

Konfigurieren von Proxy WebRTC mit CMS über Expressway mit dualer Domäne

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Technische Informationen](#)

[DNS-Konfiguration](#)

[Interne DNS-Konfiguration](#)

[Externe DNS-Konfiguration](#)

[Konfiguration von CMS, Callbridge, Webbridge und XMPP](#)

[TURN-Konfiguration](#)

[Expressway-C- und E-Konfiguration](#)

[Konfiguration auf Expressway-C](#)

[Konfiguration auf Expressway-E](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Schaltfläche "Beitreten" wird nicht angezeigt](#)

[WebRTC-Seite zeigt 'Ungültige Anfrage' an](#)

[WebRTC-Client zeigt unsichere Verbindung an](#)

[Der WebRTC-Client stellt eine Verbindung her, erhält aber nie eine Verbindung, hat dann eine Zeitüberschreitung und trennt die Verbindung.](#)

Einführung

In diesem Dokument wird eine Beispielkonfiguration des Proxys Web Real-Time Communication (webRTC) für Cisco Meeting Server (CMS) über Expressway mit einer anderen internen und externen Domäne beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CMS Single Combined Deployment Version 2.1.4 und höher
- Expressway C und Expressway E Version X8.9.2 und höher
- Konfiguration von Callbridge und Webbridge auf CMS
- Mobiler und Remote-Zugriff (MRA) auf dem Expressway-Paar

- Der zum Expressway-E hinzugefügte optionale TURN-Taste (Traversal Using Relay NAT)
- Externer auflösbarer Domain Name Server (DNS)-Datensatz für Webbridge-URL, für externe Domäne
- Interner auflösender DNS-Datensatz für CMS-IP-Adresse von externer zu interner Domäne
- Extensible Messaging and Presence Protocol (XMPP)-Multi-Domain, konfiguriert auf CMS, für interne und externe Domäne
- TCP-Port 443 auf Firewall aus dem öffentlichen Internet zur öffentlichen IP-Adresse des Expressway-E geöffnet
- TCP- und UDP-Port 3478 werden auf der Firewall vom öffentlichen Internet zur öffentlichen IP-Adresse des Expressway-E geöffnet
- Der UDP-Port-Bereich 24000-2999 wurde auf der Firewall für die öffentliche IP-Adresse des Expressway-E geöffnet.

Verwendete Komponenten

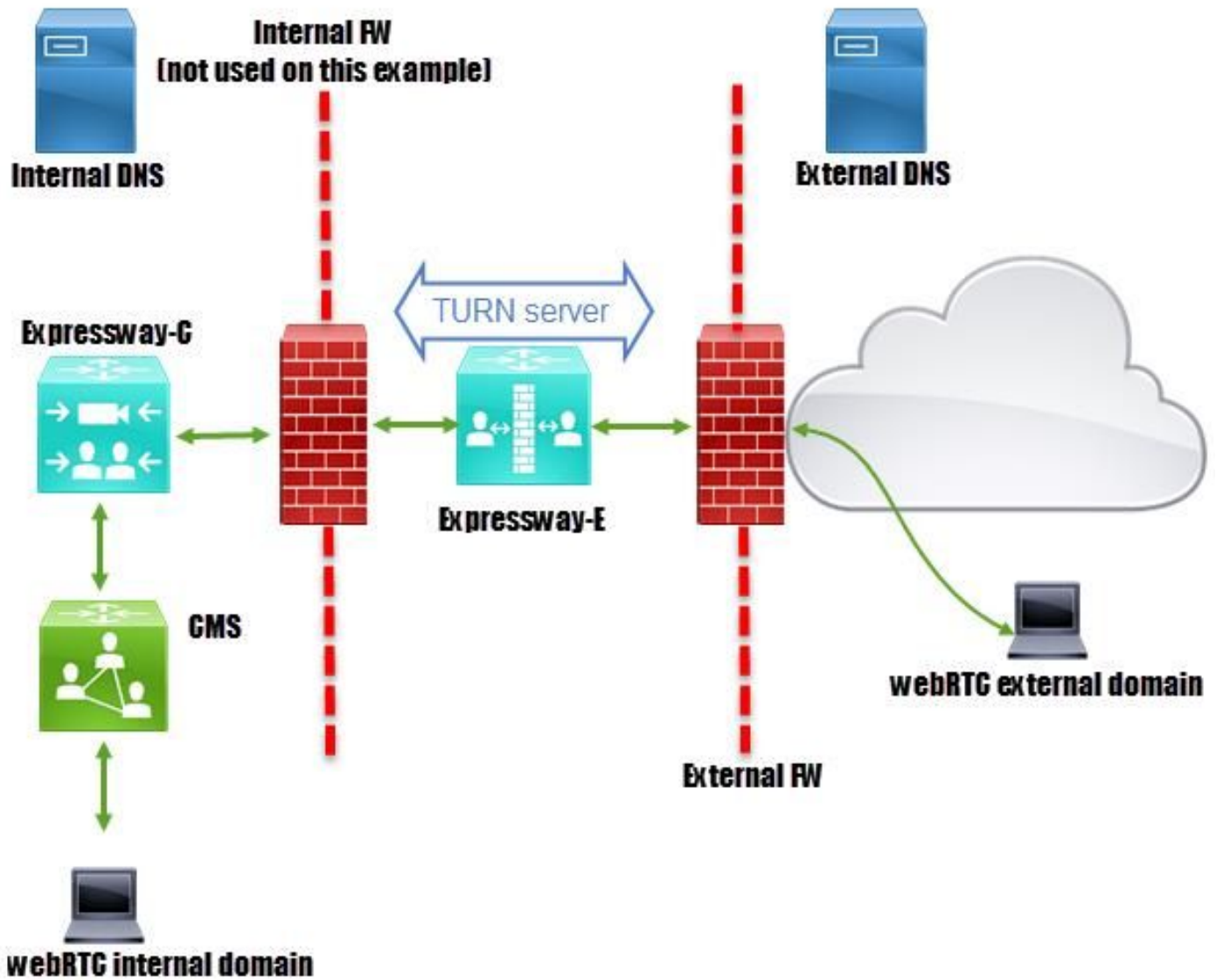
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CMS Single Combined Deployment Version 2.2.1
- Expressway-C und Expressway-E mit Dual Network Interface Card (NIC) und statischer Network Address Translation (NAT) Softwareversion X8.9.2
- Postmann

