

使用雙域的Expressway上的CMS配置代理WebRTC

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[技術問答](#)

[DNS配置](#)

[內部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](#)

[驗證](#)

[疑難排解](#)

[未顯示「加入呼叫」按鈕](#)

[WebRTC頁面顯示「錯誤請求」](#)

[WebRTC客戶端顯示不安全的連線](#)

[WebRTC客戶端連線但從未連線，然後超時並斷開](#)

簡介

本檔案介紹透過Expressway為思科會議伺服器(CMS)設定具有不同內部和外部網域的代理Web即時通訊(webRTC)的範例。

必要條件

需求

思科建議您瞭解以下主題：

- CMS單一組合部署版本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上配置的Callbridge和Webbridge
- 在Expressway對上啟用移動和遠端訪問(MRA)
- 使用中繼NAT(TURN)選項金鑰向Expressway-E新增的遍歷
- Webbridge URL的外部可解析域名伺服器(DNS)記錄 (對於外部域)

- 從外部到內部域的CMS IP地址的內部可解析DNS記錄
- 在CMS上為內部和外部域配置的可擴展消息傳送和線上狀態協定(XMPP)多域
- 從公共Internet到Expressway E的公共IP地址在防火牆上開啟的TCP埠443
- 從公共Internet到Expressway E的公共IP地址在防火牆上開啟的TCP和UDP埠3478
- 在防火牆上開啟24000-29999的UDP埠範圍與Expressway-E的公共IP地址之間的連線

採用元件

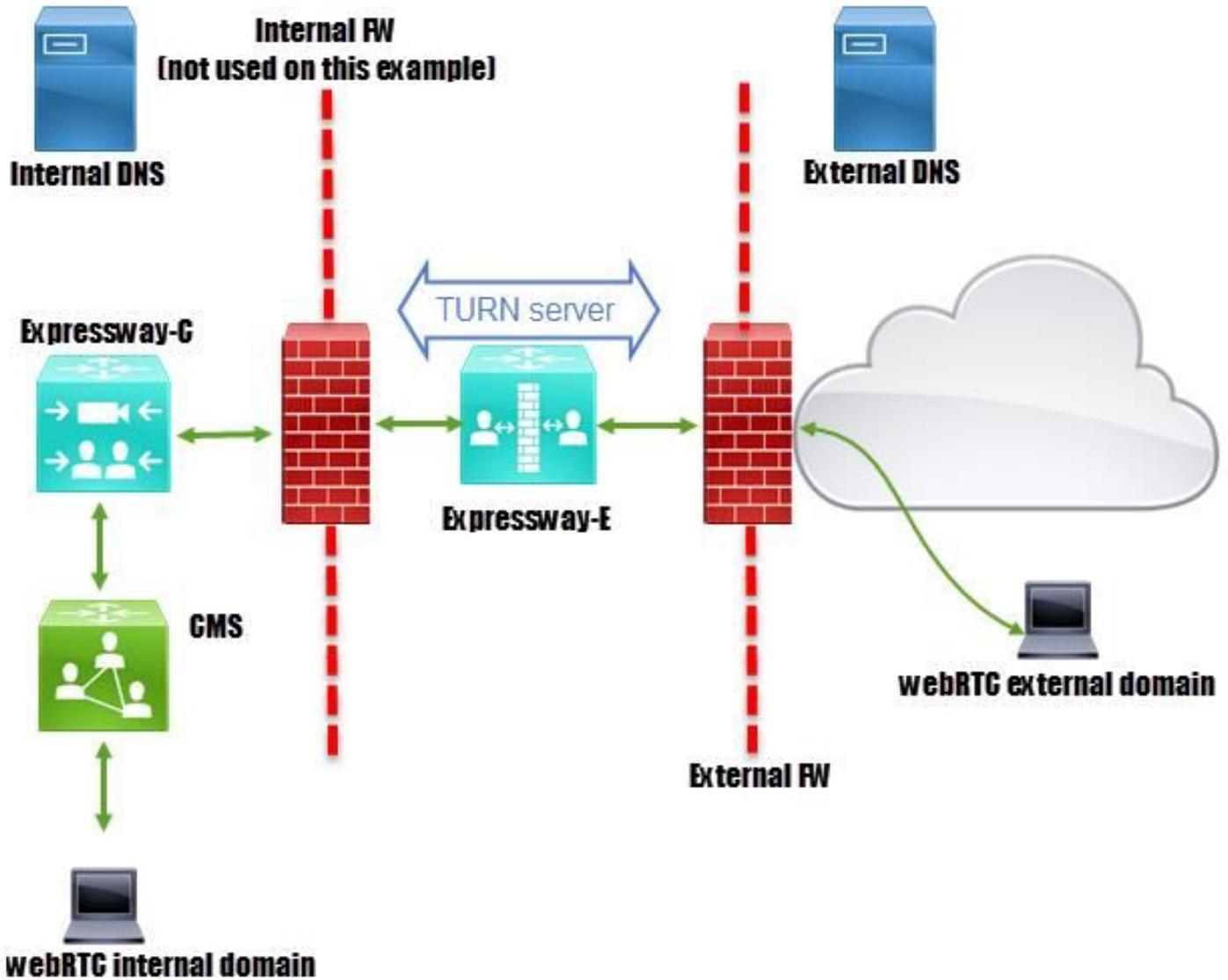
本文中的資訊係根據以下軟體和硬體版本：

- CMS單一組合部署版本2.2.1
- Expressway-C和Expressway-E，帶雙網路介面卡(NIC)和靜態網路位址轉譯(NAT)軟體版本X8.9.2
- 郵遞員

