

使用双域Expressway上的CMS配置代理WebRTC

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[技术信息](#)

[DNS 配置](#)

[内部DNS配置](#)

[外部DNS配置](#)

[CMS、Callbridge、Webbridge和XMPP配置](#)

[TURN配置](#)

[Expressway-C和E配置](#)

[Expressway-C上的配置](#)

[Expressway-E上的配置](#)

[验证](#)

[故障排除](#)

[未显示加入呼叫按钮](#)

[WebRTC页面显示“错误请求”](#)

[WebRTC客户端显示不安全连接](#)

[WebRTC客户端连接但从未连接，然后超时并断开连接](#)

简介

本文档介绍通过具有不同内部和外部域的Expressway为思科会议服务器(CMS)配置代理Web实时通信(webRTC)的示例。

先决条件

要求

Cisco 建议您了解以下主题：

- CMS单一组合部署版本2.1.4及更高版本
- Expressway C和Expressway E版本X8.9.2及更高版本
- 在CMS上配置Callbridge和Webbridge
- 在Expressway对上启用移动和远程访问(MRA)
- 使用中继NAT(TURN)选项键穿越Expressway-E
- Webbridge URL的外部可解析域名服务器(DNS)记录，用于外部域
- CMS IP地址从外部域到内部域的内部可解析DNS记录

- 在CMS上为内部和外部域配置的可扩展消息传送和在线状态协议(XMPP)多域
- 从公共互联网到 Expressway E 的公共 IP 地址的防火墙上开启 TCP 端口 443
- 在防火墙上打开的TCP和UDP端口3478从公共互联网到Expressway E的公有IP地址
- 在防火墙上打开的UDP端口范围24000-29999，以Expressway-E的公有IP地址为源

使用的组件

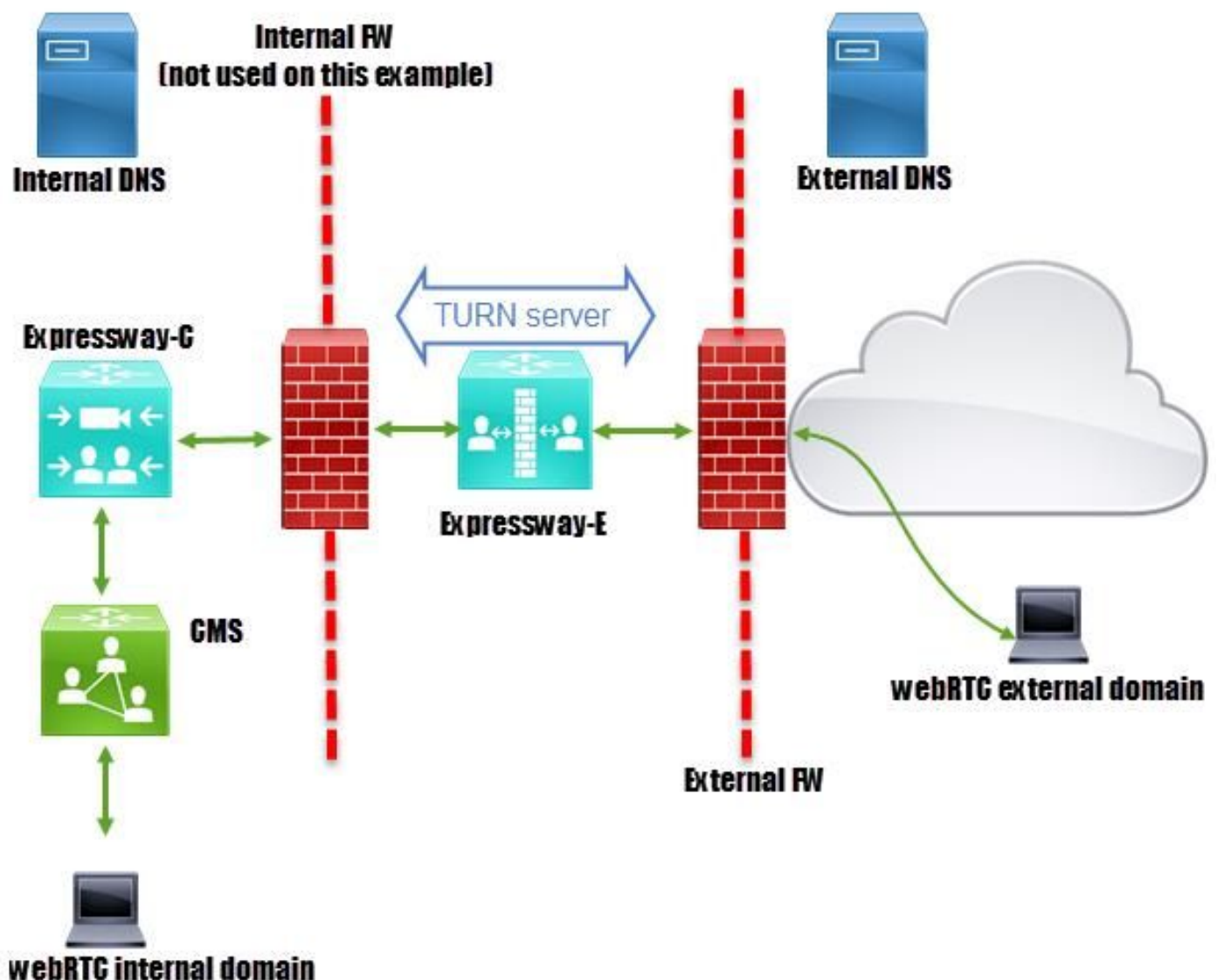
本文档中的信息基于以下软件和硬件版本：

- CMS单一组合部署版本2.2.1
- Expressway-C和Expressway-E，带双网络接口卡(NIC)和静态网络地址转换(NAT)软件版本 X8.9.2
- POSTMAN

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图



技术信息

内部域	cms.octavio.local
外部域	octavio.com
CMS IP地址	172.16.85.180
Expressway-C IP地址	172.16.85.167
Expressway-E LAN1 IP地址 (内部)	172.16.85.168
Expressway-E LAN2 IP地址 (外部)	192.168.245.61
静态NAT IP地址	10.88.246.156

DNS 配置

内部DNS配置

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] ocusp.octavio.local.	static

