

# Expressway経由のCMS WebRTCまたはWeb Appプロキシの設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

### [設定](#)

#### [ネットワーク図](#)

#### [設定手順](#)

[ステップ 1 : CMS WBのExpressway-Cへの統合](#)

[ステップ 2 : Expressway-EでTURNを有効にし、認証クレデンシャルをローカル認証データベースに追加する](#)

[ステップ 3 : Expressway-Eの管理ポートの変更](#)

[ステップ 4 : メディアNATトラバーサル用のTURNサーバとしてExpressway-EをCMSサーバに追加する](#)

### [確認](#)

[ステップ 1 : Expressway-C で WB が正しく統合されたことを確認する](#)

[ステップ 2 : TURNサーバがCMSサーバに追加されたことを確認する](#)

[ステップ 3 : 通話中のTURNリレーの使用状況の確認](#)

### [トラブルシューティング](#)

[外部 WebRTC クライアントは接続しているが、メディアがない \( ICE 障害のため \)](#)

[外部 WebRTC クライアントが Join Call オプションを取得しない](#)

[外部 WebRTC クライアントが cospace への接続時に \( ロード中のメディアで \) スタックし、WB の最初のページにリダイレクトされる](#)

[外部 WebRTC クライアントが cospace に参加できず、警告が表示される \( 接続不可 - 後でやり直す \)](#)

### [関連情報](#)

---

## はじめに

このドキュメントでは、Expressway 上の Cisco Meeting Server ( CMS ) WebRTC の設定およびトラブルシューティングの手順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が推奨されます。

- Expressway X12.6.1以降 ( x12.6.1以降は、Exp TURN動作の変更により、CMS 2.9.2以降でのみ動作可能 )

- CMS サーバ 2.9.3 以降
- ネットワーク アドレス変換 ( NAT )
- NATのリレー(TURN)を使用したトラバーサル
- NAT用のセッショントラバーサルユーティリティ(STUN)
- ドメイン ネーム システム ( DNS )

## 設定の要件

- ExpresswayでMobile and Remote Access(MRA)関連の基本設定 ( UCトラバーサルゾーン、SSHトンネル ) がすでに有効になっており設定されている必要があります。MRAのガイドについては[ここをクリック](#)してください。
- CMS 2.9.x(WB)、XMPP、およびCallBridgeが設定され、CMSで有効になっている場合は、[設定ガイド](#)を参照してください。
- TURN オプション キーが Expressway-E にインストールされている。
- [ファイアウォール ( 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。
- TCP および UDP ポート 3478 ( TURN 要求 ) が、パブリック インターネットから Expressway-E のパブリック IP アドレスへのファイアウォールで開かれている。
  - TCP 3478は、CMS APIの「turnservers」でtcpPortNumberOverrideが3478に設定されている場合にのみ必要です。
- ファイアウォールでCMSからExpressway-EのプライベートIPアドレスに対してUDPポート 3478 ( TURN要求 ) がオープンされました ( Expressway-EでデュアルNICを使用している場合 )。
  - CMS 2.9.2以前ではExp Eにバインディングリクエストを送信し、2.9.3以降ではAllocateリクエストを送信
- webbridgeの参加URLの外部DNSレコード ( Expressway-Eのパブリック側のIPアドレスに解決可能 )。
- webbridgeサーバのIPアドレスに解決可能なJoin URLの内部DNSレコード。
- X12.5.2以前のバージョンを実行している場合は、Expressway-EのパブリックIPアドレスの外部ファイアウォールでNATリフレクションが許可されていることを確認します。設定の例については、[ここをクリック](#)してください。X12.5.3では、スタンドアロンのExpresswayには必要なくなりました。
- TURNにポート443を使用する場合は、外部ファイアウォール上のメディアに対してUDPポート3478を開く必要があります。

---

 注意:TCPポート443が有効になっていると、ExpresswayはTCPポート3478で応答できなくなります。

---

 注:Jabber Guestサービスに使用されるExpresswayペアは、CMS WebRTCプロキシサービスには使用できません。

---

 注:以前のバージョンから3.0以降にアップグレードする場合は、「[Cisco Meeting Server 2.9から3.0への円滑なアップグレードのためのガイダンス](#)」を参照してください。

---

## 使用するコンポーネント

このドキュメントは、特定のソフトウェアおよびハードウェアのバージョンに限定されるものではありませんが、ソフトウェアの最小バージョン要件を満たす必要があります。

- CMS アプリケーション プログラミング インターフェイス (API)
- Expressway
- CMS サーバ

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、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

WebRTCプロキシのサポートはバージョンX8.9.2からExpresswayに追加されました。これにより、オフプレミスユーザはCisco Meeting Server Web Bridgeを参照できます。

外部クライアントおよびゲストで、サポート対象ブラウザ以外のソフトウェアを必要とせずに、スペースの管理やスペースへの参加ができます。 [サポート対象のブラウザの一覧についてはここをクリックしてください。](#)

