

デュアルドメインを使用した Expressway 経由の CMS を使用したプロキシ WebRTC の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[技術情報](#)

[DNS 設定](#)

[内部 DNS 設定](#)

[外部 DNS 設定](#)

[CMS、callbridge、webbridge、XMPP 設定](#)

[TURN 設定](#)

[Expressway-C および E の設定](#)

[Expressway-C の設定](#)

[Expressway-E 上の設定](#)

[確認](#)

[トラブルシューティング](#)

[\[Join call\] ボタンが表示されない](#)

[WebRTC ページに「Bad Request」と表示される](#)

[WebRTC クライアントに非セキュア接続が表示される](#)

[WebRTC クライアントが接続しても接続されず、タイムアウトして切断される](#)

概要

このドキュメントでは、異なる内部ドメインと外部ドメインを持つ Expressway を介した Cisco Meeting Server (CMS) のプロキシ Web リアルタイム通信 (webRTC) の設定例について説明します。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- シングル連結展開の CMS バージョン 2.1.4 以上
- Expressway-C および Expressway-E バージョン X8.9.2 以上
- CMS の callbridge と webbridge の設定
- Expressway ペアで有効なモバイルアクセス (MRA) とリモートアクセス (MRA)
- Expressway-E に追加されたリレー NAT (TURN) オプションキーを使用したトラバーサル
- webbridge URL の外部解解可能ドメインネームサーバ (DNS) レコード、外部ドメイン用

- 外部から内部ドメインに入る CMS IP アドレス用の内部解決可能な DNS レコード
- 内部および外部ドメイン用にCMSで構成されたExtensible Messaging and Presence Protocol(XMPP)マルチドメイン
- [Firewall] で TCP ポート 443 をパブリック インターネットからの入力と Expressway-E のパブリック IP アドレスへの出力に開放
- [Firewall] で TCP および UDP ポート 3478 をパブリック インターネットからの入力と Expressway-E のパブリック IP アドレスへの出力に開放
- [Firewall] で UDP ポート範囲 24000 ~ 29999 を Expressway-E のパブリック IP アドレスからの入出力に開放

使用するコンポーネント

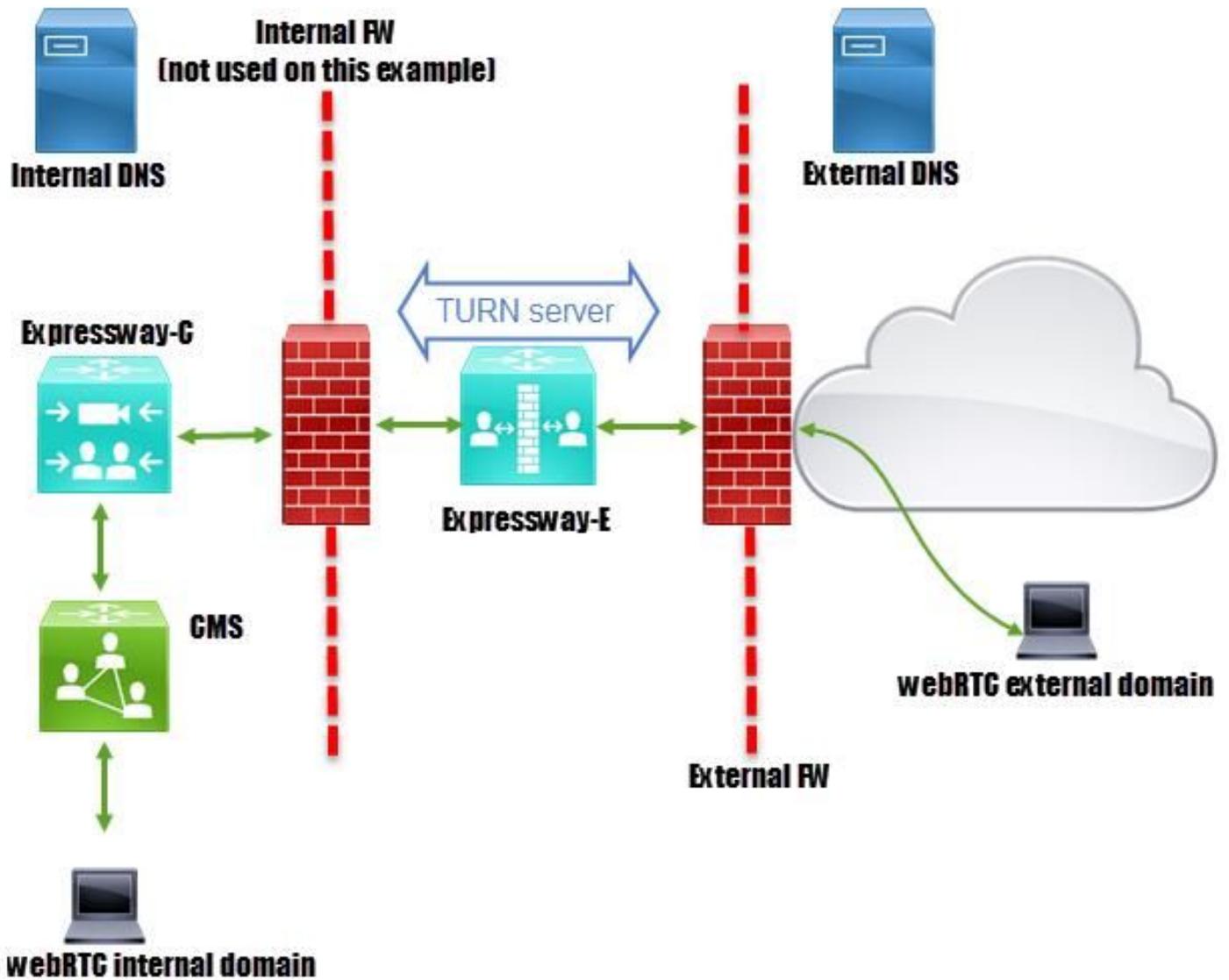
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- シングル連結展開の CMS バージョン 2.2.1
- Expressway-CおよびExpressway-E(デュアルネットワークインターフェイスカード(NIC)およびスタティックネットワークアドレス変換(NAT)ソフトウェアバージョンX8.9.2)
- Postman