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

外部DNS配置

外部DNS必须具有Webbridge URL，该URL解析为Expressway-E的静态NAT IP地址，如图所示。

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

CMS、Callbridge、Webbridge和XMPP配置

步骤1.必须激活callbridge许可证。该图显示激活的Callbridge许可证。

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

有关更多许可信息：

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

步骤2.如图所示，通过MMP启用callbridge、webbridge和XMPP。

```
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
```

请点击此链接，详细了解如何启用这些功能：

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

有关如何创建证书的详细信息，请访问以下链接：

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

步骤3. 导航至 Configuration > General 上的 CMS 网页，并配置 Webbridge 的内部和外部 URL，如图所示。

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

注意：CMS 必须至少配置一个空间。

CMS 上已配置空间的示例，如图所示。

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

注意：必须为内部和外部域配置来电

如图所示，为传入呼叫处理配置的域示例。

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

TURN配置

步骤1. TURN必须通过API通过Postman进行配置。此命令用于所有配置。

<https://>

步骤2.使用POST方法并导航至Body，以查看TURN服务器参数或编辑它们。配置到TURN服务器的参数如图所示。

The screenshot shows a Postman interface for a POST request to `https://admin.cms.octavio.local:445/api/v1/turnServers`. The request body is set to form-data with the following parameters:

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

Callouts in the image provide additional context:

- Exp-E LAN1 IP address:** Points to the `serverAddress` value (172.16.85.168).
- Static NAT IP address:** Points to the `clientAddress` value (10.88.246.156).
- This username and password has to be configured on Expressway E:** Points to the `username` (turnuser) and `password` (cisco) fields.

步骤3.运行方法GET并复制服务器ID，检查TURN服务器配置的状态。必须复制的ID如图所示。

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

- Method:** GET
- URL:** https://admin.cms.octavio.local:445/api/v1/turnServers
- Authorization:** Basic Auth
- Username:** admin
- Password:** (masked)
- Body:** XML response

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

步骤4.复制API命令末尾的ID并使用GET方法查看TURN服务器信息，如图所示。

注意：该信息不会显示服务器的密码。

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

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

```
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>
```