2021年2月5日の時点で、CMS 3.1.1でサポートされているブラウザは次のとおりです。

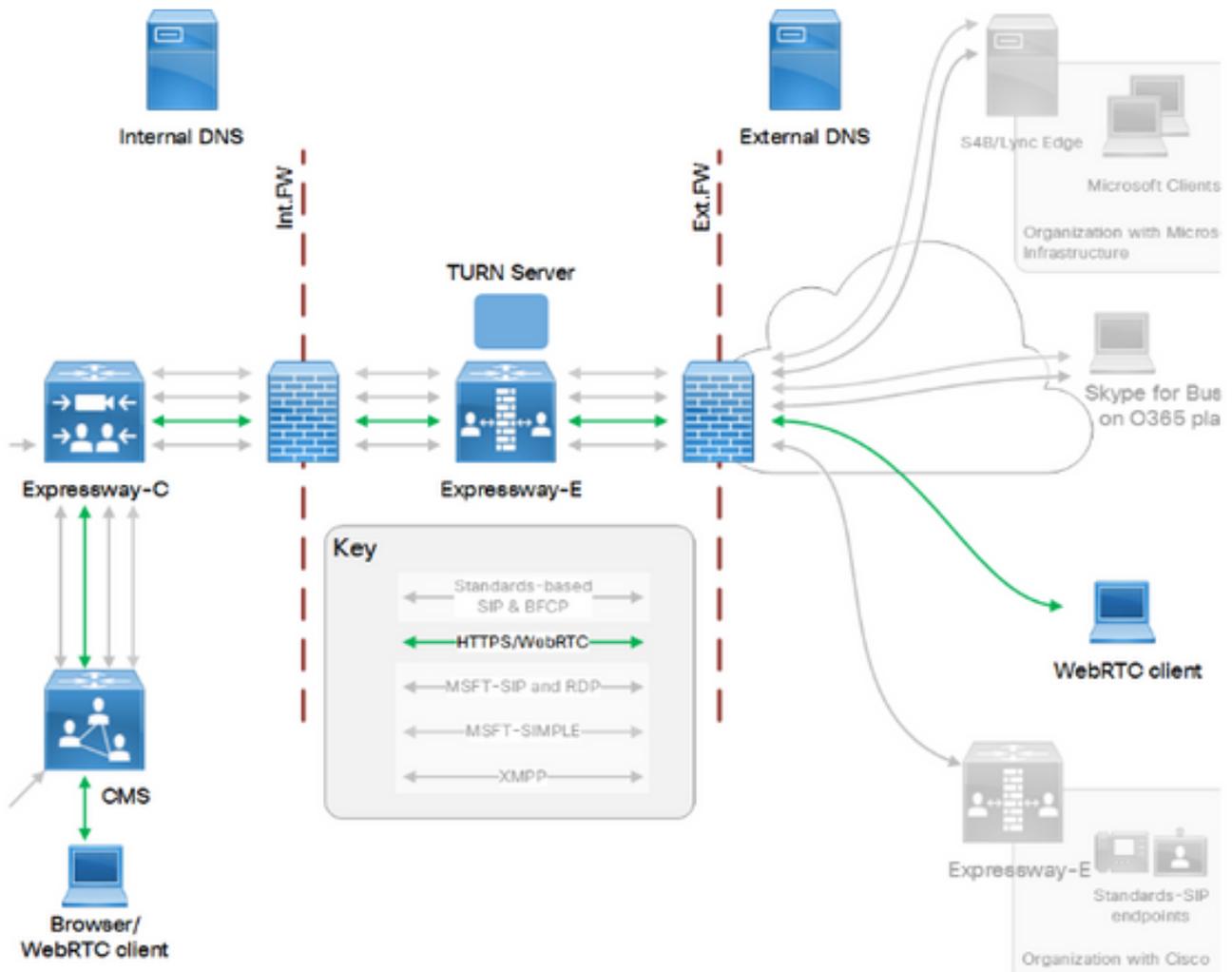
Browsers	Versions
Google Chrome (Windows, macOS and Android)	86
Mozilla Firefox (Windows)	82
Chromium-based Microsoft Edge (Windows)	86
Apple Safari for macOS	13.x and 14.0
Apple Safari for iOS	iOS versions: 13.x and 14.0
Yandex (Windows)	20.8 and 20.11

Note: Web app is not supported on the legacy Microsoft Edge.

Note: Web app is not supported on virtual machines (VMs) running these supported browsers.

