

Configurazione di Proxy WebRTC con CMS over Expressway con Dual Domain

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Informazioni tecniche](#)

[Configurazione DNS](#)

[Configurazione DNS interno](#)

[Configurazione DNS esterno](#)

[Configurazione CMS, Callbridge, Webbridge e XMPP](#)

[Configurazione TURN](#)

[Configurazione Expressway-C ed E](#)

[Configurazione su Expressway-C](#)

[Configurazione su Expressway-E](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Il pulsante Partecipa alla chiamata non è visualizzato](#)

[Pagina WebRTC con 'Richiesta non valida'](#)

[Il client WebRTC mostra una connessione non protetta](#)

[Il client WebRTC si connette ma non si connette mai, quindi si interrompe e si disconnette](#)

Introduzione

In questo documento viene descritto un esempio di configurazione del proxy Web Real-Time Communication (webRTC) per Cisco Meeting Server (CMS) tramite Expressway con dominio interno ed esterno diverso.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Distribuzione combinata singola CMS versione 2.1.4 e successive
- Expressway C e Expressway E versione X8.9.2 e successive
- Callbridge e webbridge configurati su CMS
- MRA (Mobile and Remote Access) abilitato sulla coppia Expressway
- Traversal Using Relay NAT (TURN) tasto di opzione aggiunto a Expressway-E

- Record DNS (Domain Name Server) risolvibile esterno per URL di webbridge, per dominio esterno
- Record DNS interno risolvibile per indirizzo IP CMS da dominio esterno a dominio interno
- Multidominio XMPP (Extensible Messaging and Presence Protocol) configurato su CMS, per dominio interno ed esterno
- La porta TCP 443 è stata aperta sul firewall da Internet pubblica all'indirizzo IP pubblico di Expressway-E
- Le porte TCP e UDP 3478 vengono aperte sul firewall da Internet pubblica all'indirizzo IP pubblico di Expressway-E
- Intervallo porte UDP 2400-2999 aperto sul firewall da e per l'indirizzo IP pubblico di Expressway-E

Componenti usati

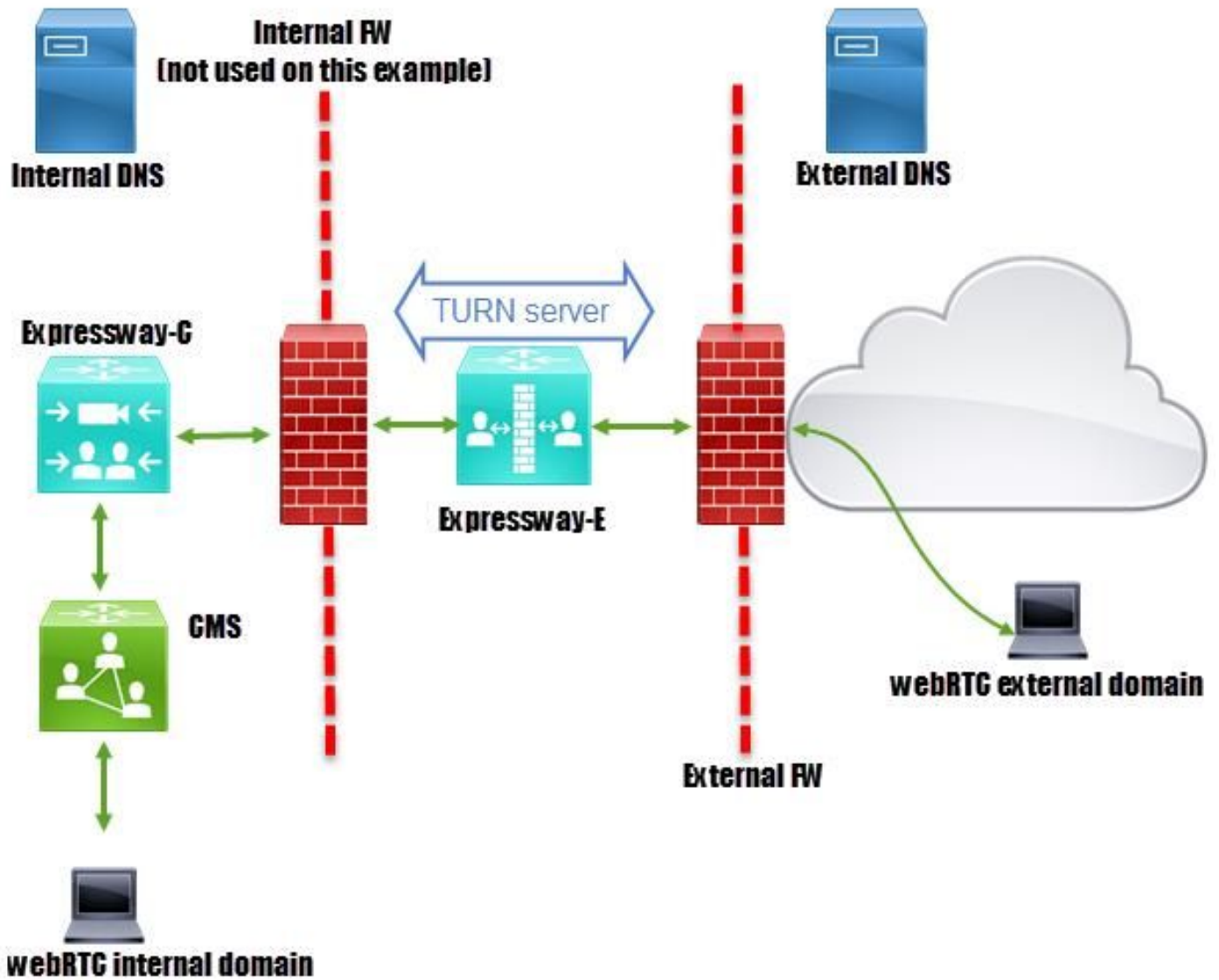
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Distribuzione combinata singola CMS versione 2.2.1
- Expressway-C e Expressway-E con software a doppia scheda di interfaccia di rete (NIC) e NAT (Network Address Translation) statico versione X8.9.2
- Postino