步骤5.单击send获取服务器状态。如图所示，配置成功的示例。

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>
```

Expressway-C和E配置

步骤1. Expressway-C必须具有内部域(octavio.local),Expressway-E必须具有外部域(octavio.com), 如图所示。



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

步骤2.必须在Expressway C和E上启用MRA，如图所示。

Unified Communications You are here Configuration > Unified Communications > Configuration

Configuration

Unified Communications mode Mobile and remote access

步骤3.如图所示，在Expressway-C和E之间创建统一通信穿越区域。



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="....."/> ⓘ

This credentials are configured on Exp-E

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"/> ⓘ

Expressway-C上的配置

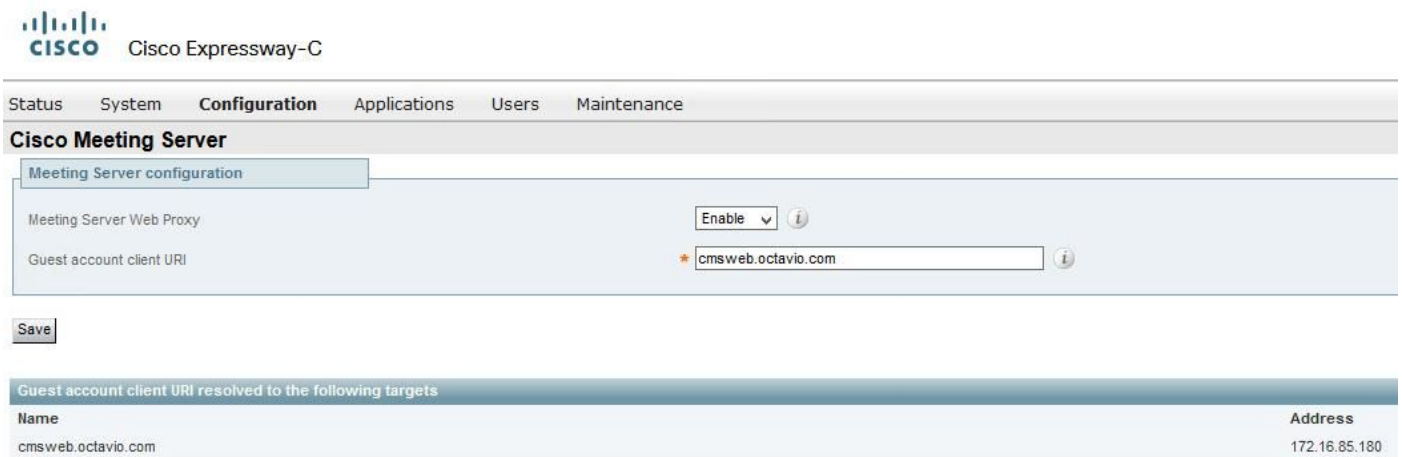
步骤1.在Expressway-C上配置内部域和外部域，如图所示。

Status System **Configuration** Application

Domains

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

步骤2. 启用思科会议配置。导航至配置 > 统一通信 > 思科 Meeting Server。如图所示，在Guest帐户客户端URI字段上配置外部Webbridge URL。



Cisco Expressway-C

Status System **Configuration** Applications Users Maintenance

Cisco Meeting Server

Meeting Server configuration

Meeting Server Web Proxy

Guest account client URI

Guest account client URI resolved to the following targets

Name	Address
cmsweb.octavio.com	172.16.85.180

注意：内部DNS应将外部网桥URL(cmsweb.octavio.com)解析为内部CMS网桥IP地址。在本例中，IP为172.16.85.180。

Expressway-C上的安全外壳(SSH)隧道必须在几秒钟后变为活动状态，如图所示。



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

注意：服务器必须具有服务器证书和CA证书。

Expressway-E上的配置


步骤1. Expressway-E必须具有TURN许可证，如图所示。

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

步骤2. 必须使用外部域配置Expressway-E，如图所示。

 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 (callout pointing to Address 1)

步骤3. 为TURN服务器和统一通信穿越区域创建用户，如图所示。

 Cisco Expressway-E

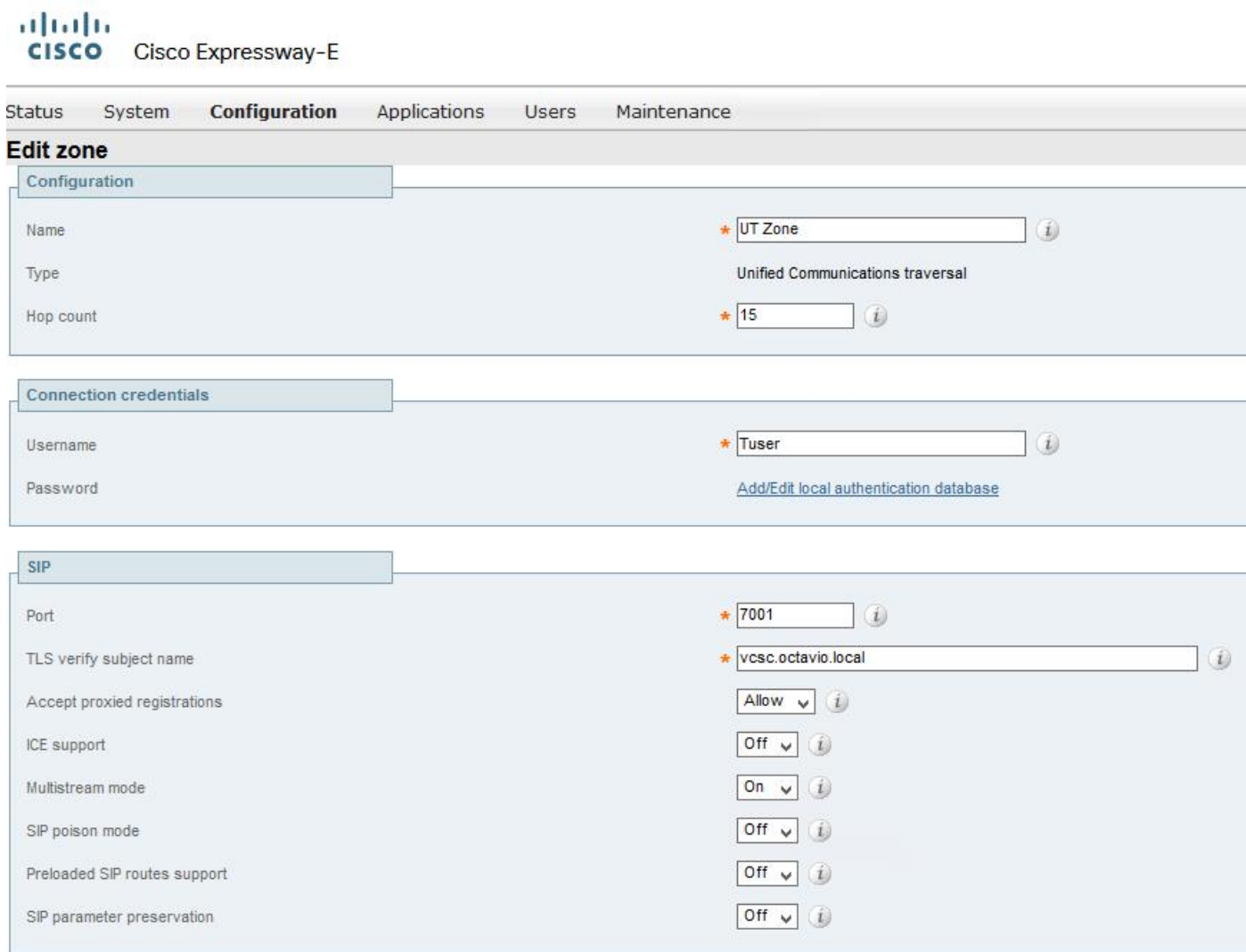
Status System **Configuration** Applications Users Maintenance

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

步骤4.创建统一通信穿越区域，如图所示。