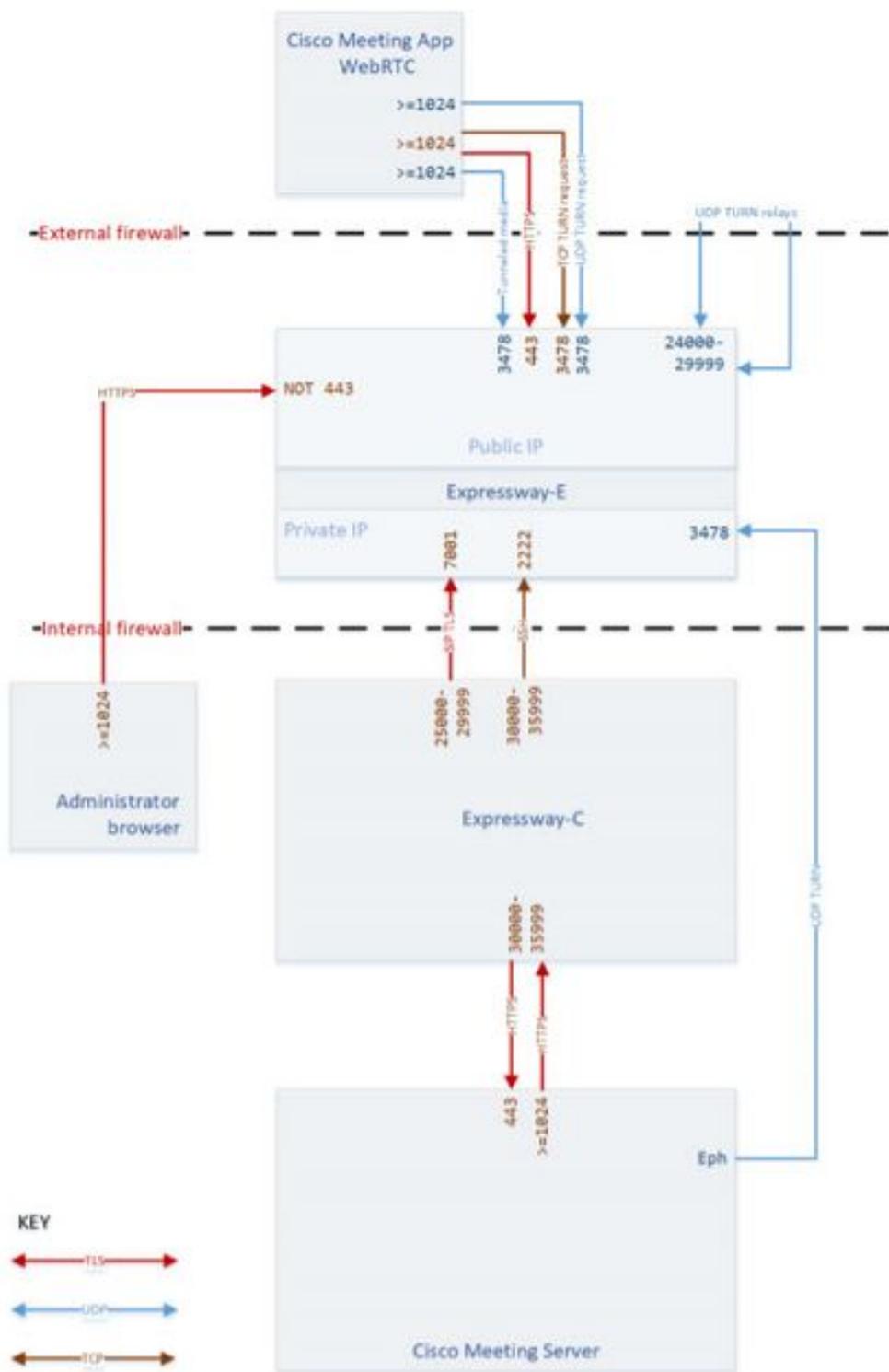
## 設定

### ネットワーク図



この図は、CMS WebRTCのWebプロキシの接続フローの例を示しています(Exp IPポート使用[設定ガイド](#)から)。

# Web Proxy for Cisco Meeting Server Connections



注: X12.5.2以前のバージョンを実行している場合は、Expressway-EおよびパブリックIPアドレスに対してNATリフレクションを許可するように外部ファイアウォールを設定する必要があります(ファイアウォールは通常、送信元と宛先のIPアドレスが同じパケットを信頼しません)。X12.5.3では、スタンドアロンのExpresswayには必要なくなりました。

## 設定手順

### ステップ 1 : CMS WBのExpressway-Cへの統合

- a. Configuration > Unified Communication > Cisco Meeting Serverの順に移動します。
- b. Meeting Server Web Proxyを有効にします。
- c. ゲストアカウントクライアントURIフィールドに参加URLを入力します。
- d. Saveをクリックします。
- e. CMS参加URLをサブジェクト代替名(SAN)としてExpressway-Eサーバ証明書に追加します。『[Cisco VCS Certificate Creation and Use Deployment Guide](#)』を参照してください。

The screenshot shows the Cisco Meeting Server configuration interface. At the top, there are navigation tabs: Status, System, Configuration, Applications, Users, and Maintenance. Below these is the 'Cisco Meeting Server' header. The 'Meeting Server configuration' tab is selected. In the configuration area, 'Meeting Server Web Proxy' is set to 'Enable'. The 'Guest account client URI' field is highlighted with a red border and contains the text 'webbridge.alero.aca'. A 'Save' button is located at the bottom left of the configuration area.

### ステップ 2 : Expressway-EでTURNを有効にし、認証クレデンシャルをローカル認証データベースに追加する

- a. Configuration > Traversal > TURNの順に移動します。
- b. TURNサービスをoffからonの間で有効にします。
- c. Configure TURN client credentials on local databaseの順に選択し、クレデンシャル ( ユーザ名とパスワード ) を追加します。

 注: Expressway-Eのクラスタがあり、それらすべてをTURNサーバとして使用する場合は、すべてのノードで有効にしてください。API経由で2つの個別のturnServerインスタンスを設定し、それらをクラスタ内の各Expressway-Eサーバをポイントする必要があります ( ステップ4に示す設定プロセスに従って、1つのExpressway-Eサーバのプロセスを示します。2つ目のturnServerの設定も同様で、対応するIPアドレスと他のExpressway-Eサーバのturnクレデンシャルのみを使用します ) 。

 注 : TCP/HTTPSトラフィック用にExpresswayの前でネットワークロードバランサを使用できますが、TURNメディアはクライアントからTURNサーバのパブリックIPに送信する必要があります。TURNメディアはネットワークロードバランサを通過できません

### ステップ 3 : Expressway-Eの管理ポートの変更

WebRTC接続はTCP 443で受信されますが、Exp 12.7では443に使用できる新しい専用管理インターフェイス(DMI)が導入されているため、この手順が必要です。

a. System > Administrationの順に移動します。

b. Web server configurationで、ドロップダウンオプションからWeb administrator port を445に変更し、Saveをクリックします。

c. WebRTCプロキシサービスに使用するすべてのExpressway-Eで手順3a ~ 3bを繰り返します。

 注:WebRTCクライアントは443を使用するため、管理ポートを変更することをお勧めします。WebRTC ブラウザがポート 80 にアクセスしようとする時、Expressway-E は接続を 443 にリダイレクトします。

