

# Proxy WebexRTC met CMS configureren via expressie met dubbel domein

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Technische informatie](#)

[DNS-configuratie](#)

[Interne DNS-configuratie](#)

[Externe DNS-configuratie](#)

[Configuratie CMS, Callbridge, Webbridge en XMPP](#)

[Configuratie omdraaien](#)

[Configuratie van I/U](#)

[Configuratie via sneltoets-C](#)

[Configuratie op Express-E](#)

[Verifiëren](#)

[Problemen oplossen](#)

[De selectieknop oproepen wordt niet weergegeven](#)

[WebexRTC-pagina toont 'Slecht verzoek'](#)

[WebexRTC-client toont onveilige verbinding](#)

[WebexRTC-client wordt aangesloten maar nooit aangesloten en dan uitgeschakeld](#)

## Inleiding

Dit document beschrijft een voorbeeldconfiguratie van de proxy-Web Real-Time Communication (webRTC) voor Cisco Meeting Server (CMS) via Expressway met verschillende interne en externe domein.

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

- CMS, versie 2.1.4 en hoger
- Snelweg C en snelweg E, versie X8.9.2 en hoger
- Callbridge en webbridge ingesteld op CMS
- Mobiele en Remote Access (MRA) ingeschakeld op het snelpaar
- Verplaatsing met behulp van de optie Relay NAT (TURN) toegevoegd aan de sneltoets

## Expressway-E

- Externe oplosbare Domain Name Server (DNS)-record voor webbridge URL, voor extern domein
- Interne oplosbare DNS-record voor CMS IP-adres van extern naar intern domein
- Extensible Messaging and Presence Protocol (XMPP) voor meerdere domeinen ingesteld op CMS, voor intern en extern domein
- TCP-poort 443 openen op Firewall van het openbare internet naar het openbare IP-adres van de snelweg-E
- TCP- en UDP-poort 3478 geopend op firewall vanaf het openbare internet naar het openbare IP-adres van de snelweg-E
- UDP-poortbereik 2400-2999 geopend op firewall van en vanaf het openbare IP-adres van de expressway-E

## Gebruikte componenten

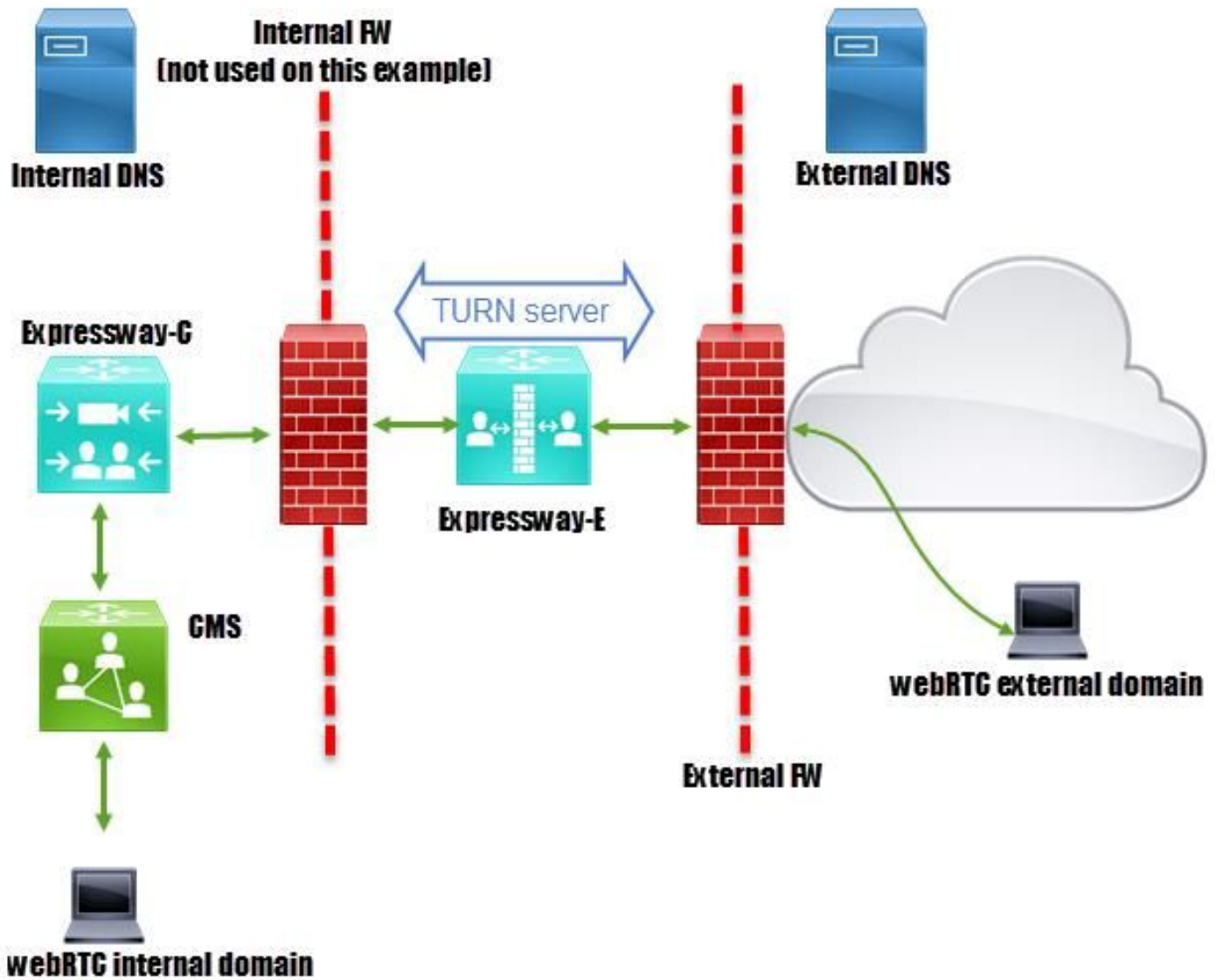
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CMS-versie 2.2.1
- Software voor Express-C en Express-E met dubbele netwerkinterfacekaart (NIC) en statische netwerkadresomzetting (NAT), versie X8.9.2
- Postman