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Informazioni tecniche

Dominio interno	cms.octavio.local
Dominio esterno	octavio.com
Indirizzo IP CMS	172.16.85.180
Indirizzo IP Expressway-C	172.16.85.167
Indirizzo IP Expressway-E LAN1 (interno)	172.16.85.168
Indirizzo IP LAN2 Expressway-E (esterno)	192.168.245.61
Indirizzo IP NAT statico	10.88.246.156

Configurazione DNS

Configurazione DNS interno

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

Configurazione DNS esterno

Il DNS esterno deve avere l'URL webbridge che si risolve nell'indirizzo IP NAT statico di Expressway-E, come mostrato nell'immagine.

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

Configurazione CMS, Callbridge, Webbridge e XMPP

Passaggio 1. È necessario che la licenza callbridge sia attivata. Nell'immagine è illustrata una licenza callbridge attiva.

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

Per ulteriori informazioni sulle licenze:

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

Passaggio 2. Abilitare callbridge, webbridge e XMPP tramite MMP come mostrato nell'immagine.

```
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
```

Seguire questo collegamento per un processo dettagliato su come attivarli:

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

Fare clic su questo collegamento per informazioni dettagliate sulla creazione di un certificato:

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

Passaggio 3. Passare alla pagina Web CMS in **Configurazione > Generale** e configurare l'URL interno ed esterno per il webbridge come mostrato nell'immagine.

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

Nota: Il CMS deve essere configurato con almeno uno spazio.

Esempio di spazio configurato su CMS come mostrato nell'immagine.

<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

Nota: Le chiamate in ingresso devono essere configurate per i domini interni ed esterni

Un esempio di domini configurati per la gestione delle chiamate in ingresso è quello mostrato nell'immagine.

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

Configurazione TURN

Passaggio 1. TURN deve essere configurato dall'API tramite Postman. Questo comando viene

utilizzato in tutta la configurazione.

<https://>

Passaggio 2. Utilizzare il metodo POST e passare a **Body** per visualizzare i parametri del server TURN o modificarli. I parametri configurati per il server TURN sono quelli mostrati nell'immagine.

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

Passaggio 3. Controllare lo stato della configurazione del server TURN eseguendo il metodo GET e copiando l'ID del server. L'ID che deve essere copiato è come mostrato nell'immagine.

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

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>
```

Passaggio 4. Copiare l'ID alla fine del comando API e utilizzare il metodo GET per visualizzare le informazioni sul server TURN come mostrato nell'immagine.

Nota: Le informazioni non visualizzeranno la password del server.

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>
```

Passaggio 5. Fare clic su **send** per ottenere lo stato del server. Esempio di configurazione riuscita come mostrato nell'immagine.