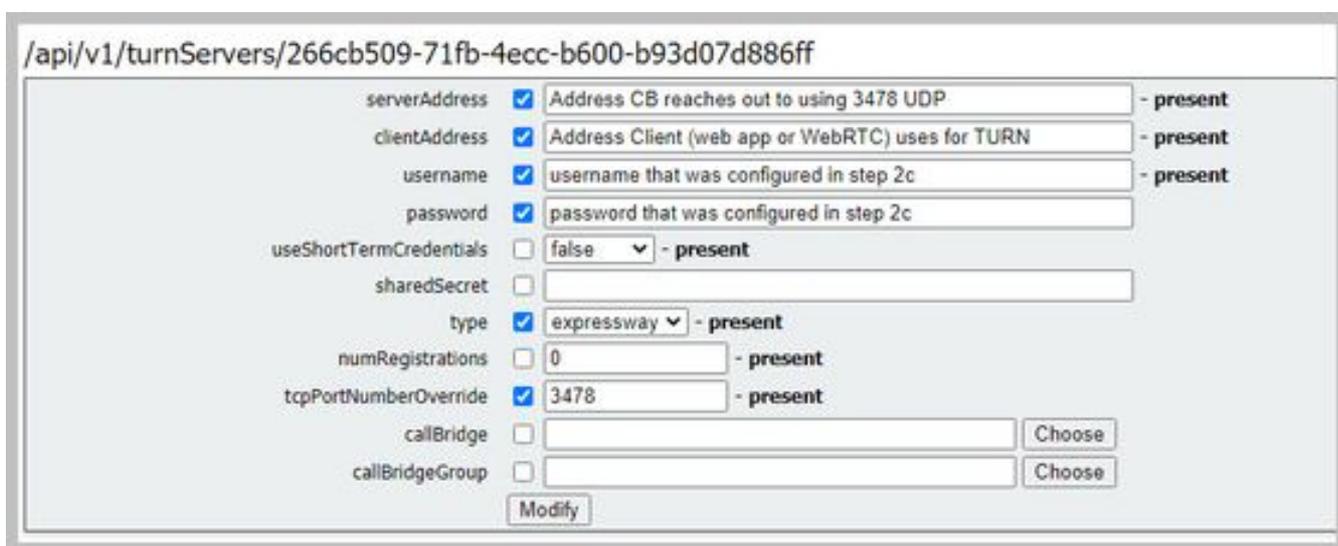
### ステップ 4 : メディアNATトラバーサル用のTURNサーバとしてExpressway-EをCMSサーバに追加する

CMS 2.9.x以降では、Configuration → APIメニューを使用してturnサーバを追加します。

- serverAddress: ( ExpresswayのプライベートIPアドレス )
- clientAddress: ( ExpresswayのパブリックIPアドレス )
- タイプ : (expressway)
- ユーザ名 : ( ステップ2cで設定 )
- パスワード : ( ステップ2cで設定したとおりに )
- tcpPortNumberOverride: 3478

d. TURNに使用するすべてのExpressway-Eサーバに対してステップ4cを繰り返します。

次の図に、設定手順の例を示します。



Field	Value	Required
serverAddress	Address CB reaches out to using 3478 UDP	present
clientAddress	Address Client (web app or WebRTC) uses for TURN	present
username	username that was configured in step 2c	present
password	password that was configured in step 2c	present
useShortTermCredentials	false	present
sharedSecret		
type	expressway	present
numRegistrations	0	present
tcpPortNumberOverride	3478	present
callBridge		Choose
callBridgeGroup		Choose

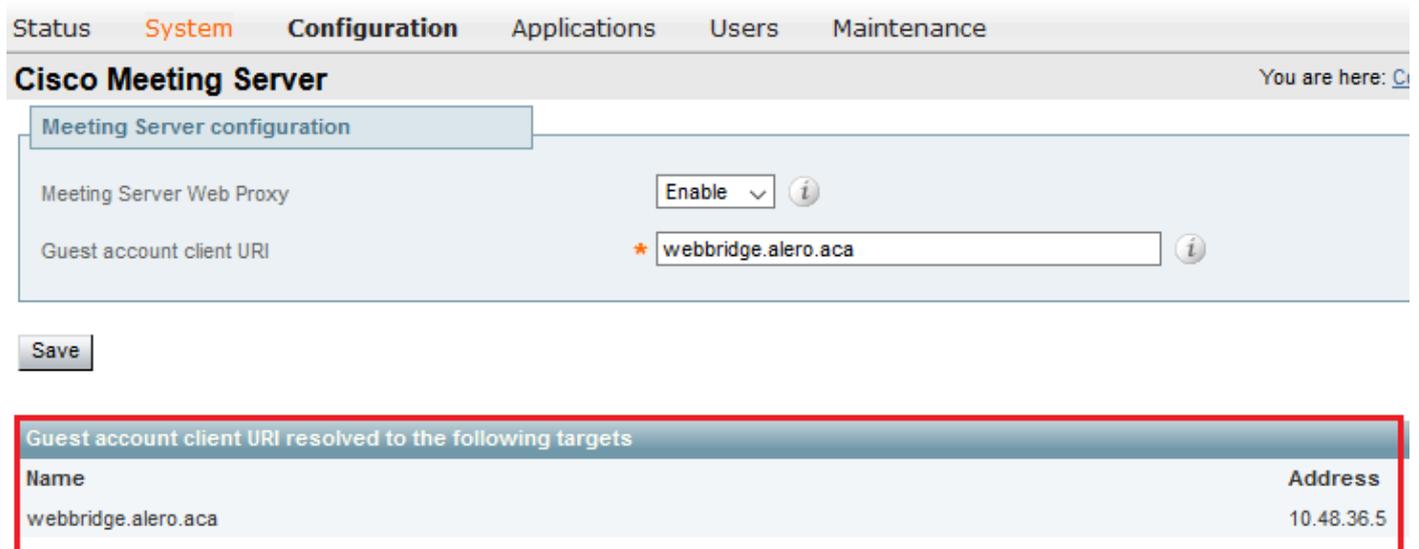
Modify

## 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 : Expressway-C で WB が正しく統合されたことを確認する

a. Configuration > Unified Communication > Cisco Meeting Serverの順に移動します。WBのIPアドレスを確認する必要があります。