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Configureren

## Netwerkdigram



## Technische informatie

Intern domein	cms.octavio.plaatselijk
Extern domein	octavio.com
CMS IP-adres	172.16.85.180
IP-adres snelweg-C	172.16.85.167
Expressway-E LAN1 IP-adres (intern)	172.16.85.168
Expressway-E LAN2 IP-adres (extern)	192.168.245.61
Statisch NAT IP-adres	10.88.246.156

## DNS-configuratie

### Interne DNS-configuratie

DNS		Name	Type	Data	Timestamp
ACTIVEDIRECTORY	Forward Lookup Zones	_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

## Externe DNS-configuratie

De externe DNS moet de URL van de webbridge hebben die oplost aan het statische NAT IP-adres van de Expressway-E zoals in de afbeelding wordt getoond.

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

## Configuratie CMS, Callbridge, Webbridge en XMPP

Stap 1. De bellenlicentie moet zijn geactiveerd. De afbeelding toont een callbridge-licentie die actief is.

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

Voor meer licentieinformatie:

[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](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)

Stap 2. Schakel de brug, de webbridge en de XMPP in zoals in de afbeelding.

```
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
```

Volg deze link voor een detailproces over de manier waarop u deze:

[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](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)

Volg deze link voor een detailproces over het maken van een certificaat:

[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](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)

Stap 3. Navigeer naar de CMS-webpagina op **Configuration > General** en stel de interne en externe URL voor de webbridge in zoals in de afbeelding.

**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*

Opmerking: Het CMS moet worden geconfigureerd met ten minste één ruimte.

Een voorbeeld van een ingestelde ruimte op CMS zoals in de afbeelding.

<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

Opmerking: De inkomende oproepen moeten worden geconfigureerd voor de interne en externe domeinen

Een voorbeeld van geconfigureerde domeinen voor inkomende gespreksafhandeling is zoals in de afbeelding weergegeven.

### 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

### Configuratie omdraaien

Stap 1. TURN moet via Postman door API worden geconfigureerd. Deze opdracht wordt in alle configuratie gebruikt.

<https://>

Stap 2. Gebruik de POST-methode en navigeer naar **Tekst** om de TURN-serverparameters te bekijken of te bewerken. De parameters die op de TURN-server zijn ingesteld, worden in de afbeelding weergegeven.

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

Stap 3. Controleer de status van de TURN-serverconfiguratie door de methode GET uit te voeren en kopieer de server-ID. De ID die moet worden gekopieerd, wordt weergegeven in de afbeelding.

```
<?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>
```

Stap 4. Kopieer de ID aan het einde van de API-opdracht en gebruik de GET methode om de TURN server-informatie zoals in de afbeelding te zien.

Opmerking: De informatie toont het wachtwoord van de server niet.

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` (The ID `2aa16ccc-87d1-424d-9d3d-3d007f23243a` is highlighted with a red box).
- Authorization:** Basic Auth
- Username:** admin
- Password:** ..... (masked)
- Body:** XML
- Status:** 200

The XML response body is as follows:

```
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>
```

Stap 5. Klik op **verzenden** om de serverstatus te krijgen. Een voorbeeld van een succesvolle configuratie zoals getoond in het beeld.