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>
```

Configurazione Expressway-C ed E

Passaggio 1. Il dominio interno di expressway-C (octavio.local) e quello esterno di Expressway-E (octavio.com) devono essere configurati come mostrato nell'immagine.



DNS

DNS settings

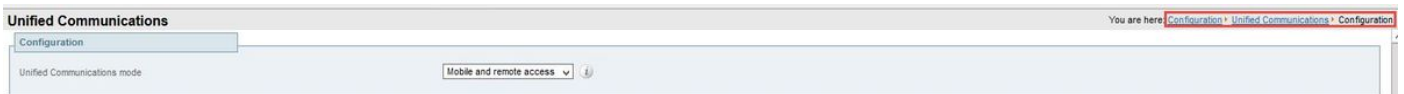
System host name	<input type="text" value="vcsc"/>	
Domain name	<input type="text" value="octavio.local"/>	
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>	

Default DNS servers

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

Internal DNS server

Passaggio 2. L'Autorità registrazione integrità deve essere abilitata sia su Expressway C che su Expressway E come illustrato nell'immagine.



Passaggio 3. Creare una zona di attraversamento comunicazioni unificate tra Expressway-C ed E come mostrato nell'immagine.



Edit zone

Configuration	
Name	<input type="text" value="UT Zone"/> <i>i</i>
Type	<input type="text" value="Unified Communications traversal"/>
Hop count	<input type="text" value="15"/> <i>i</i>

Connection credentials	
Username	<input type="text" value="Tuser"/> <i>i</i>
Password	<input type="password" value="....."/> <i>i</i>

This credentials are configured on Exp-E

SIP	
Port	<input type="text" value="7001"/> <i>i</i>
Accept proxied registrations	<input type="text" value="Allow"/> <i>i</i>
ICE support	<input type="text" value="Off"/> <i>i</i>
Multistream mode	<input type="text" value="On"/> <i>i</i>
SIP poison mode	<input type="text" value="Off"/> <i>i</i>
Preloaded SIP routes support	<input type="text" value="Off"/> <i>i</i>
SIP parameter preservation	<input type="text" value="Off"/> <i>i</i>

Authentication	
Authentication policy	<input type="text" value="Do not check credentials"/> <i>i</i>

Configurazione su Expressway-C

Passaggio 1. Configurare il dominio interno ed esterno su Expressway-C come mostrato nell'immagine.



Status System **Configuration** Applicat

Domains

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

Passaggio 2. Abilitare la configurazione della riunione Cisco. Selezionare **Configurazione > Unified Communications > Cisco Meeting Server**. Configurare l'URL del webbridge esterno nel campo URI client account Guest come illustrato nell'immagine.



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