The image shows the 'Edit zone' configuration page in Cisco Expressway-E. The page is divided into three main sections: Configuration, Connection credentials, and SIP. The Configuration section includes fields for Name (UT Zone), Type (Unified Communications traversal), and Hop count (15). The Connection credentials section includes Username (Tuser) and a link to Add/Edit local authentication database. The SIP section includes fields for Port (7001), TLS verify subject name (vcsc.octavio.local), and several toggle options: Accept proxied registrations (Allow), ICE support (Off), Multistream mode (On), SIP poison mode (Off), Preloaded SIP routes support (Off), and SIP parameter preservation (Off).

Configuration

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

Connection credentials

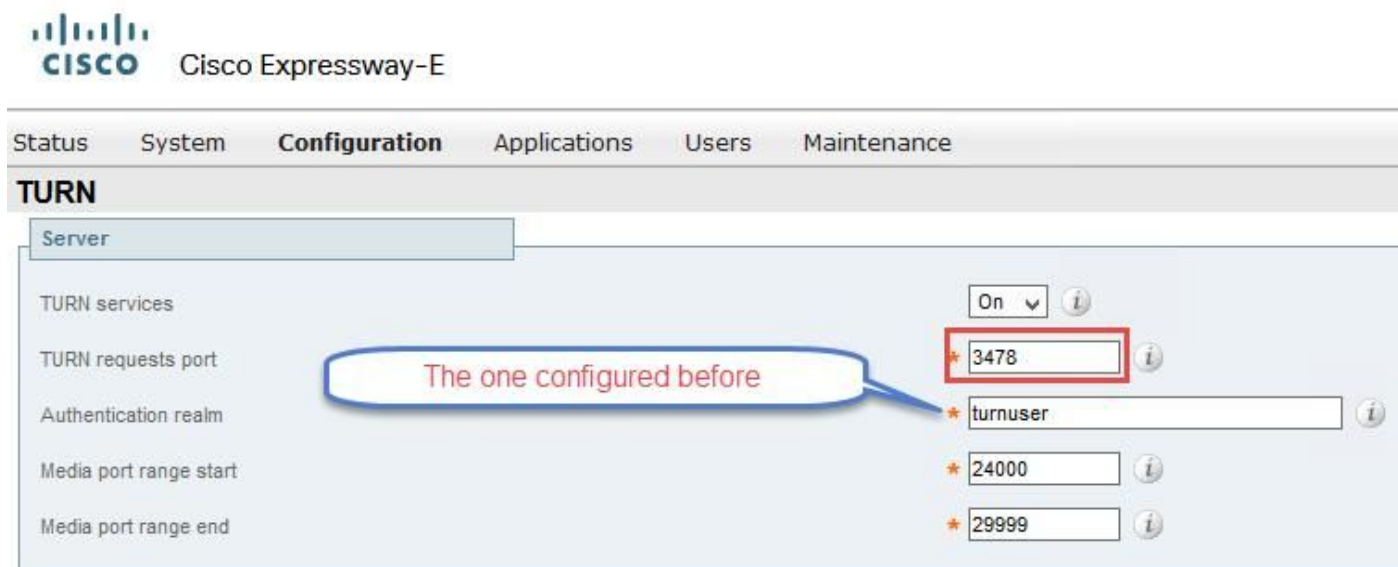
Username	* Tuser
Password	Add/Edit local authentication database

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

步骤5.配置TURN服务器。如图所示，导航至Configuration > Traversal > TURN。

注意：TURN请求必须到达端口3478，因为它是Web客户端请求TURN连接的端口。



The image shows the 'TURN Server' configuration page in Cisco Expressway-E. The page is divided into two main sections: Server and TURN services. The Server section includes fields for TURN requests port (3478), Authentication realm (turnuser), Media port range start (24000), and Media port range end (29999). The TURN services section includes a toggle for TURN services (On). A red box highlights the 'TURN requests port' field, and a callout bubble points to it with the text 'The one configured before'.

TURN

Server

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

TURN services

TURN services	On
---------------	----

出现“Turn (开启)”后，状态显示“Active (活动)”，如图所示。

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

步骤6.导航至System > Administration。WebRTC客户端请求访问端口443，因此Expressway-E的管理端口必须更改为其他端口，在本例中，它更改为445，如图所示。

Web server configuration	
Redirect HTTP requests to HTTPS	On <input type="button" value="i"/>
HTTP Strict Transport Security (HSTS)	On <input type="button" value="i"/>
Web administrator port	445 <input type="button" value="i"/>
Client certificate-based security	Not required <input type="button" value="i"/>

步骤7.为Expressway-E创建证书：必须将Webbridge URL添加为服务器证书上的SAN，如图所示。