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ネットワーク図



技術情報

内部ドメイン	cms.octavio.local
外部ドメイン	octavio.com
CMS IP アドレス	172.16.85.180
Expressway-C IP アドレス	172.16.85.167
Expressway-E LAN1 IP アドレス (内部)	172.16.85.168
Expressway-E LAN2 IP アドレス (外部)	192.168.245.61
スタティック NAT IP アドレス	10.88.246.156

DNS 設定

内部 DNS 設定

Name	Type	Data	Timestamp
ACTIVEDIRECTORY			
Forward Lookup Zones			
_msdcs.octavio.local			
octavio.com			
_tcp			
_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

外部 DNS 設定

図に示すように、外部DNSには、Expressway-EのスタティックNAT IPアドレスに解決される webbridge URLが必要です。

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[7], mxdc.mx.lab., hostmaster.mx...
(same as parent folder)	Name Server (NS)	mxdc.mx.lab.
cmsweb	Host (A)	10.88.246.156
vcse	Host (A)	10.88.246.156

CMS、callbridge、webbridge、XMPP 設定

ステップ1:callbridgeライセンスをアクティブにする必要があります。次の画像には有効な callbridge ライセンスが表示されています。

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

ライセンスの詳細は次を参照してください。

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

ステップ2：図に示すように、MMPを使用してcallbridge、webbridge、およびXMPPを有効にします。

```
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
```

有効にする手順の詳細は、次のリンクを参照してください。

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

証明書の作成手順の詳細は、次のリンクを参照してください。

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

ステップ3:[Configuration] > [General]でCMS Webページに移動し、図に示すようにWebブリッジの内部URLと外部URLを設定します。

Web bridge settings

Guest account client URI

Guest account JID domain

Custom background image URI

Custom login logo URI

Guest access via ID and passcode

Guest access via hyperlinks

User sign in

Joining scheduled Lync conferences by ID

IVR

IVR numeric ID

Joining scheduled Lync conferences by ID

External access

Web Bridge URI

IVR telephone number

This FQDN has to be set as SAN on Expressway-E certificate

注：CMSには、少なくとも1つのスペースを設定する必要があります。

図に示すように、CMSに設定されたスペースの例。

<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

注：内部および外部ドメインの着信コールを設定する必要があります。

図に示すように、着信コール処理に設定されたドメインの例を示します。

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 設定

ステップ1:TURNはPostmanを介してAPIで設定する必要があります。このコマンドはすべての設定で使用します。

<https://>

ステップ2: POSTメソッドを使用し、TURNサーバのパラメータを表示するか、TURNサーバのパラメータを編集するか、Bodyに移動します。TURNサーバに設定されているパラメータは、図に示すとおりです。

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

ステップ3: GETメソッドを実行してサーバIDをコピーし、TURNサーバ設定のステータスを確認します。コピーする必要があるIDは図に示すとおりです。

```
<?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>
```

ステップ4: APIコマンドの最後にあるIDをコピーし、GETメソッドを使用して、図に示すようにTURNサーバ情報を表示します。

注：この情報には、サーバのパスワードは表示されません。

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 is highlighted in red)
- Authorization:** Basic Auth
- Username:** admin
- Password:** (masked with dots)
- Body:** XML response (Status: 200)

```
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>
```

ステップ 5 : [send] をクリックしてサーバのステータスを取得します。図に示すように、正常な設定の例です。

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 および E の設定

ステップ1: expressway-Cには内部ドメイン(octavio.local)が、Expressway-Eには外部ドメイン(octavio.com)が設定されている必要があります。



Status System Configuration Applications Users Maintenance

DNS

DNS settings

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

Default DNS servers

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

Internal DNS server

ステップ2 : 図に示すように、Expressway CとEの両方でMRAを有効にする必要があります。

Unified Communications You are here Configuration > Unified Communications > Configuration