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

網路圖表



技術問答

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
靜態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] ocupsp.octavio.local.	static

External domain resolves to internal

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

外部DNS配置

外部DNS必須具有解析為Expressway-E的靜態NAT IP地址的webbridge URL，如圖所示。

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和XMPP配置

步驟1.您必須啟用callbridge許可證。該圖顯示了處於活動狀態的callbridge許可證。

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

有關更多許可資訊：

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

步驟2.通過MMP啟用callbridge、webbridge和XMPP，如下圖所示。

```
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
```

請點選此連結瞭解有關如何啟用這些功能的詳細流程：

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

請點選以下連結瞭解有關如何建立證書的詳細流程：

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

步驟3.導覽至Configuration > General上的CMS網頁，並設定Webbridge的內部和外部URL，如下圖所示。

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

附註：CMS必須至少配置一個空間。

CMS上已配置空間的示例，如圖所示。

<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

附註：必須為內部域和外部域配置來電

下圖所示為傳入呼叫處理配置的域。

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

步驟1.必須通過Postman通過API配置TURN。此命令用於所有配置。

<https://>

步驟2.使用POST方法並導航到Body，以檢視TURN伺服器引數或對其進行編輯。配置給TURN伺服器的引數如下圖所示。

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

步驟3.通過運行方法GET檢查TURN伺服器配置的狀態並復制伺服器ID。必須複製的ID如下圖所示。

```
<?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>
```

步驟4.複製API命令結尾的ID，然後使用GET方法檢視TURN伺服器資訊，如下圖所示。

附註：該資訊不會顯示伺服器的密碼。

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>
```

步驟5.按一下**send**以取得伺服器狀態。成功配置的示例，如下圖所示。

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

步驟1. Expressway-C必須具有內部域(octavio.local)，而Expressway-E必須配置外部域(octavio.com)，如下圖所示。



DNS

DNS settings

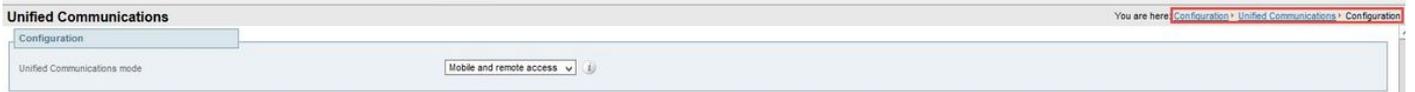
System host name	<input type="text" value="vcsc"/>	
Domain name	<input type="text" value="octavio.local"/>	
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>	

Default DNS servers

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

Internal DNS server

步驟2.必須在Expressway C和E上啟用MRA，如下圖所示。



步驟3.在Expressway-C和E之間建立統一通訊遍歷區域，如下圖所示。



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

Expressway-C上的配置

步驟1.在Expressway-C上配置內部域和外部域，如下圖所示。



Status System **Configuration** Application

Domains

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

步驟2. 啟用思科會議配置。導覽至 Configuration > Unified Communications > Cisco Meeting Server。在「Guest account client URI」欄位上設定外部webbridge URL，如下圖所示。



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

附註： 內部DNS應將外部webbridge URL(cmsweb.octavio.com)解析為內部CMS webbridge IP地址。在本例中，IP是172.16.85.180。

Expressway-C上的安全外殼(SSH)隧道必須在幾秒鐘後變為活動狀態，如下圖所示。



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： 伺服器必須具有伺服器證書和CA證書。

Expressway-E上的配置

步驟1. Expressway-E必須具有TURN許可證，如下圖所示。

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

步驟2. 必須使用外部域配置Expressway-E，如下圖所示。

CISCO Cisco Expressway-E

Status **System** Configuration Applications Users Maintenance

DNS

DNS settings

System host name: vcse

Domain name: octavio.com

Default DNS servers

Address 1: 10.88.246.210

Address 2:

External DNS server

步驟3. 為TURN伺服器 and 統一通訊穿越區域建立使用者，如下圖所示。

CISCO 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

步驟4. 建立統一通訊遍歷區域，如下圖所示。

The screenshot 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

步驟5. 配置TURN伺服器。導覽至Configuration > Traversal > TURN，如下圖所示。

附註： TURN請求必須傳送到埠3478，因為Web客戶端請求TURN連線的埠。

The screenshot shows the 'TURN' 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
---------------	----

出現「Turn up (開啟)」後，狀態顯示「Active (活動)」，如下圖所示。

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

步驟6. 導航到 **System > Administration**。WebRTC 客戶端請求埠 443 上的訪問，因此 Expressway-E 的管理埠必須更改為其他管理埠，在本例中該埠將更改為 445，如下圖所示。

The screenshot shows the 'Web server configuration' page. The 'Web administrator port' is highlighted in yellow and set to 445. Other settings include 'Redirect HTTP requests to HTTPS' (On), 'HTTP Strict Transport Security (HSTS)' (On), and 'Client certificate-based security' (Not required).

步驟7. 為 Expressway-E 建立證書：webbridge URL 必須新增為伺服器證書上的 SAN，如下圖所示。

