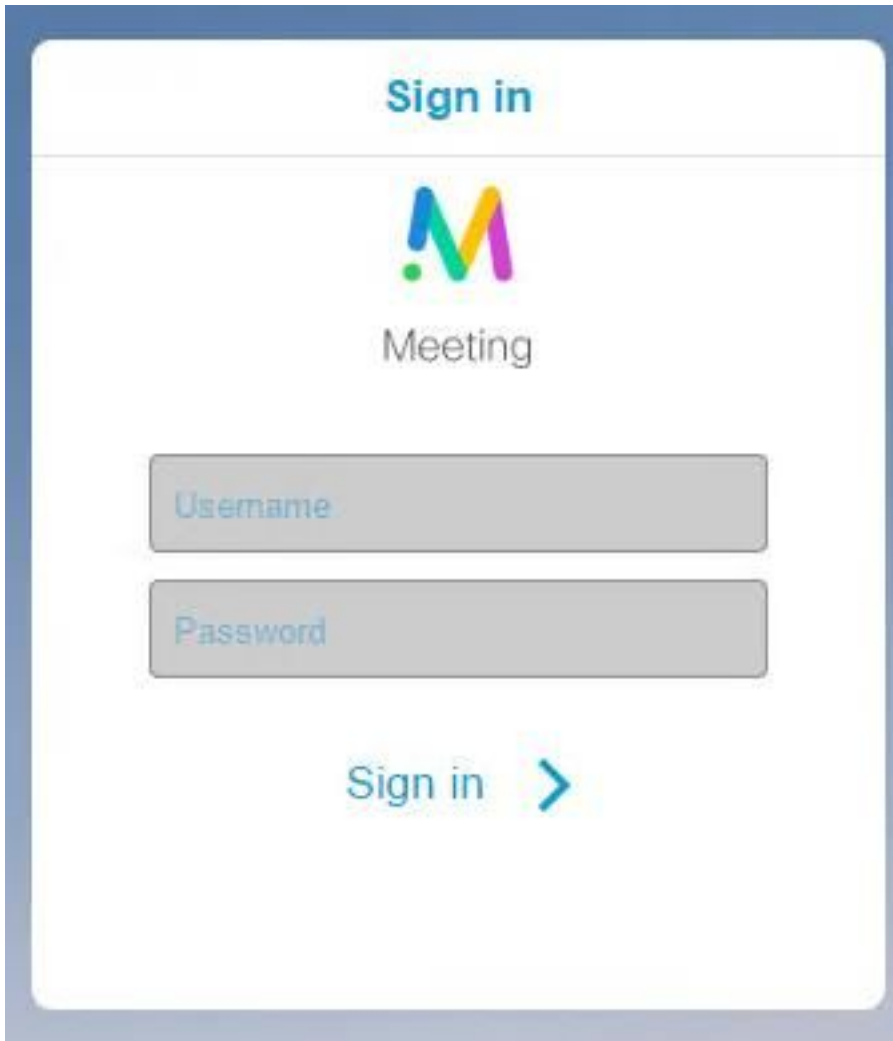


Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

No se muestra el botón Conectar a llamada

El botón **Unirse a llamada** no se muestra cuando abre la página de webbridge y ve el error que se muestra en la segunda imagen cuando ingresa a la página web de CMS como se muestra en la imagen.



Fault conditions

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

El problema ocurre cuando el webbridge no se comunica correctamente con el call bridge.