Configuration

Unified Communications mode Mobile and remote access

ステップ3 : 図に示すように、Expressway-CとEの間にユニファイドコミュニケーショントラバースルゾーンを作成します。



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"/> ⓘ

This credentials are configured on Exp-E

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"/> ⓘ

Expressway-Cの設定

ステップ1：図に示すように、Expressway-Cで内部ドメインと外部ドメインを設定します。



Status System **Configuration** Application

Domains

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

ステップ 2 : Cisco Meeting 設定を有効にします。[Configuration] > [Unified Communications] > [Cisco Meeting Server] の順に開きます。図に示すように、[ゲストアカウントクライアント URI]フィールドに外部webbridge URLを設定します。



Status System **Configuration** Applications Users Maintenance

Cisco Meeting Server

Meeting Server configuration

Meeting Server Web Proxy

Guest account client URI

Guest account client URI resolved to the following targets

Name	Address
cmsweb.octavio.com	172.16.85.180

注：内部 DNS は、外部 webbridge URL (cmsweb.octavio.com) を内部 CMS webbridge IP アドレスに解決する必要があります。この例では IP アドレスは 172.16.85.180 です。

図に示すように、Expressway-Cのセキュアシェル(SSH)トンネルは、数秒後にアクティブになる必要があります。



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：サーバには、サーバ証明書とCA証明書が必要です。

Expressway-E 上の設定

ステップ1：図に示すように、expressway-EにはTURNライセンスが必要です。

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

ステップ2 : 図に示すように、Expressway-Eに外部ドメインを設定する必要があります。

 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

ステップ3 : 図に示すように、TURNサーバとUnified Communicationトラバーサルゾーンのユーザーを作成します。

 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

ステップ4：図に示すように、ユニファイドコミュニケーショントラバーサルゾーンを作成します。



Cisco Expressway-E

Status System **Configuration** Applications Users Maintenance

Edit zone

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 ⓘ

ステップ5:TURNサーバを設定します。図に示すように、[Configuration] > [Traversal] > [TURN]に移動します。

注：TURN 要求は、Web クライアントが TURN 接続を要求するポートであるポート 3478 宛てにする必要があります。



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

Turnが起動すると、図に示すようにステータスがActiveと表示されます。

TURN server status

Status	Active
Listening address 1	172.16.85.168 <input type="text" value="3478"/>
Listening address 2	192.168.245.61 <input type="text" value="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

ステップ6:[System] > [Administration]に移動します。webRTCクライアントはポート443へのアクセスを要求します。このため、Expressway-Eの管理ポートを別のポートに変更する必要があります。この例では、図のように445に変更します。

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*

ステップ7: Expressway-E の証明書を作成: 図に示すように、webbridge URLをサーバ証明書のSANとして追加する必要があります。

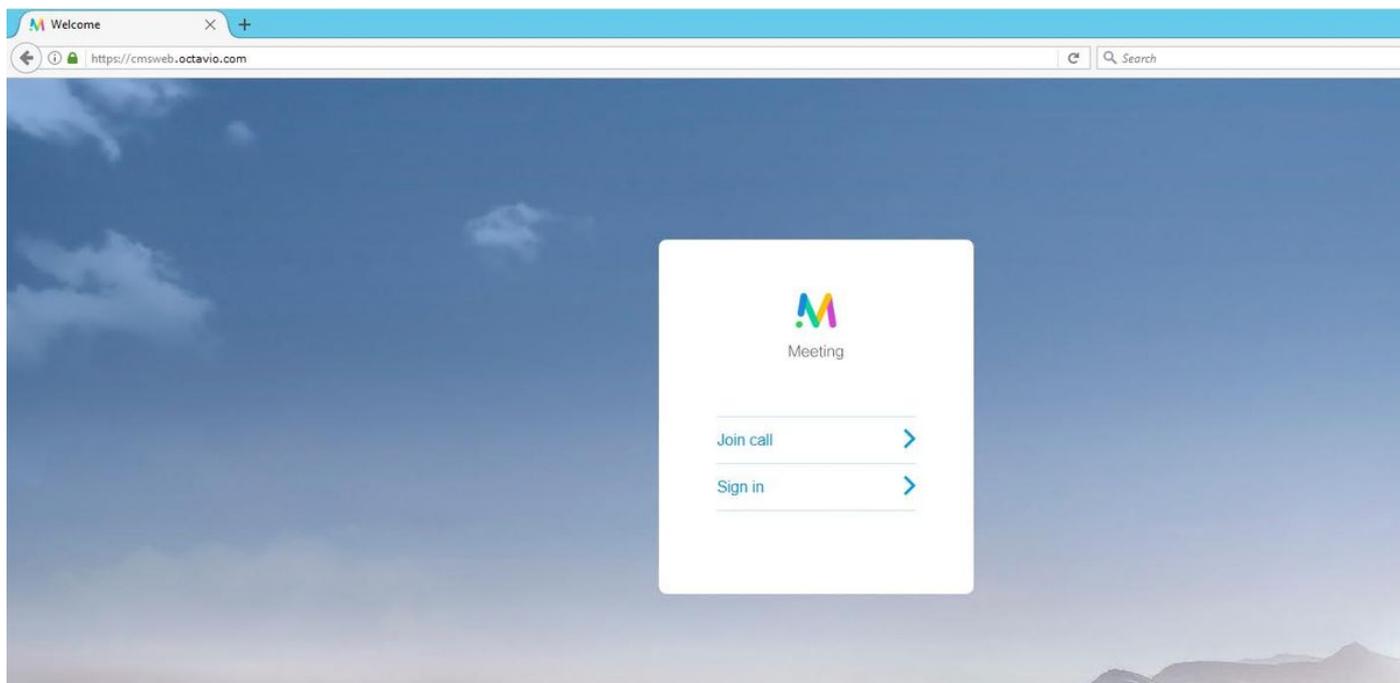
X509v3 Subject Alternative Name:
DNS:vcse.octavio.com, DNS:vcse.octavio.local, DNS:cmsweb.octavio.com, DNS:cmsweb.octavio.local, DNS:octavio.local, DNS:cms.octavio.local, DNS:octavio.com

