Configurer le proxy WebRTC avec CMS sur Expressway avec double domaine

Contenu

Introduction

Ce document décrit un exemple de configuration du proxy Web Real-Time Communication (WebRTC) pour Cisco Meeting Server (CMS) via Expressway avec des domaines internes et externes différents.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur ces sujets :

- Déploiement combiné unique CMS version 2.1.4 et ultérieure
- Expressway C et Expressway E version X8.9.2 et ultérieure
- Callbridge et webbridge configurés sur CMS
- Accès mobile et à distance (MRA) activé sur la paire Expressway
- Clé d'option Traversal Using Relay NAT (TURN) ajoutée à l'Expressway-E

- Enregistrement DNS (Domain Name Server) externe résolvable pour l'URL du pont Web, pour le domaine externe
- Enregistrement DNS interne résolu pour l'adresse IP CMS de domaine externe à interne
- Extensible Messaging and Presence Protocol (XMPP) multidomaine configuré sur CMS, pour les domaines interne et externe
- Le Port 443 TCP est ouvert sur le pare-feu de l’Internet public à l’adresse IP publique de l’Expressway-E
- Le port TCP et UDP 3478 s’est ouvert sur le pare-feu depuis Internet public jusqu’à l’adresse IP publique de l’Expressway-E
- Plage de ports UDP 24000-2999 ouverte sur le pare-feu depuis et vers l’adresse IP publique de l’Expressway-E

Components Used

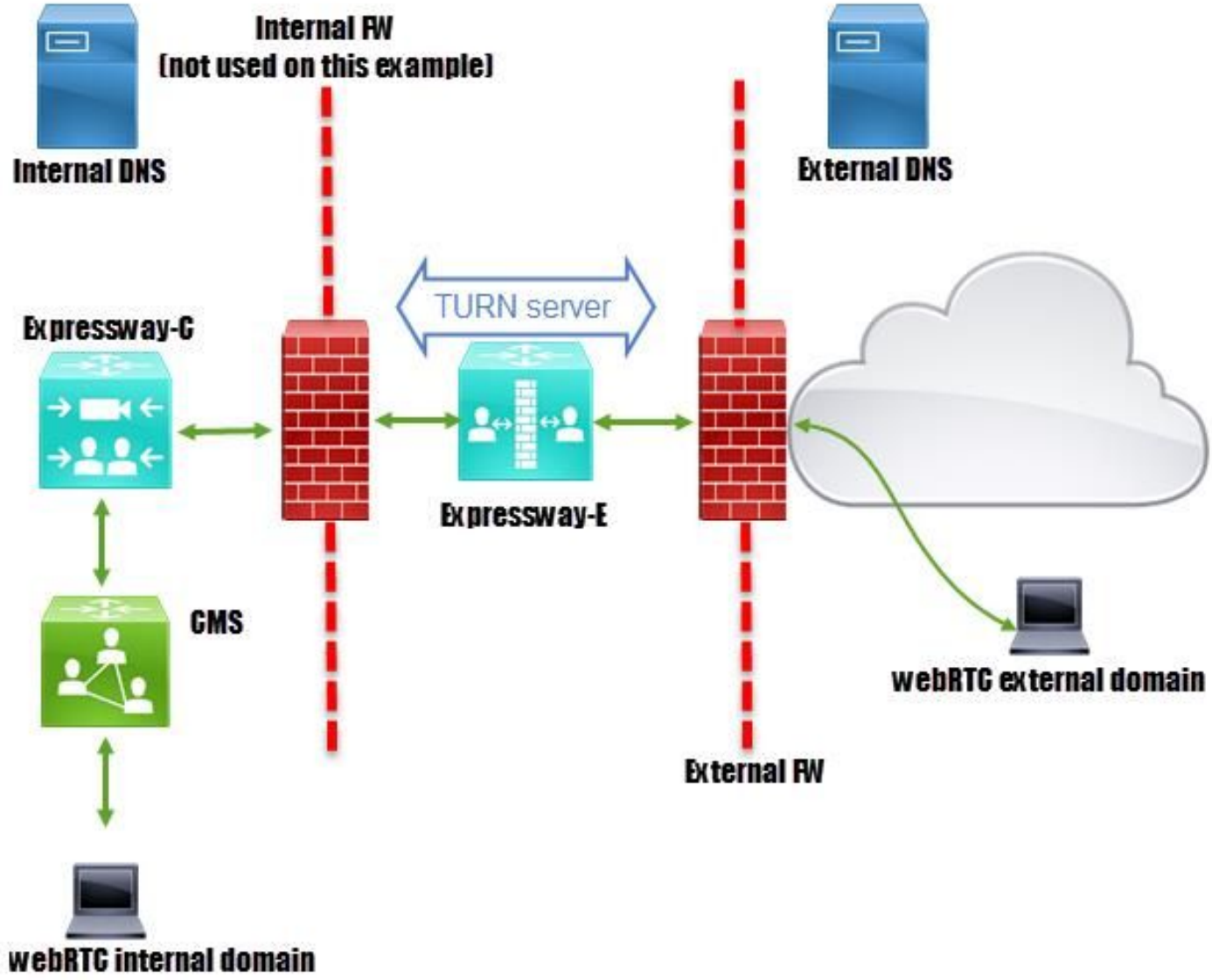
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Déploiement combiné unique CMS version 2.2.1
- Expressway-C et Expressway-E avec deux cartes d’interface réseau (NIC) et logiciel NAT (Network Address Translation) version X8.9.2
- POSTMAN

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Diagramme du réseau

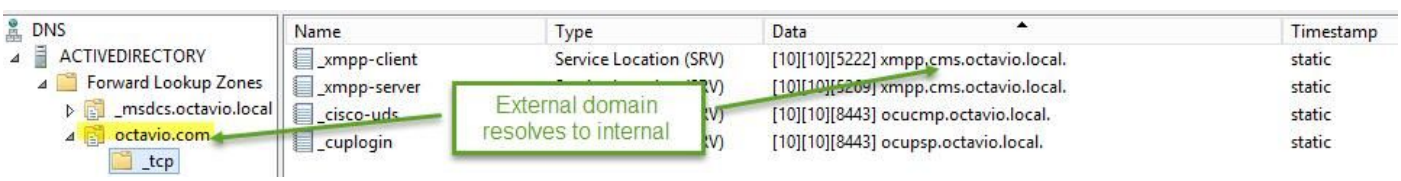


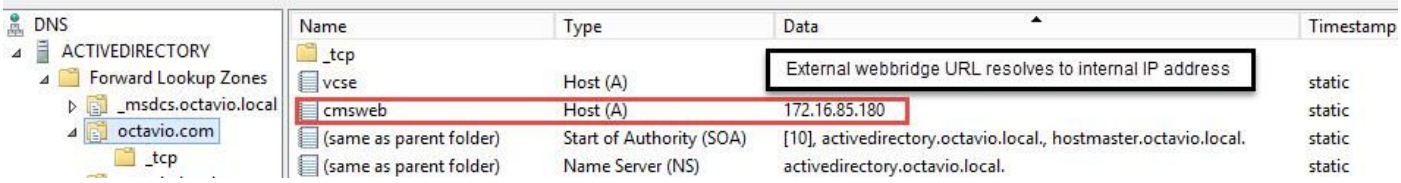
Informations techniques

Domaine interne	cms.octavio.local
Domaine externe	octavio.com
Adresse IP CMS	172.16.85.180
Adresse IP Expressway-C	172.16.85.167
Adresse IP du réseau local LAN1 Expressway-E (interne)	172.16.85.168
Adresse IP LAN2 Expressway-E (externe)	192.168.245.61
Adresse IP NAT statique	10.88.246.156