```
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
```

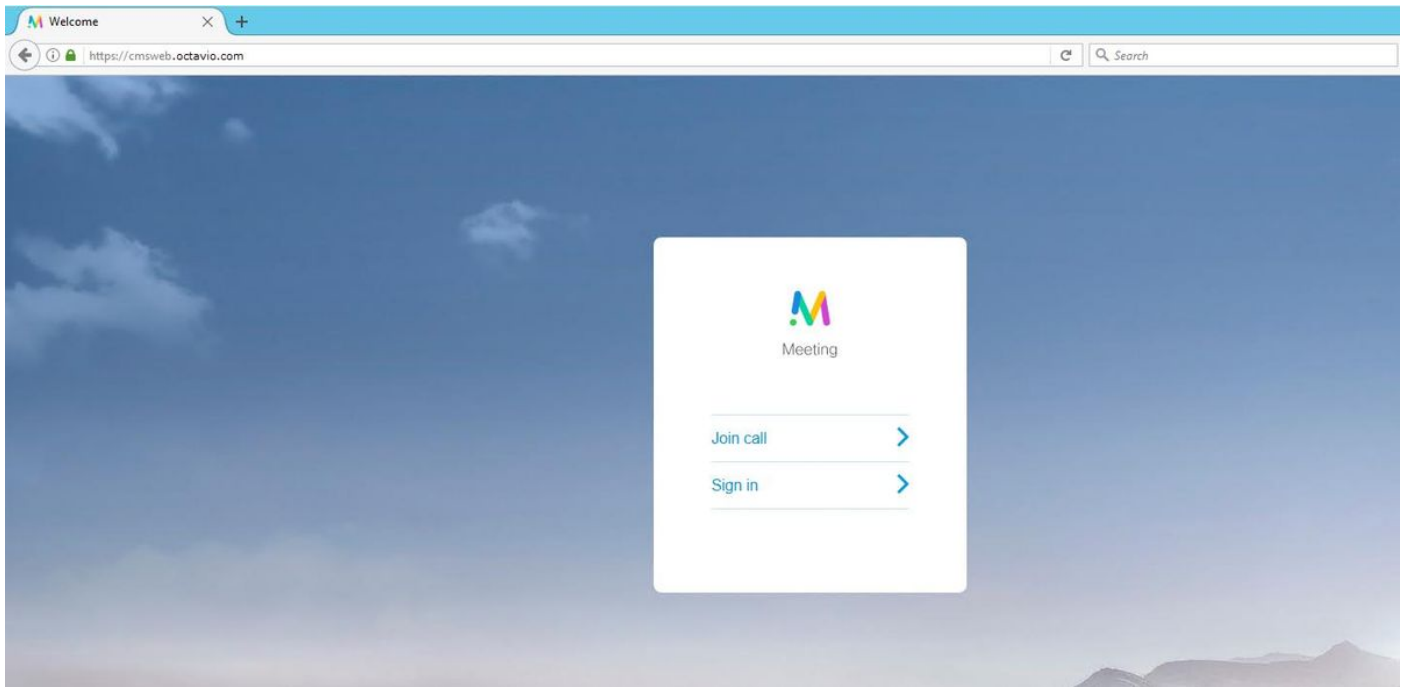
验证

使用本部分可确认配置能否正常运行。

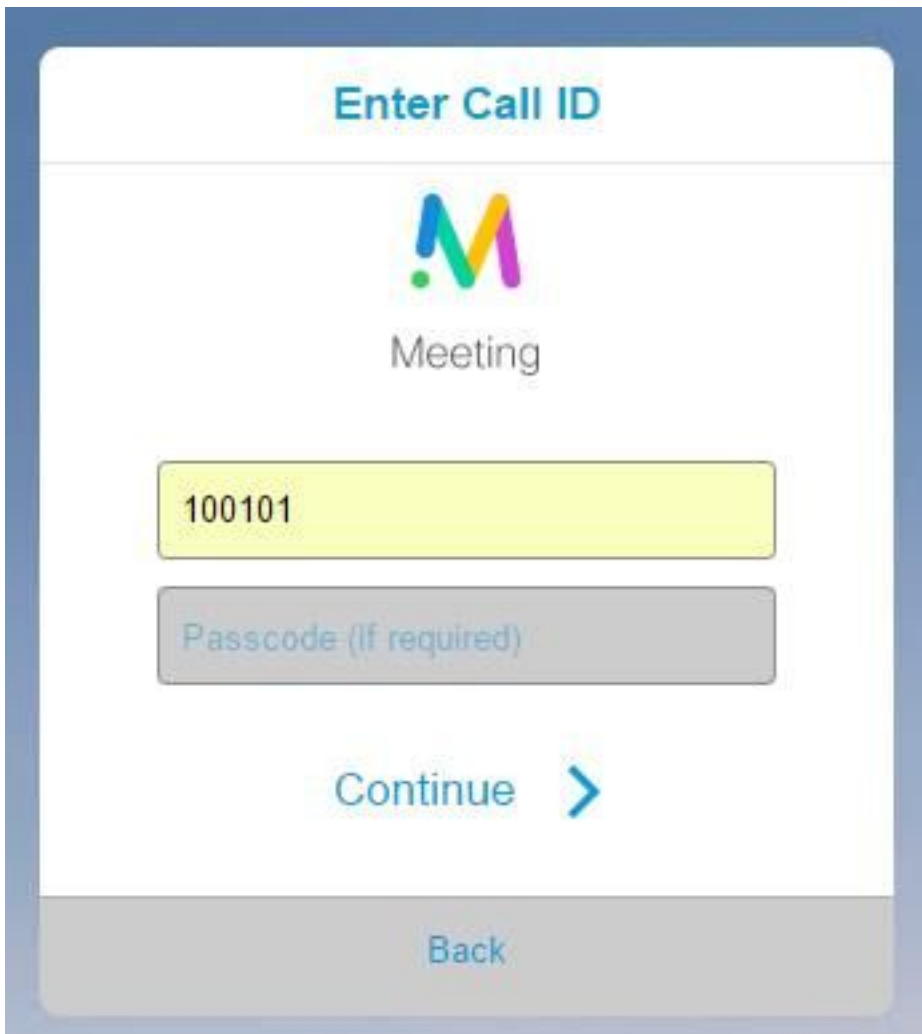
步骤1.选择支持的Web浏览器并输入外部Webbridge URL，您必须看到下一个屏幕，如图所示。

注意：您可以在链接中找到支持的浏览器和版本列表

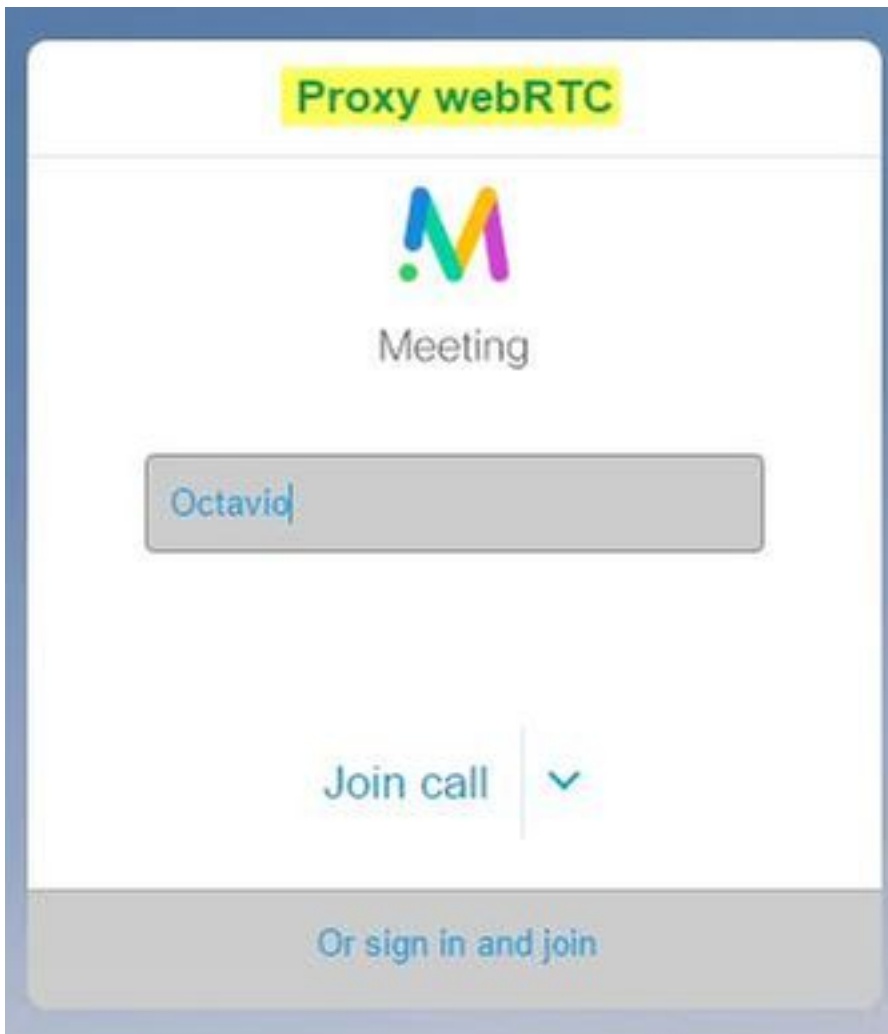
：<https://kb.acano.com/content/2/4/en/what-versions-of-browsers-do-we-support-for-webrtc.html?highlight=html%5C-5%20compliant%20browsers#content>



步骤2.选择Join call并输入先前配置的空间ID，如图所示。