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



Technische Informationen

Interne Domäne	cms.octavio.local
Externe Domäne	Octavio.com
CMS-IP-Adresse	172,16,85,180
Expressway-C-IP-Adresse	172,16,85,167
Expressway-E LAN1 IP-Adresse (intern)	172,16,85,168
Expressway-E LAN2-IP-Adresse (extern)	192.168.245,61
Statische NAT-IP-Adresse	10.88.246.156

DNS-Konfiguration

Interne DNS-Konfiguration

Name	Type	Data	Timestamp
octavio.com	Service Location (SRV)	[10][10][5222] xmpp.cms.octavio.local.	static
octavio.com	Service Location (SRV)	[10][10][5209] xmpp.cms.octavio.local.	static
octavio.com	Service Location (SRV)	[10][10][8443] ocucmp.octavio.local.	static
octavio.com	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

Externe DNS-Konfiguration

Der externe DNS muss über die Webbridge-URL verfügen, die wie im Bild gezeigt zur statischen NAT-IP-Adresse des Expressway-E aufgelöst wird.

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

Konfiguration von CMS, Callbridge, Webbridge und XMPP

Schritt 1: Sie müssen die Callbridge-Lizenz aktivieren lassen. Das Bild zeigt eine aktive Callbridge-Lizenz.

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

Weitere Lizenzinformationen:

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

Schritt 2: Aktivieren Sie Callbridge, Webbridge und XMPP über MMP, wie im Bild gezeigt.

```
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
```

Unter diesem Link finden Sie weitere Informationen zur Aktivierung:

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

Unter diesem Link finden Sie weitere Informationen zum Erstellen eines Zertifikats:

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

Schritt 3: Navigieren Sie zur CMS-Webseite unter **Konfiguration > Allgemein**, und konfigurieren Sie die interne und externe URL für die Webbridge, wie im Bild gezeigt.

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

Hinweis: Das CMS muss mit mindestens einem Leerzeichen konfiguriert werden.

Ein Beispiel für ein konfiguriertes Leerzeichen auf dem CMS, wie im Bild gezeigt.

<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

Hinweis: Die eingehenden Anrufe müssen für die internen und externen Domänen konfiguriert werden.

Ein Beispiel für konfigurierte Domänen für die Verarbeitung eingehender Anrufe ist im Bild dargestellt.

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-Konfiguration

Schritt 1: TURN muss über die API von Postman konfiguriert werden. Dieser Befehl wird in der gesamten Konfiguration verwendet.

<https://>

Schritt 2: Verwenden Sie die POST-Methode, und navigieren Sie zum **Body**, um entweder die TURN-Serverparameter anzuzeigen oder sie zu bearbeiten. Die Parameter, die für den TURN-Server konfiguriert sind, sind im Bild dargestellt.

POST ▼ https://admin.cms.octavio.local:445/api/v1/turnServers Params

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

form-data x-www-form-urlencoded raw binary

<input checked="" type="checkbox"/>	serverAddress	172.16.85.168
<input checked="" type="checkbox"/>	clientAddress	10.88.246.156
<input checked="" type="checkbox"/>	username	turnuser
<input checked="" type="checkbox"/>	password	cisco
<input checked="" type="checkbox"/>	type	standard
<input checked="" type="checkbox"/>	tcpPortNumberOverride	3478

key value

Exp-E LAN1 IP address

Static NAT IP address

This username and password has to be configured on Expressway E

Schritt 3: Überprüfen Sie den Status der TURN-Serverkonfiguration, indem Sie die GET-Methode ausführen und die Server-ID kopieren. Die zu kopierende ID ist im Bild dargestellt.

GET ▼ https://admin.cms.octavio.local:445/api/v1/turnServers P

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

Type Basic Auth ▼

Username admin

Password *****

The authorization header will be generated and added as a custom header

Save helper data to request

Show Password

Body Cookies Headers (10) Tests

Pretty Raw Preview XML ▼

```
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>
```

Schritt 4: Kopieren Sie die ID am Ende des API-Befehls, und verwenden Sie die GET-Methode, um die TURN-Serverinformationen wie im Bild dargestellt anzuzeigen.

Hinweis: Die Informationen zeigen das Kennwort des Servers nicht an.