Configuration DNS

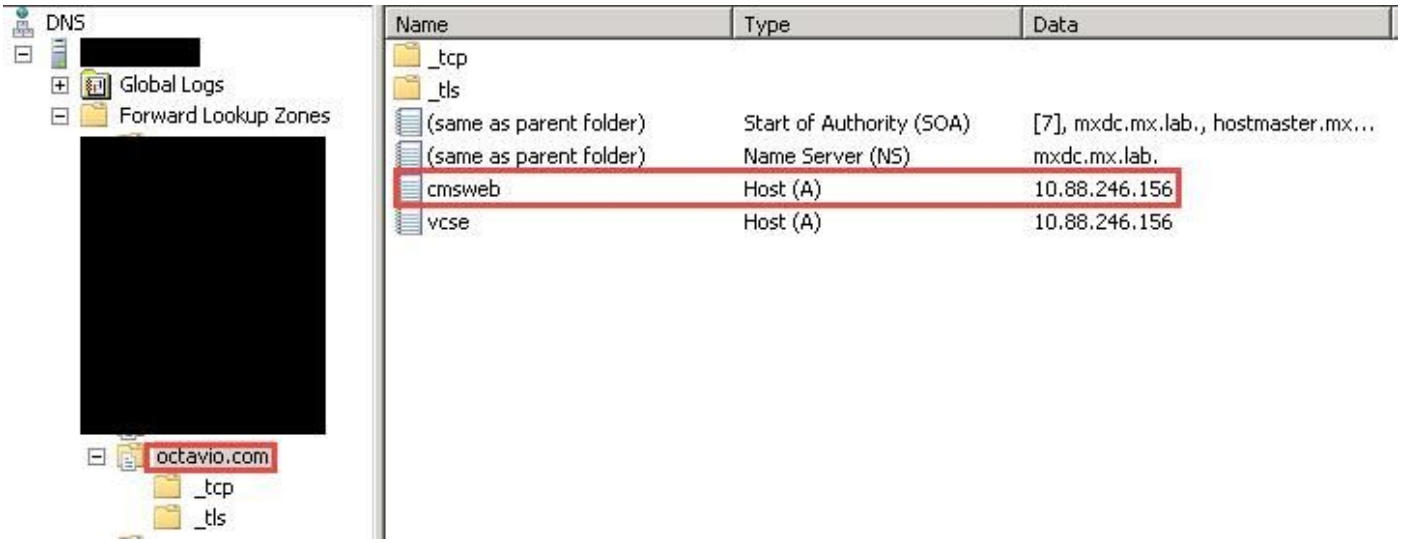
Configuration DNS interne





Configuration DNS externe

Le DNS externe doit disposer de l'URL du pont Web qui se résout à l'adresse IP NAT statique de l'Expressway-E, comme l'illustre l'image.



Configuration CMS, Callbridge, Webbridge et XMPP

Étape 1. La licence callbridge doit être activée. L'image montre une licence callbridge active.

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

Pour plus d'informations sur les licences :

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

Étape 2. Activez callbridge, webbridge et XMPP via MMP comme l'illustre l'image.

```
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
```

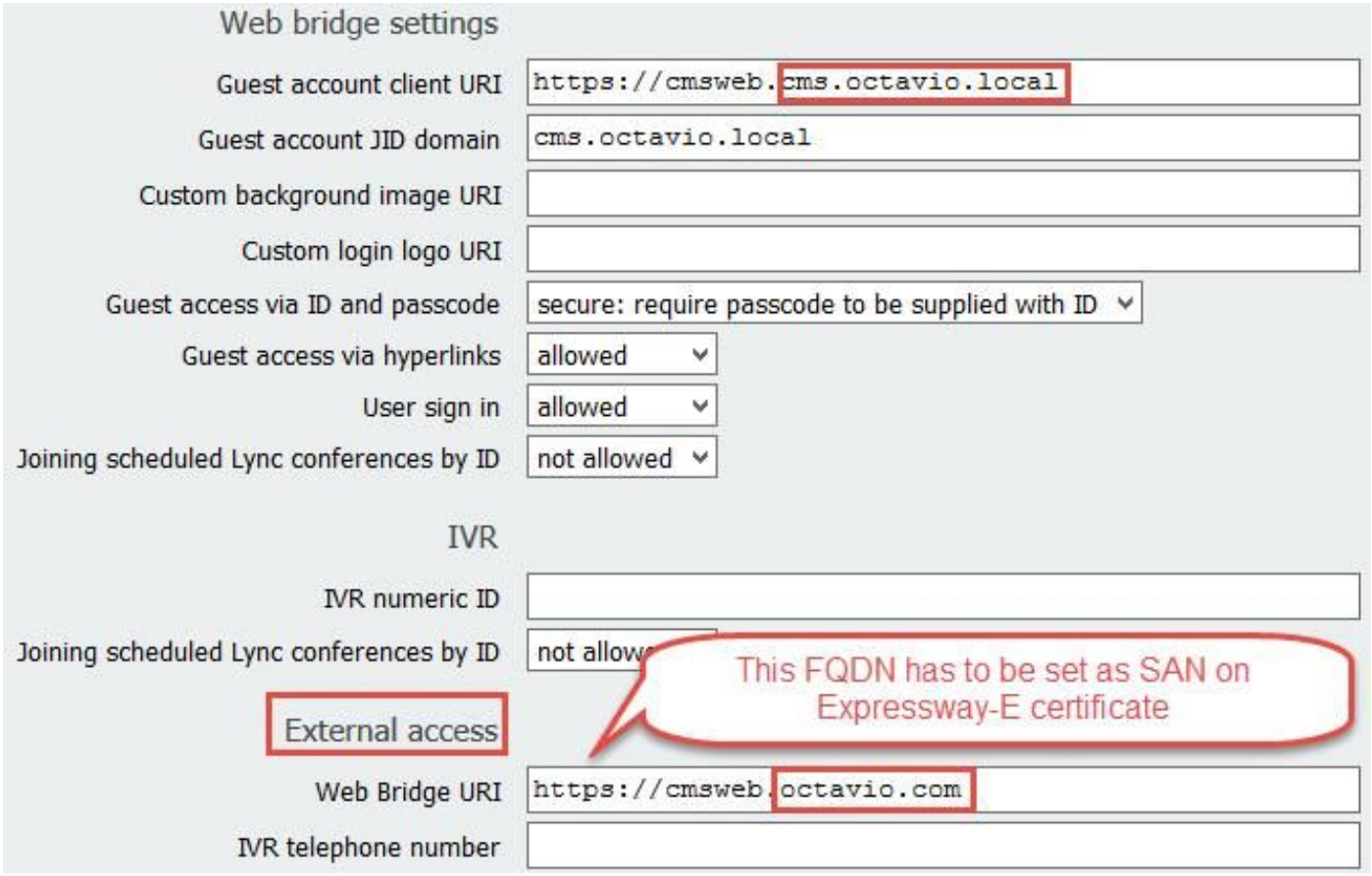
Suivez ce lien pour obtenir des détails sur la façon de les activer :

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

Suivez ce lien pour obtenir des détails sur la création d'un certificat :

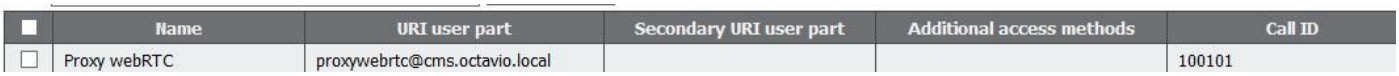
http://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-2/Certificate-Guidelines-Single-Combined-Server-Deployment-2-2.pdf

Étape 3. Accédez à la page Web CMS sur **Configuration > General** et configurez l'URL interne et externe du pont Web comme indiqué dans l'image.



Note: Le CMS doit être configuré avec au moins un espace.

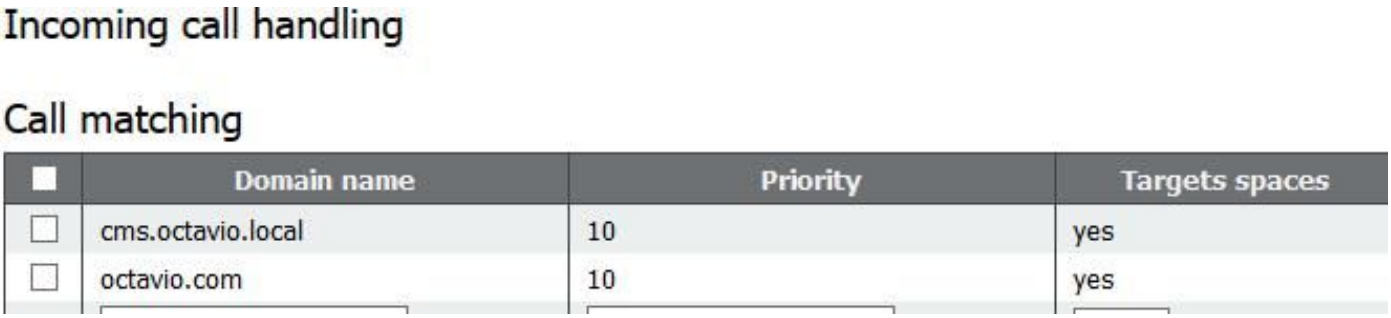
Exemple d'espace configuré sur CMS, comme illustré dans l'image.