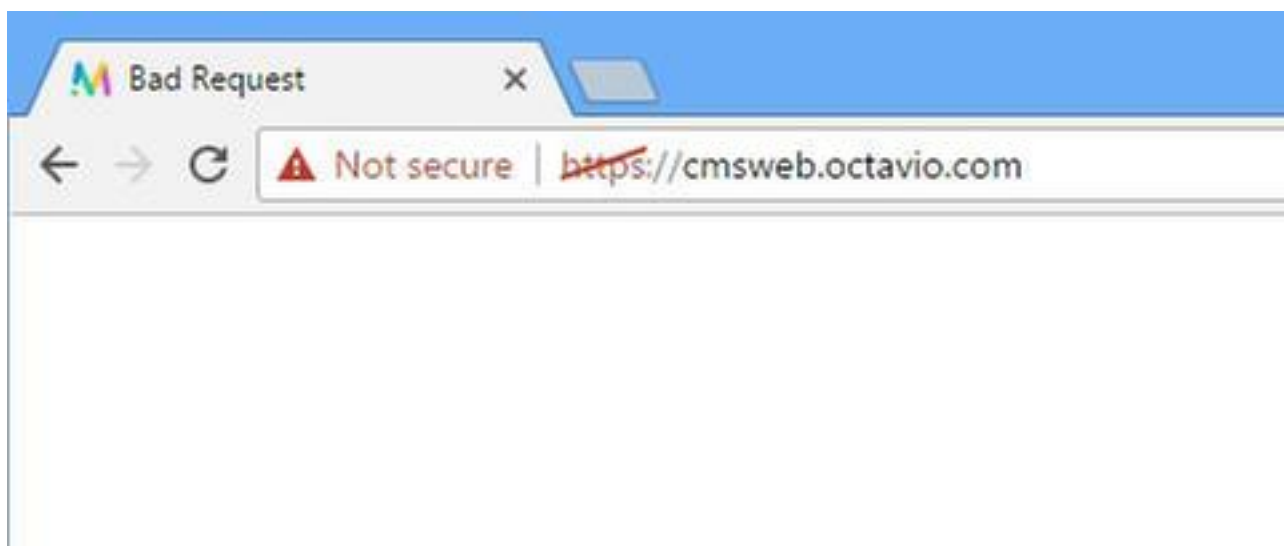
Solución

- Verifique que la URL de webbridge esté configurada correctamente en la página web del administrador de CMS. Navegue hasta **Configuración > General** para este fin.
- El webbridge y callbridge deben confiar entre sí, verifique que el paquete de confianza se agregue a la configuración de webbridge como se muestra en las imágenes:

```
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>
```

Nota: El paquete de confianza es el certificado de Call Bridge.

La página WebRTC muestra 'Solicitud incorrecta'



Solución

- Verifique que el URI del cliente de cuenta de invitado correcto esté configurado en Expressway-C. Navegue hasta **Configuración > Unified Communication > Cisco Meeting Server** para este fin.

Si la URL interna se configura en la URL del cliente de cuenta de invitado, Expressway-C la resolverá porque hay un registro creado en el servidor DNS, pero esto puede causar el mensaje de error "bad request" (solicitud incorrecta) en el navegador web. En este caso de ejemplo, la URL interna se configura para mostrar el error como se muestra en la imagen.