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>
```

## Configuratie van I/U

Stap 1. De snelweg-C moet het interne domein (octavio.local) hebben en de snelweg-E moet het externe domein (octavio.com) hebben dat zoals in de afbeelding is ingesteld.



## DNS

### DNS settings

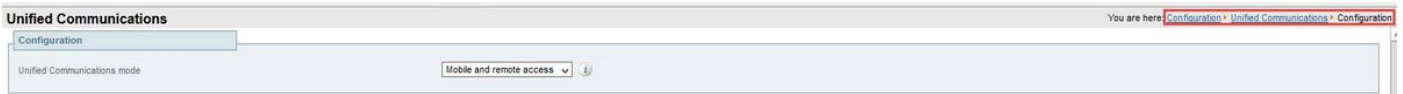
System host name	<input type="text" value="vcsc"/>	
Domain name	<input type="text" value="octavio.local"/>	
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>	

### Default DNS servers

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

Internal DNS server

Stap 2. De MRA moet zowel op sneltoets C als op toets E zijn ingeschakeld zoals in de afbeelding.



Stap 3. Maak een Unified Communications-traversale zone tussen de sneltoets-C en E zoals in de afbeelding.



### 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

## Configuratie via sneltoets-C

Stap 1. Configureer het interne en externe domein van de expressway-C zoals in de afbeelding.



Status System **Configuration** Applicat

## Domains

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

Stap 2. Schakel de Cisco-vergaderconfiguratie in. Navigeer naar **Configuratie > Unified Communications > Cisco Meeting Server**. Configureer de externe webbridge URL in het veld URI van de Guest-account, zoals in de afbeelding wordt weergegeven.



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

Opmerking: De interne DNS moet de externe webbridge-URL (cmsweb.octavio.com) op het interne CMS-webbridge-adres plaatsen. In dit voorbeeld is het IP 172.16.85.180.

De tunnels Secure Shell (SSH) in de expressway-C moeten na enkele seconden zoals in het beeld worden geactiveerd.



Status System Configuration Applications Users Maintenance

You are here: Status > Unified Communications

## Unified Communications SSH tunnels status

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

Opmerking: de server moet beschikken over een servercertificaat en een CA-certificaat.