Nota: Il DNS interno deve risolvere l'URL del webbridge esterno (cmsweb.octavio.com) nell'indirizzo IP del webbridge CMS interno. Nell'esempio, il valore IP è 172.16.85.180.

I tunnel Secure Shell (SSH) su Expressway-C devono diventare attivi dopo alcuni secondi, come mostrato nell'immagine.



Status System Configuration Applications Users Maintenance

Unified Communications SSH tunnels status

You are here: Status > Unified Communications

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

Nota: il server deve disporre di un certificato server e di un certificato CA.

Configurazione su Expressway-E

Passaggio 1. L'expressway-E deve avere una licenza TURN come mostrato nell'immagine.

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

Passaggio 2. Expressway-E deve essere configurato con il dominio esterno come mostrato nell'immagine.

Status **System** Configuration Applications Users Maintenance

DNS

DNS settings

System host name ⓘ

Domain name ⓘ

Default DNS servers

Address 1 ⓘ

Address 2 ⓘ

External DNS server

Passaggio 3. Creare gli utenti per il server TURN e per la zona trasversale Unified Communications, come mostrato nell'immagine.



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

Passaggio 4. Creare una zona di attraversamento comunicazioni unificate come mostrato nell'immagine.



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 ⓘ

Passaggio 5. Configurare il server TURN. Passare a **Configurazione > Attraversamento > TORNITURA** come mostrato nell'immagine.

Nota: La richiesta TURN deve essere indirizzata alla porta 3478 in quanto si tratta della

porta su cui il client Web richiede la connessione TURN.



Cisco Expressway-E

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

Una volta che l'Attivazione è attiva, lo stato mostra Attivo come mostrato nell'immagine.

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

Passaggio 6. Passare a **Sistema > Amministrazione**. Il client webRTC richiede l'accesso alla porta 443. Per questo motivo, la porta di amministrazione di Expressway-E deve essere modificata in una diversa, in questo caso esempio viene modificata in 445 come mostrato nell'immagine.

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*