步骤3.单击continue并输入您的名称，此时您必须看到要加入的空间的名称，在本例中，空间名称为Proxy webRTC。单击Join call，如图所示。



步骤4.加入另一台设备，您必须看到会议中连接的两台设备，如图所示。

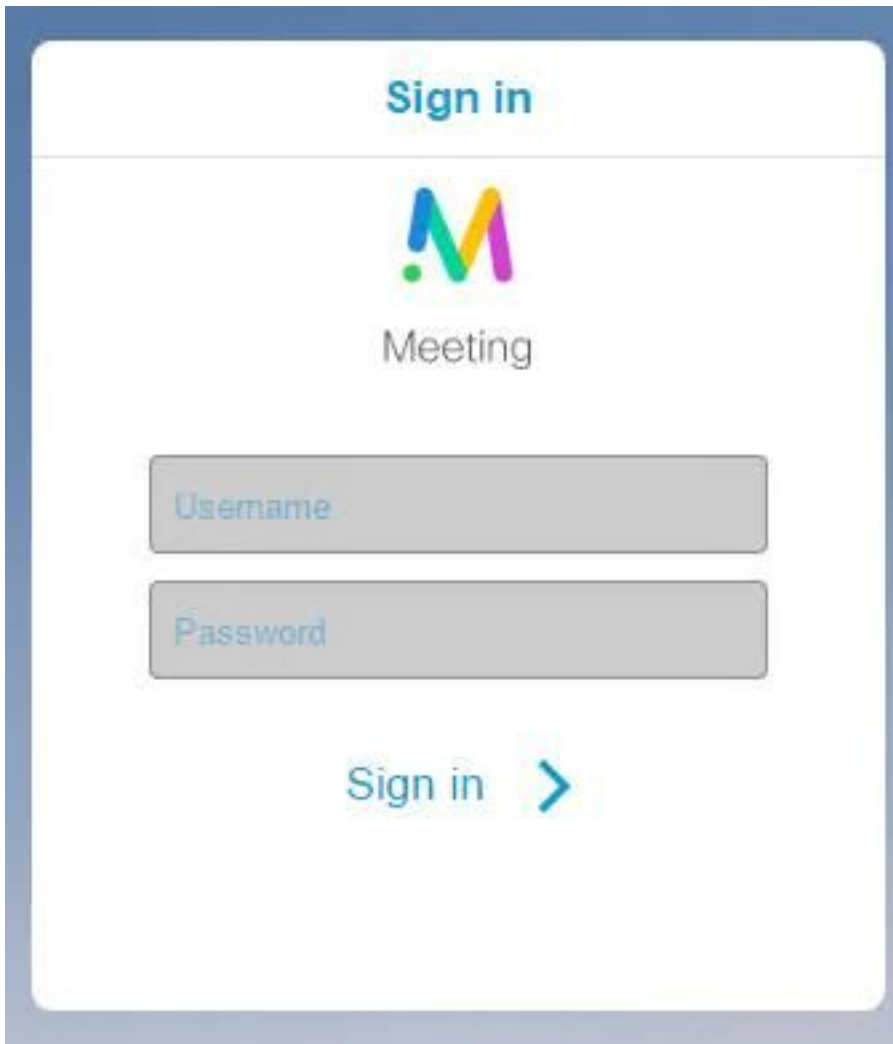


故障排除

本部分提供的信息可用于对配置进行故障排除。

未显示加入呼叫按钮

打开Webbridge页时，加入呼叫按钮不显示，当您输入CMS网页时，您会看到第二个图像中显示的错误，如图所示。



Fault conditions

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

当网桥无法与呼叫网桥正确通信时，会发生问题。

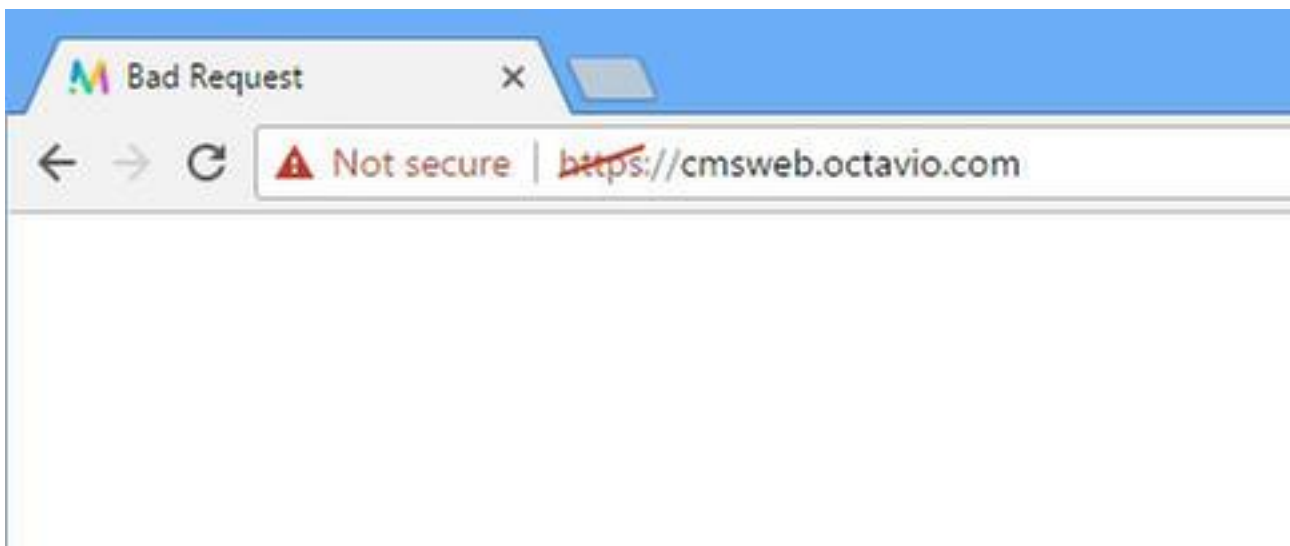
解决方案

- 检查CMS管理员网页上的Webbridge URL配置是否正确。为此，请导航至“配置”>“常规”。
- Webbridge和Callbridge必须相互信任，请检查信任捆绑是否已添加到Webbridge配置中，如图所示：


