

Configurar o proxy WebRTC com CMS sobre Expressway com domínio duplo

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Informações técnicas](#)

[Configuração DNS](#)

[Configuração interna de DNS](#)

[Configuração de DNS externo](#)

[Configuração de CMS, Callbridge, Webbridge e XMPP](#)

[Configuração de TURN](#)

[Configuração do Expressway-C e E](#)

[Configuração no Expressway-C](#)

[Configuração no Expressway-E](#)

[Verificar](#)

[Troubleshoot](#)

[O botão Participar de chamada não é exibido](#)

[A página WebRTC mostra 'Solicitação inválida'](#)

[Cliente WebRTC mostra conexão não segura](#)

[O cliente WebRTC se conecta, mas nunca se conecta e, em seguida, o tempo limite é excedido e desconecta](#)

Introduction

Este documento descreve um exemplo de configuração da Web Real-Time Communication (WebRTC) de proxy para o Cisco Meeting Server (CMS) através do Expressway com diferentes domínios internos e externos.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- Implantação única combinada CMS versão 2.1.4 e superior
- Expressway C e Expressway E versão X8.9.2 e superior
- Callbridge e webbridge configurados no CMS
- Acesso móvel e remoto (MRA) habilitado no par Expressway

- Tecla de opção Traversal Using Relay NAT (TURN) adicionada ao Expressway-E
- Registro do Servidor de Nomes de Domínio (DNS) resolvível externo para URL da webbridge, para domínio externo
- Registro DNS resolvível interno para endereço IP CMS de domínio externo para domínio interno
- Multidomínio Extensible Messaging and Presence Protocol (XMPP) configurado no CMS, para domínio interno e externo
- Porta TCP 443 aberta no Firewall da internet pública para o endereço IP público do Expressway-E
- Porta TCP e UDP 3478 aberta no Firewall da Internet Pública para o endereço IP público do Expressway-E
- Intervalo de portas UDP 24000-29999 abertas no Firewall para e do endereço IP público do Expressway-E

Componentes Utilizados

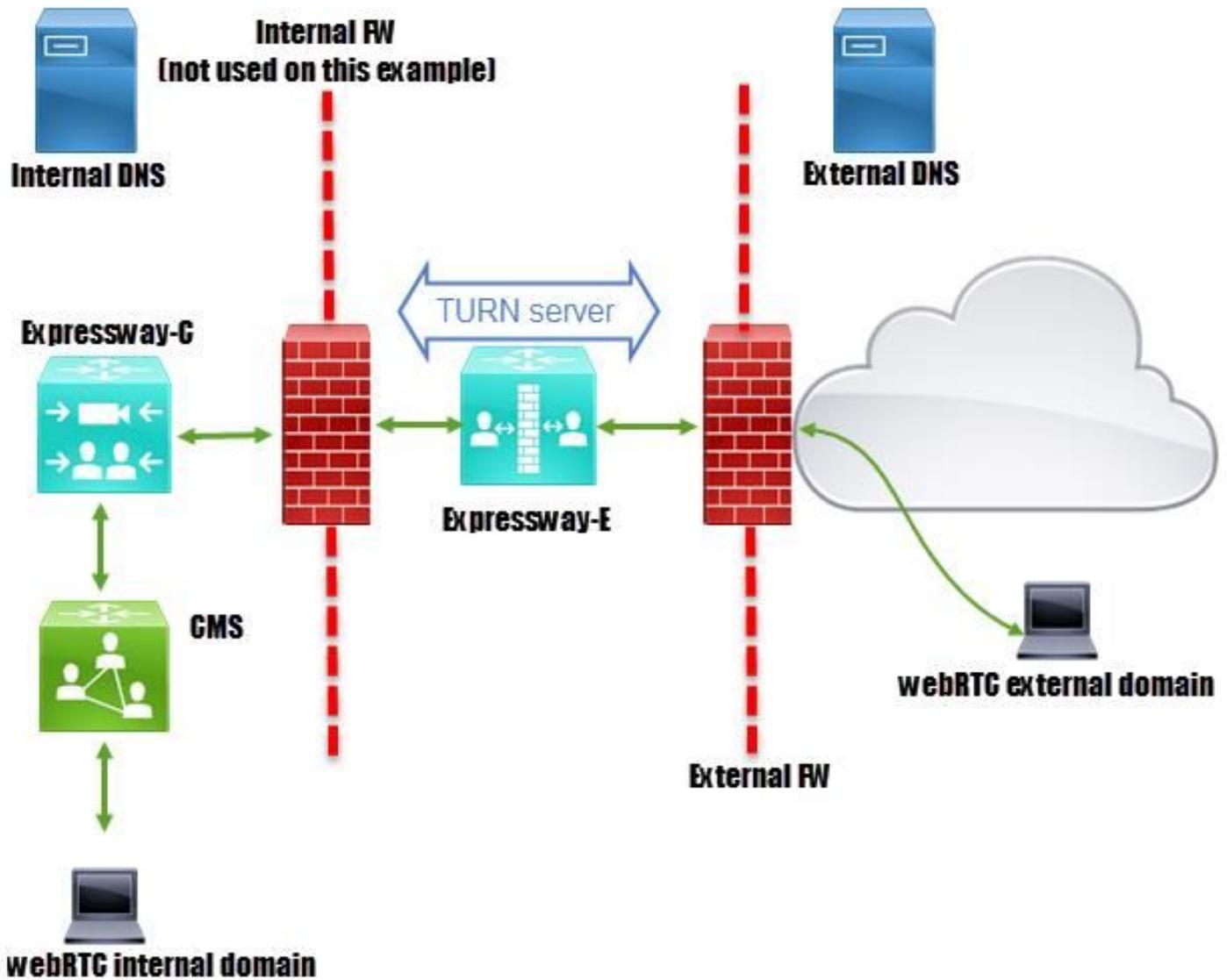
As informações neste documento são baseadas nestas versões de software e hardware:

- Implantação única combinada CMS versão 2.2.1
- Expressway-C e Expressway-E com placa de interface de rede (NIC) dupla e software de conversão de endereço de rede (NAT) estático versão 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 Rede



Informações técnicas

Domínio interno	cms.octavio.local
Domínio externo	octavio.com
endereço IP CMS	172.16.85.180
Endereço IP do Expressway-C	172.16.85.167
Endereço IP da LAN1 Expressway-E (interno)	172.16.85.168
Endereço IP da LAN2 Expressway-E (externo)	192.168.245.61
Endereço IP NAT estático	10.88.246.156

Configuração DNS

Configuração interna de DNS

Name	Type	Data	Timestamp
_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

A green box highlights the text "External domain resolves to internal" with arrows pointing to the SRV records for xmpp.octavio.local and ocucmp.octavio.local.

Name	Type	Data	Timestamp
_tcp			
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

Configuração de DNS externo

O DNS externo deve ter a URL da webbridge que é resolvida para o endereço IP de NAT estático do Expressway-E como mostrado na imagem.

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

Configuração de CMS, Callbridge, Webbridge e XMPP

Etapa 1. Você deve ter a licença callbridge ativada. A imagem mostra uma licença callbridge ativa.

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

Para obter mais informações sobre licenciamento:

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

Etapa 2. Ative callbridge, webbridge e XMPP por meio do MMP, como mostrado na imagem.

```
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 link para obter um processo detalhado sobre como habilitá-los:

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 link para obter um processo detalhado sobre como criar um 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

Etapa 3. Navegue até a página da Web do CMS em **Configuration > General** e configure a URL interna e externa para a webbridge como mostrado na imagem.

Note: O CMS deve ser configurado com pelo menos um espaço.

Um exemplo de um espaço configurado no CMS, como mostrado na imagem.

<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

Note: As chamadas recebidas devem ser configuradas para os domínios interno e externo

Um exemplo de domínios configurados para o tratamento de chamadas recebidas é mostrado na imagem.

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

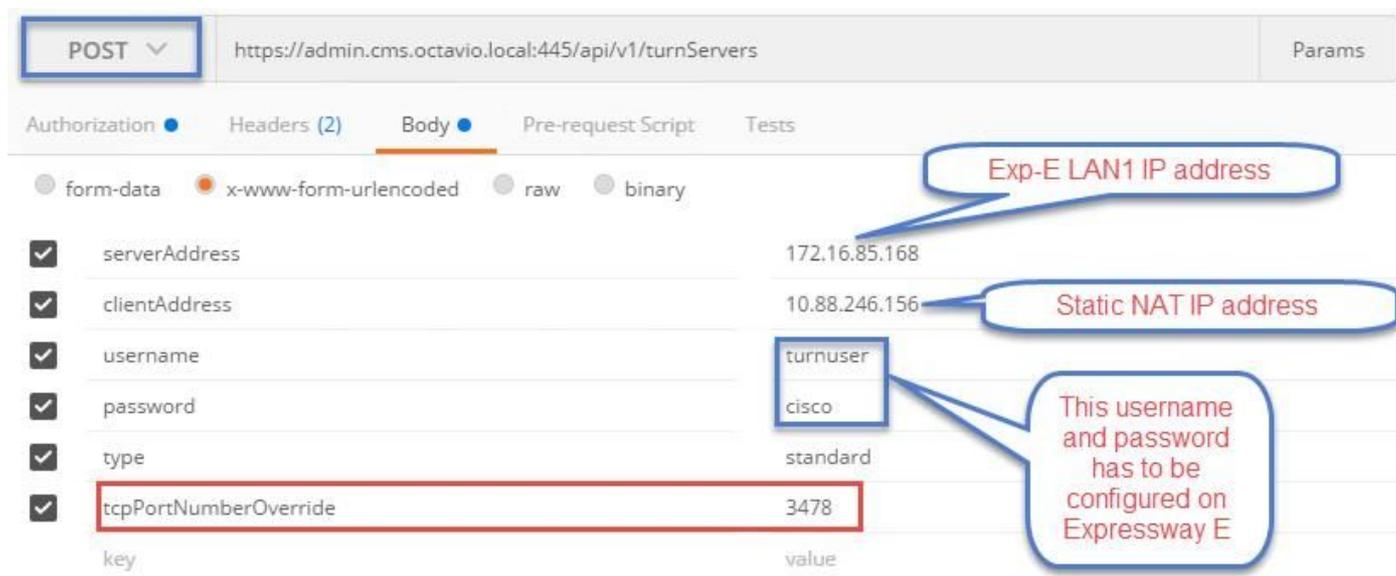
Configuração de TURN

Etapa 1. TURN deve ser configurado pela API através do Postman. Esse comando é usado em

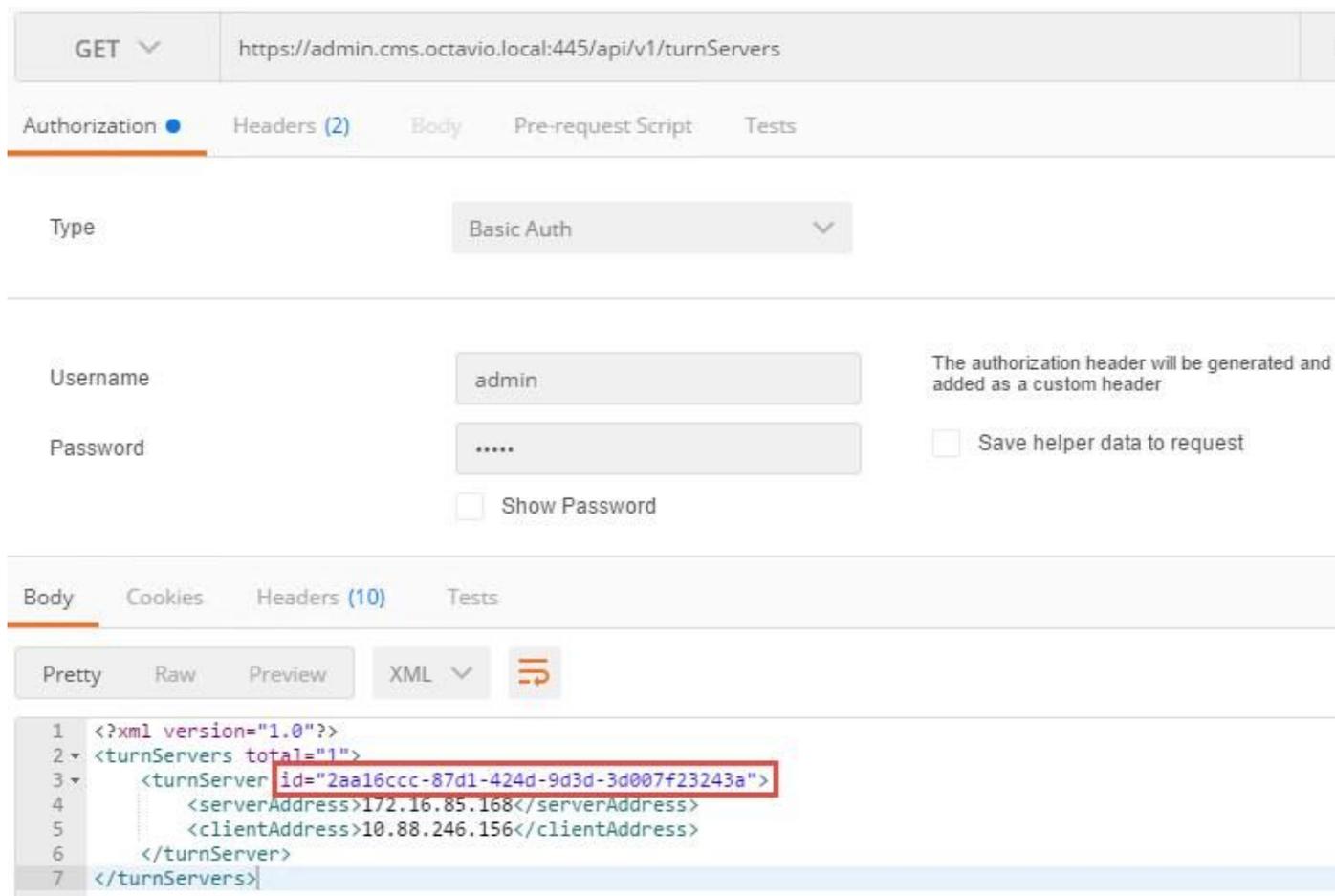
toda a configuração.

<https://>

Etapa 2. Use o método POST e navegue até **Body** para exibir os parâmetros do servidor TURN ou editá-los. Os parâmetros configurados para o servidor TURN são como mostrado na imagem.



Etapa 3. Verifique o status da configuração do servidor TURN executando o método GET e copiando a ID do servidor. O ID que deve ser copiado é como mostrado na imagem.



Etapa 4. Copie a ID no final do comando API e use o método GET para ver as informações do servidor TURN como mostrado na imagem.

Note: As informações não mostrarão a senha do servidor.

The screenshot displays a REST client interface. At the top, a GET request is configured to `https://admin.cms.octavio.local:445/api/v1/turnServer/2aa16ccc-87d1-424d-9d3d-3d007f23243a`. The `Authorization` tab is active, showing `Basic Auth` selected. The `Username` is `admin` and the `Password` is masked with dots. Below the form, there are checkboxes for `Save helper data to request` and `Show Password`. The `Body` tab is also active, showing the XML response in `XML` format:

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

Etapa 5. Clique em **enviar** para obter o status do servidor. Um exemplo de uma configuração bem-sucedida como mostrado na imagem.

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

Authorization ● Headers (2) Body Pre-request Script Tests

Type Basic Auth

Username admin

Password *****

Save helper data to request

Show Password

The authorization header will be generated as a custom header

Body Cookies Headers (10) Tests

Pretty Raw Preview XML