	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
☐	Proxy webRTC	proxywebrtc@cms.octavio.local			100101

Note: Les appels entrants doivent être configurés pour les domaines interne et externe

Un exemple de domaines configurés pour la gestion des appels entrants est illustré dans l'image.



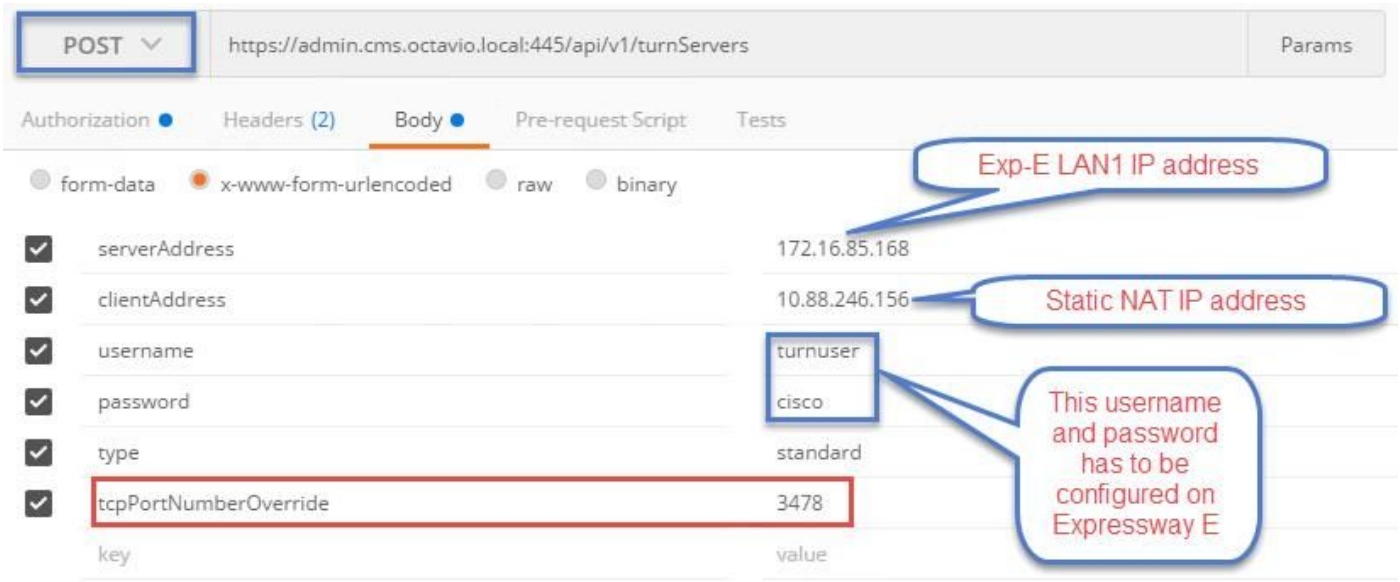
	Domain name	Priority	Targets spaces
☐	cms.octavio.local	10	yes
☐	octavio.com	10	yes

Configuration TURN

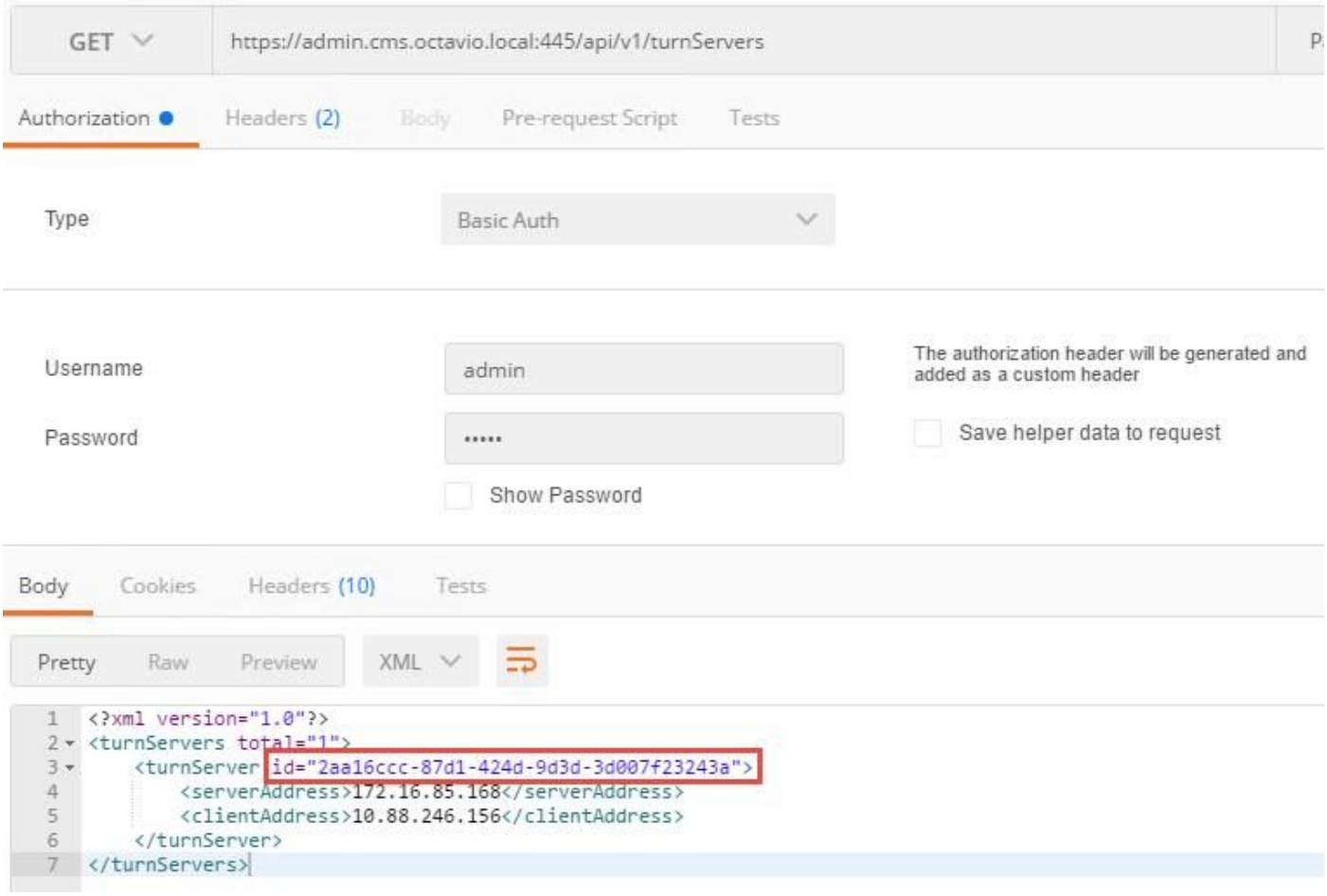
Étape 1. TURN doit être configuré par l'API via Postman. Cette commande est utilisée dans toute la configuration.

https://

Étape 2. Utilisez la méthode POST et accédez à **Body** pour afficher les paramètres du serveur TURN ou les modifier. Les paramètres configurés sur le serveur TURN sont tels qu'ils apparaissent dans l'image.