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ1：サポートされているWebブラウザを選択し、外部webbridge URLを入力します。次の画面が図のように表示されている必要があります。

注：サポートされているブラウザの種類やバージョンの一覧はこちらからご確認いただけます。<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>



ステップ2:[Join call]を選択し、図に示すように、前に設定したスペースIDを入力します。

Enter Call ID

Meeting

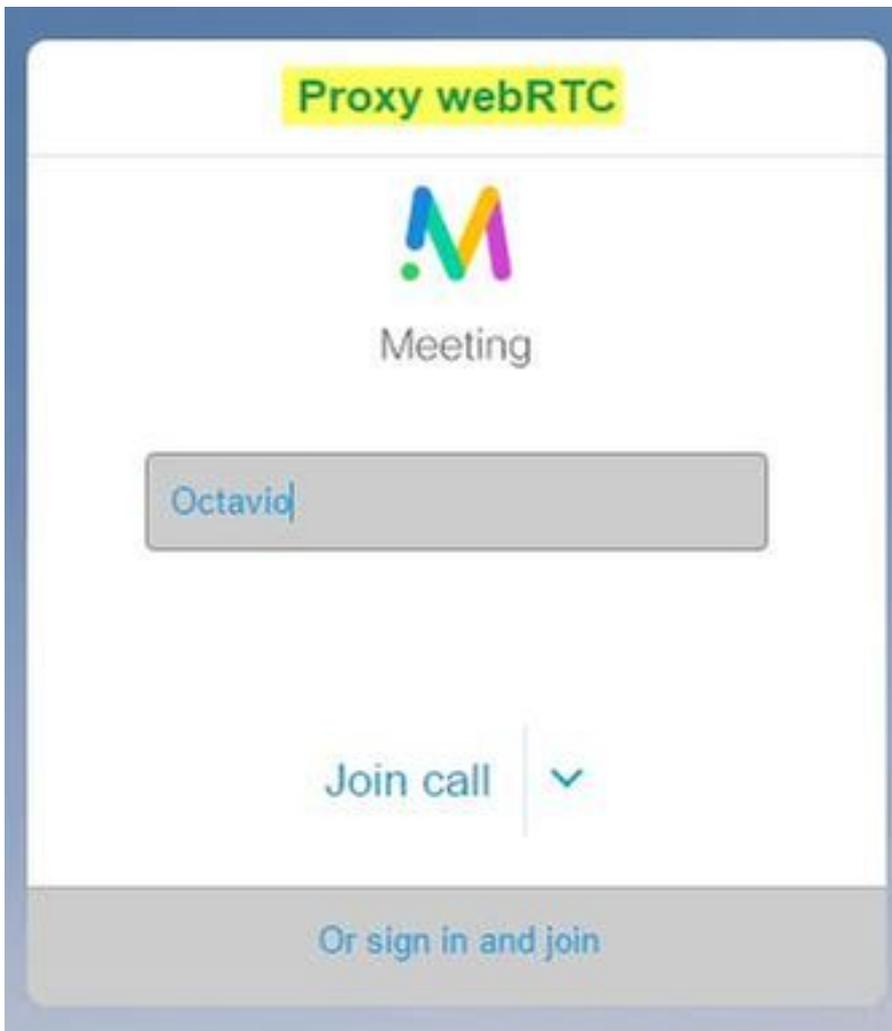
100101

Passcode (if required)

Continue >

Back

ステップ 3 : [Continue] をクリックして名前を入力します。このとき、参加するスペース名が表示されていることを確認します。この例では Proxy webRTC がスペース名です。図に示すように [Join call] をクリックします。