```
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
```

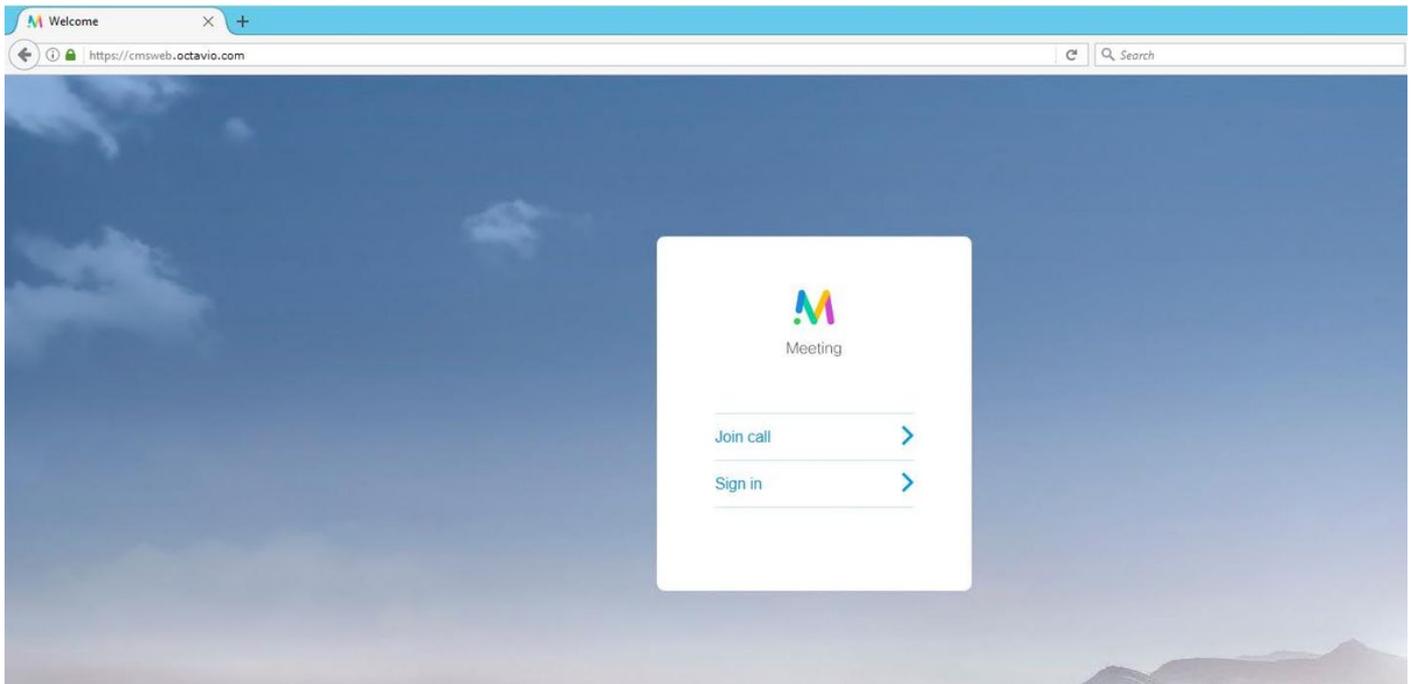
驗證

使用本節內容，確認您的組態是否正常運作。

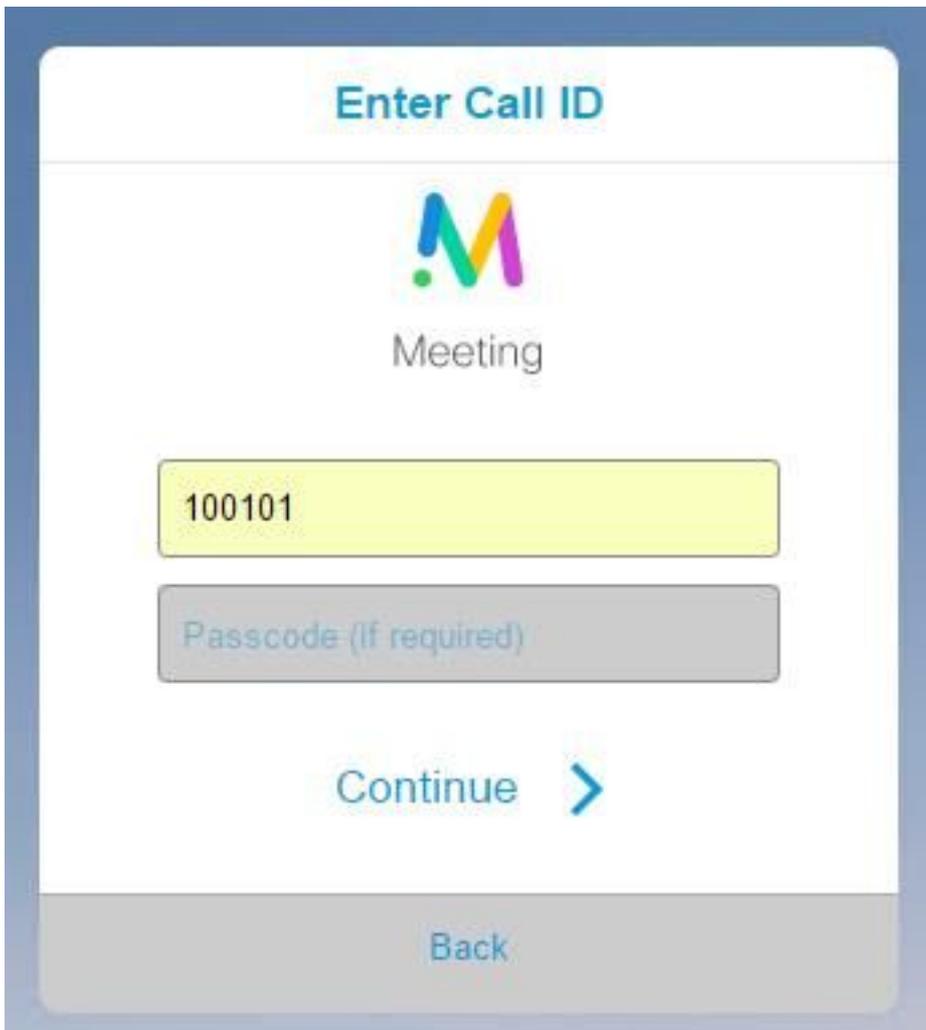
步驟1. 選擇支援的 Web 瀏覽器並輸入外部 Webbridge URL，您必須看到下一個畫面，如下圖所示。

附註：您可以在連結上找到支援的瀏覽器和版本的清單

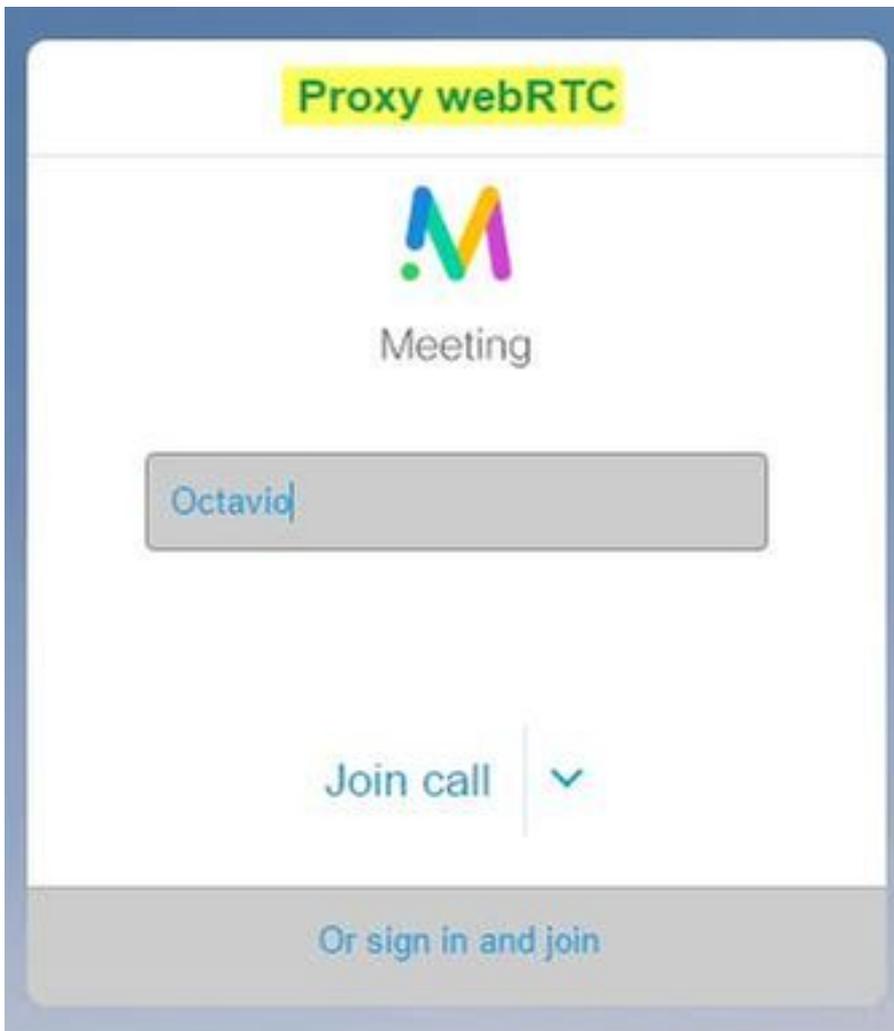
：<https://kb.acano.com/content/2/4/en/what-versions-of