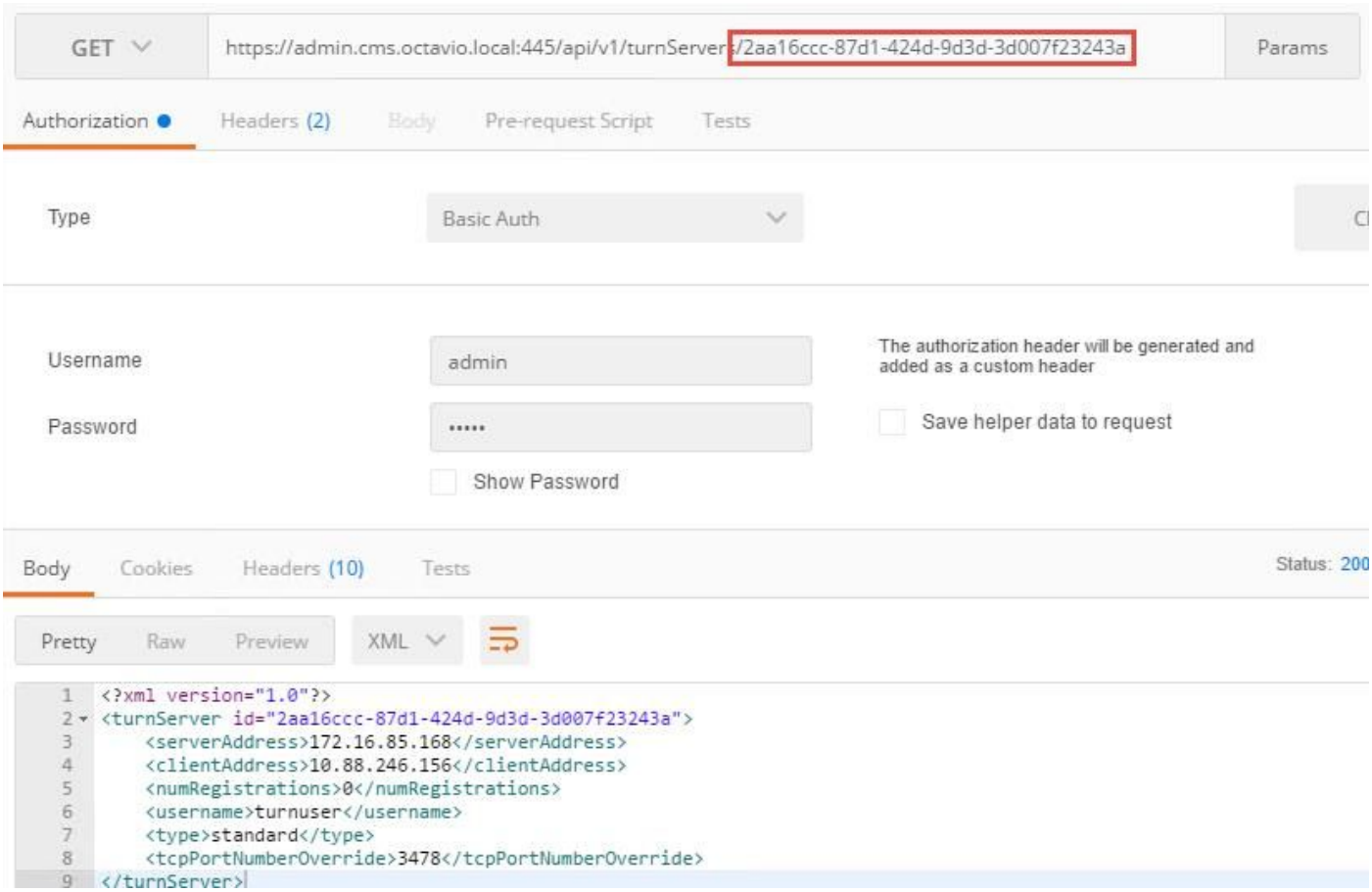


Étape 3. Vérifiez l'état de la configuration du serveur TURN en exécutant la méthode GET et copiez l'ID du serveur. L'ID qui doit être copié est tel qu'illustré dans l'image.

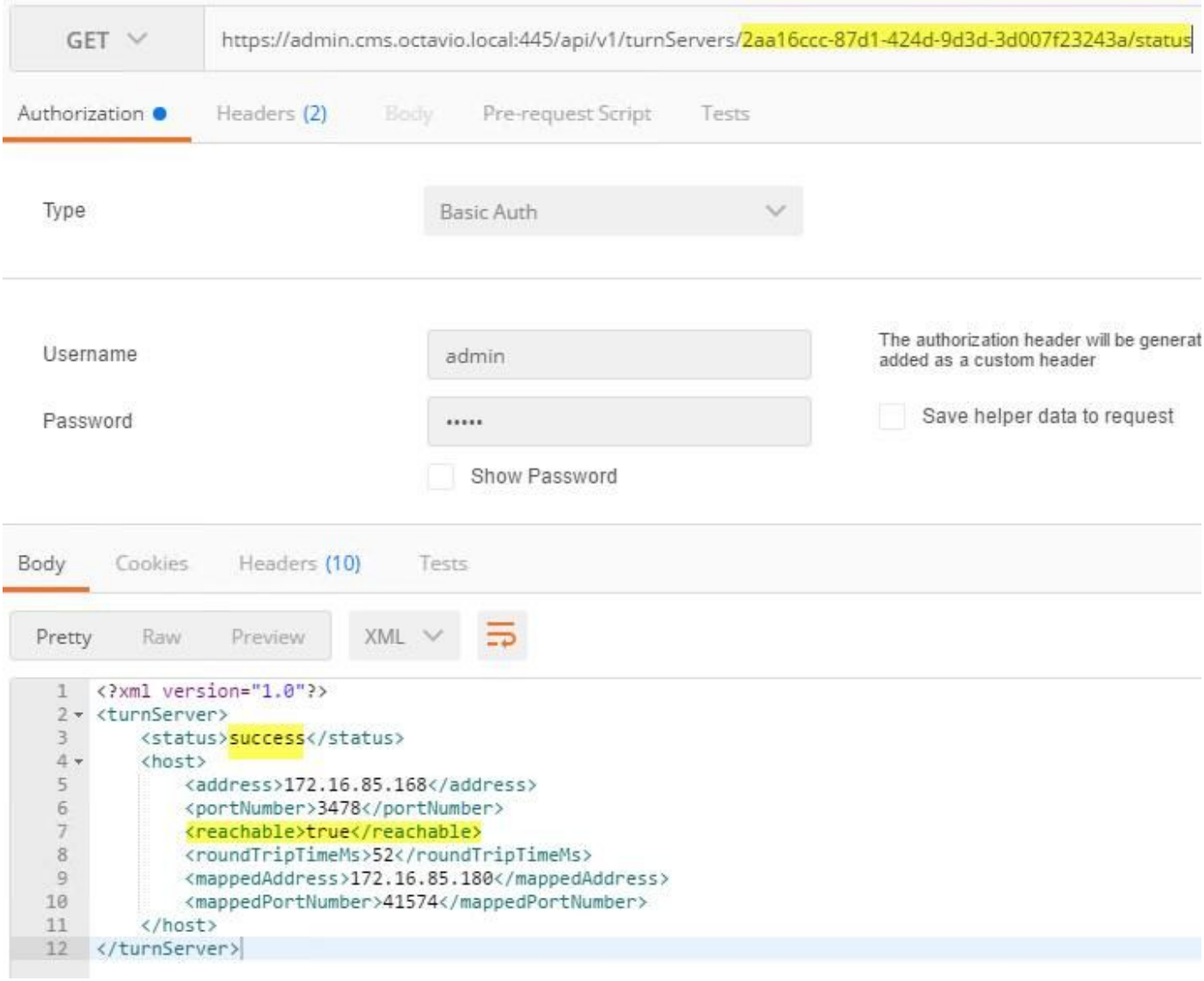


Étape 4. Copiez l'ID à la fin de la commande API et utilisez la méthode GET afin de voir les informations du serveur TURN comme indiqué dans l'image.

Note: Les informations n'affichent pas le mot de passe du serveur.