ステップ4：別のデバイスに参加します。図に示すように、会議に接続された両方のデバイスが表示されている必要があります。

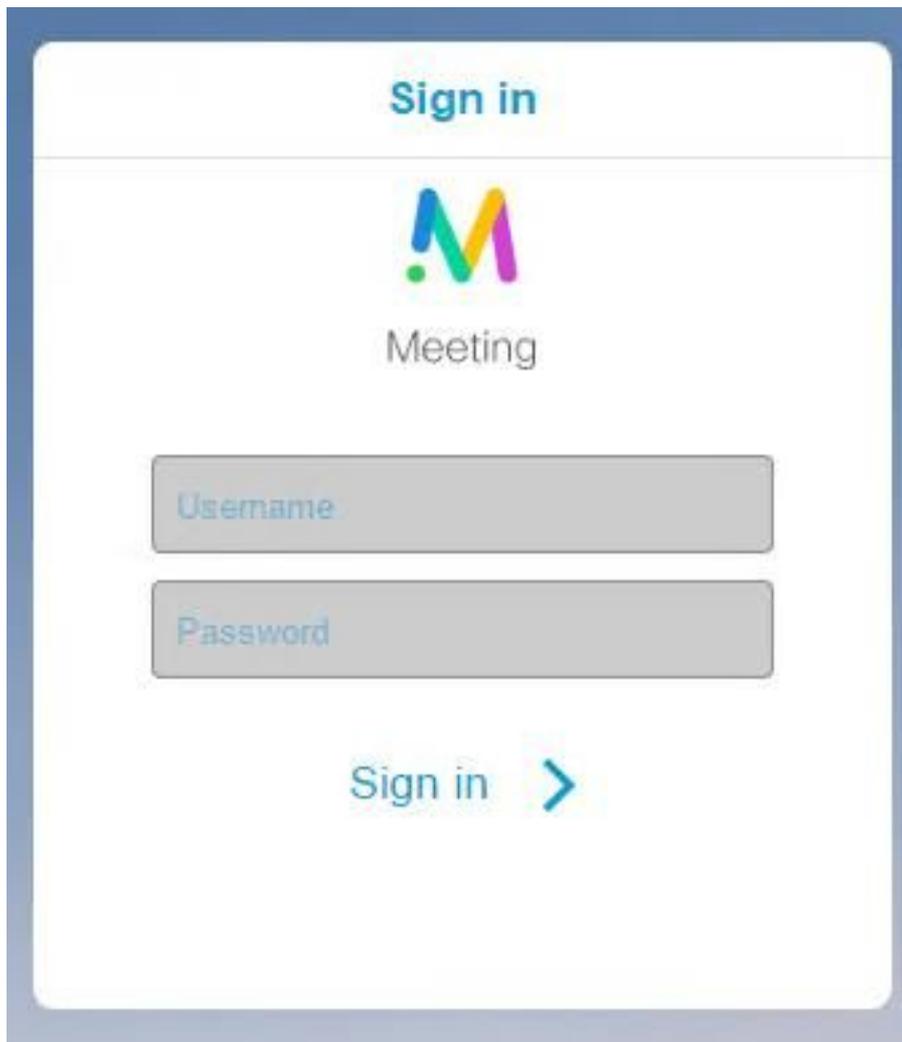


トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

[Join call] ボタンが表示されない

webbridgeページを開くとJoin callボタンが表示されず、図に示すようにCMS Webページに入力すると2番目の図に示すエラーが表示されます。



Fault conditions

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

この問題は、webbridgeがコールブリッジと正しく通信しない場合に発生します。

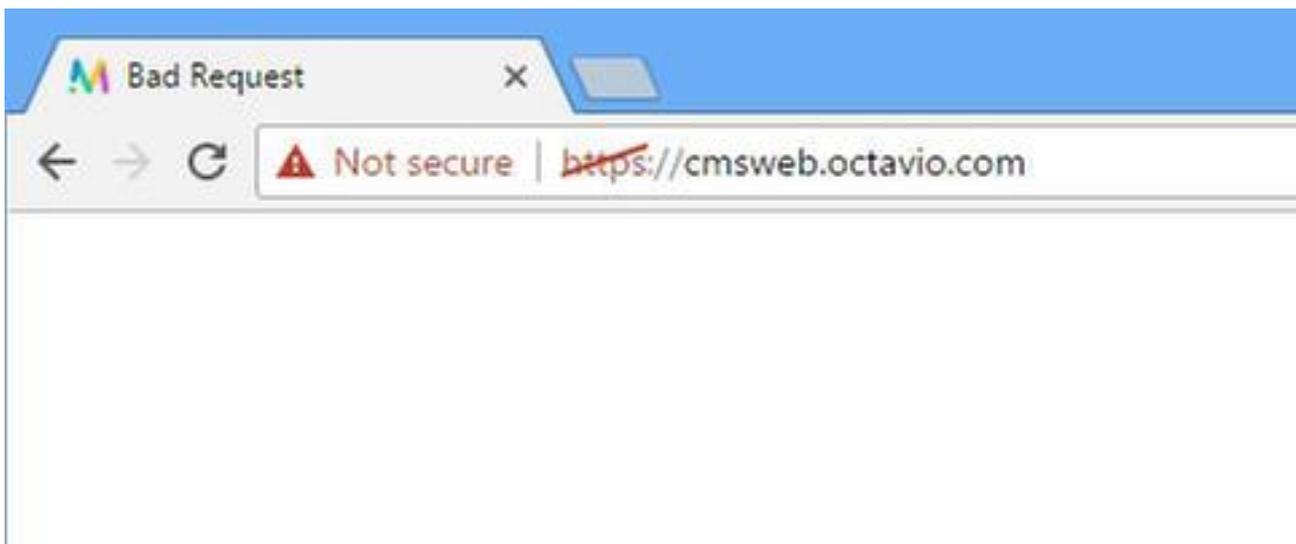
解決方法

- CMS 管理 Web ページで webbridge URL が正しく設定されているかを確認します。
[Configuration] > [General] の順に開いて確認します。
- webbridgeとcallbridgeは互いを信頼する必要があります。図に示すように、信頼バンドルがwebbridge設定に追加されていることを確認します。

```
proxyWebRTC> webbridge
Enabled                : true
Interface whitelist    : a:443
Key file                : webbridge.key
Certificate file       : webbridge.cer
CA Bundle file         : root.cer
Trust bundle           : none
HTTP redirect          : Enabled
Clickonce URL          : none
MSI download URL       : none
DMG download URL       : none
iOS download URL       : none
proxyWebRTC>
proxyWebRTC>
```

注：[Trust bundle] とは Call Bridge 証明書です。

WebRTCページに「Bad Request」と表示される



解決方法

- Expressway-Cで正しいゲストアカウントクライアントURIが設定されていることを確認します。この目的で、[Configuration] > [Unified Communication] > [Cisco Meeting Server]に移動します。

[Guest account client URI] に内部 URL が設定されていると、Expressway-C は DNS サーバで作成されたレコードに基づいて解決させますが、Web ブラウザで「Bad Request」エラーメッセージがトリガーされる可能性があります。この例では、図に示すように、エラーを表示するために内部URLが設定されています。