-browsers-do-we-support-for-webrtc.html?highlight=html%5C-5%20compliant%20browsers#content>



步驟2.選擇Join call，然後輸入先前配置的空間ID，如下圖所示。



步驟3.按一下continue並輸入您的名稱，此時您必須看到要加入的空間名稱，在這種情況下，空間名稱是Proxy webRTC。按一下「Join call」，如下圖所示。



步驟4.加入另一台裝置，您必須看到兩台裝置在會議中連接，如下圖所示。

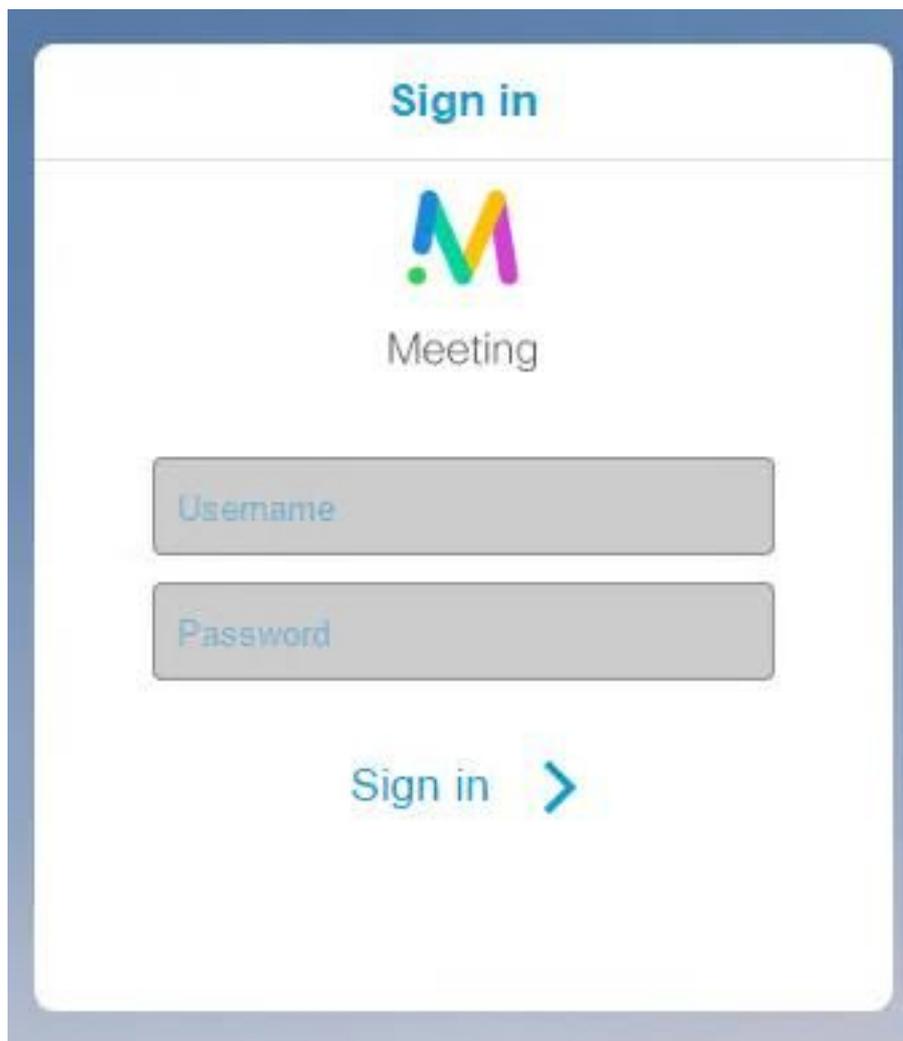


疑難排解

本節提供的資訊可用於對組態進行疑難排解。

未顯示「加入呼叫」按鈕