```
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>
```

Configuração do Expressway-C e E

Etapa 1. O expressway-C deve ter o domínio interno (octavio.local) e o Expressway-E deve ter o domínio externo (octavio.com) configurado como mostrado na imagem.



Status **System** Configuration Applications Users Maintenance

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

Etapa 2. O MRA deve ser ativado no Expressway C e E conforme mostrado na imagem.

Unified Communications You are here [Configuration](#) > [Unified Communications](#) > [Configuration](#)

Configuration

Unified Communications mode

Etapa 3. Crie uma zona de passagem de comunicação unificada entre o Expressway-C e E conforme mostrado na imagem.

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

This credentials are configured on Exp-E

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"/>
-----------------------	---

Configuração no Expressway-C

Etapa 1. Configure o domínio interno e externo no Expressway-C como mostrado na imagem.



Cisco Expressway-C

Status System **Configuration** Application

Domains

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

Etapa 2. Ative a configuração da reunião Cisco. Navegue até **Configurarion > Unified Communications > Cisco Meeting Server** (Configuração > Comunicações unificadas > Cisco Meeting Server). Configure a URL da webbridge externa no campo URI do cliente de conta de convidado como mostrado na imagem.



Cisco Expressway-C

Status System **Configuration** Applications Users Maintenance

Cisco Meeting Server

Meeting Server configuration

Meeting Server Web Proxy Enable ⓘ

Guest account client URI ⓘ

Guest account client URI resolved to the following targets

Name	Address
cmsweb.octavio.com	172.16.85.180

Note: O DNS interno deve resolver o URL externo da webbridge (cmsweb.octavio.com) para o endereço IP interno da webbridge do CMS. Nesse caso, o IP é 172.16.85.180.

Os túneis Secure Shell (SSH) no Expressway-C devem ficar ativos após alguns segundos como mostrado na imagem.



Cisco Expressway-C

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: O servidor deve ter um certificado de servidor e um certificado CA.

Configuração no Expressway-E

Etapa 1. O expressway-E deve ter uma licença TURN conforme mostrado na imagem.

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

Etapa 2. O Expressway-E deve ser configurado com o domínio externo como mostrado na imagem.

 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

Etapa 3. Crie usuários para o servidor TURN e para a zona de passagem da Comunicação Unificada conforme mostrado na imagem.



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

Etapa 4. Crie uma zona de passagem de comunicação unificada conforme mostrado na imagem.



Edit zone

Configuration

Name ⓘ

Type Unified Communications traversal

Hop count ⓘ

Connection credentials

Username ⓘ

Password [Add/Edit local authentication database](#)

SIP

Port ⓘ

TLS verify subject name ⓘ

Accept proxied registrations ⓘ

ICE support ⓘ

Multistream mode ⓘ

SIP poison mode ⓘ

Preloaded SIP routes support ⓘ

SIP parameter preservation ⓘ

Etapa 5. Configure o servidor TURN. Navegue até **Configuration > Traversal > TURN** como mostrado na imagem.

Note: A solicitação TURN deve ser para a porta 3478, pois é a porta onde o cliente Web solicita a conexão 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

Quando a opção Turn up (Ativar) for exibida, o status mostrará Ative (Ativo) como mostrado na imagem.

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

Etapa 6. Navegue até **Sistema > Administração**. O cliente webRTC solicita acesso na porta 443, por esse motivo, a porta de administração do Expressway-E deve ser alterada para outra, neste caso de exemplo, ela é alterada para 445 como mostrado na imagem.

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*

Passo 7. Criação de certificado para o Expressway-E: o URL da webbridge deve ser adicionado como uma SAN no certificado do servidor conforme mostrado na imagem.

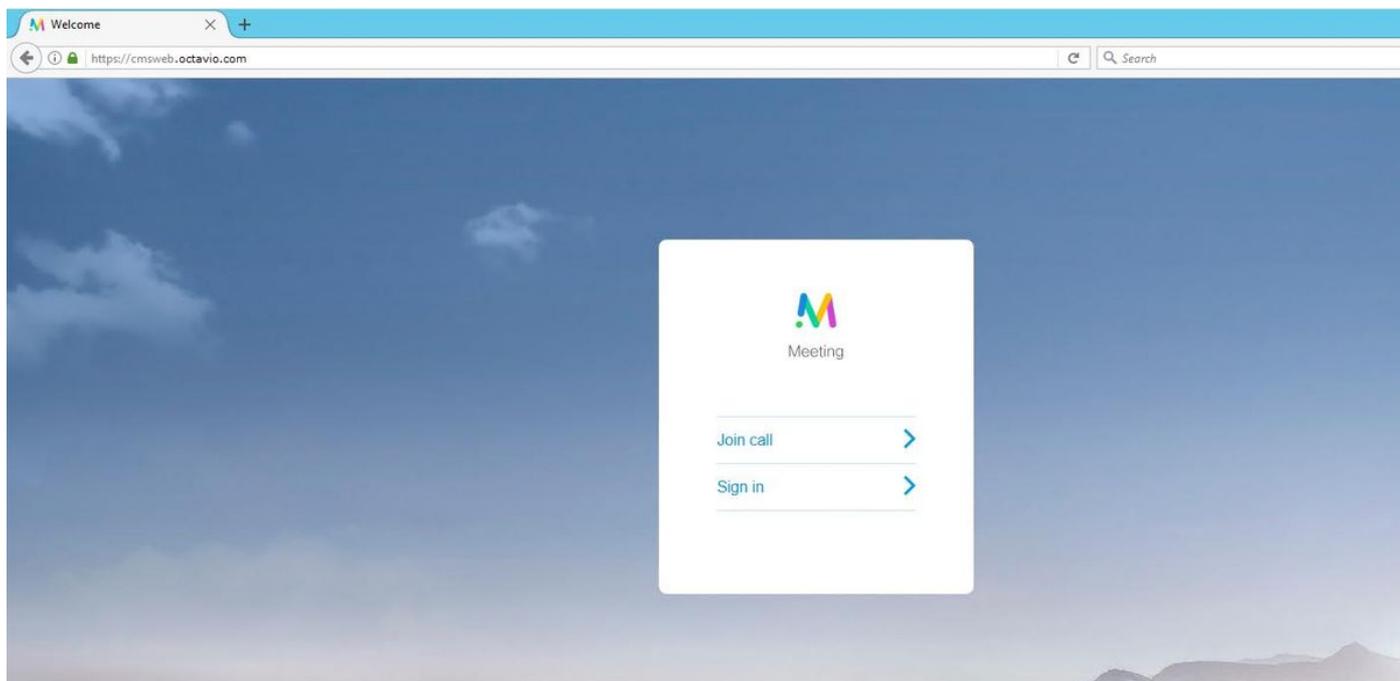
```
X509v3 Subject Alternative Name:  
DNS:vcse.octavio.com, DNS:vcse.octavio.local, DNS:cmsweb.octavio.com, DNS:cmsweb.octavio.local, DNS:octavio.local, DNS:cms.octavio.local, DNS:octavio.com
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Selecione um navegador da Web suportado e insira o URL externo da webbridge. Você deve ver a próxima tela como mostrado na imagem.