The screenshot shows the Cisco Meeting Server configuration interface. The 'Meeting Server Web Proxy' is set to 'Enable' and the 'Guest account client URI' is 'webbridge.alero.aca'. Below the configuration, a table shows the resolved targets for the URI.

Guest account client URI resolved to the following targets	
Name	Address
webbridge.alero.aca	10.48.36.5

b. Configuration > Unified Communication > HTTP allow list > Automatically added rulesの順に移動します。これがルールに追加されたことを確認します。

```
Meeting Server web bridges    https    443    Prefix    /    GET, POST, PUT, HEAD, DELETE
Meeting Server web bridges    wss     443    Prefix    /    GET, POST, PUT, HEAD, DELETE
```

 注：ルールは単にWBへのHTTPSトラフィックのプロキシを許可するためのものであり、必ずしもユニファイドコミュニケーションのために許可されているわけではないため、検出されたノード内にWBがあると想定されていません。

c. WB FQDNのセキュアシェル(SSH)トンネルがExpressway-CからExpressway-Eへの接続に対して構築されており、アクティブであることを確認します。Status > Unified Communications > Unified Communications SSH tunnels statusの順に移動します。WBのFQDNが表示され、ターゲットがExpressway-Eである必要があります。

Target	Domain	Status	Peer
vcs-e.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e.alero.local	alero.lab	Active	10.48.36.247
vcs-e.alero.local	alero.local	Active	10.48.36.247
vcs-e2.alero.local	alero.lab	Active	10.48.36.247
vcs-e2.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e2.alero.local	alero.local	Active	10.48.36.247

ステップ 2 : TURNサーバがCMSサーバに追加されたことを確認する

CMS APIメニューでturnサーバを検索し、それぞれをクリックします。各オブジェクトには、ステータスを確認するためのリンクがあります。

Related objects: </api/v1/turnServers>  
</api/v1/turnServers/266cb509-71fb-4ecc-b600-b93d07d886ff/status>

Table view XML view

Object configuration	
serverAddress	10.0.0.36
clientAddress	175.12.5.1
numRegistrations	0
username	cmsturn
useShortTermCredentials	false
type	expressway
tcpPortNumberOverride	3478

出力に表示される情報に、TURNサーバに関連するミリ秒 ( Ms ) 単位のラウンドトリップ時間 ( RTT ) が含まれています。この情報は、使用する最適な TURN サーバの CB を選択するうえで重要になります。

ステップ 3 : 通話中のTURNリレーの使用状況の確認

WebRTCクライアントを使用して行われたライブコールで、ExpresswayのTURNメディアリレーのステータスを確認できます。Status > TURN relay usageの順に移動し、viewを選択します。

## トラブルシュート

便利なツール :

- ブラウザからのHARファイル([ChromeまたはFirefoxでHARファイルを生成する方法](#))
- ブラウザのWebRTC内部ダンプ - chrome://webrtc-internalsまたはedge://webrtc-internals -