當您開啟Webbridge頁面時，不會顯示Join call按鈕；當您進入CMS網頁時，會看到第二個影象中所示的錯誤，如下圖所示。



Fault conditions

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

當Webbridge無法與呼叫網橋正確通訊時會發生此問題。

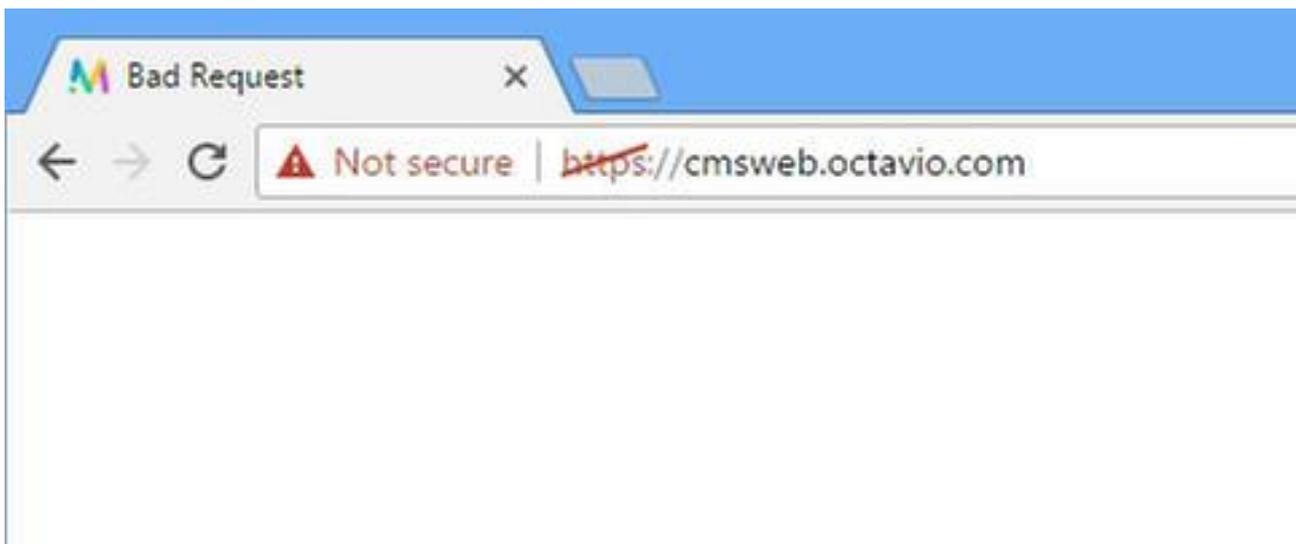
解決方案

- 檢查CMS管理網頁上的Webbridge URL是否配置正確。為此，請導覽至**Configuration > General**。
- Webbridge和callbridge必須彼此信任，請檢查信任捆綁是否已新增到Webbridge配置，如下圖所示：