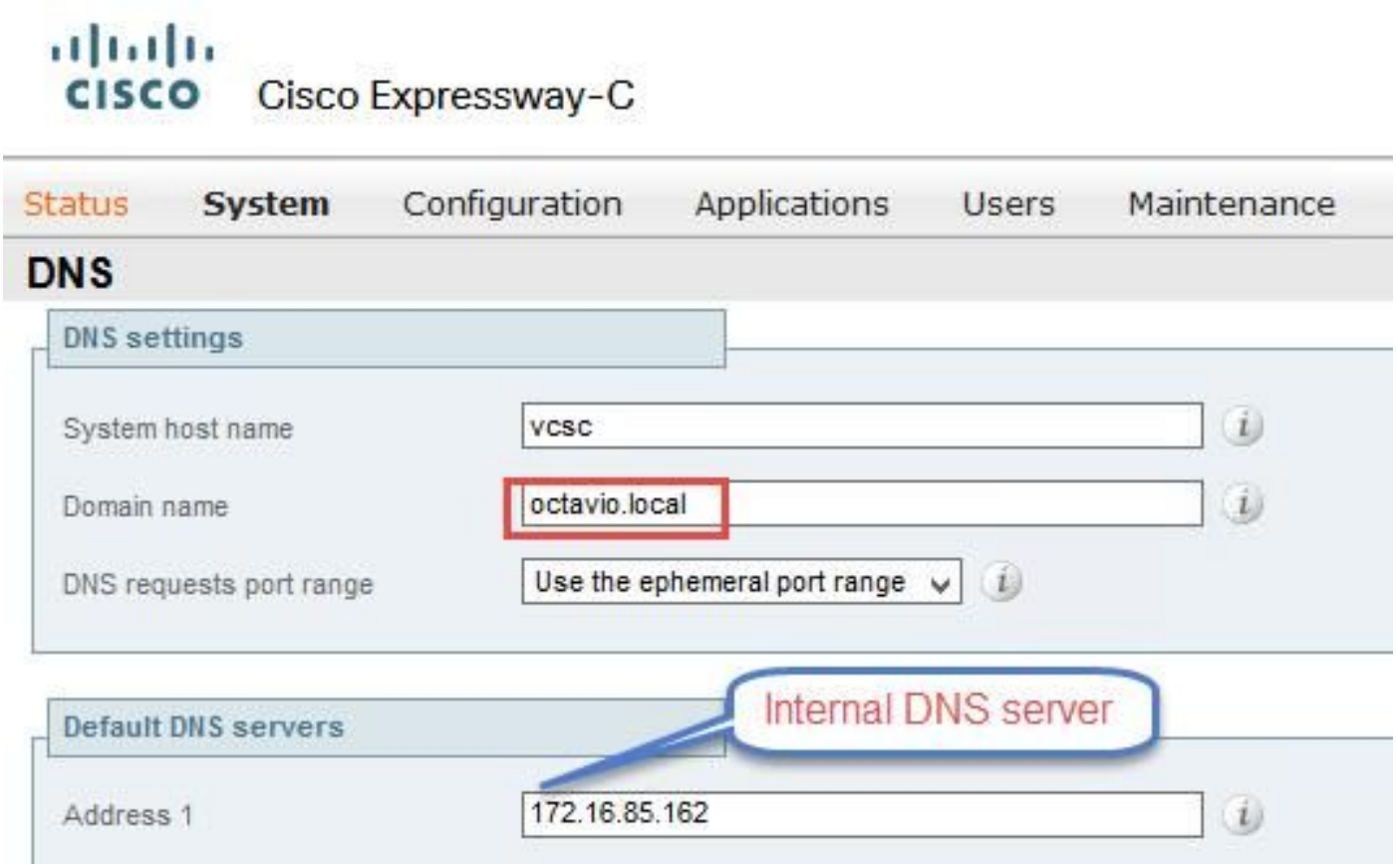


Étape 5. Cliquez sur **Envoyer** pour obtenir l'état du serveur. Exemple de configuration réussie comme illustré dans l'image.



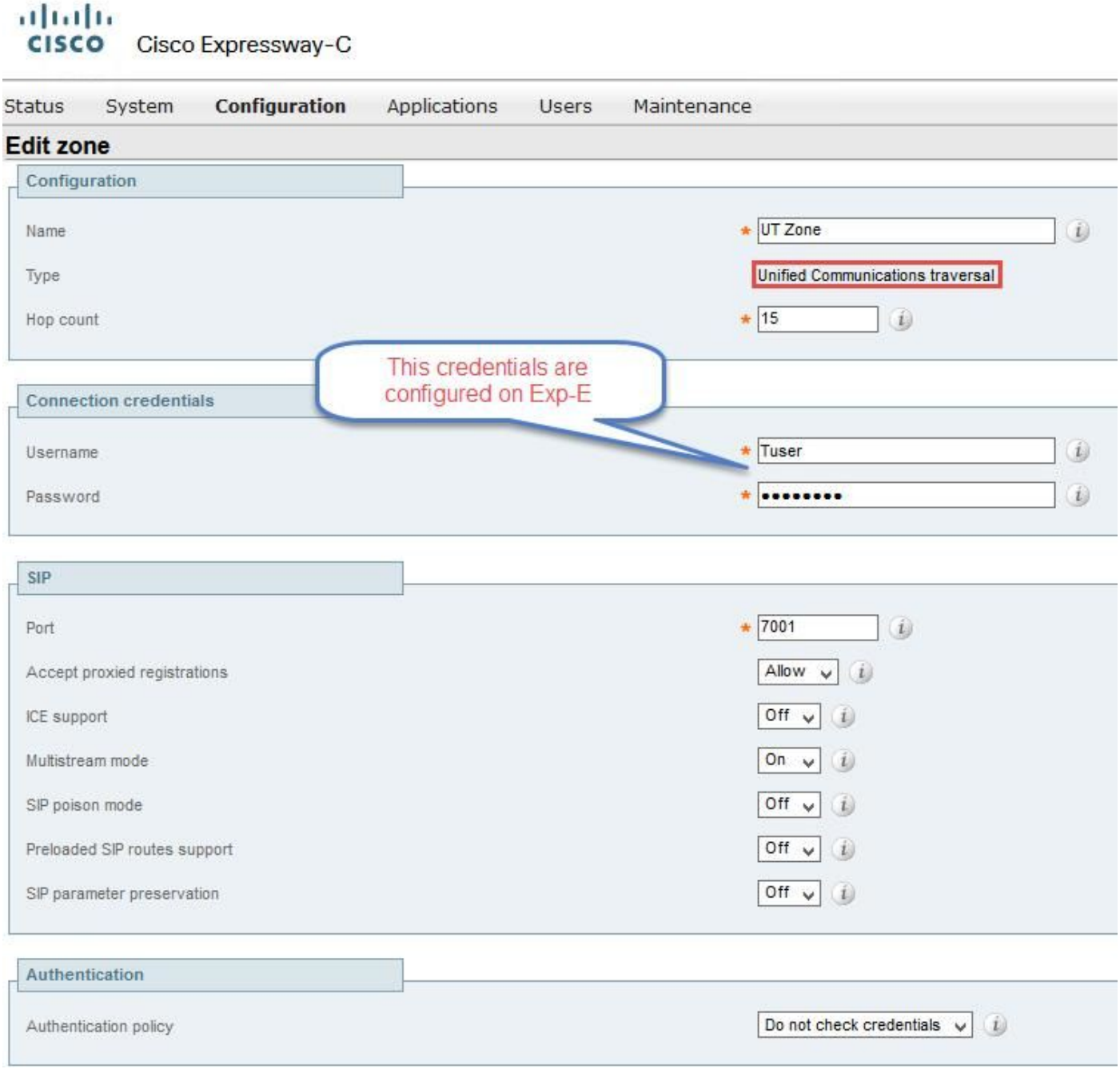
Configuration d'Expressway-C et d'E

Étape 1. L'autoroute-C doit avoir le domaine interne (octavio.local) et l'Expressway-E doit avoir le domaine externe (octavio.com) configuré comme indiqué dans l'image.



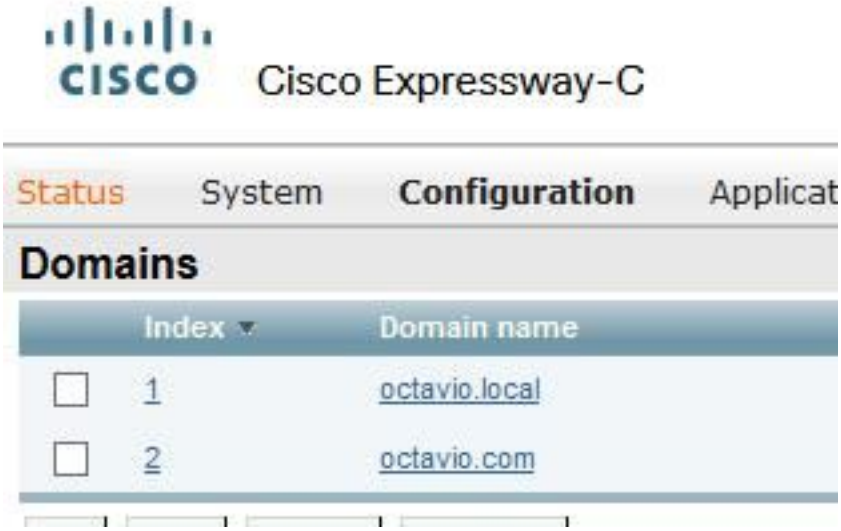
Étape 2. MRA doit être activé sur Expressway C et E comme le montre l'image.