```
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>
```

注意：信任捆绑包是呼叫网桥证书。

WebRTC页面显示“错误请求”



解决方案

- 检查Expressway-C上配置了正确的访客帐户客户端URI。为此，请导航至**Configuration > Unified Communication > Cisco Meeting Server**。

如果内部URL在访客帐户客户端URL中配置，则Expressway-C将解析它，因为DNS服务器上已创建记录，但这可能导致Web浏览器中出现“错误请求”错误消息。在本例中，配置内部URL以显示错误，如图所示。

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 ⓘ

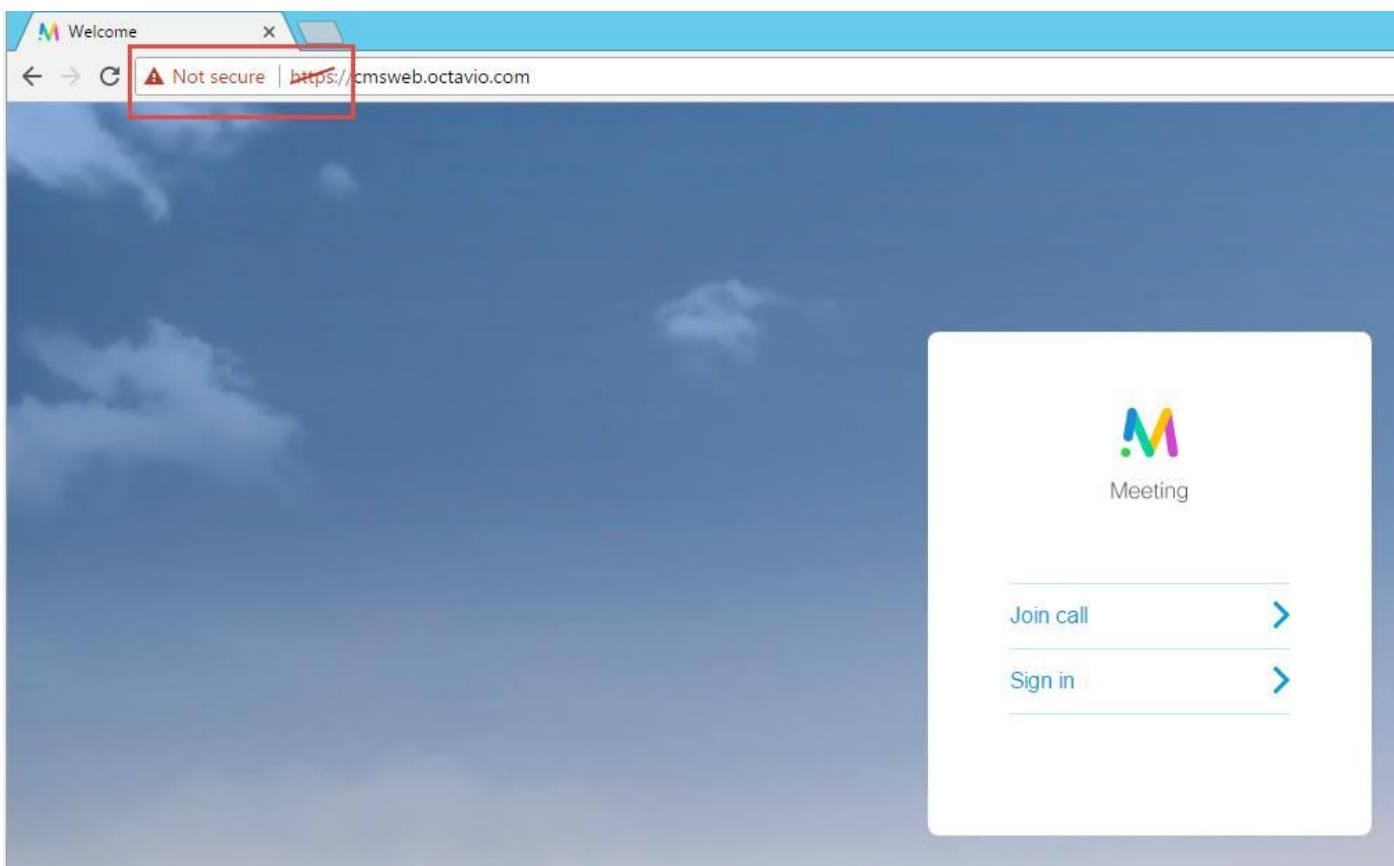
Guest account client URI

* cmsweb.cms.octavio.local ⓘ

Guest account client URI resolved to the following targets

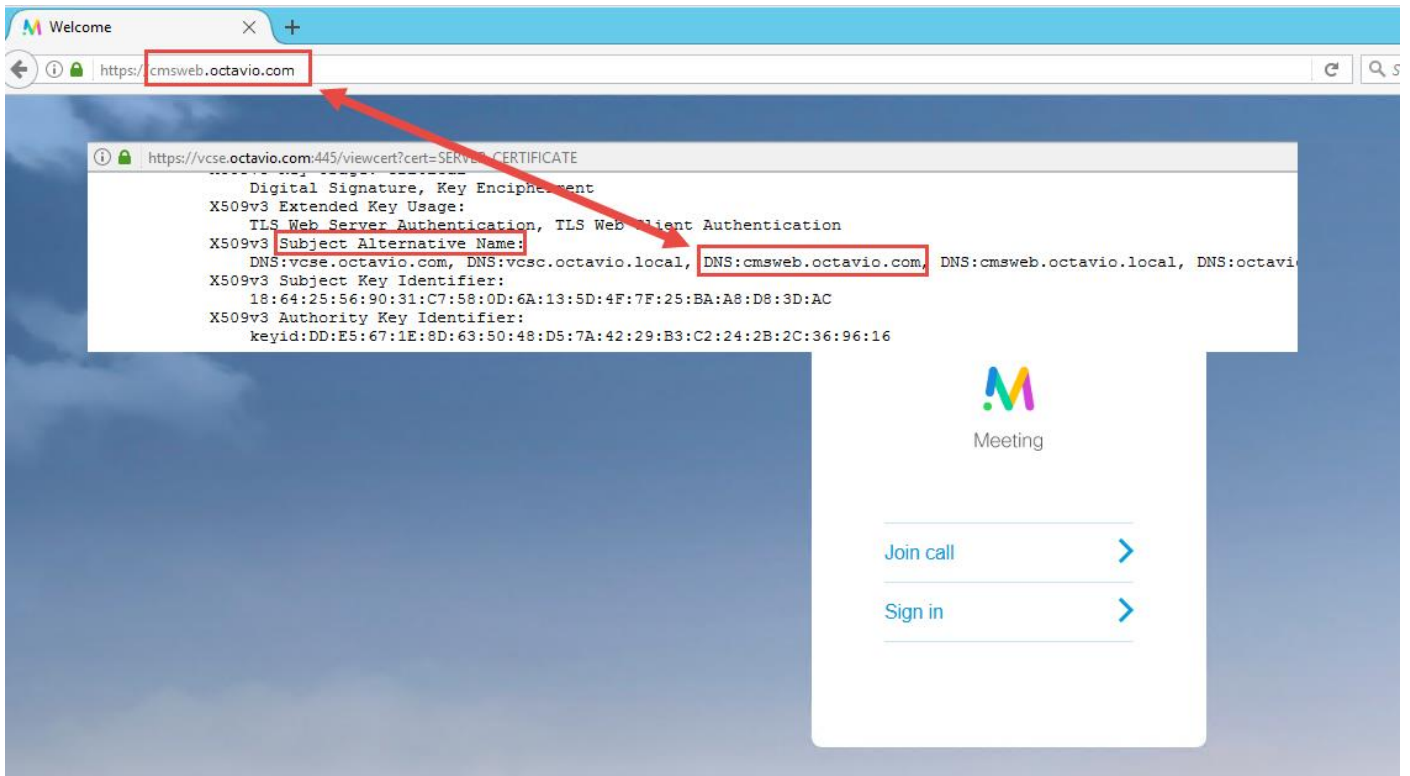
Name	Address
cmsweb.cms.octavio.local	172.16.85.180

WebRTC客户端显示不安全连接

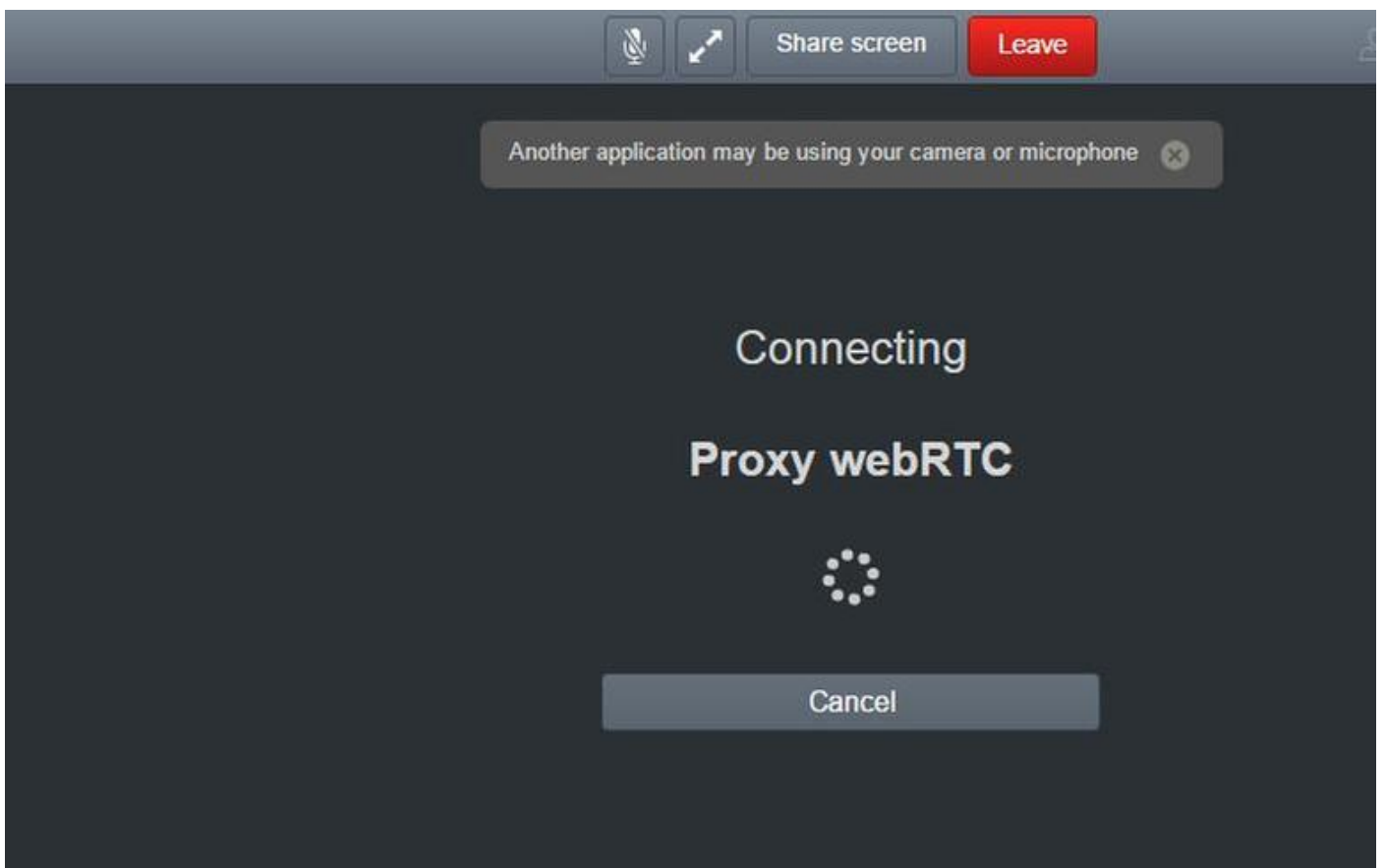


解决方案

- 证书是自签名的，导致服务器不信任源。将Expressway-E上的证书更改为受支持的第三方证书颁发机构。
- 检查外部Webbridge URL是否作为SAN添加到Expressway-E服务器证书上，如图所示。



WebRTC客户端连接但从未连接，然后超时并断开连接



TURN服务器用户名或密码在expressway-E或CMS中通过API配置错误。日志包含图像中显示的错误。

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

也可以通过数据包捕获确认错误。在运行WebRTC客户端的PC上运行Wireshark。完成数据包捕获后，按STUN过滤数据包。您必须看到图中显示的错误。

1458	2017-05-20 19:52:48.784809	172.16.84.124	10.88.246.156	STUN	182 0x1e4a (7754)	Default	Allocate Request UDP user: turnuser	real: turnuser with nonce
1462	2017-05-20 19:52:48.714894	10.88.246.156	172.16.84.124	STUN	262 0x8abc (2748)	Default	Allocate Error Response user: turnuser with nonce	real: turnuser UDP error-code: 431 ("Unknown error code") Integrity Check Failure

PC发送分配请求，Expressway NAT地址回应“完整性检查失败”消息。

解决方案

要修复错误，请查看用户名和密码。必须在TURN服务器参数上正确配置它们，如图所示。

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

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

The bottom screenshot is from the Cisco Expressway-E configuration page, showing the "Local authentication database" configuration. The "Name" field is set to "turnuser" and the "Password" field is masked with dots.