```
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>
```

附註：信任捆綁包是呼叫網橋證書。

WebRTC頁面顯示「錯誤請求」



解決方案

- 檢查Expressway-C上配置的正确訪客帳戶客戶端URI。為此，請導航到**配置>統一通訊>思科會議伺服器**。

如果在訪客帳戶客戶端URL中配置了內部URL，Expressway-C將解析該內部URL，因為DNS伺服器上建立了記錄，但這可能會導致Web瀏覽器中出現「錯誤請求」錯誤消息。在此範例中，內部URL設定為顯示錯誤，如下圖所示。

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 ⓘ

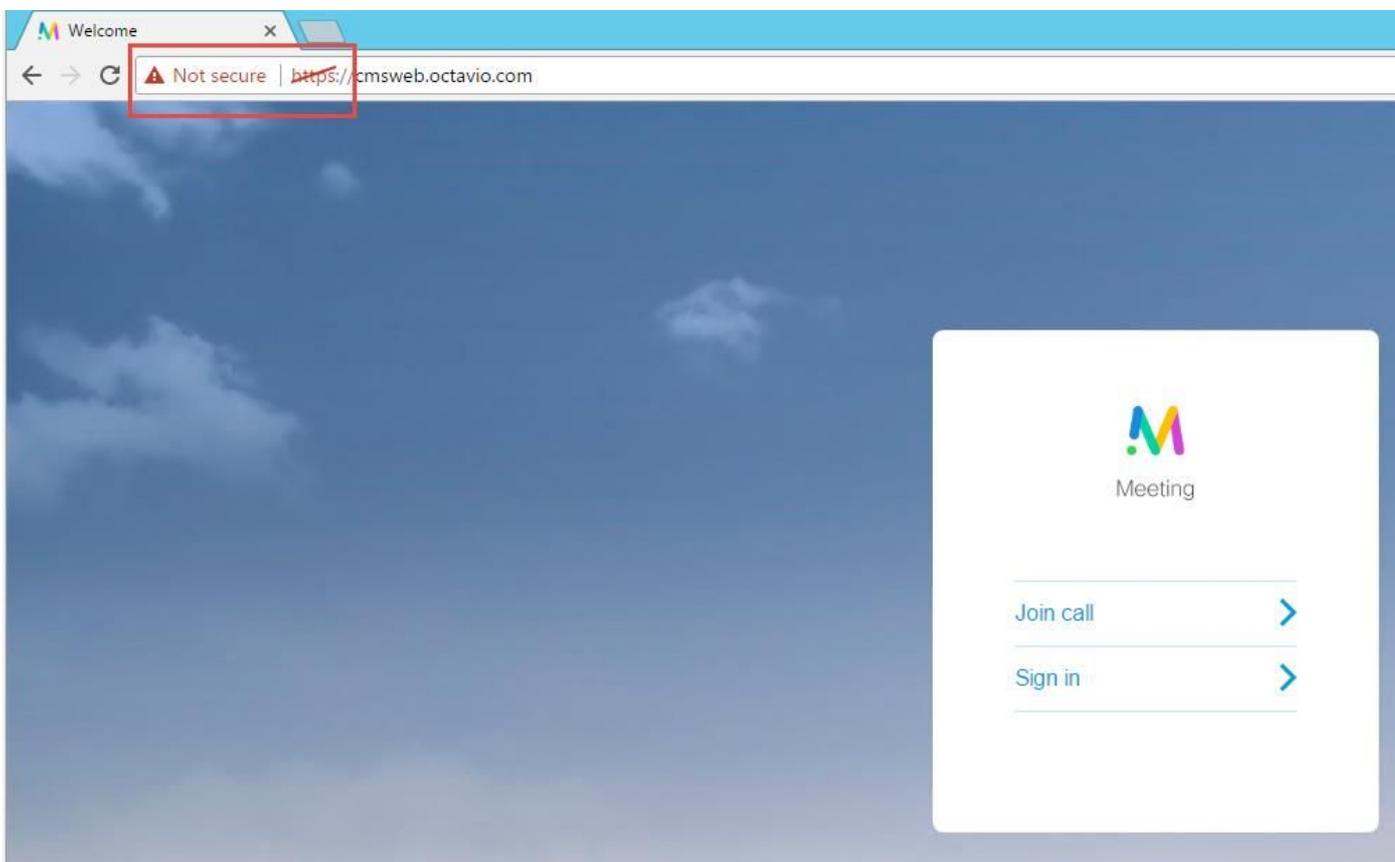
Guest account client URI

* cmsweb.cms.octavio.local ⓘ

Guest account client URI resolved to the following targets