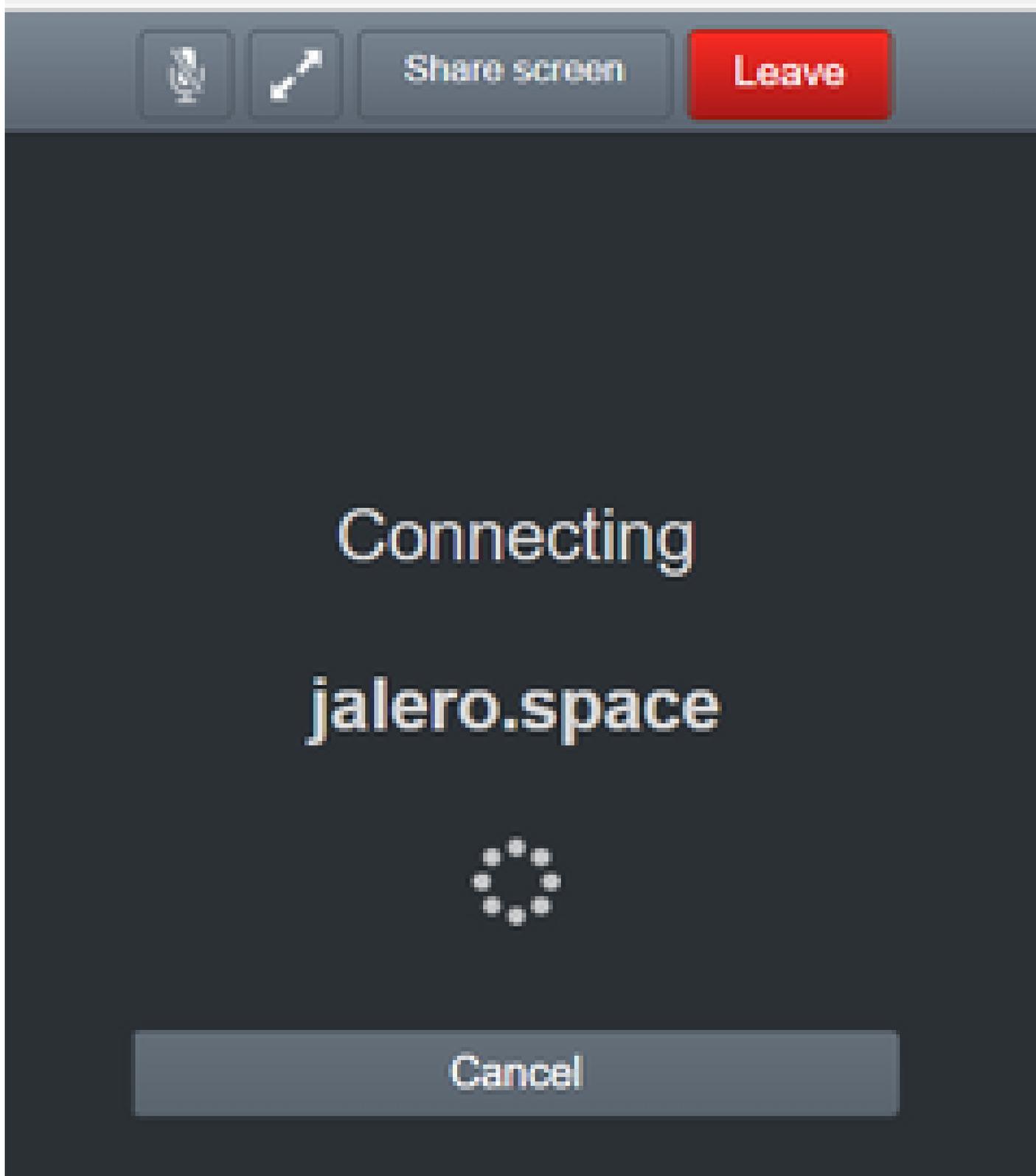
Joinが試行されるとすぐにダンプを作成します。

- ブラウザのコンソールログも役立ちます。
- クライアント、Exp E、Exp C、およびCMSからのWiresharkキャプチャ
- Exp E network.http.trafficserverデバッグは、websocketのトラブルシューティングに役立ちます。

外部 WebRTC クライアントは接続しているが、メディアがない ( ICE 障害のため )

このシナリオでは、RTCクライアントはコールIDをjalero.spaceに解決できますが、自分の名前を入力してJoin callを選択すると、次の図に示すようにクライアントにConnectingと表示されます

。



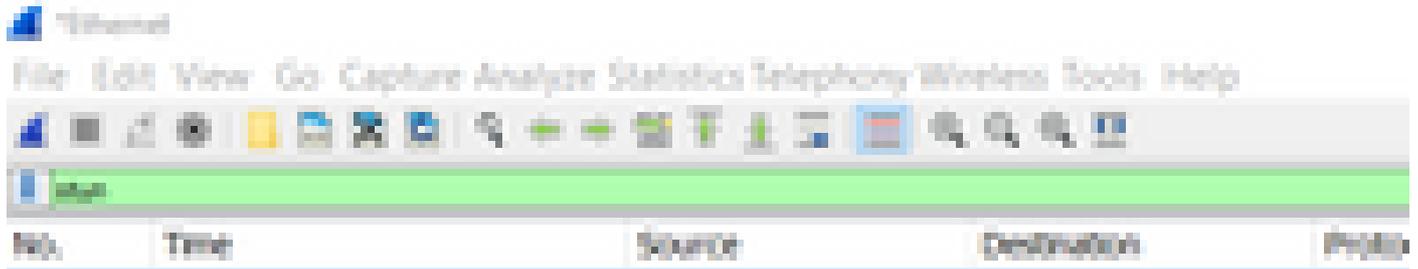
約 30 秒後に、最初の WB ページにリダイレクトされます。

トラブルシューティングを行うには、次の手順を実行します。

- コールを試みたときにRTCクライアントでwiresharkを起動し、障害が発生したらキャプチャを停止します。
- この問題が発生した後、CMSイベントログを確認します。

CMS WebAdminでLogs > Event logsの順に移動します。

- stunを使用してWiresharkトレースをフィルタリングします。例：



Wireshark トレースで、クライアントが設定されたクレデンシャルを使用して Allocate 要求をポート 3478 上の Expressway-E TURN サーバに送信していることがわかります。

```
1329    2017-04-15 10:26:42.108282    10.55.157.229    10.48.36.248    STUN    186
    Allocate Request UDP user: expturncreds realm: TANDBERG with nonce
```

サーバは Allocate エラーで応答します。

```
1363    2017-04-15 10:26:42.214119    10.48.36.248    10.55.157.229    STUN    254
    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 431
    (*Unknown error code*) Integrity Check Failure
```

または

```
3965    2017-04-15 10:34:54.277477    10.48.36.248    10.55.157.229    STUN    218
    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 401
    (Unauthorized) Unauthorized
```