Note: Você pode encontrar uma lista de navegadores e versões compatíveis no 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>



Etapa 2. Selecione **Unir chamada** e introduza a ID de espaço previamente configurada como mostrado na imagem.

Enter Call ID


Meeting

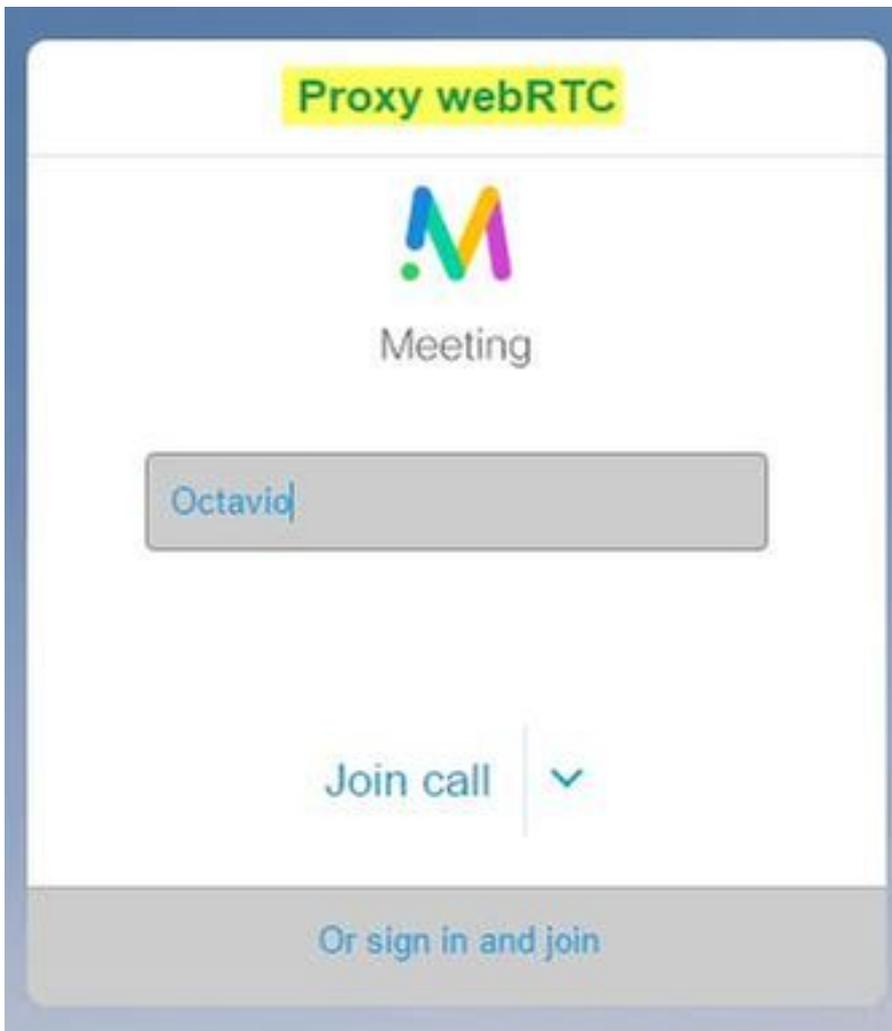
100101

Passcode (if required)

Continue >

Back

Etapa 3. Clique em **continuar** e digite seu nome. Nesse ponto, você deve ver o nome do espaço no qual você vai se unir. Nesse caso, o nome do espaço é Proxy webRTC. Clique em **Unir chamada** conforme mostrado na imagem.



Etapa 4. Junte-se a outro dispositivo e você deve ver ambos os dispositivos conectados na conferência como mostrado na imagem.