Étape 3. Créez une zone de traversée de communications unifiées entre l'Expressway-C et l'E comme illustré dans l'image.

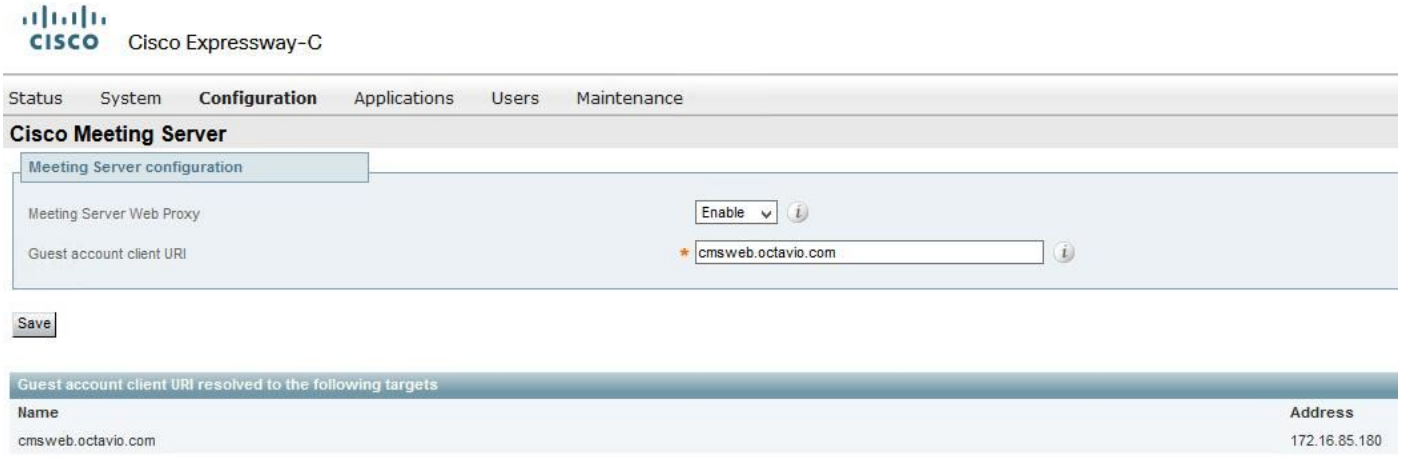


Configuration sur Expressway-C

Étape 1. Configurez le domaine interne et externe sur l'Expressway-C comme indiqué dans l'image.



Étape 2. Activez la configuration de Cisco Meeting. Naviguez jusqu'à **Configuration > Unified Communications > Cisco Meeting Server (Configuration > Communications unifiées > Serveur de réunion Cisco**. Configurez l'URL du pont Web externe sur le champ URI du client de compte invité comme indiqué dans l'image.



Note: Le DNS interne doit résoudre l'URL du pont Web externe (cmsweb.octavio.com) en adresse IP interne du pont Web CMS. Dans cet exemple, l'adresse IP est 172.16.85.180.

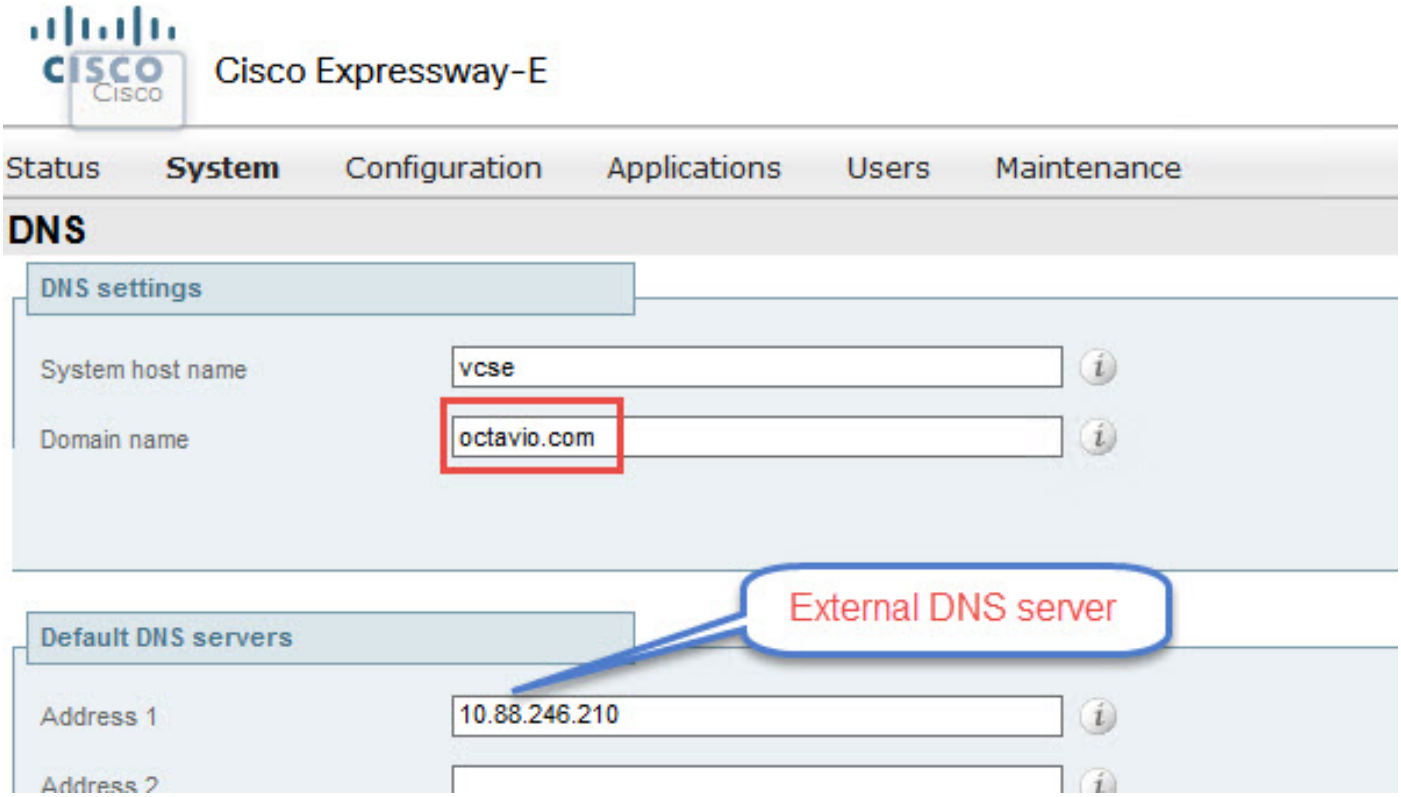
Les tunnels Secure Shell (SSH) de l'Expressway-C doivent être actifs après quelques secondes comme le montre l'image.

Remarque : le serveur doit avoir un certificat de serveur et un certificat d'autorité de certification.