CMSログに、次のログメッセージが表示されます。

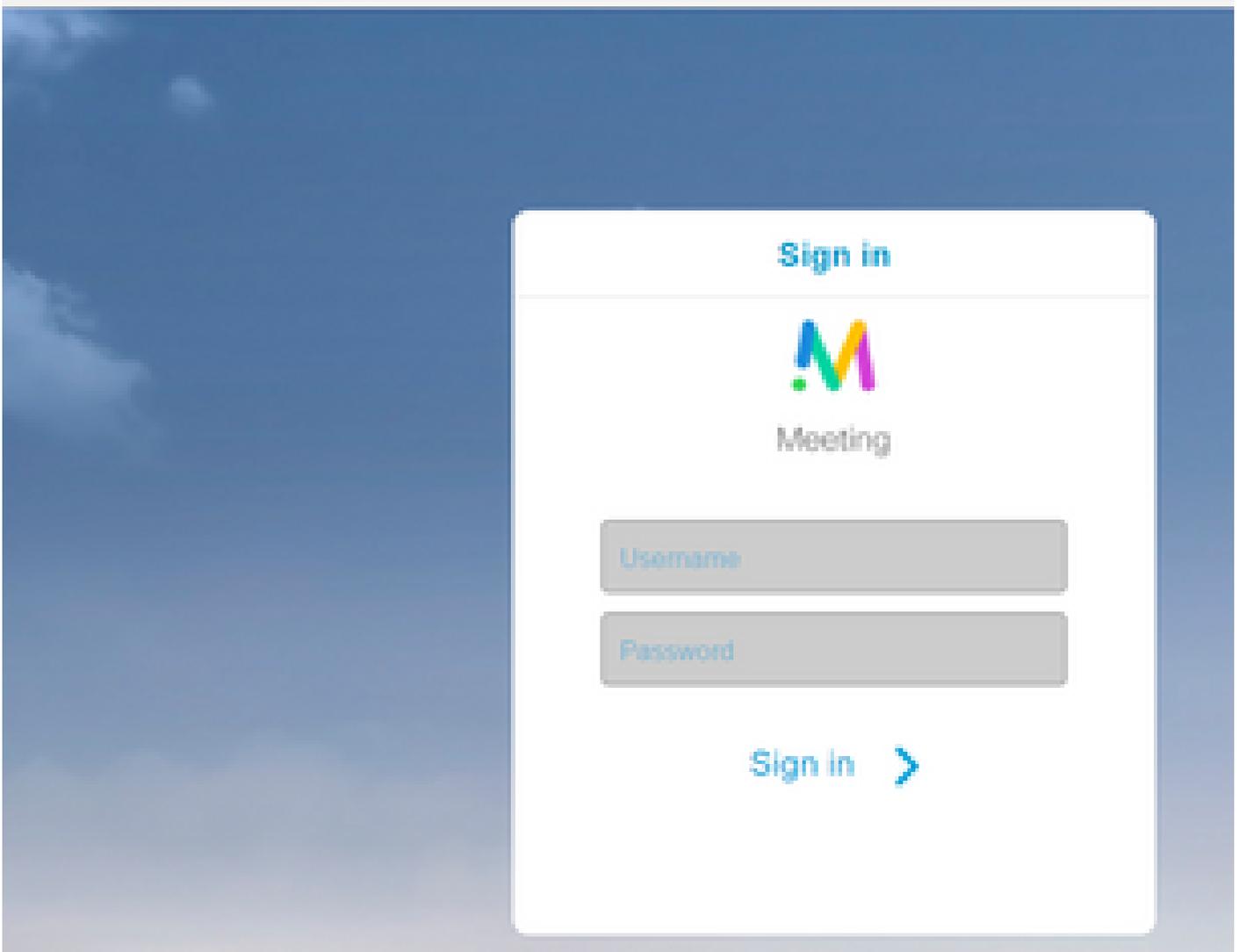
```
2017-04-15    10:34:56.536    Warning    call 7: ICE failure 4 (unauthorized - check credentials)
```

ソリューション：

CMSで設定されているTURNクレデンシャルをチェックし、それがExpressway-Eローカル認証データベースで設定されているものと一致することを確認します。

外部 WebRTC クライアントが Join Call オプションを取得しない

⚠ Not secure | <https://webbridge.alero.aca>



コールブリッジの [Status] > [General] ページに、以下のように表示されます。

```
2017-04-15 12:09:06.647 Web bridge connection to "webbridge.alero.aca" failed (DNS failure)
2017-04-15 12:10:11.634 Warning web bridge link 2: name resolution for "webbridge.alero.aca" f
2017-04-15 11:55:50.835 Info failed to establish connection to web bridge link 2 (unknown erro
```

ソリューション :

- CallbridgeがJoin URLをwebbridge FQDNに解決できることを確認します ( CallbridgeはこれをExpressway-EのIPアドレスに解決できません )。
- コマンド `dns flush` を使用して、コマンドライン インターフェイス ( CLI ) 経由で、コールブリッジ上の DNS キャッシュをフラッシュします。
- WB がコールブリッジ サーバ証明書 ( 発行元ではなく ) を信頼していることを確認します。

外部 WebRTC クライアントが cospace への接続時に (ロード中のメディアで) スタックし、WBの最初のページにリダイレクトされる

ソリューション :

- CMSがCBドメインの内部ネットワークで\_xmpp-client SRVレコードを解決できること、およびWebRTC接続が内部で機能することを確認します。
- 外部クライアントとの接続を試みている間に、クライアントでWiresharkキャプチャを収集し、Expressway-Eでtcpdumpを含む診断ログを収集します。

Maintenance > Diagnostics > Diagnostic loggingの順に移動し、Start new logを選択する前に、次の図に示すようにTake tcpdump while loggingにチェックマークが入っていることを確認します。