Passaggio 7. Creazione del certificato per Expressway-E: l'URL di webbridge deve essere aggiunto come SAN nel certificato del server come mostrato nell'immagine.

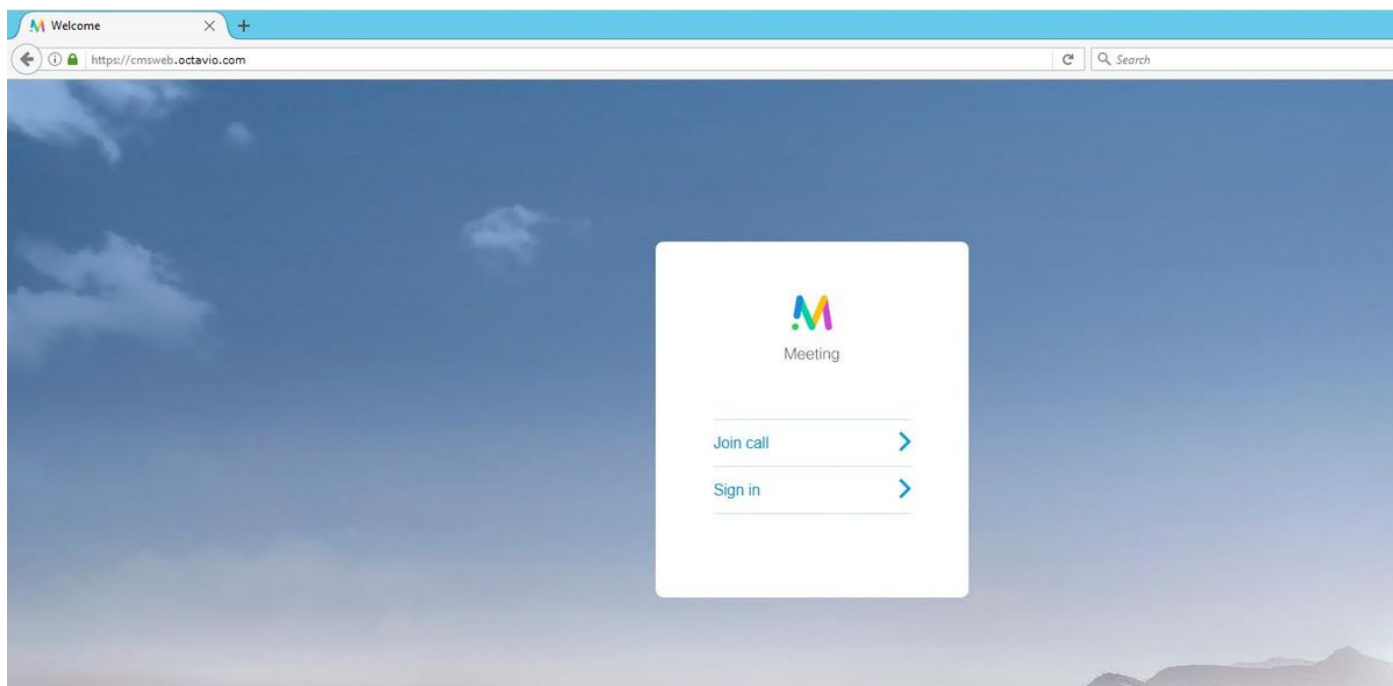
X509v3 Subject Alternative Name:
DNS:vcse.octavio.com, DNS:vcse.octavio.local, DNS:cmsweb.octavio.com, DNS:cmsweb.octavio.local, DNS:octavio.local, DNS:cms.octavio.local, DNS:octavio.com

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.


Passaggio 1. Selezionare un browser Web supportato e immettere l'URL del webbridge esterno. È necessario visualizzare la schermata successiva come illustrato nell'immagine.

Nota: L'elenco dei browser e delle versioni supportati è disponibile sul collegamento: <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>



Passaggio 2. Selezionare **Unisci chiamata** e immettere l'ID spazio precedentemente configurato come mostrato nell'immagine.

Enter Call ID


Meeting

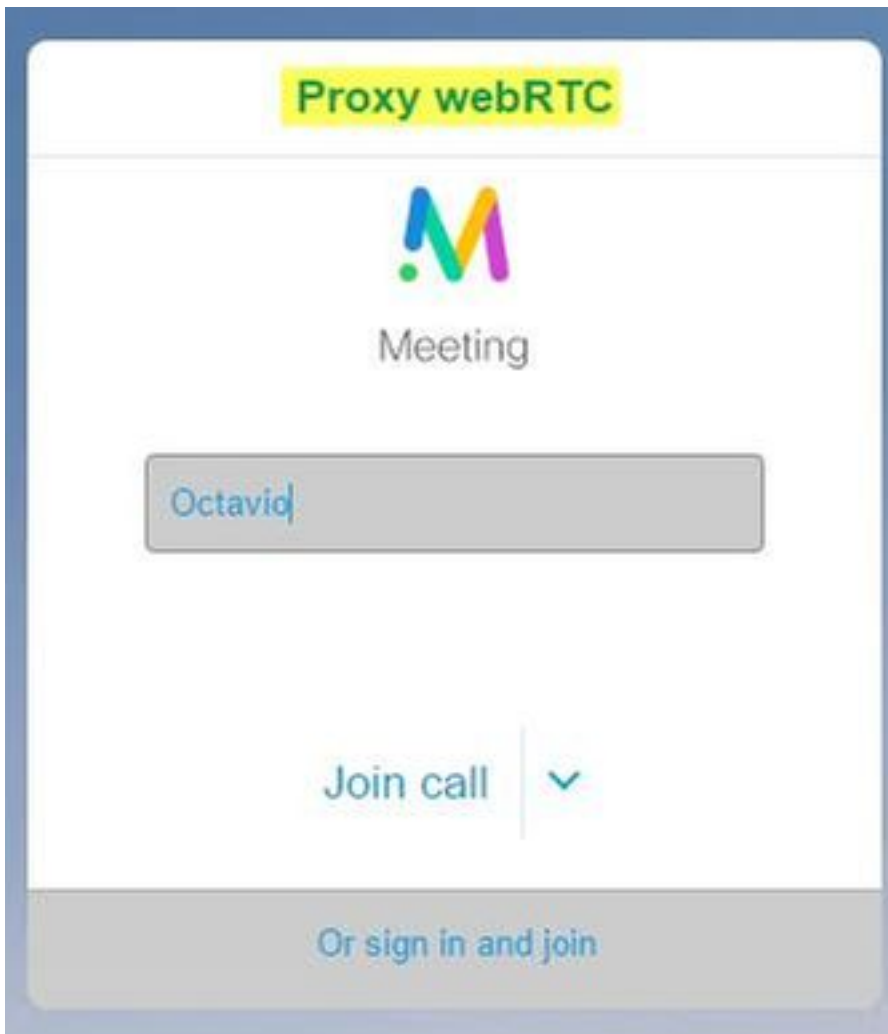
100101

Passcode (if required)

Continue >

Back

Passaggio 3. Fare clic su **Continua** e immettere il proprio nome. A questo punto è necessario visualizzare il nome dello spazio a cui si intende partecipare, in questo caso il nome dello spazio è Proxy webRTC. Fare clic su **Partecipa alla chiamata** come mostrato nell'immagine.



Passaggio 4. Unirsi a un altro dispositivo e visualizzare entrambi i dispositivi collegati nella conferenza come mostrato nell'immagine.

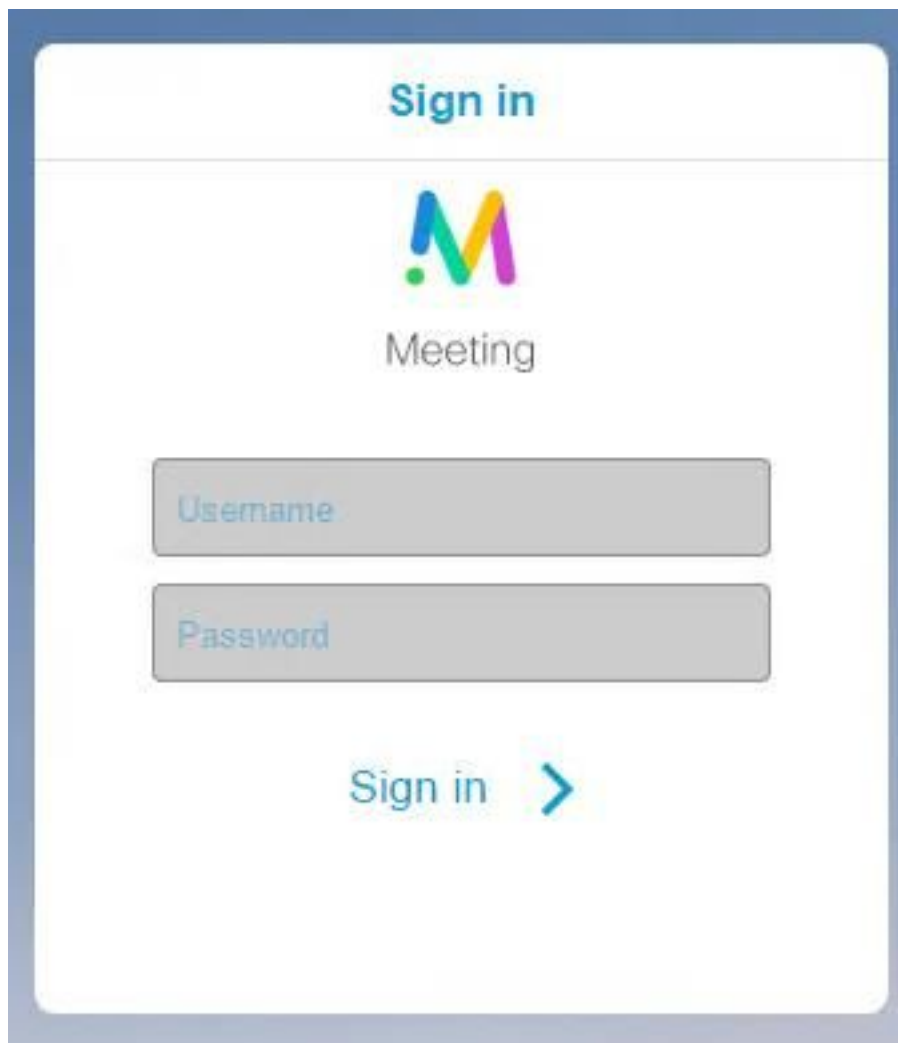


Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Il pulsante **Partecipa alla chiamata** non è visualizzato

Il pulsante **Partecipa alla chiamata** non viene visualizzato quando si apre la pagina di webbridge e viene visualizzato l'errore mostrato nella seconda immagine quando si accede alla pagina Web CMS come mostrato nell'immagine.



Fault conditions

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

Il problema si verifica quando il bridge Web non comunica correttamente con il bridge di chiamate.

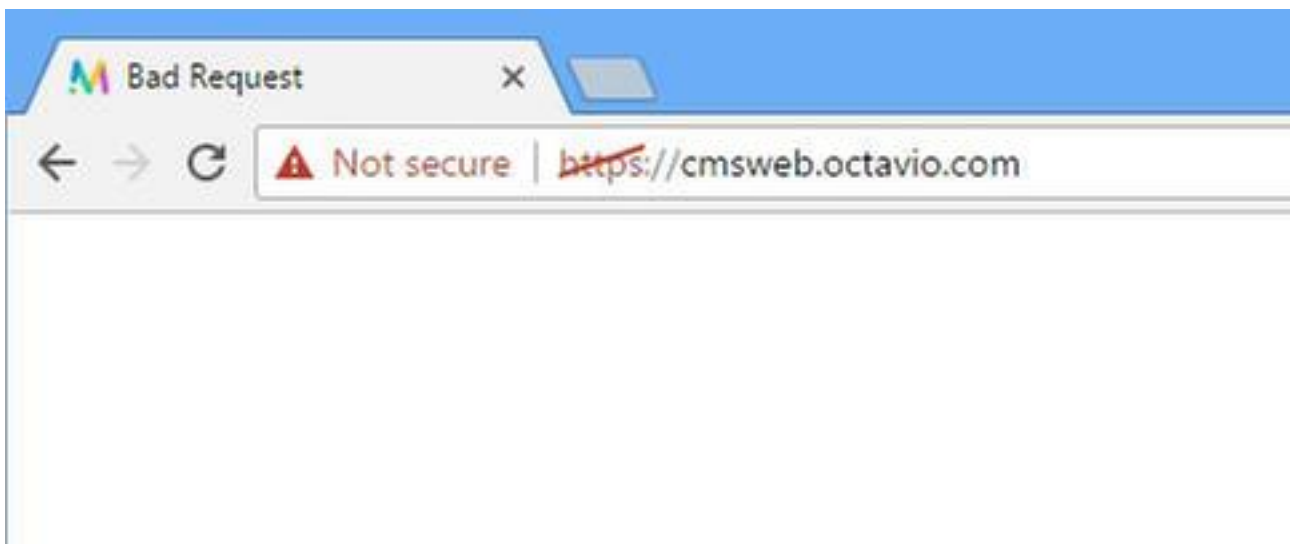
Soluzione

- Verificare che l'URL di webbridge sia configurato correttamente nella pagina Web CMS admin. A questo scopo, selezionare **Configurazione > Generale**.
- Il webbridge e il callbridge devono considerarsi reciprocamente attendibili. Verificare che il trust bundle sia stato aggiunto alla configurazione del webbridge come mostrato nelle immagini:

```
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>
```

Nota: Il trust bundle è il certificato del bridge di chiamate.

Pagina WebRTC con 'Richiesta non valida'



Soluzione

- Verificare che l'URI del client dell'account Guest corretto sia configurato in Expressway-C. A tale scopo, passare a **Configurazione > Comunicazione unificata > Cisco Meeting Server**.

Se l'URL interno è configurato nell'URL del client dell'account Guest, Expressway-C lo risolverà poiché nel server DNS è stato creato un record, ma ciò potrebbe causare il messaggio di errore "richiesta non valida" nel browser Web. In questo caso, l'URL interno è configurato in modo da visualizzare l'errore come mostrato nell'immagine.

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

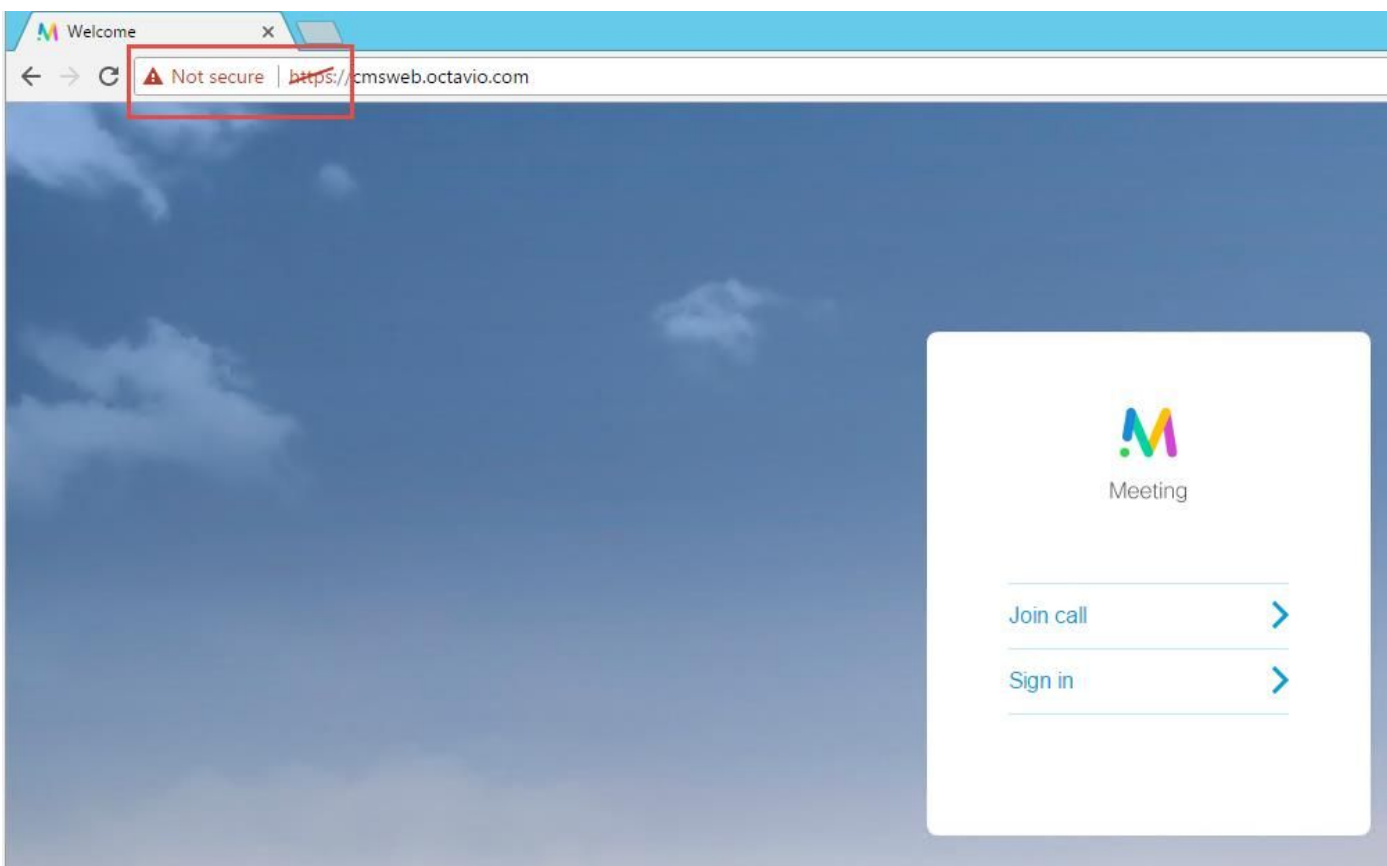
* cmsweb.cms.octavio.local

Save

Guest account client URI resolved to the following targets