Cisco Expressway-C

Status System **Configuration** Applications Users Maintenance

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 ⓘ

Guest account client URI ⓘ

Guest account client URI resolved to the following targets

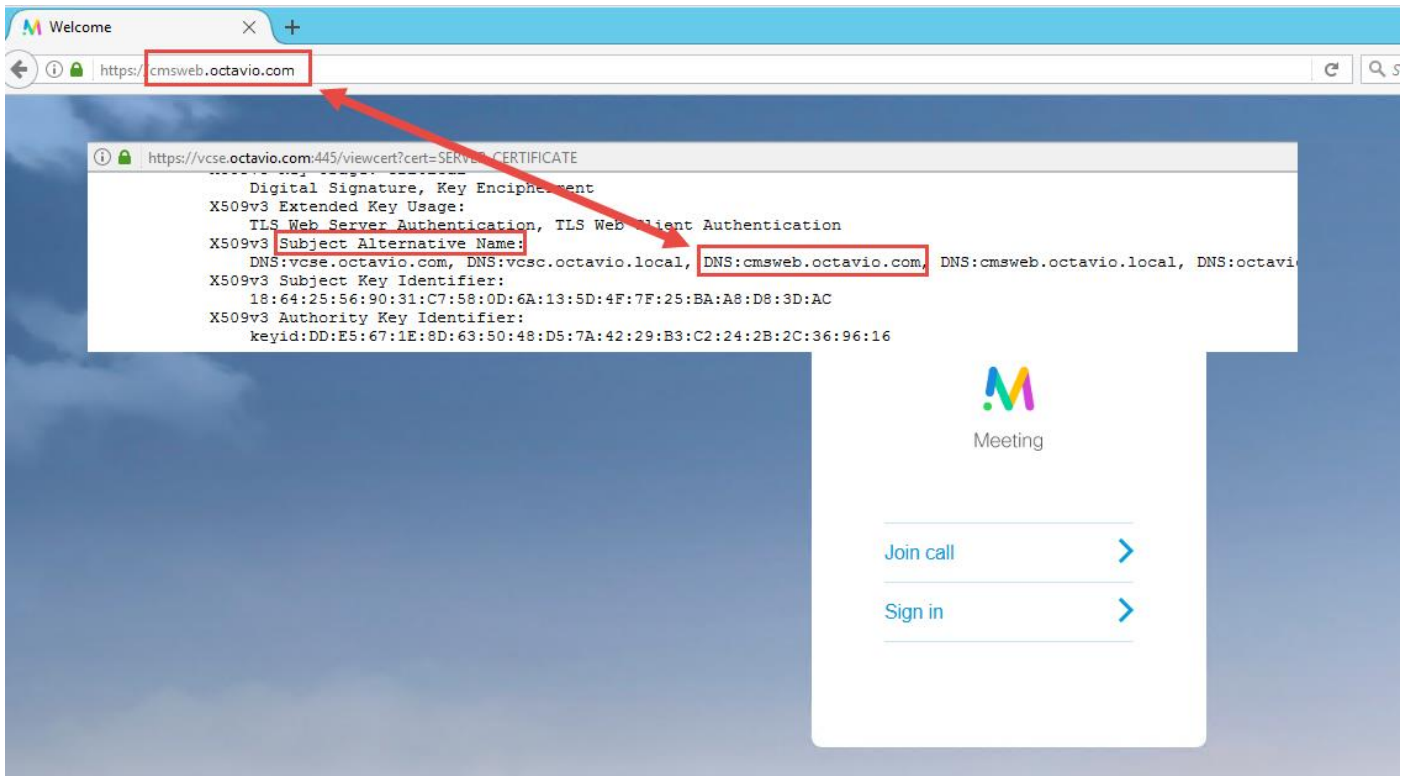
Name	Address
cmsweb.cms.octavio.local	172.16.85.180

El cliente WebRTC muestra una conexión no segura

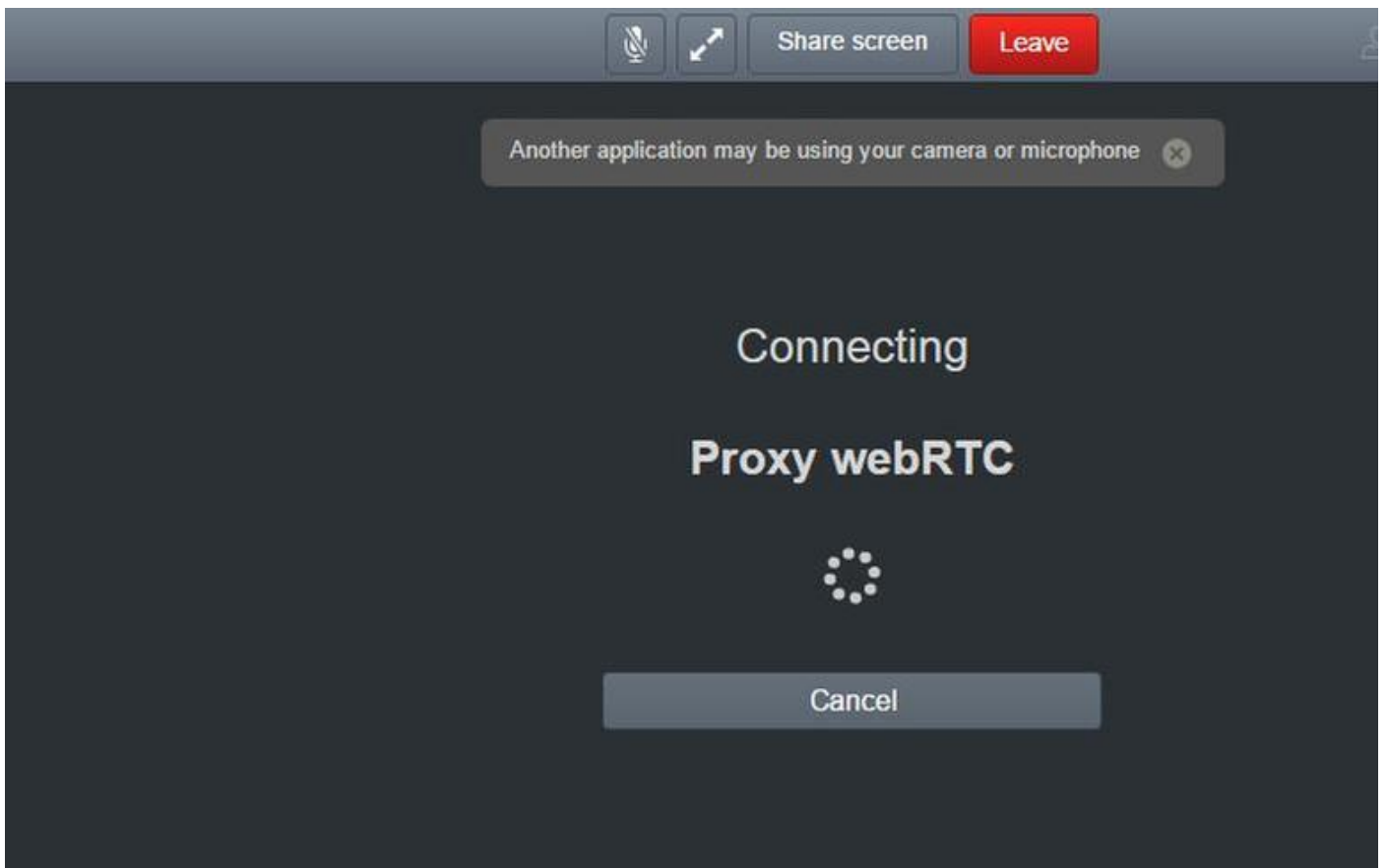
The screenshot shows a web browser window with a 'Welcome' tab. The address bar displays a red warning icon and the text 'Not secure | https://cmsweb.octavio.com'. The main content area features a blue sky background with a white 'Meeting' card on the right. The card contains the Cisco Meeting logo and two buttons: 'Join call' and 'Sign in', both with right-pointing arrows.