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 in red).
- Authorization:** Basic Auth
- Username:** admin
- Password:** (masked with dots)
- Body Tab:** Shows the 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>
```

Schritt 5: Klicken Sie auf **Senden**, um den Serverstatus abzurufen. Ein Beispiel für eine erfolgreiche Konfiguration wie im Bild gezeigt.

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>
```

Expressway-C- und E-Konfiguration

Schritt 1: Auf der Autobahn-C muss die interne Domäne (octavio.local) und auf der Expressway-E die externe Domäne (octavio.com) konfiguriert sein, wie im Bild gezeigt.



DNS

DNS settings

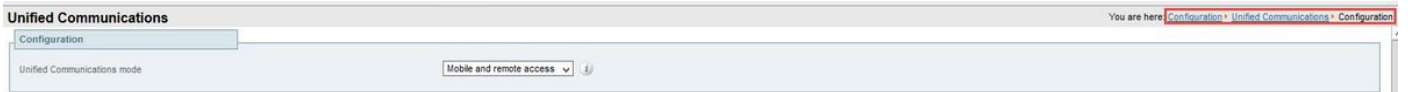
System host name	<input type="text" value="vcsc"/>	
Domain name	<input type="text" value="octavio.local"/>	
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>	

Default DNS servers

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

Internal DNS server

Schritt 2: MRA muss auf Expressway C und E aktiviert werden, wie im Bild gezeigt.



Schritt 3: Erstellen Sie eine Unified Communication Traversal-Zone zwischen Expressway-C und E, wie im Bild gezeigt.



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

Konfiguration auf Expressway-C

Schritt 1: Konfigurieren Sie die interne und externe Domäne auf dem Expressway-C wie im Bild gezeigt.



Status System **Configuration** Applicat

Domains

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

Schritt 2: Aktivieren Sie die Cisco Meeting-Konfiguration. Navigieren Sie zu **Konfiguration > Unified Communications > Cisco Meeting Server**. Konfigurieren Sie die externe Webbridge-URL im URI-Feld des Gastkonto-Clients wie im Bild gezeigt.

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

Hinweis: Der interne DNS sollte die externe Webbridge-URL (cmsweb.octavio.com) zur internen CMS-Webbridge-IP-Adresse auflösen. In diesem Beispiel lautet die IP-Adresse 172.16.85.180.

Die Secure Shell (SSH)-Tunnel auf dem Expressway-C müssen nach einigen Sekunden aktiv werden, wie im Bild gezeigt.

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

Hinweis: Der Server muss über ein Serverzertifikat und ein Zertifizierungsstellenzertifikat verfügen.

Konfiguration auf Expressway-E

Schritt 1: Die Autobahn E muss eine TURN-Lizenz besitzen, wie im Bild gezeigt.




Cisco Expressway-E

Status System Configuration Applications Users **Maintenance**

Option keys

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

Schritt 2: Der Expressway-E muss mit der externen Domäne konfiguriert werden, wie im Bild gezeigt.



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

Schritt 3: Erstellen Sie Benutzer für den TURN-Server und für die Unified Communication Traversal-Zone wie im Bild gezeigt.



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

Schritt 4: Erstellen Sie eine Unified Communication Traversal-Zone wie im Bild gezeigt.



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 ⓘ

Schritt 5: Konfigurieren Sie den TURN-Server. Navigieren Sie zu **Configuration > Traversal > TURN** (Konfiguration > Traversal > TURN), wie im Bild gezeigt.

Hinweis: Die TURN-Anfrage muss an den Port 3478 gesendet werden, da dieser der Port ist, an dem der Web-Client die TURN-Verbindung anfordert.

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

Sobald die Option "Turn" (Einschalten) aktiviert ist, wird der Status wie im Bild gezeigt "Active" (Aktiv) angezeigt.

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

Schritt 6: Navigieren Sie zu **System > Administration (System > Verwaltung)**. Der webRTC-Client fordert Zugriff auf Port 443 an. Aus diesem Grund muss der Administrations-Port des Expressway-E auf einen anderen Port geändert werden, in diesem Fall wird er auf 445 geändert, wie im Bild gezeigt.

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*

Schritt 7: Zertifikatserstellung für Expressway-E: Die Webbridge-URL muss dem Serverzertifikat als SAN hinzugefügt werden, wie im Bild gezeigt.