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

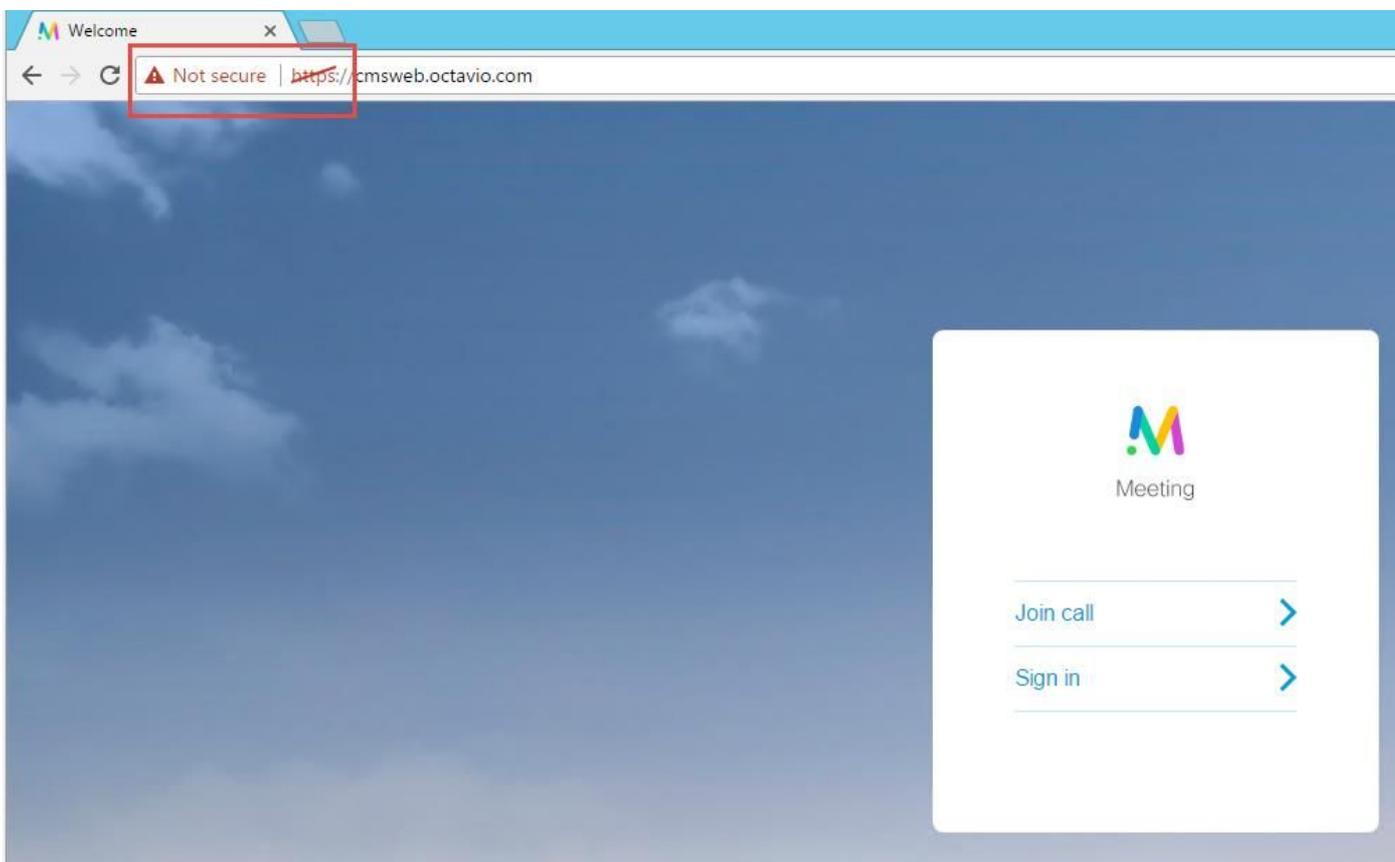
* cmsweb.cms.octavio.local

Save