Configuration sur Expressway-E

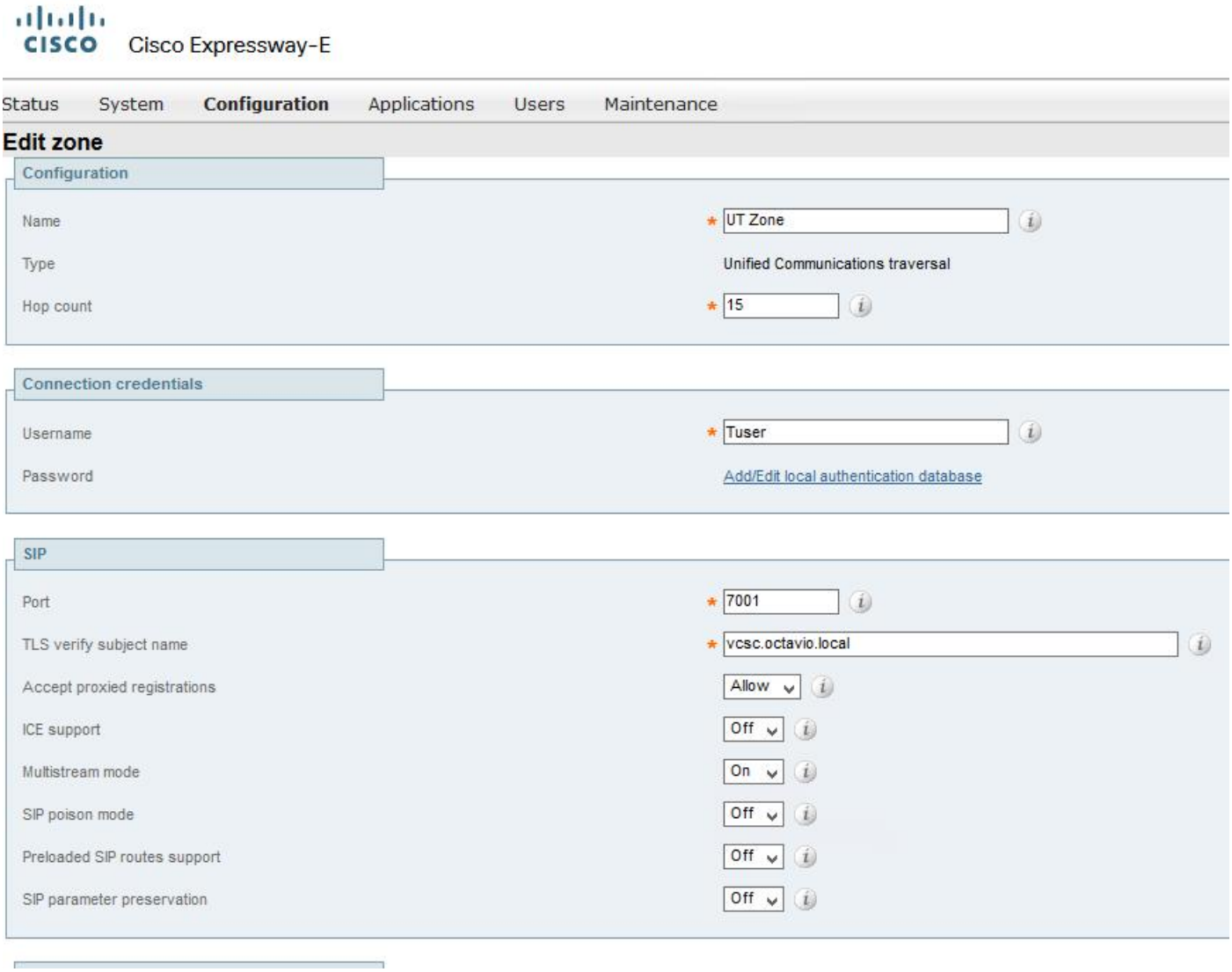
Étape 1. L'autoroute E doit avoir une licence TURN comme le montre l'image.

Étape 2. L'Expressway-E doit être configuré avec le domaine externe tel qu'illustré dans l'image.



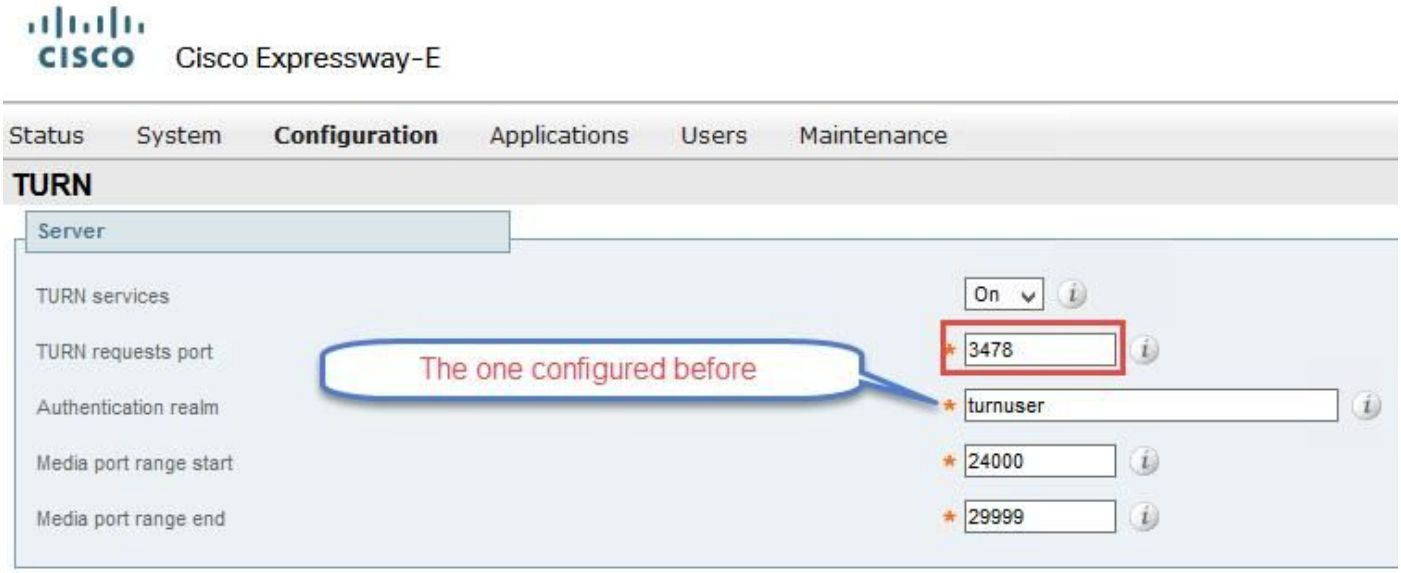
Étape 3. Créez des utilisateurs pour le serveur TURN et pour la zone de traversée de communications unifiées comme indiqué dans l'image.

Étape 4. Créez une zone de traversée de communications unifiées comme indiqué dans l'image.



Étape 5. Configurez le serveur TURN. Accédez à **Configuration > Traversée > TURN** comme indiqué dans l'image.

> **Note**: La requête TURN doit être envoyée au port 3478, car il s'agit du port où le client Web demande la connexion TURN.



Une fois que le bouton Activer apparaît, l'état affiche Actif comme indiqué dans l'image.

Étape 6. Accédez à **System > Administration.** Le client webRTC demande l'accès sur le port 443, c'est pourquoi le port d'administration de l'Expressway-E doit être changé en un port différent, dans cet exemple, il est changé en 445 comme indiqué dans l'image.

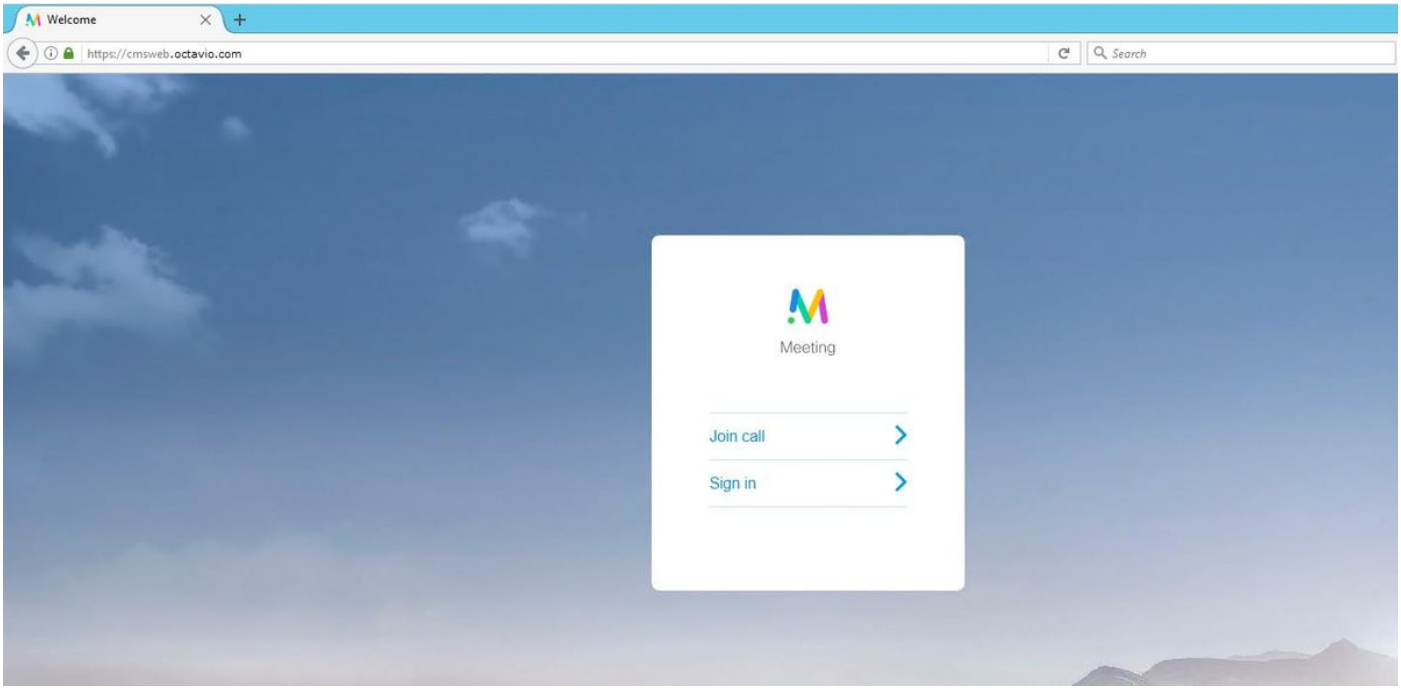
Étape 7. Création de certificat pour l'Expressway-E : l'URL de webbridge doit être ajoutée en tant que SAN sur le certificat du serveur comme indiqué dans l'image.