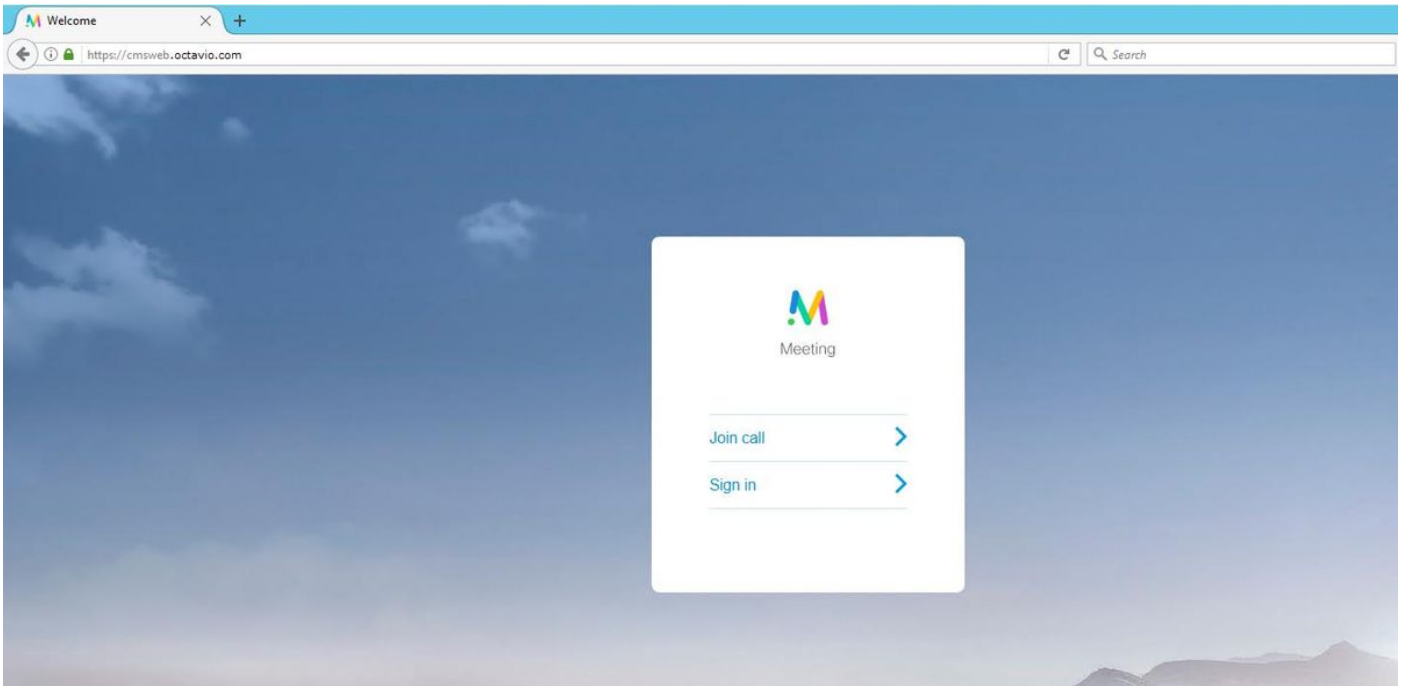
X509v3 Subject Alternative Name:
 DNS:vcse.octavio.com, DNS:vcsc.octavio.local, DNS:cmsweb.octavio.com, DNS:cmsweb.octavio.local, DNS:octavio.local, DNS:cms.octavio.local, DNS:octavio.com

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.


Schritt 1: Wählen Sie einen unterstützten Webbrowser aus, und geben Sie die externe Webbridge-URL ein. Sie müssen den nächsten Bildschirm sehen, wie im Bild gezeigt.

Hinweis: Eine Liste der unterstützten Browser und Versionen finden Sie unter:
<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>



Schritt 2: Wählen Sie **Anruf beitreten aus**, und geben Sie die zuvor konfigurierte Leerzeichen-ID ein, wie im Bild gezeigt.

Enter Call ID


Meeting

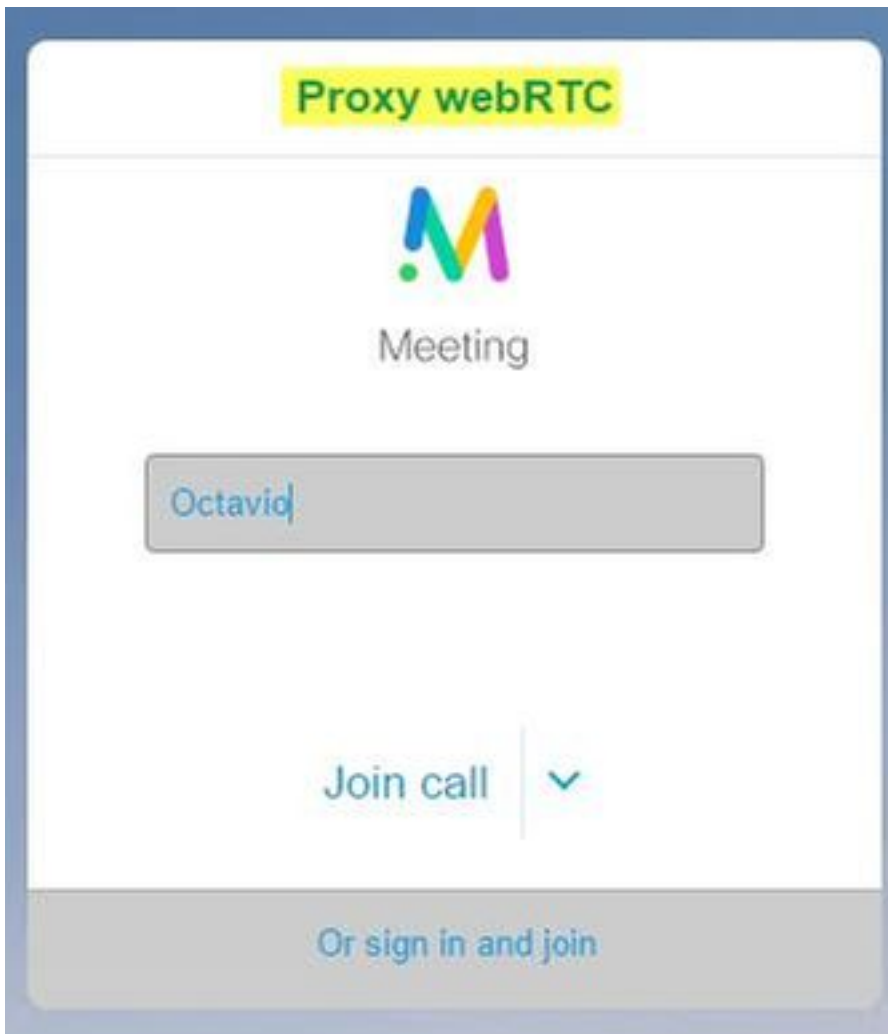
100101

Passcode (if required)

Continue >

Back

Schritt 3: Klicken Sie auf **Weiter**, und geben Sie Ihren Namen ein. An diesem Punkt müssen Sie den Namen des Speicherplatzes sehen, dem Sie beitreten werden. In diesem Fall ist der Platzname Proxy webRTC. Klicken Sie auf **Anruf beitreten** wie im Bild gezeigt.