Guest account client URI resolved to the following targets

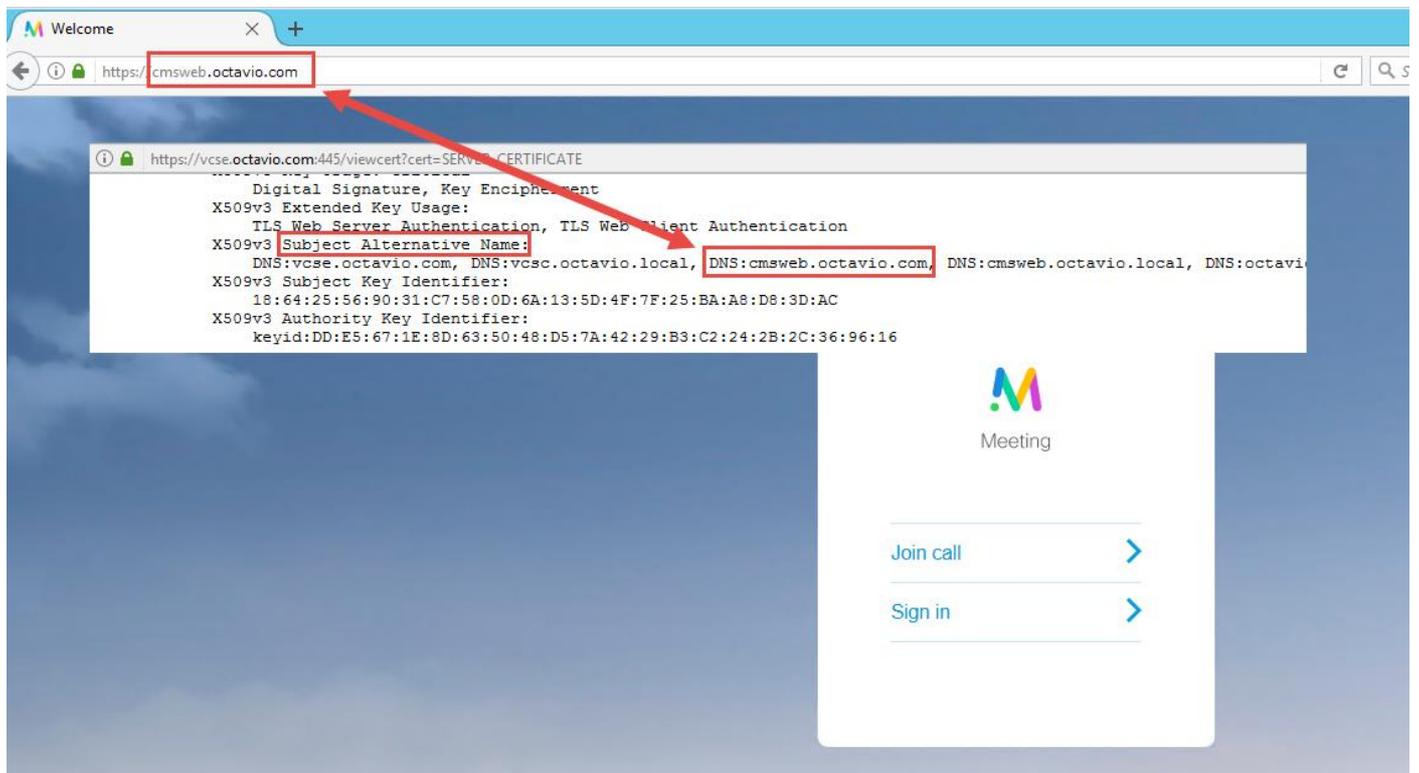
Name	Address
cmsweb.cms.octavio.local	172.16.85.180