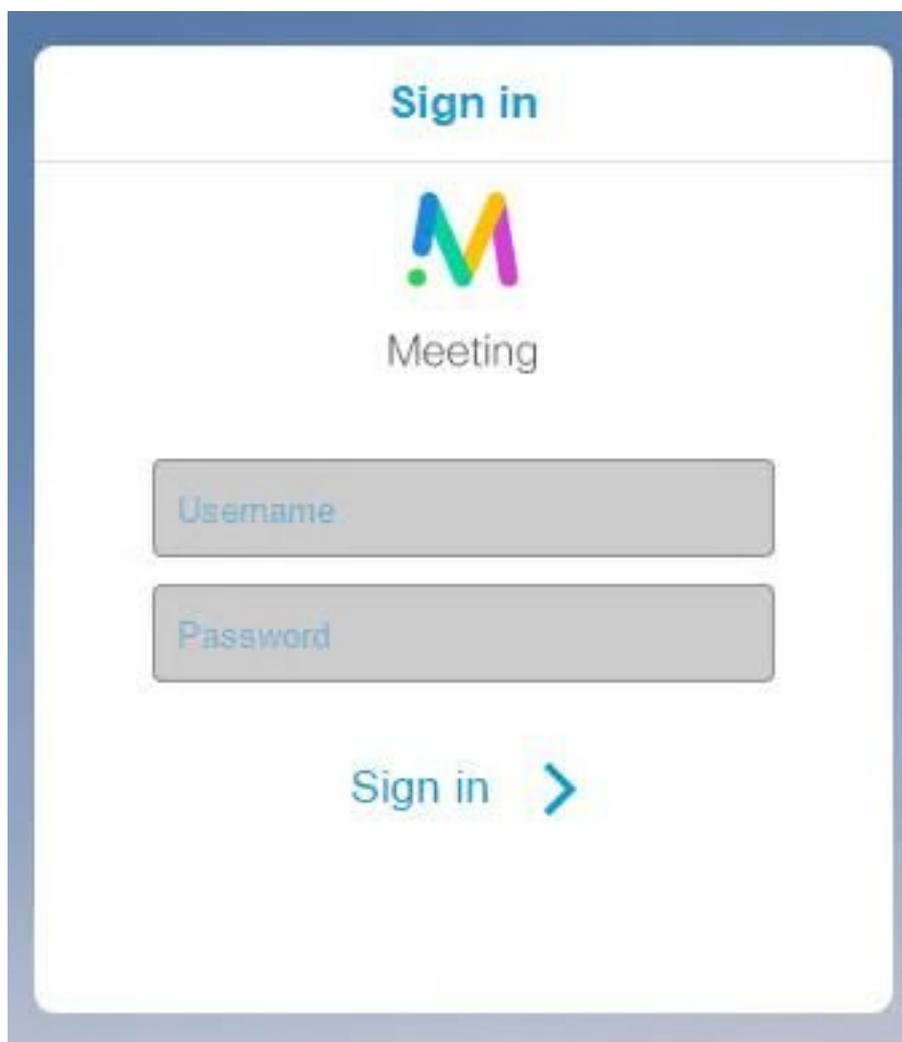


Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

O botão Participar de chamada não é exibido

O botão **Participar da chamada** não é mostrado quando você abre a página da webbridge e o erro mostrado na segunda imagem é exibido quando você entra na página da Web do CMS como mostrado na imagem.



Fault conditions

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

O problema acontece quando a webbridge não se comunica corretamente com a call bridge.