Schritt 4: Werden Sie mit einem anderen Gerät verbunden, müssen Sie beide Geräte in der Konferenz sehen, wie im Bild gezeigt.

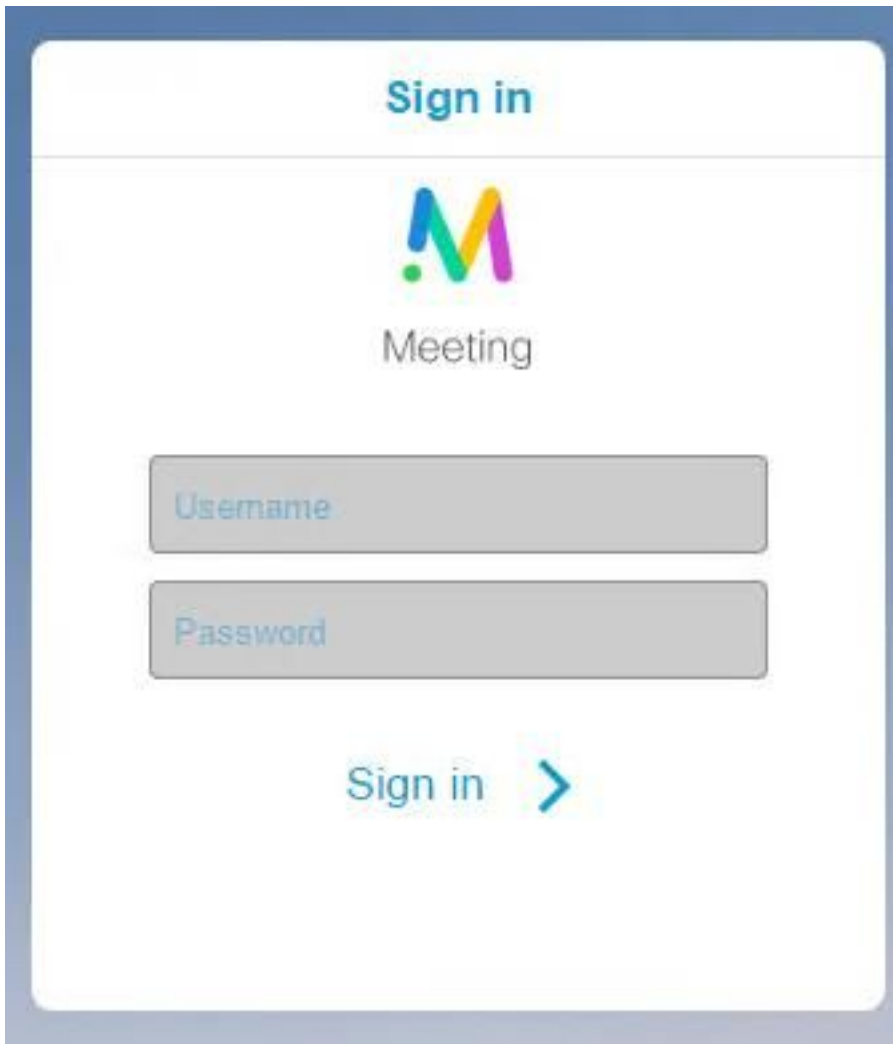


Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Schaltfläche "Beitreten" wird nicht angezeigt

Die Schaltfläche **Anruf verbinden** wird beim Öffnen der Webbridge-Seite nicht angezeigt. Der Fehler im zweiten Bild wird angezeigt, wenn Sie zur CMS-Webseite gelangen, wie im Bild gezeigt.



Fault conditions

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

Das Problem tritt auf, wenn die Webbridge nicht richtig mit der Anrufbrücke kommuniziert.