WebRTC クライアントに非セキュア接続が表示される

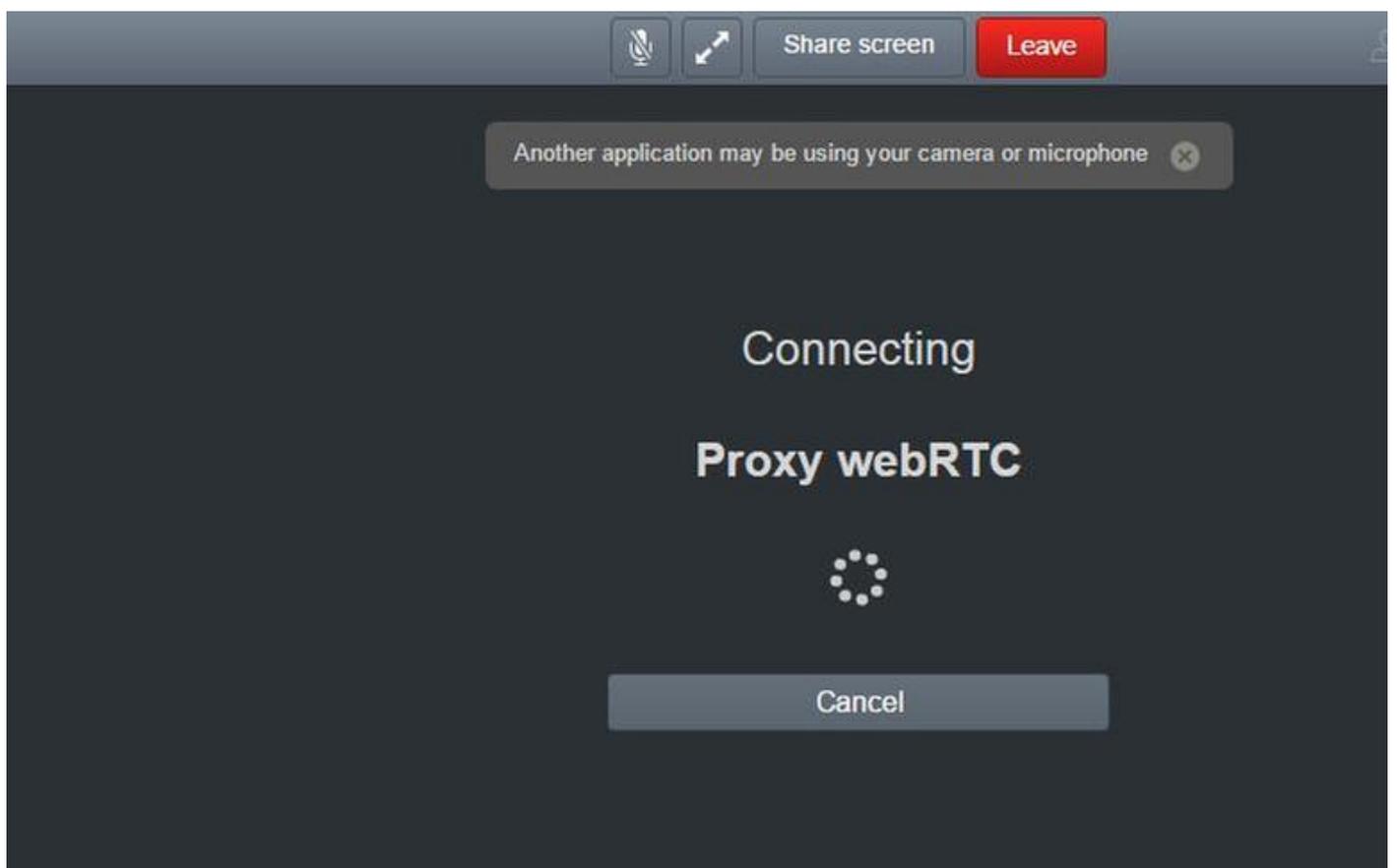


解決方法

- 証明書が自己署名であるため、サーバが送信元を信頼していない状態です。Expressway-E の証明書をサポートされているサードパーティ認証局の証明書に変更します。
- 図に示すように、Expressway-Eサーバ証明書で外部webbridge URLがSANとして追加されていることを確認します。



WebRTCクライアントが接続しても接続されず、タイムアウトして切断される



Expressway-E または API で CMS に設定した TURN サーバのユーザ名またはパスワードに誤りがあります。ログには、図に示すエラーが含まれています。

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

エラーはパケット キャプチャでも確認することができます。webRTC クライアントを実行する PC で Wireshark を実行します。パケット キャプチャができたなら、パケットを「STUN」でフィルタ処理します。図に示されているエラーが表示されている必要があります。

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	0x0abc (2748)	Default	Allocate Error Response user: turnuser with nonce realm: turnuser UDP error-code: 431 ("Unknown error code") Integrity Check Failure

PCがAllocate Requestを送信し、Expressway NATアドレスが「Integrity check failure」メッセージで応答します。

解決方法

エラーを修正するには、ユーザ名とパスワードを確認します。これらは、図に示すように、TURNサーバパラメータで正しく設定されている必要があります。

The image shows a REST client interface for a POST request to the Expressway API. The URL is `https://admin.cms.octavio.local:445/api/v1/turnServers/2aa16ccc-87d1-424d-9d3d-3d007f23243a/`. The request body is form-data encoded. The parameters are:

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

Below the REST client, the Cisco Expressway-E configuration page is shown. The 'Local authentication database' section is active, and the configuration for the 'turnuser' entry is visible:

- Name: turnuser
- Password: [Redacted]