Solución

- El certificado se firma automáticamente, lo que hace que el servidor no confíe en el origen. Cambie el certificado de Expressway-E a una autoridad de certificados de terceros admitida.
- Verifique que la URL de webbridge externa se agregue como una SAN en el certificado de servidor de Expressway-E como se muestra en la imagen.



El cliente WebRTC se conecta pero nunca se conecta y luego se agota el tiempo de espera y se desconecta



El nombre de usuario o la contraseña del servidor de activación se configuran incorrectamente en Expressway-E o en CMS a través de la API. Los registros contienen los errores que se muestran en la imagen.

2017-05-20	19:43:14.133	Info	web bridge link 3: new quest 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

El error también se puede confirmar con una captura de paquetes. Ejecute Wireshark en el PC donde se ejecuta el cliente webRTC. Una vez que haya capturado el paquete, filtre los paquetes por STUN. Debe ver los errores mostrados en la imagen.

1458	2017-05-20	19:52:48.704889	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	0x08abc (2748)	Default	Allocate Error Response user: turnuser with nonce realm: turnuser error-code: 431 ("Unknown error code") Integrity Check Failure

La PC envía una solicitud de asignación y la dirección NAT de Expresssway responde con el mensaje "Error de verificación de integridad".

Solución

Para corregir el error, revise el nombre de usuario y la contraseña. Deben configurarse correctamente en los parámetros del servidor de activación como se muestra en las imágenes.

The image shows two screenshots related to a configuration issue. The top screenshot is from a REST client showing a POST request to the endpoint `https://admin.cms.octavio.local:445/api/v1/turnServers/2aa16ccc-87d1-424d-9d3d-3d007f23243a/`. The request body is `x-www-form-urlencoded` and contains the following parameters:

- `serverAddress`: 172.16.85.168
- `clientAddress`: 10.88.246.156
- `username`: turnuser
- `password`: cisco
- `type`: standard
- `tcpPortNumberOverride`: 3478

The bottom screenshot shows the Cisco Expressway-E configuration page for the "Local authentication database". The "Configuration" tab is active, and the "Name" field is set to "turnuser". The "Password" field is masked with dots, indicating it is not visible.