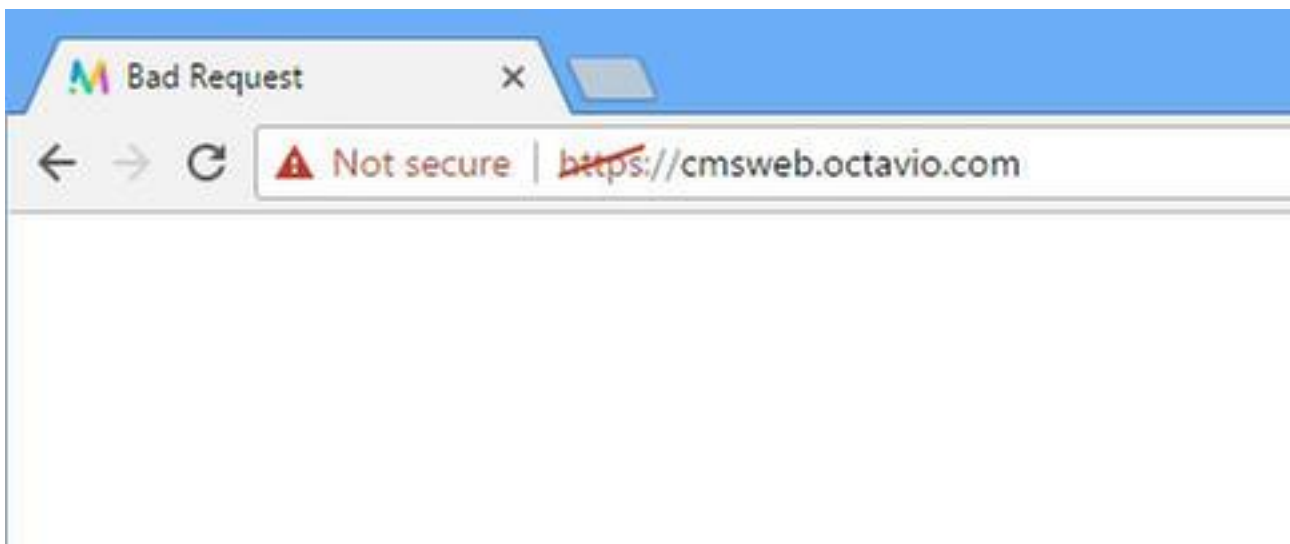
Lösung

- Überprüfen Sie, ob die Webbridge-URL auf der CMS-Admin-Webseite richtig konfiguriert ist. Navigieren Sie zu **Konfiguration > Allgemein**.
- Die Webbridge und die Callbridge müssen sich gegenseitig vertrauen. Überprüfen Sie, ob das Vertrauenspaket der Webbridge-Konfiguration hinzugefügt wird, wie in den Bildern gezeigt:

```
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>
```

Hinweis: Das Vertrauensbündel ist das Anruf-Bridge-Zertifikat.

WebRTC-Seite zeigt 'Ungültige Anfrage' an



Lösung

- Überprüfen Sie, ob der richtige Client-URI für das Gastkonto auf Expressway-C konfiguriert ist. Navigieren Sie zu **Konfiguration > Unified Communication > Cisco Meeting Server**.

Wenn die interne URL in der Client-URL des Gastkontos konfiguriert ist, wird sie vom Expressway-C aufgelöst, da auf dem DNS-Server ein Datensatz erstellt wurde. Dies kann jedoch die Fehlermeldung "bad request" im Webbrowser auslösen. In diesem Beispiel wird die interne URL so konfiguriert, dass der Fehler wie im Bild dargestellt angezeigt wird.