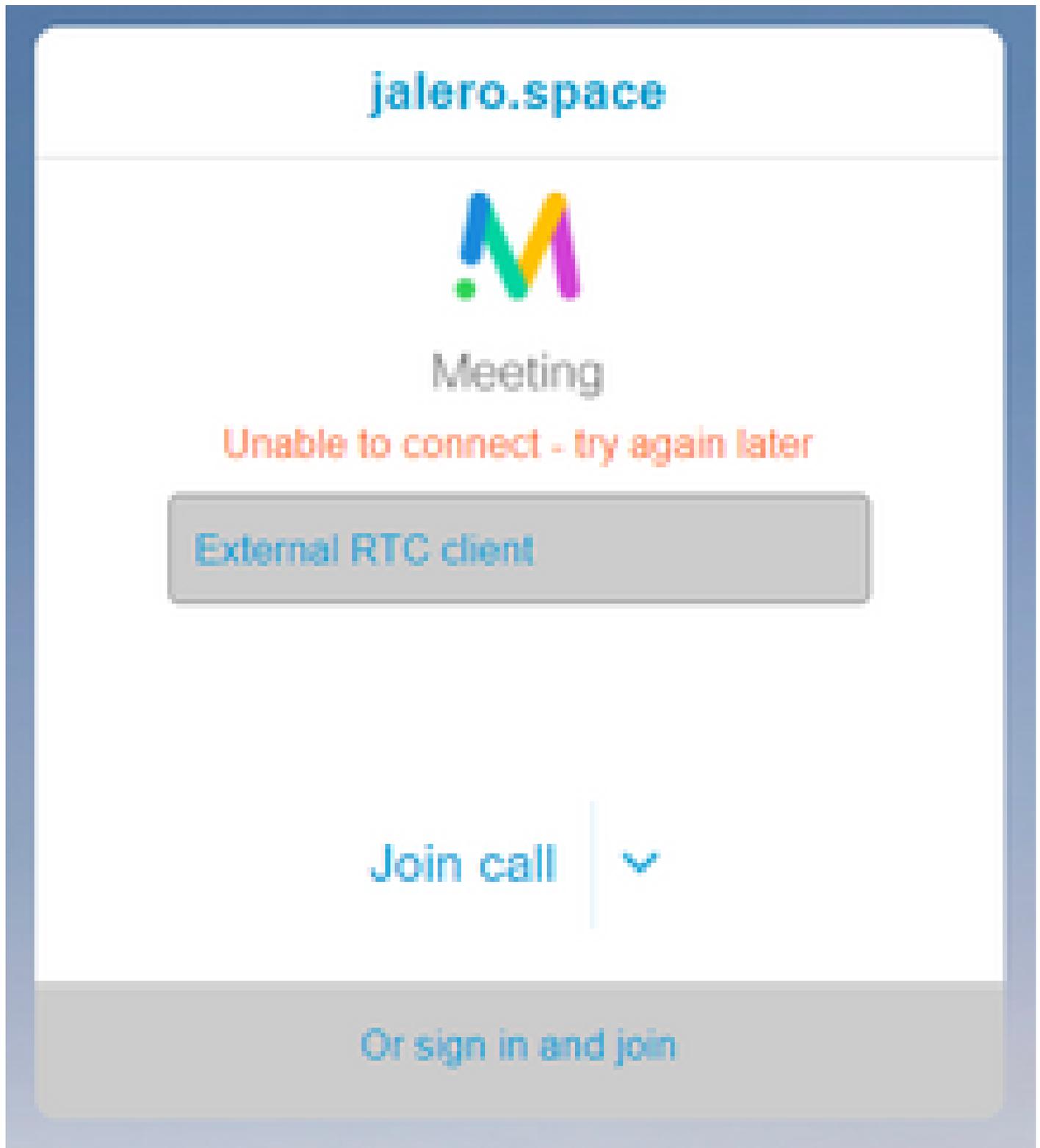
 注 : 障害が発生したコールを再現する前に、クライアントのデバイスのWiresharkキャプチャとExpressway-Eのロギングが開始されていることを確認してください。障害が発生したコールが再現されたら、Expressway-Eでのロギングとクライアントでのキャプチャを停止してダウンロードします。

- Expressway-Eからダウンロードしたログバンドルを解凍し、パブリック側インターフェイスで取得した.pcapファイルを開きます。
- stunを使用して両方のパケットキャプチャをフィルタリングします。
  - 次に、外部クライアントからExpressway-EパブリックIPアドレスへのバインディング要求を探して右クリックし、Follow > UDP Streamの順に選択します。
  - 通常、クライアントからのバインディング要求の宛先ポートは24000 ~ 29999の範囲にあり、これはExpressway-E上のTURNリレーポートの範囲です。
- クライアント側でバインディング要求に対する応答が受信されない場合、要求が到着しているかどうかをExpressway-Eのキャプチャで確認します。
- 要求が着信していて、Expressway-Eがクライアントに応答している場合は、外部FWが発信UDPトラフィックを許可しているかどうかを確認します。
- 要求が届かない場合は、FWをチェックして、前述のポート範囲がブロックされていないことを確認します。
- Expressway-Eが、スタティックNATモードが有効なデュアルネットワークインターフェイスコントローラ(DUAL-NIC)を使用して導入され、X12.5.2以前である場合は、NATリフレクションが外部FWでサポートされ、設定されていることを確認します。X12.5.3では、スタンドアロンのExpresswayでは必要なくなりました。

外部 WebRTC クライアントが cospace に参加できず、警告が表示される (接続不可 - 後でやり

直す )

このシナリオでは、RTCクライアントはコールIDをjalero.spaceに解決できますが、自分の名前を入力してJoin callを選択すると、すぐにUnable to connect - try again laterという警告が表示されます。



ソリューション :

CMS が内部ネットワークで常に CB ドメインの \_xmpp-client SRV レコードを解決できることを確認します。

## 関連情報

- [VCS/Expressway IP ポート使用ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。