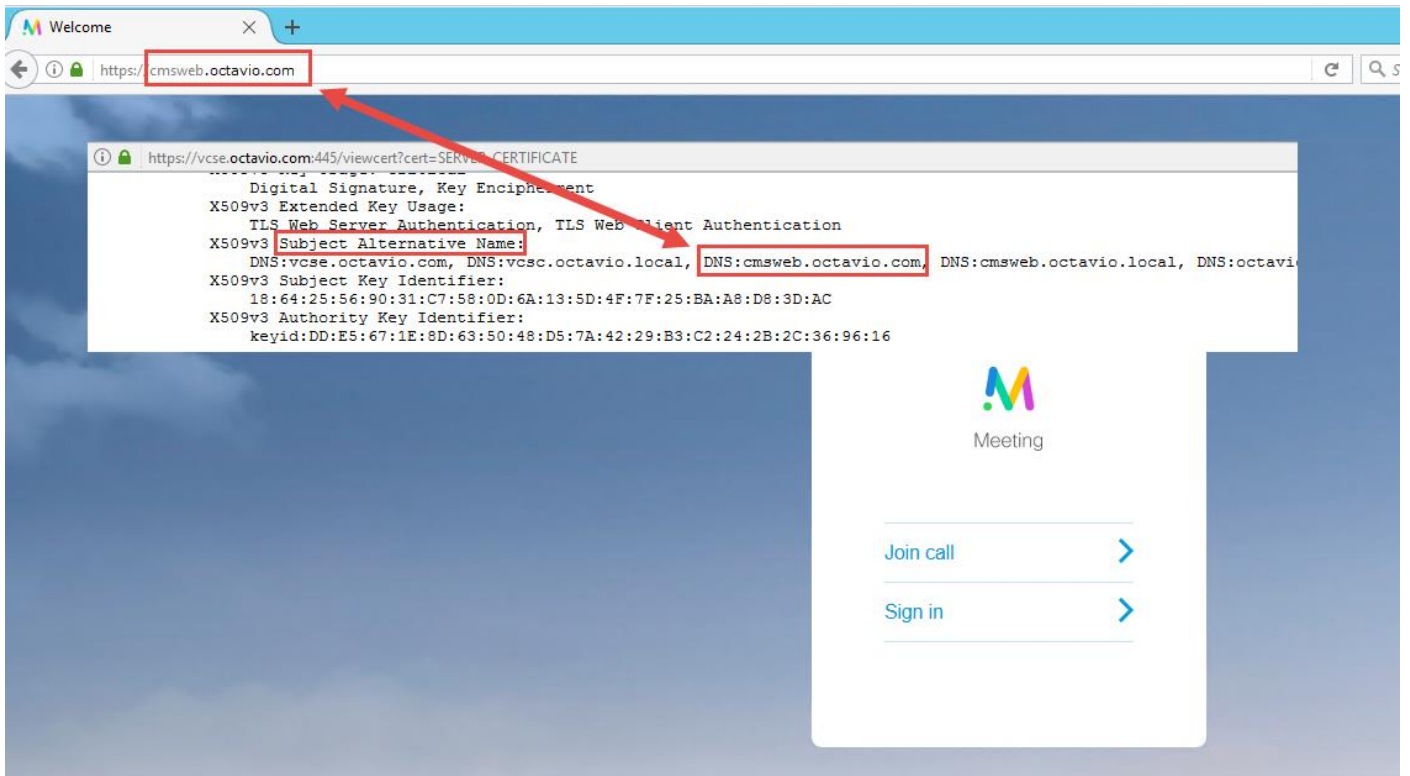
Name	Address
cmsweb.cms.octavio.local	172.16.85.180

Il client WebRTC mostra una connessione non protetta

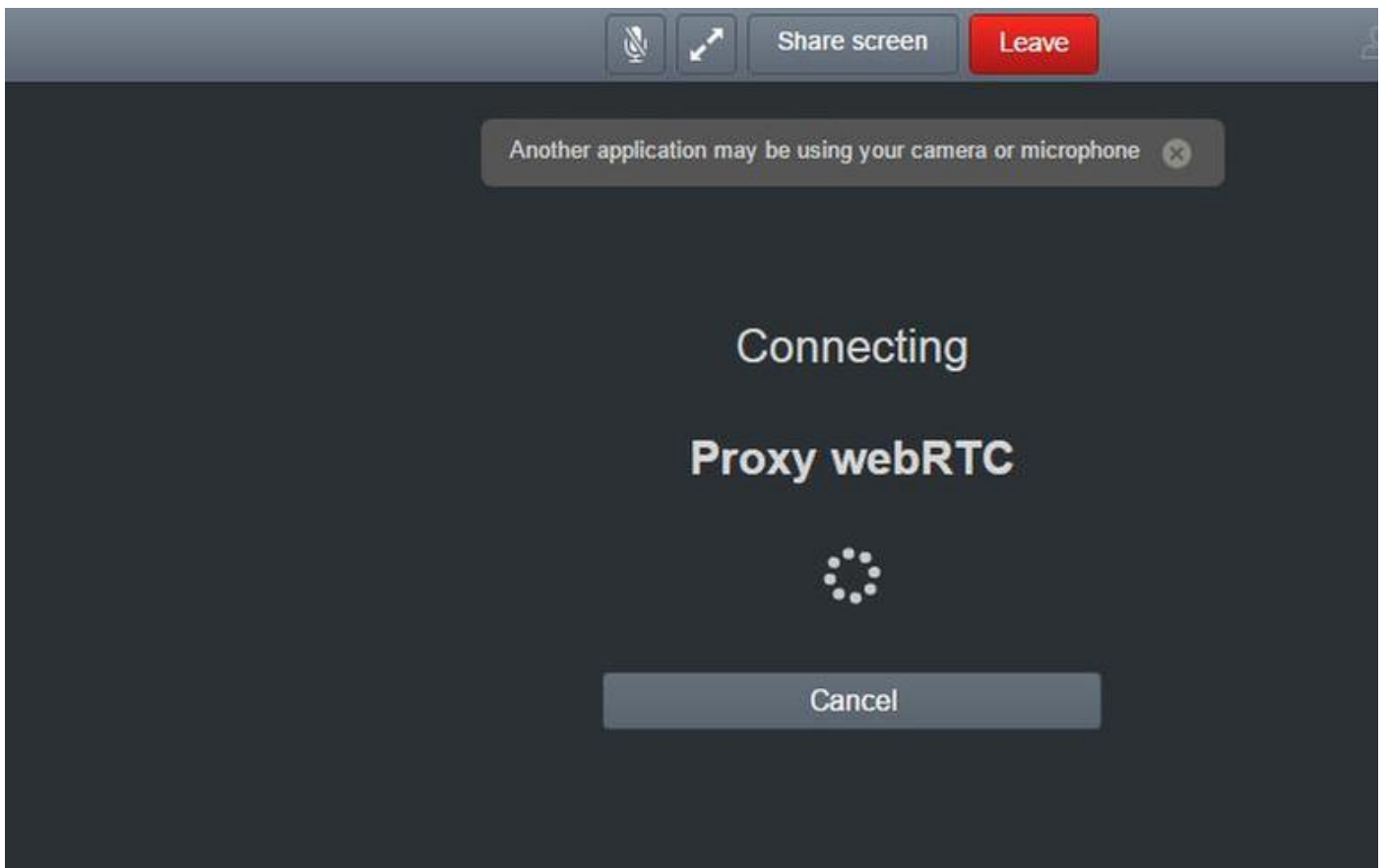


Soluzione

- Il certificato è autofirmato, pertanto il server non considera attendibile l'origine. Modificare il certificato in Expressway-E in un'autorità di certificazione di terze parti supportata.
- Verificare che l'URL del webbridge esterno venga aggiunto come SAN sul certificato del server Expressway-E come mostrato nell'immagine.



Il client WebRTC si connette ma non si connette mai, quindi si interrompe e si disconnette



Il nome utente o la password del server TURN non sono configurati correttamente né su expressway-E né nel CMS via API. I log contengono gli errori mostrati nell'immagine.

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

L'errore può essere confermato anche con l'acquisizione di un pacchetto. Eseguire Wireshark sul PC su cui è in esecuzione il client webRTC. Dopo aver acquisito il pacchetto, filtrarlo per STUN. Gli errori devono essere visualizzati nell'immagine.

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	0x08bc (2748)	Default	Allocate Error Response user: turnuser with nonce realm: turnuser UDP error-code: 431 ("Unknown error code") Integrity Check Failure

Il PC invia una richiesta di allocazione e l'indirizzo NAT di Expressway risponde con il messaggio 'Controllo di integrità non riuscito'.

Soluzione

Per correggere l'errore, rivedere il nome utente e la password. Devono essere configurati correttamente sui parametri del server TURN come mostrato nelle immagini.

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 selected, and the configuration for the 'turnuser' entry is shown:

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