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

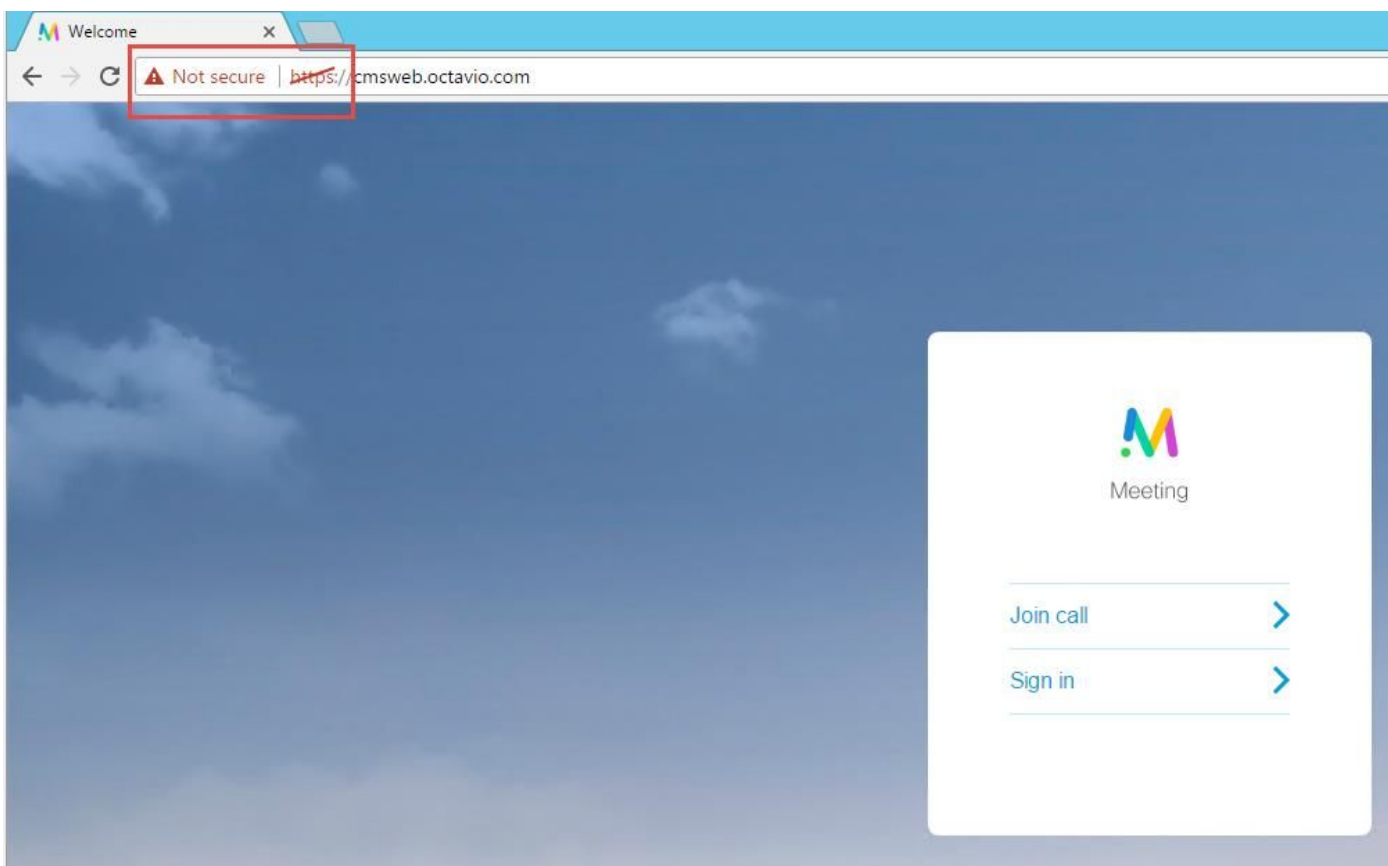
Guest account client URI

* cmsweb.cms.octavio.local **X**

Guest account client URI resolved to the following targets

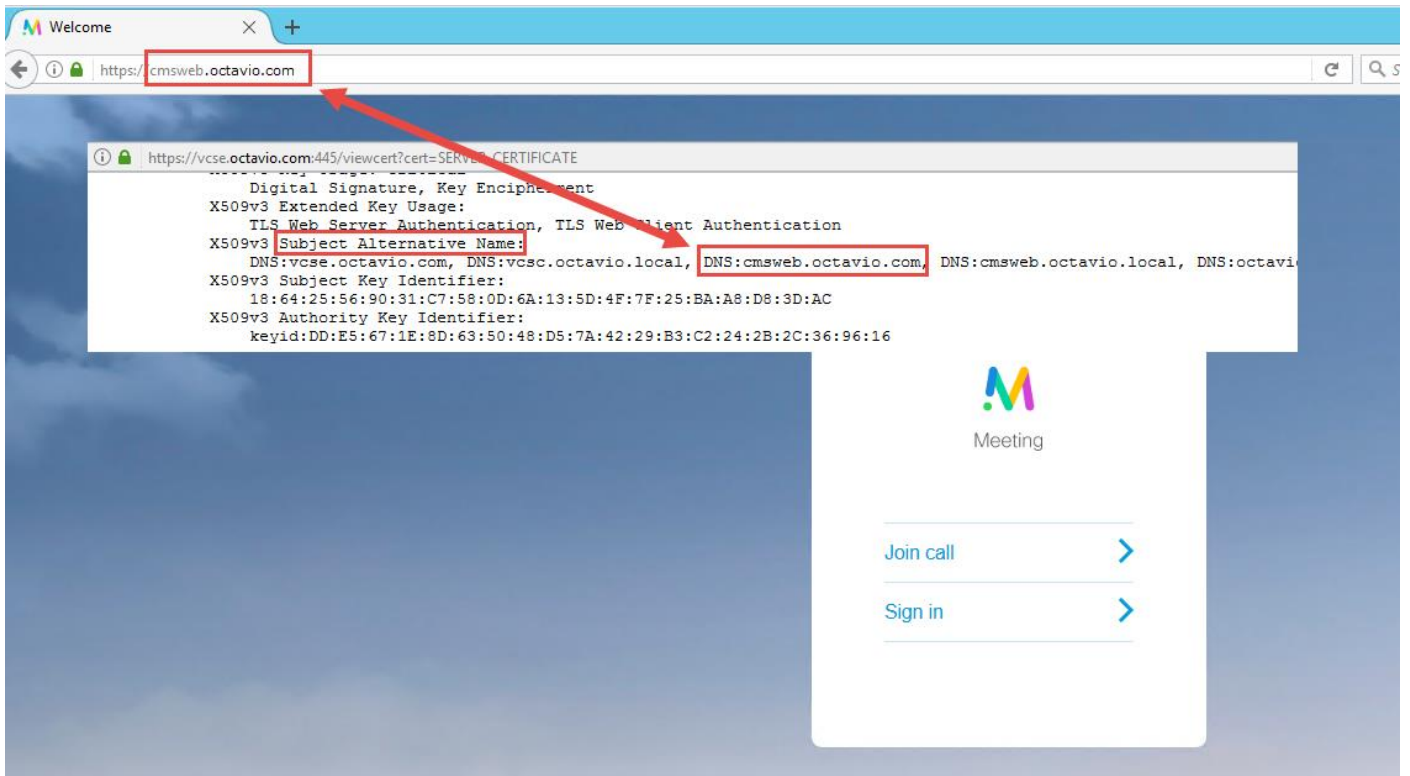
Name	Address
cmsweb.cms.octavio.local	172.16.85.180