## Configuratie op Express-E

Stap 1. De snelweg-E moet een TURN-licentie hebben zoals in de afbeelding.

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

Stap 2. De snelweg-E moet met het externe domein worden geconfigureerd zoals in de afbeelding.

Status **System** Configuration Applications Users Maintenance

**DNS**

**DNS settings**

System host name  ⓘ

Domain name  ⓘ

**Default DNS servers**

Address 1  ⓘ

Address 2  ⓘ

**External DNS server**

Stap 3. Maak gebruikers voor de TURN-server en voor de Unified Communications traversal-zone zoals in de afbeelding.



## Local authentication database

Records: 3

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

Stap 4. Maak een Unified Communications-traversale zone zoals in de afbeelding.



### 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  ⓘ

Stap 5. Configuratie van de TURN server. Navigeer naar **Configuration > Traversal > TURN** zoals in de afbeelding.

Opmerking: Het TURN-verzoek moet betrekking hebben op haven 3478 aangezien het de haven is waar de web client om de TURN-verbinding verzoekt.

Status System **Configuration** Applications Users Maintenance

**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*

Zodra de Draai naar boven is gekomen, toont de status Actief zoals in de afbeelding weergegeven.

**TURN server status**

Status	<b>Active</b>
Listening address 1	172.168.168.3478
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

Stap 6. Navigeer naar **Systeem > Beheer**. De webRTC client vraagt toegang op poort 443, om deze reden moet de beheerpoort van de Expressway-E worden gewijzigd in een ander, in dit voorbeeld geval wordt het gewijzigd in 445 zoals in de afbeelding.

**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*

Stap 7. certificaataanmaak voor de snelweg-E: de webbridge-URL moet als een SAN op het servercertificaat worden toegevoegd zoals in de afbeelding wordt getoond.

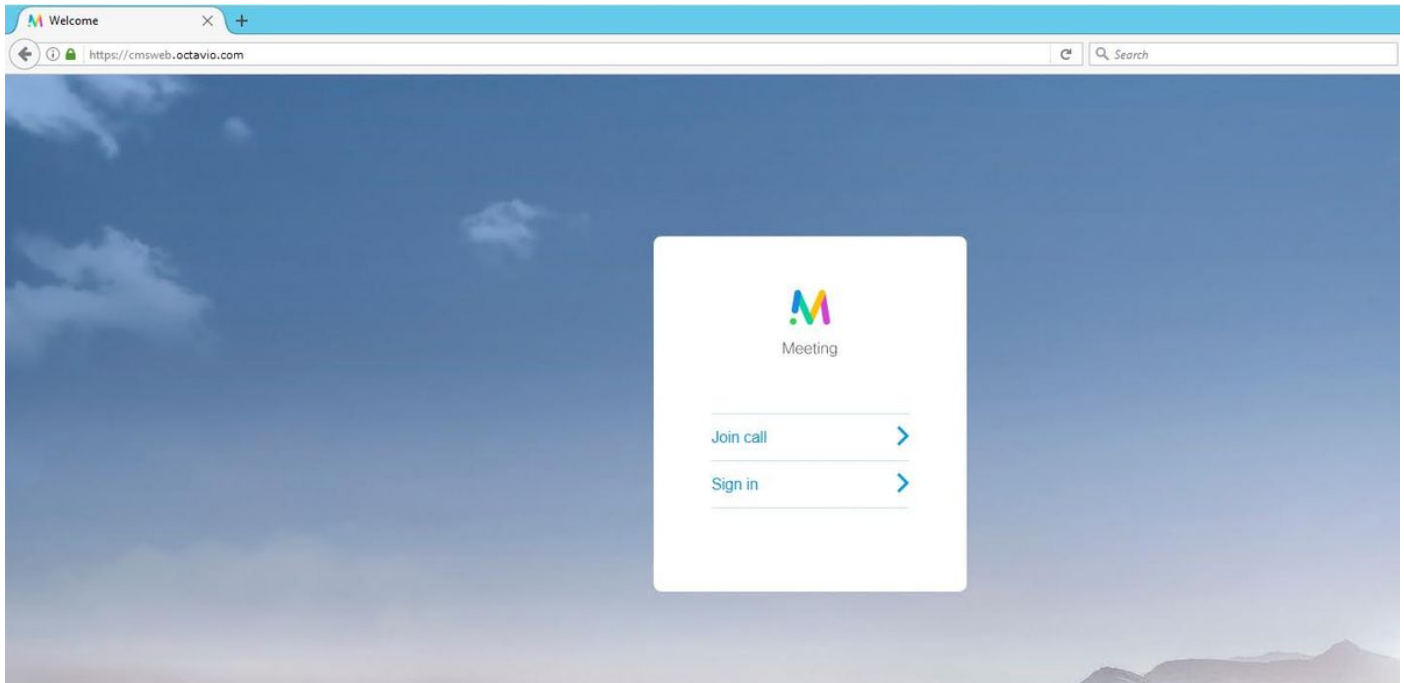
```
X509v3 Subject Alternative Name:
DNS:vcse.octavio.com, DNS:vcse.octavio.local, DNS:cmsweb.octavio.com, DNS:cmsweb.octavio.local, DNS:octavio.local, DNS:cms.octavio.local, DNS:octavio.com
```

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Stap 1. Selecteer een ondersteunde webbrowser en voer de externe webbridge-URL in. U moet het volgende scherm zien zoals in de afbeelding.


Opmerking: U vindt in de link een lijst met ondersteunde browsers en versies:  
<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>



Stap 2. Selecteer de optie **Aansluiten** en voer de eerder geconfigureerde spatie-ID in zoals in de afbeelding.



Enter Call ID



Meeting

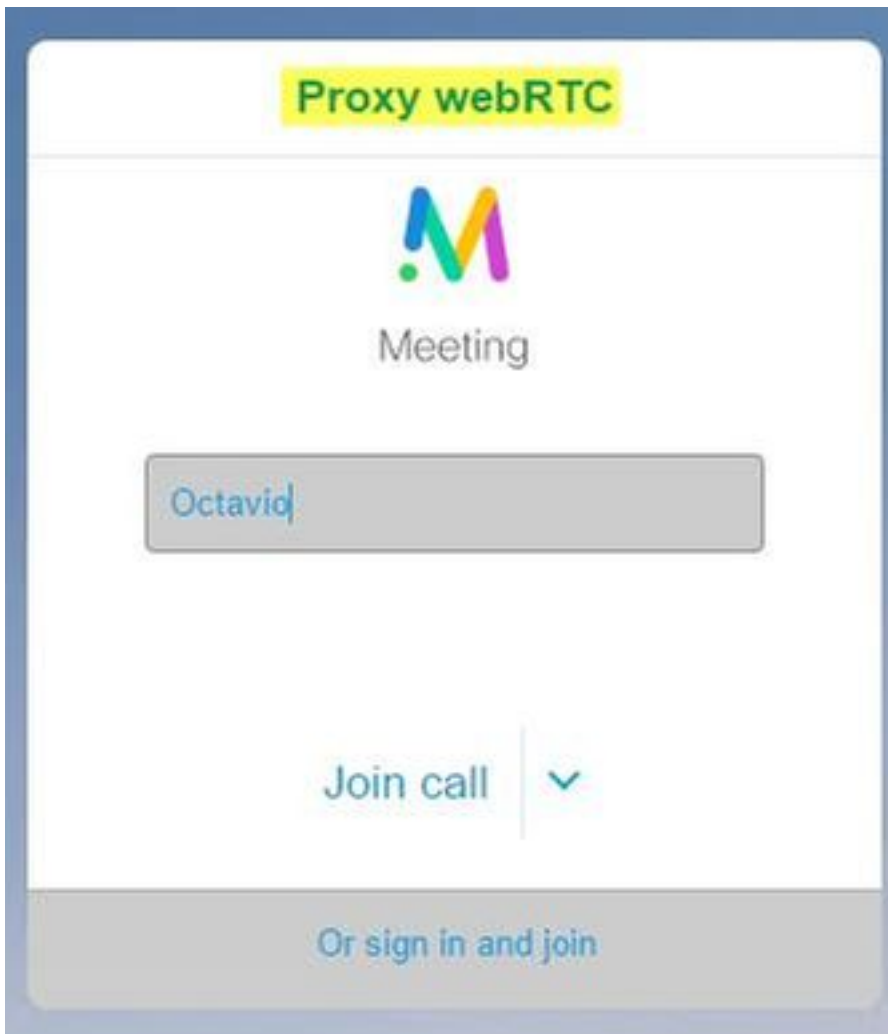
100101

Passcode (if required)

Continue >

Back

Stap 3. Klik op **Doorgaan** en voer uw naam in. Op dit punt moet u de naam van de ruimte zien waar u zich bij gaat aansluiten. In dit geval is de ruimtename Proxy webRTC. Klik op **Aansluiten** zoals in de afbeelding wordt weergegeven.



Stap 4. Doe mee met een ander apparaat en u moet beide apparaten zien die in de conferentie zijn aangesloten zoals in de afbeelding.

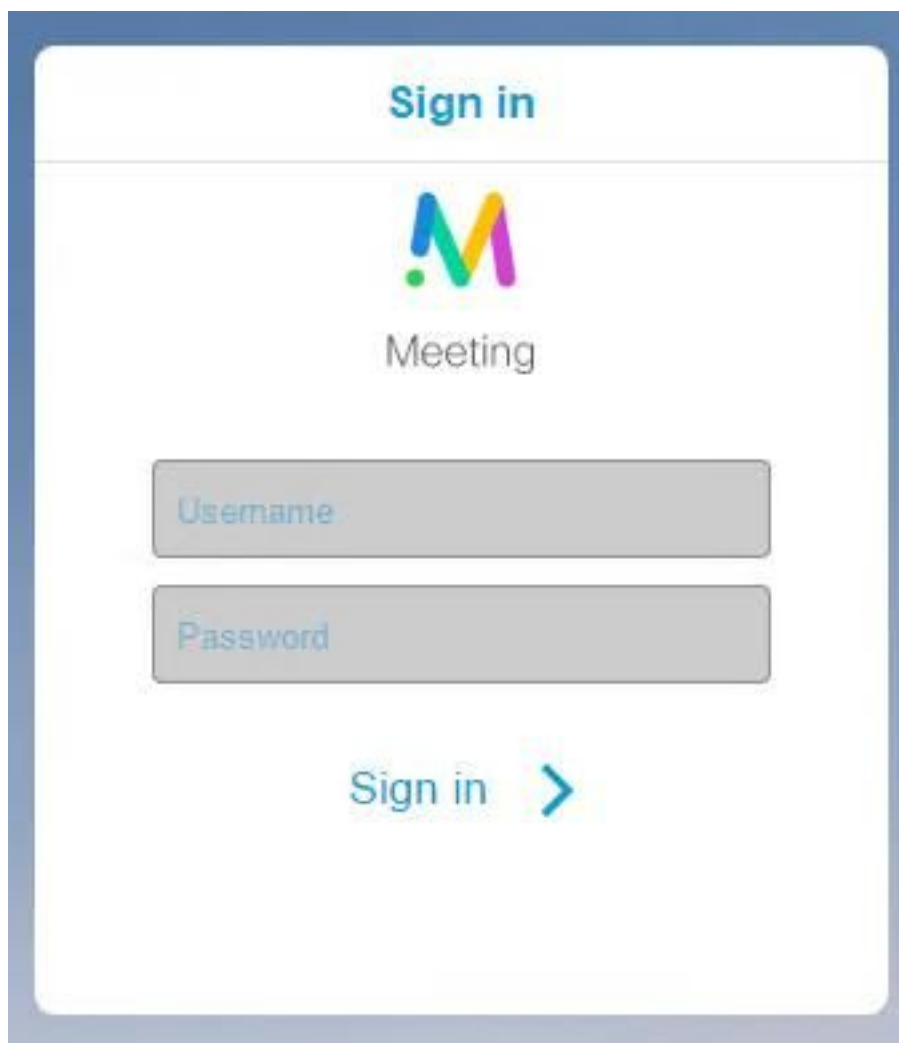


## Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

## De selectieknop oproepen wordt niet weergegeven

De knop **Aansluiten** wordt niet weergegeven wanneer u de webbridge pagina opent en u de fout ziet die in de tweede afbeelding wordt weergegeven wanneer u naar de CMS-webpagina zoals in de afbeelding gaat.



### Fault conditions

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

Het probleem gebeurt wanneer de webbridge niet goed met de callbridge communiceert.

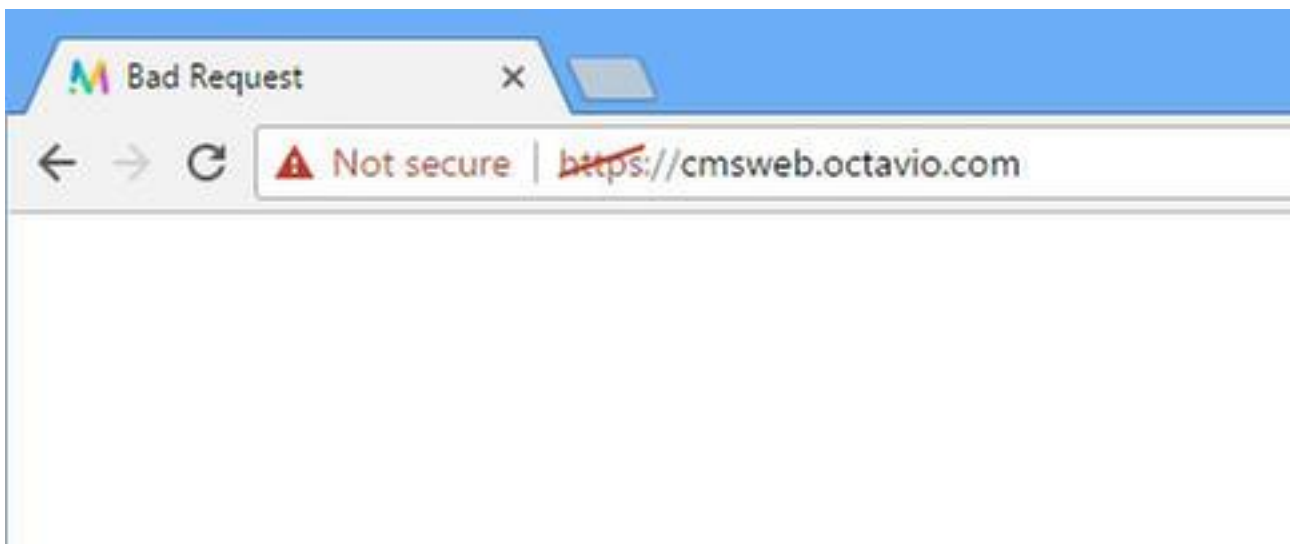
### Oplossing

- Controleer of de URL van de webbridge correct is ingesteld op de CMS-ADM-website. Blader naar **Configuratie > Algemeen** voor dit doel.
- De webbridge en de callbridge moeten elkaar vertrouwen, en controleren of de trust bundel is toegevoegd aan de configuratie van de webbridge zoals getoond in de afbeeldingen:

```
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>
```

Opmerking: De trust bundel is het overbruggingscertificaat.

## WebexRTC-pagina toont 'Slecht verzoek'



## Oplossing

- Controleer de juiste versie van de Guest account client URI wordt ingesteld op Expressway-C. Navigeer naar **Configuration > Unified Communications > Cisco Meeting Server** voor dit doel.

Als de interne URL is geconfigureerd in de URL van de client voor de Guest-account, lost de expressway-C deze op omdat er een record is gecreëerd op de DNS-server, maar dit kan de foutmelding "slechte aanvraag" in de webbrowser veroorzaken. In dit voorbeeld wordt de interne URL ingesteld om de fout zoals in de afbeelding te tonen.

### 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  ⓘ

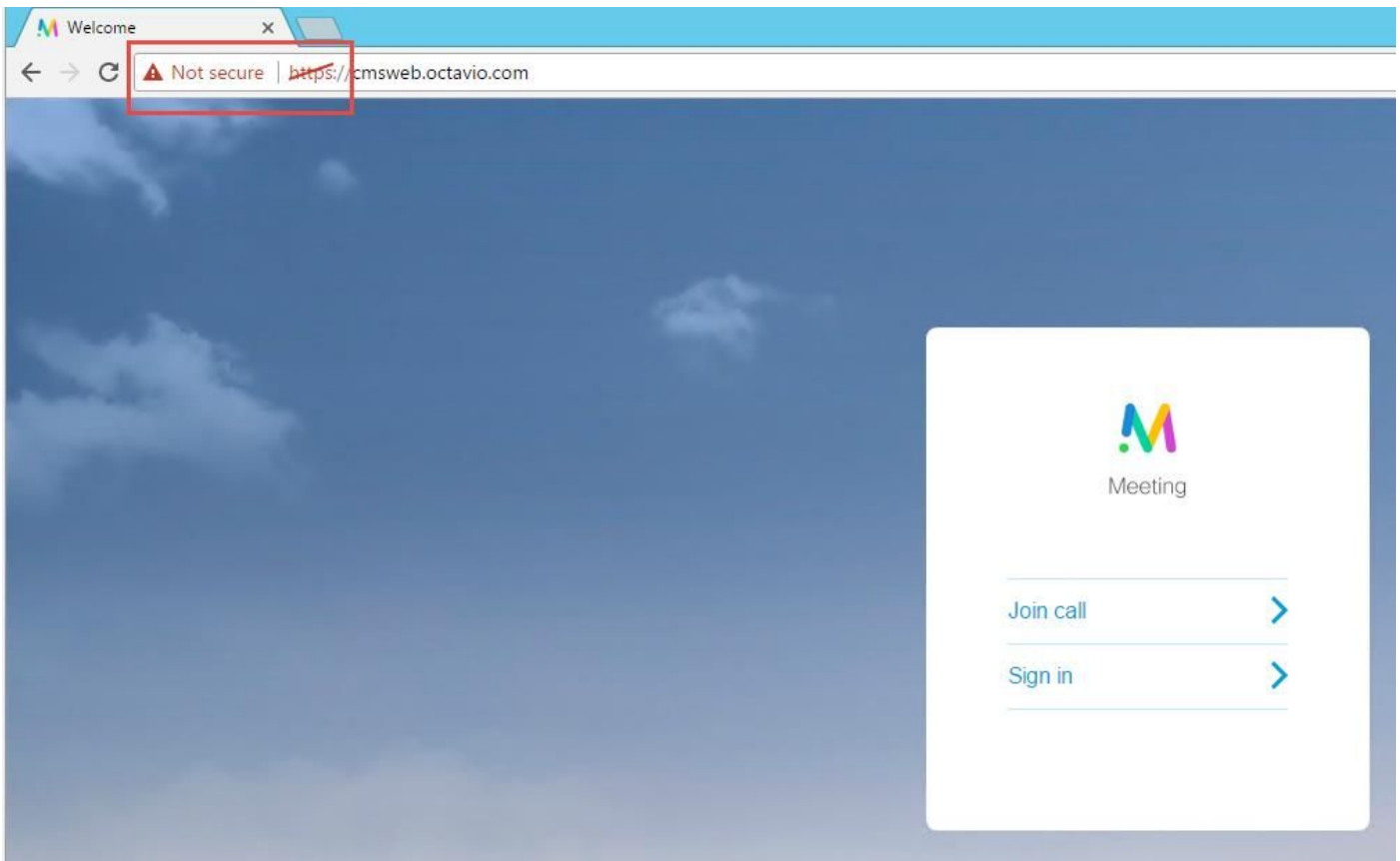
Guest account client URI