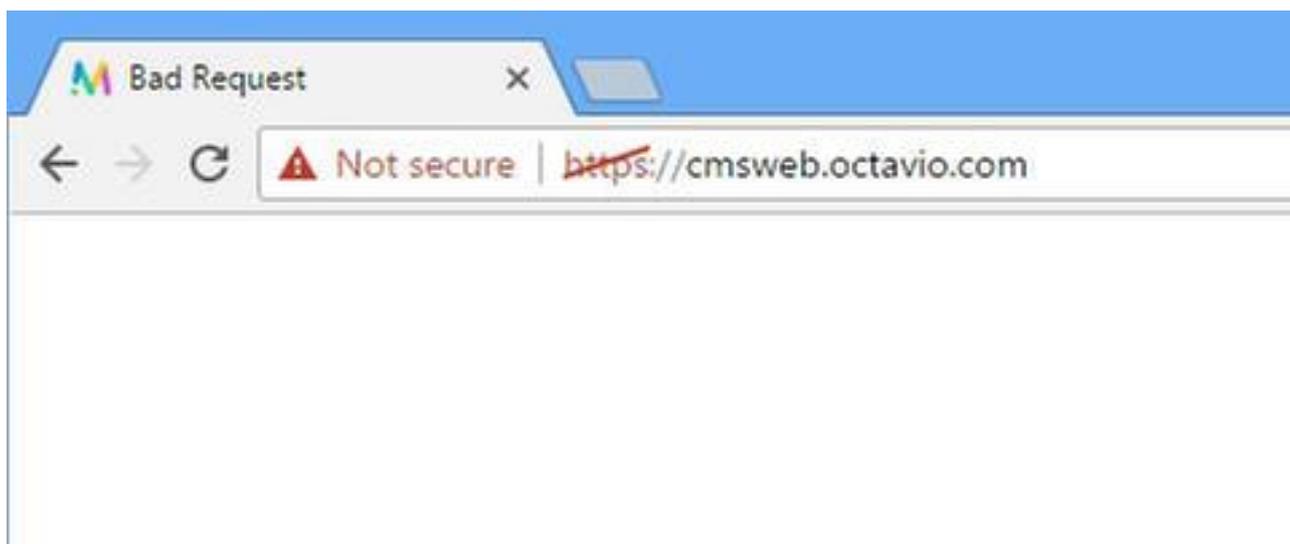
Solução

- Verifique se o URL da webbridge está configurado corretamente na página da Web do administrador do CMS. Navegue até **Configuration > General** para esse fim.
- O webbridge e o callbridge devem confiar um no outro, verifique se o pacote de confiança é adicionado à configuração do webbridge como mostrado nas imagens:

```
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: O pacote de confiança é o certificado de ponte de chamada.

A página WebRTC mostra 'Solicitação inválida'



Solução

- Verifique se a URI do cliente de conta de convidado correta está configurada no Expressway-C. Navegue até **Configuration > Unified Communication > Cisco Meeting Server** para esse fim.

Se o URL interno estiver configurado no URL do cliente de conta de convidado, o Expressway-C o resolverá, pois há um registro criado no servidor DNS, mas isso pode causar a mensagem de erro "solicitação inválida" no navegador da Web. Neste caso de exemplo, o URL interno é configurado para mostrar o erro como mostrado na imagem.

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 Enable ⓘ

Guest account client URI ⓘ

Guest account client URI resolved to the following targets

Name	Address
cmsweb.cms.octavio.local	172.16.85.180

Cliente WebRTC mostra conexão não segura

Welcome x

← → ↻ ⚠ Not secure | ~~https://~~cmsweb.octavio.com

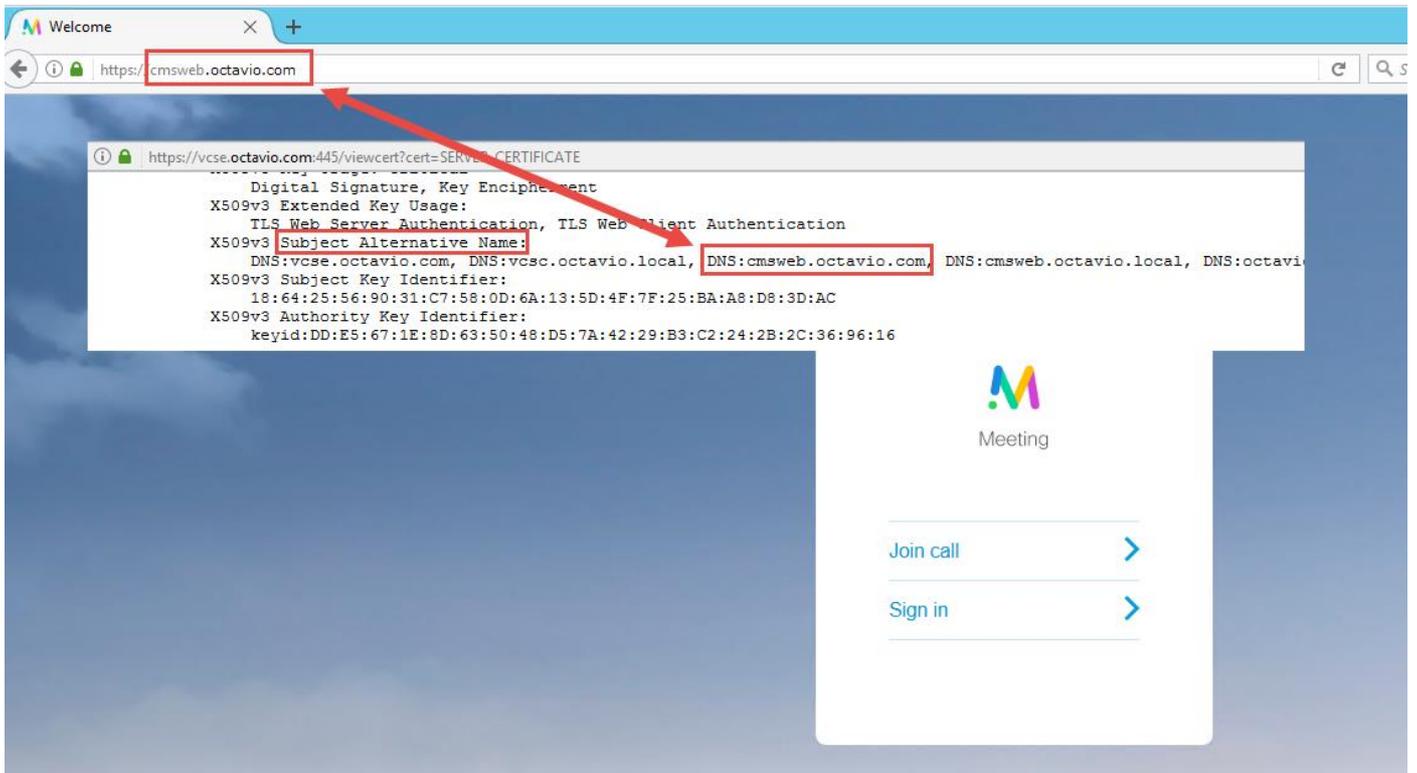
Meeting

Join call >

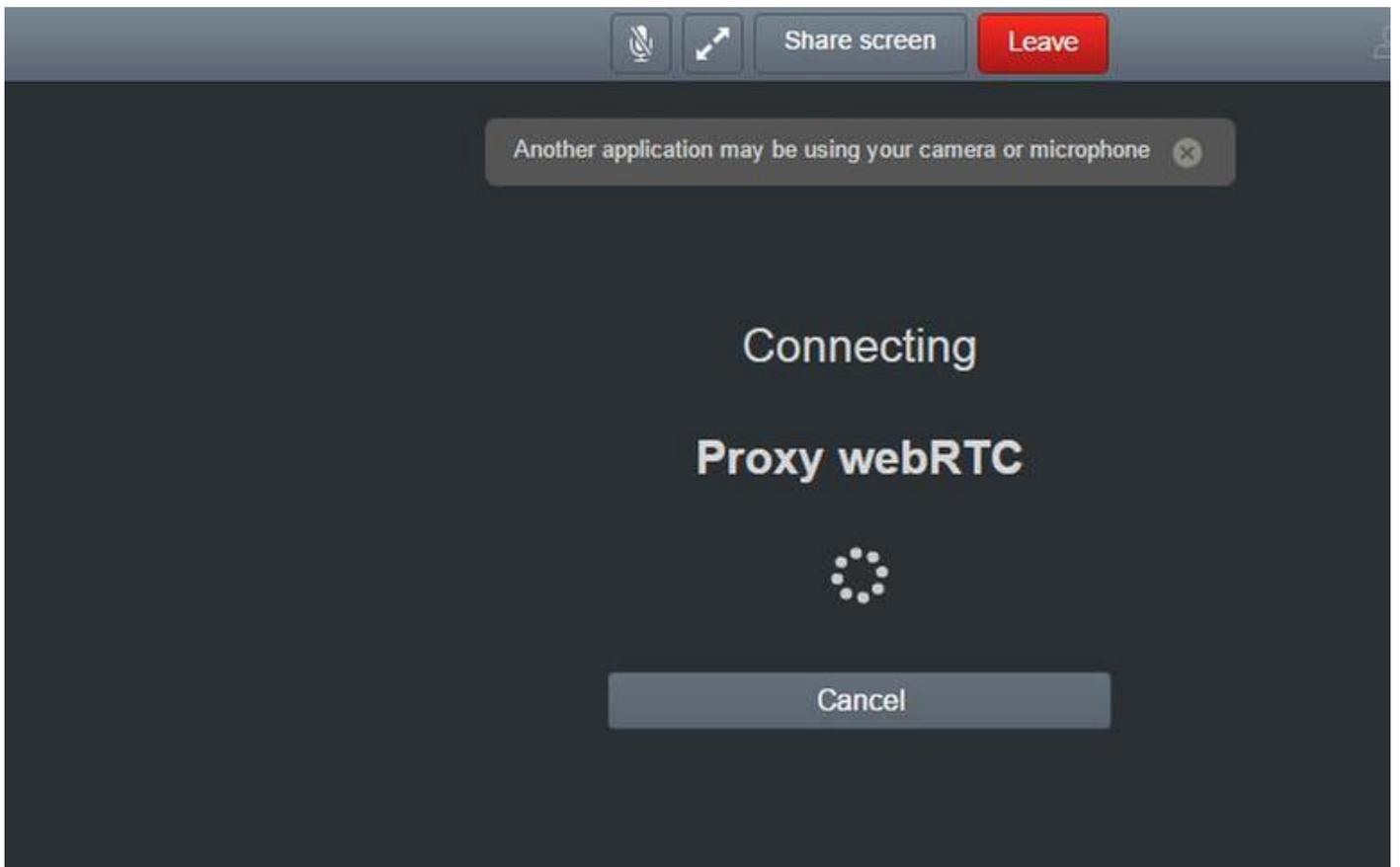
Sign in >

Solução