WebRTC-Client zeigt unsichere Verbindung an

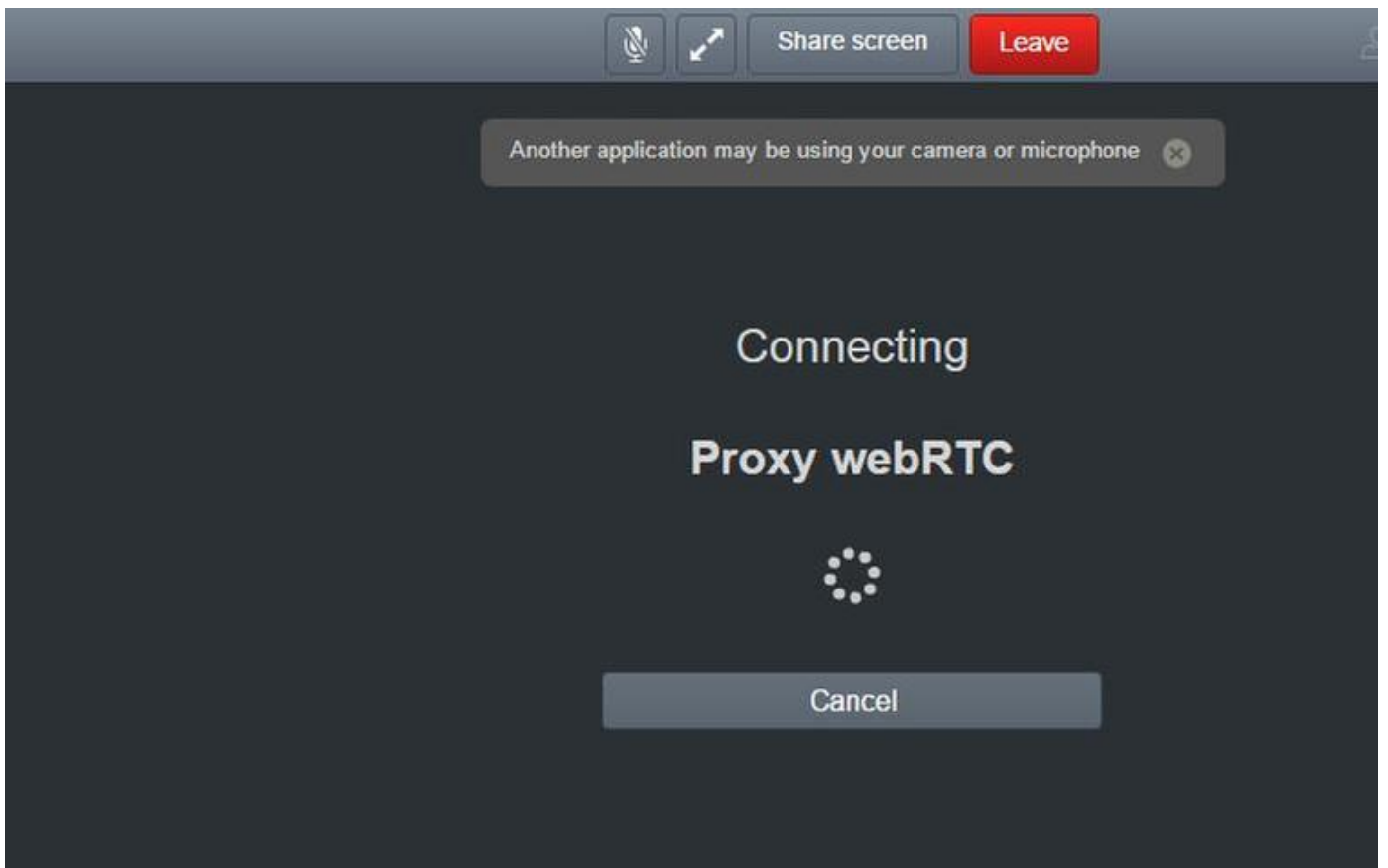


Lösung

- Das Zertifikat ist selbstsigniert, wodurch der Server der Quelle nicht vertraut. Ändern Sie das Zertifikat auf dem Expressway-E in eine unterstützte Zertifizierungsstelle eines Drittanbieters.
- Überprüfen Sie, ob die externe Webbridge-URL als SAN auf dem Expressway-E-Serverzertifikat hinzugefügt wird, wie im Bild gezeigt.



Der WebRTC-Client stellt eine Verbindung her, erhält aber nie eine Verbindung, hat dann eine Zeitüberschreitung und trennt die Verbindung.



Der TURN-Server-Benutzername oder das -Kennwort sind auf der Schnellstraße E oder im CMS über API falsch konfiguriert. Die Protokolle enthalten die im Bild angezeigten Fehler.

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

Der Fehler kann auch durch eine Paketerfassung bestätigt werden. Führen Sie Wireshark auf dem PC aus, auf dem der webRTC-Client ausgeführt wird. Sobald Sie über die Paketerfassung verfügen, filtern Sie die Pakete nach STUN. Sie müssen die im Bild angezeigten Fehler sehen.

1458	2017-05-20 19:52:48.704889	172.16.84.124	10.88.246.156	STUN	182	0x1e4a (7754)	Default	Allocate Request UDP user: turnuser realm: turnuser with nonce
1462	2017-05-20 19:52:48.714894	10.88.246.156	172.16.84.124	STUN	262	0x08abc (2748)	Default	Allocate Error Response user: turnuser with nonce realm: turnuser error-code: 431 ("Unknown error code") Integrity Check Failure

Der PC sendet eine Allocation-Anforderung und die Expresssway NAT-Adresse antwortet mit der Meldung 'Integrity Check failure' (Fehler bei Integritätsprüfung).

Lösung

Um den Fehler zu beheben, überprüfen Sie den Benutzernamen und das Kennwort. Sie müssen auf den TURN-Serverparametern korrekt konfiguriert sein, wie in den Bildern gezeigt.

The image shows a REST client interface for 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

Below the request, the Cisco Expressway-E configuration page for the local authentication database is shown. The configuration includes:

- Name**: turnuser
- Password**: [Redacted]