\* cmsweb.cms.octavio.local  ⓘ

Guest account client URI resolved to the following targets

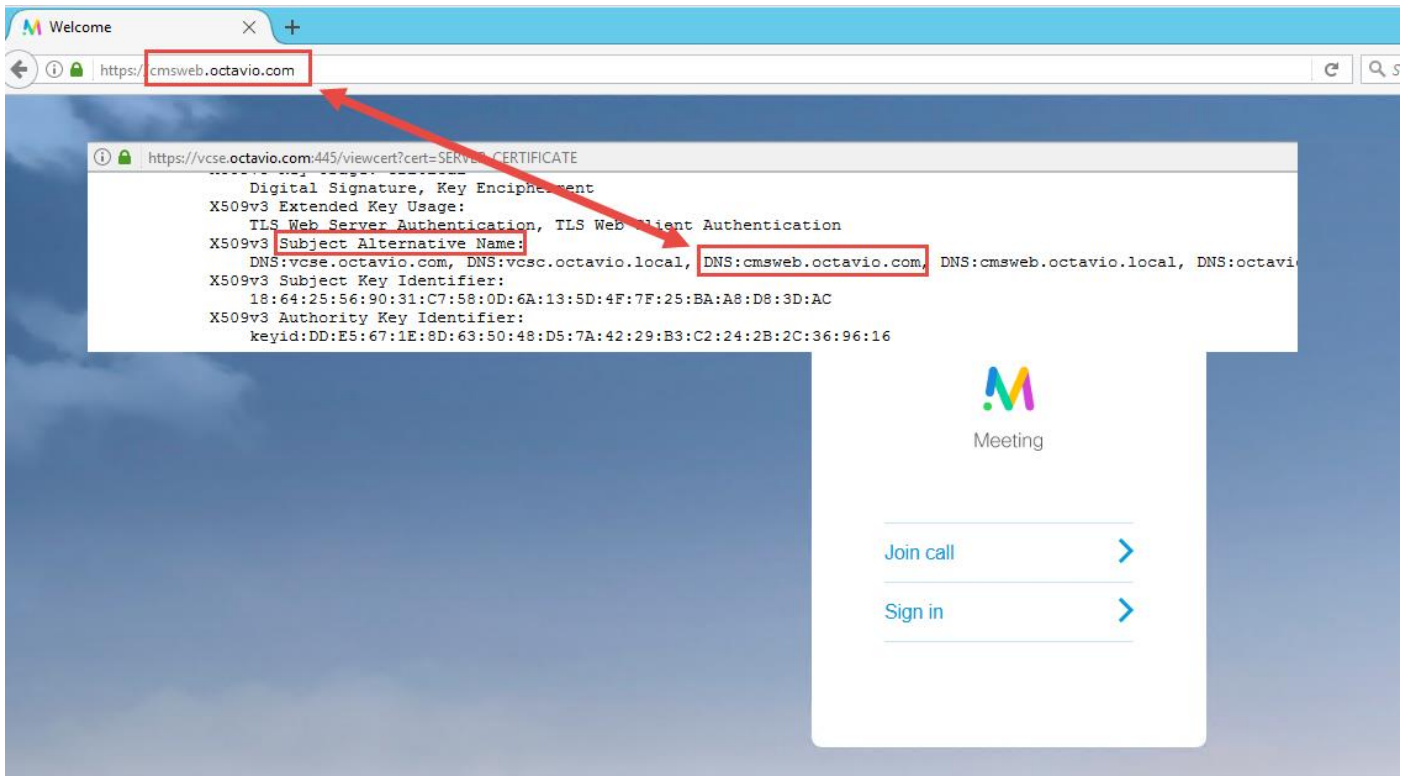
Name	Address
cmsweb.cms.octavio.local	172.16.85.180

## WebexRTC-client toont onveilige verbinding

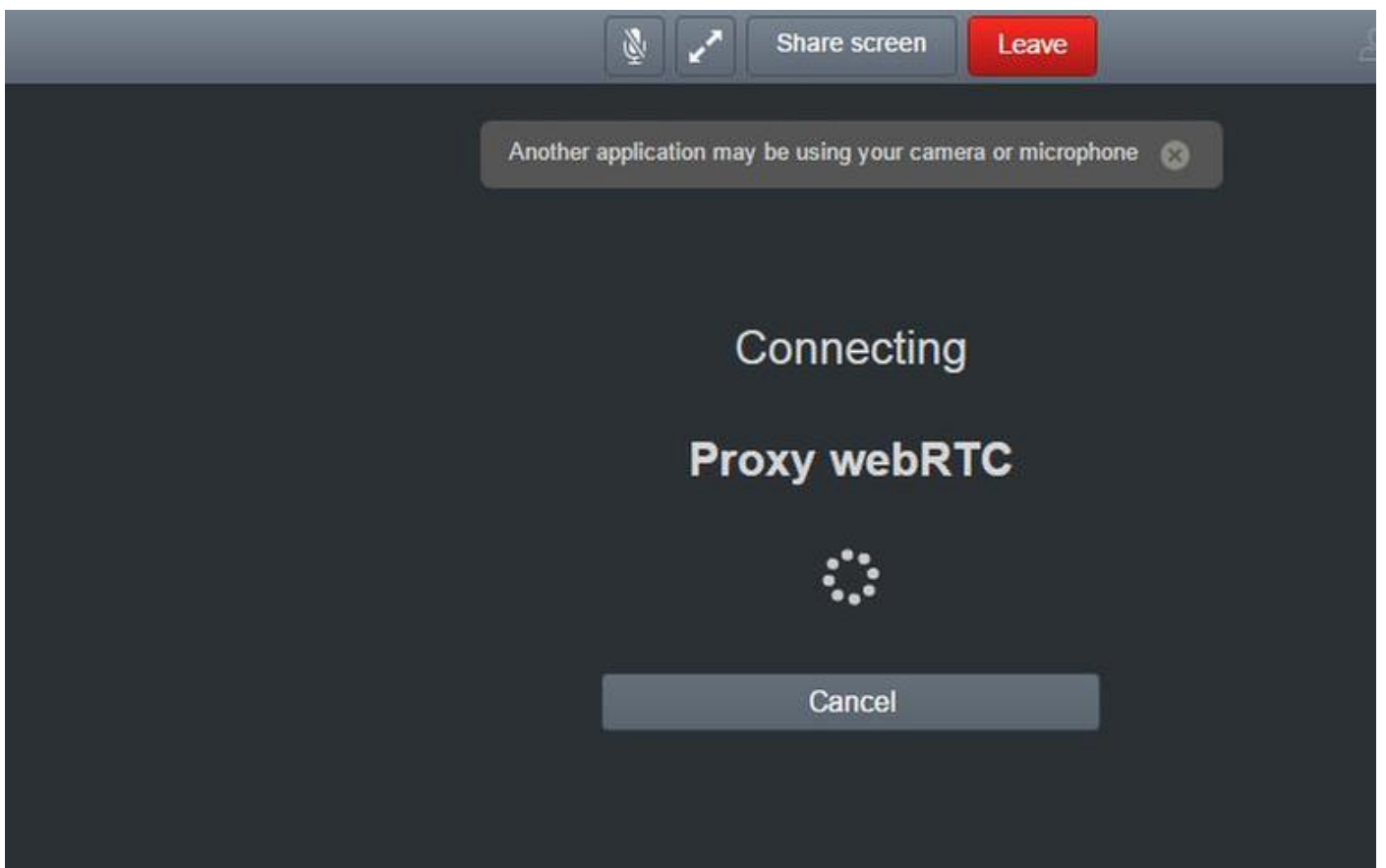


## Oplossing

- Het certificaat is zelf ondertekend en veroorzaakt dat de server de bron niet vertrouwt. Verander het certificaat van de snelweg-E in een ondersteunde certificeringsinstantie van derden.
- Controleer of de externe webbridge-URL als een SAN is toegevoegd op het expressway-E-servercertificaat zoals in de afbeelding wordt getoond.



WebexRTC-client wordt aangesloten maar nooit aangesloten en dan uitgeschakeld



De gebruikersnaam of het wachtwoord voor de TURN-server wordt onjuist ingesteld in de snelweg-E of in de CMS via API. De logboeken bevatten de fouten die in de afbeelding worden weergegeven.

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

De fout kan ook worden bevestigd met een pakketvastlegging. Draai Wireshark op de PC waar de webRTC client draait. Nadat u het pakket hebt opgenomen, filtert u de pakketten door STUN. De fouten in de afbeelding moeten worden weergegeven.

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

De PC stuurt een Allocation-verzoek en de Expressway NAT-adresantwoorden met het "Integrity check-defect"-bericht.

### Oplossing

Om de fout te repareren, controleert u de gebruikersnaam en het wachtwoord. Ze moeten correct worden ingesteld op de TURN server parameters zoals in de afbeeldingen wordt weergegeven.

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 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.