- O certificado é autoassinado, o que faz com que o servidor não confie na origem. Altere o certificado no Expressway-E para uma autoridade de certificado de terceiros suportada.
- Verifique se o URL externo da webbridge é adicionado como uma SAN no certificado do servidor Expressway-E como mostrado na imagem.



O cliente WebRTC se conecta, mas nunca se conecta e, em seguida, o tempo limite é excedido e desconecta



O nome de usuário ou a senha do servidor TURN estão configurados incorretamente no expressway-E ou no CMS via API. Os registros contêm os erros mostrados na imagem.

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

O erro também pode ser confirmado com uma captura de pacote. Execute o Wireshark no PC onde o cliente WebRTC é executado. Depois de ter a captura de pacotes, filtre os pacotes pelo STUN. Você deve ver os erros mostrados na imagem.

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 UDP error-code: 431 ("Unknown error code") Integrity Check Failure

O PC envia uma solicitação de alocação e o endereço NAT do Expressway responde com a mensagem 'Falha na verificação de integridade'.

Solução

Para corrigir o erro, revise o nome de usuário e a senha. Eles devem ser configurados corretamente nos parâmetros do servidor TURN conforme mostrado nas imagens.

The image shows two screenshots related to a TURN server configuration. 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 web interface. It displays the 'Local authentication database' configuration page. The 'Name' field is set to 'turnuser' and the 'Password' field is masked with dots.