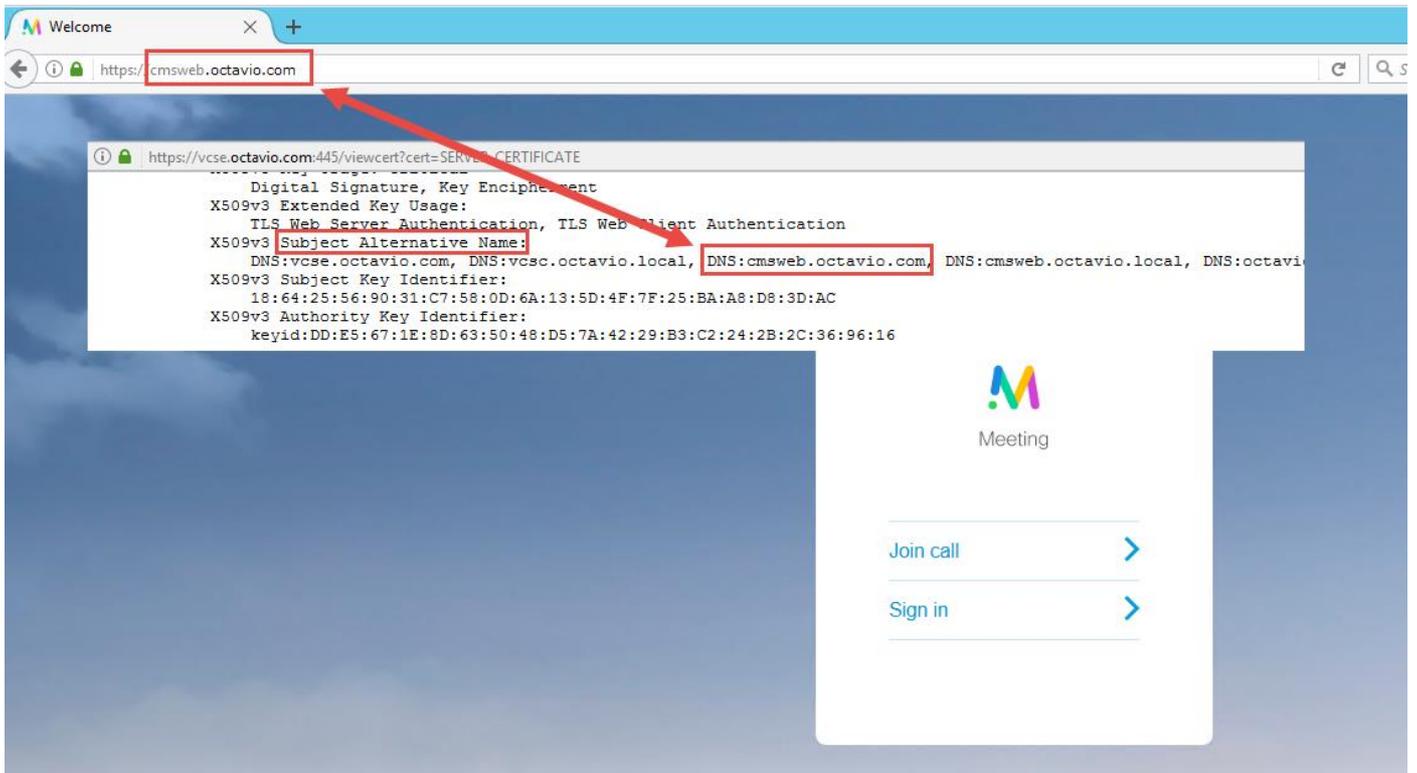
Name	Address
cmsweb.cms.octavio.local	172.16.85.180

WebRTC客戶端顯示不安全的連線

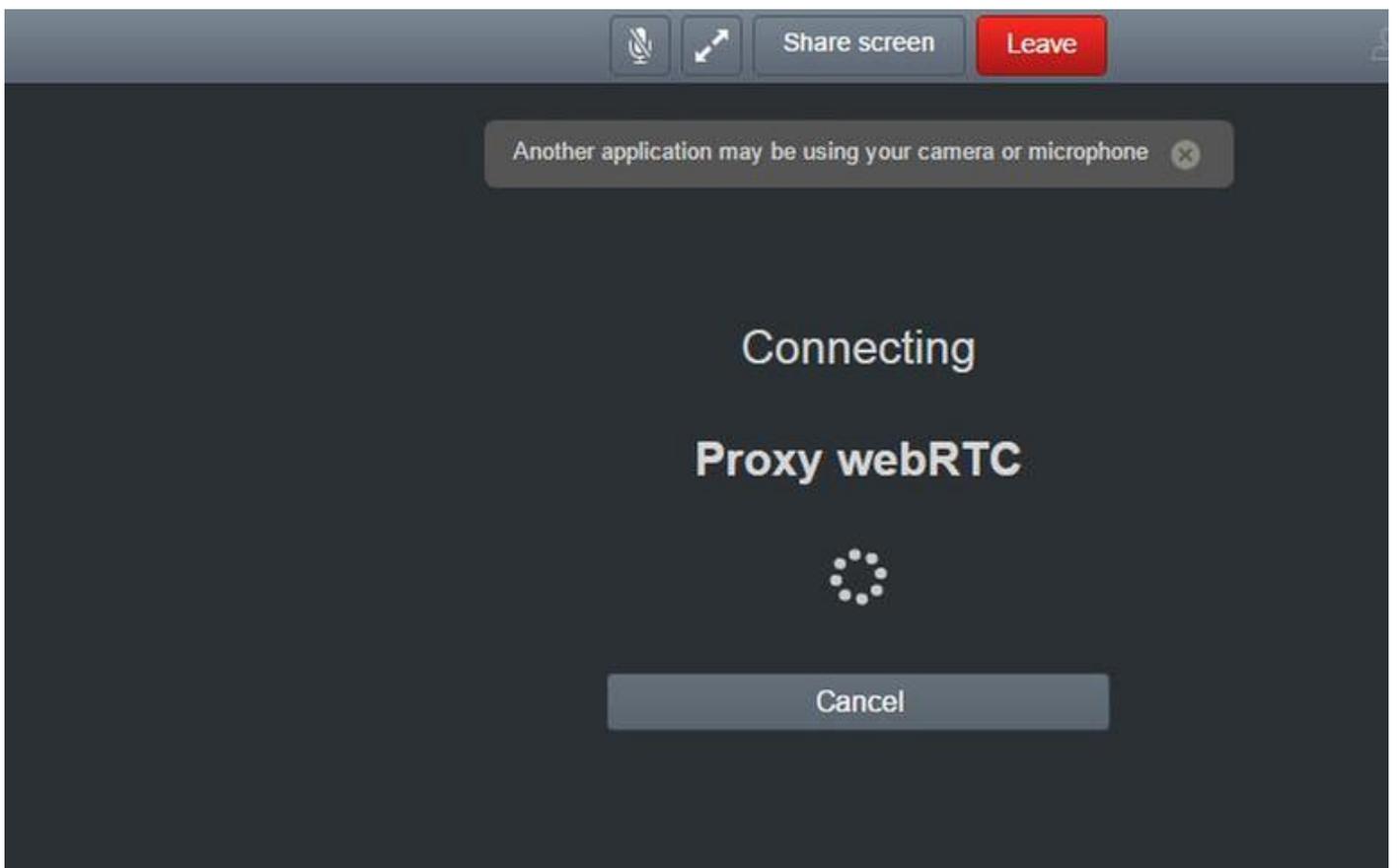


解決方案

- 證書是自簽名的，這導致伺服器不信任源。將Expressway-E上的證書更改為支援的第三方證書頒發機構。
- 檢查外部Webbridge URL是否作為SAN新增到Expressway-E伺服器證書，如下圖所示。



WebRTC客戶端連線但從未連線，然後超時並斷開



通過API在expressway-E或CMS中錯誤配置了TURN伺服器使用者名稱或密碼。日誌中包含圖中所示的錯誤。

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

錯誤也可以通過資料包捕獲來確認。在運行webRTC客戶端的PC上運行Wireshark。擷取封包後，請按STUN過濾封包。您必須看到圖中所示的錯誤。

1458	2017-05-20	19:52:48.784889	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傳送Allocate Request消息，Expressway NAT地址將以「完整性檢查失敗」消息回覆。

解決方案

若要修正錯誤，請檢視使用者名稱和密碼。必須正確配置TURN伺服器引數，如圖所示。

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 `x-www-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 "Configuration" tab is active, and the "Name" field is set to "turnuser". The "Password" field is masked with dots.