Vérification

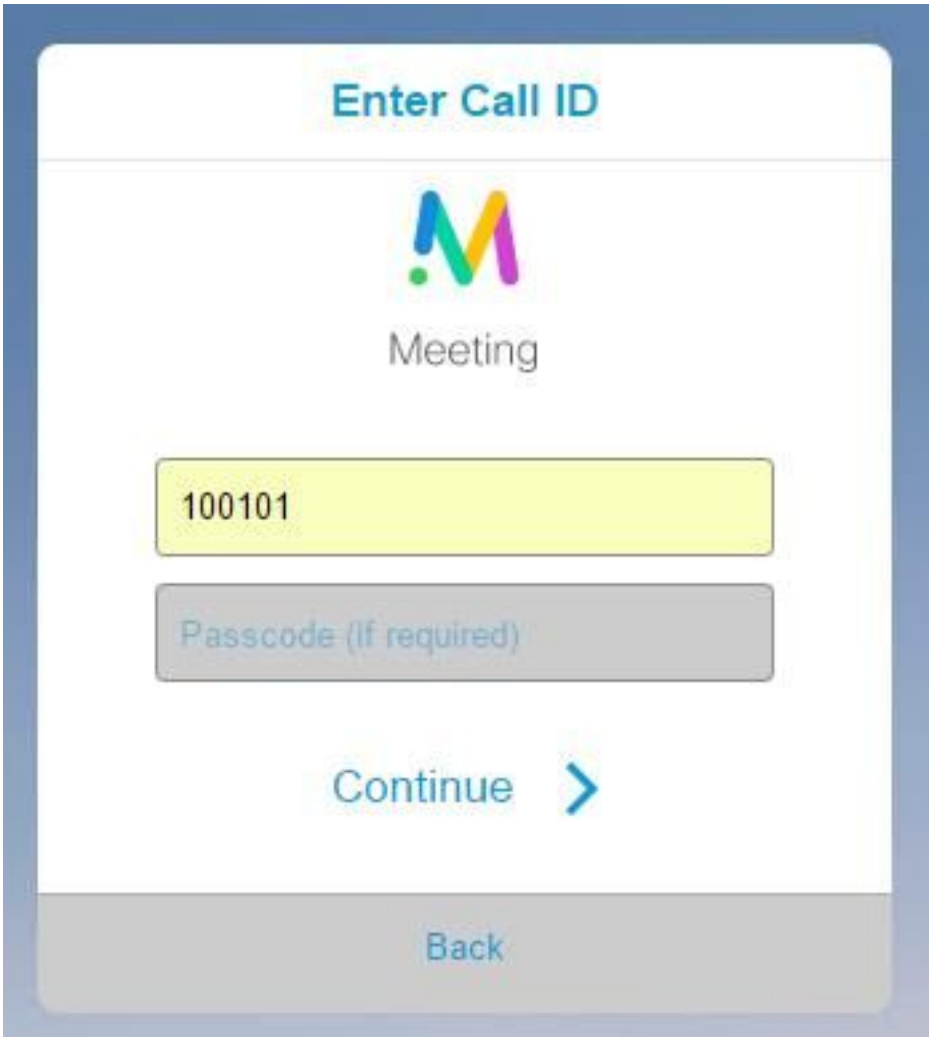
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Étape 1. Sélectionnez un navigateur Web pris en charge et saisissez l'URL du pont Web externe. L'écran suivant doit s'afficher comme indiqué dans l'image.

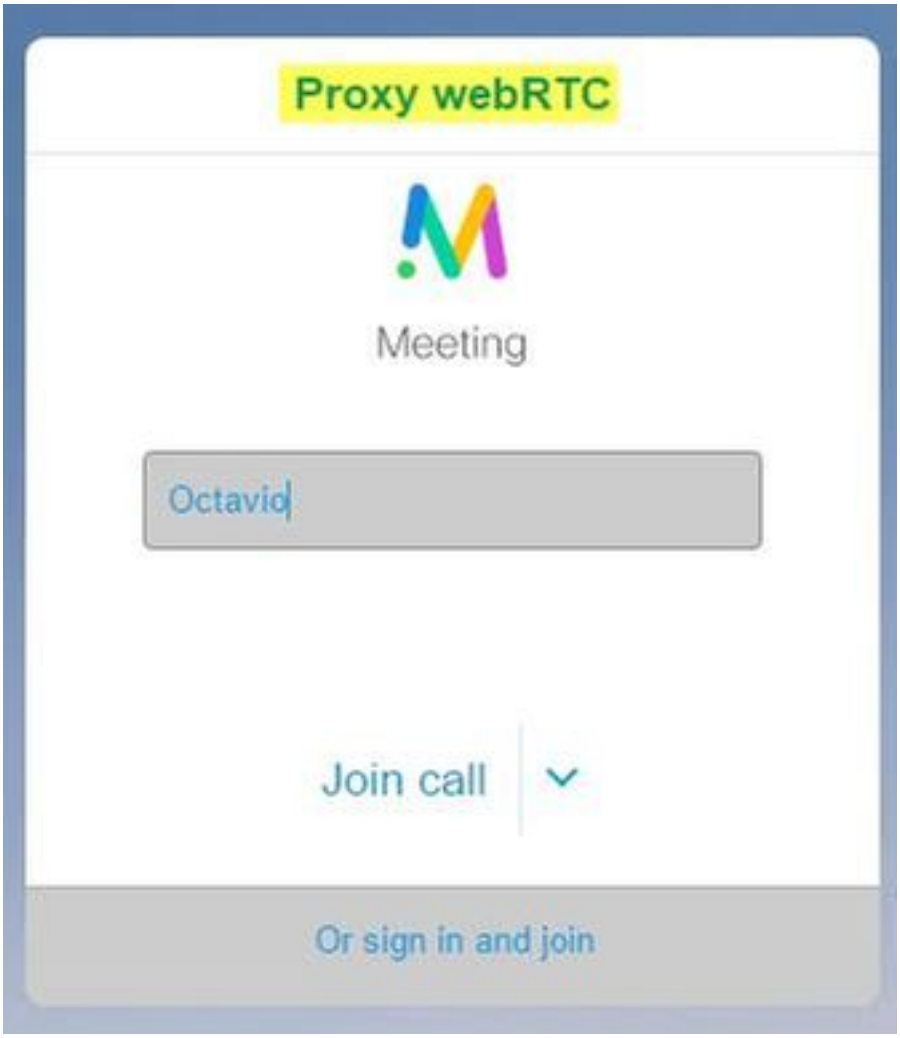
> **Note**: Vous trouverez une liste des navigateurs et des versions pris en charge sur le lien : https://kb.acano.com/content/2/4/en/what-versions-of-browsers-do-we-support-for-webrtc.html?highlight=html%5C-5%20compliant%20browsers#content



Étape 2. Sélectionnez **Joindre l'appel** et saisissez l'ID d'espace précédemment configuré comme indiqué dans l'image.



Étape 3. Cliquez sur **Continuer** et saisissez votre nom. À ce stade, vous devez voir le nom de l'espace auquel vous allez vous joindre. Dans ce cas, le nom de l'espace est Proxy webRTC**.** Cliquez sur **Joindre l'appel** comme indiqué dans l'image.



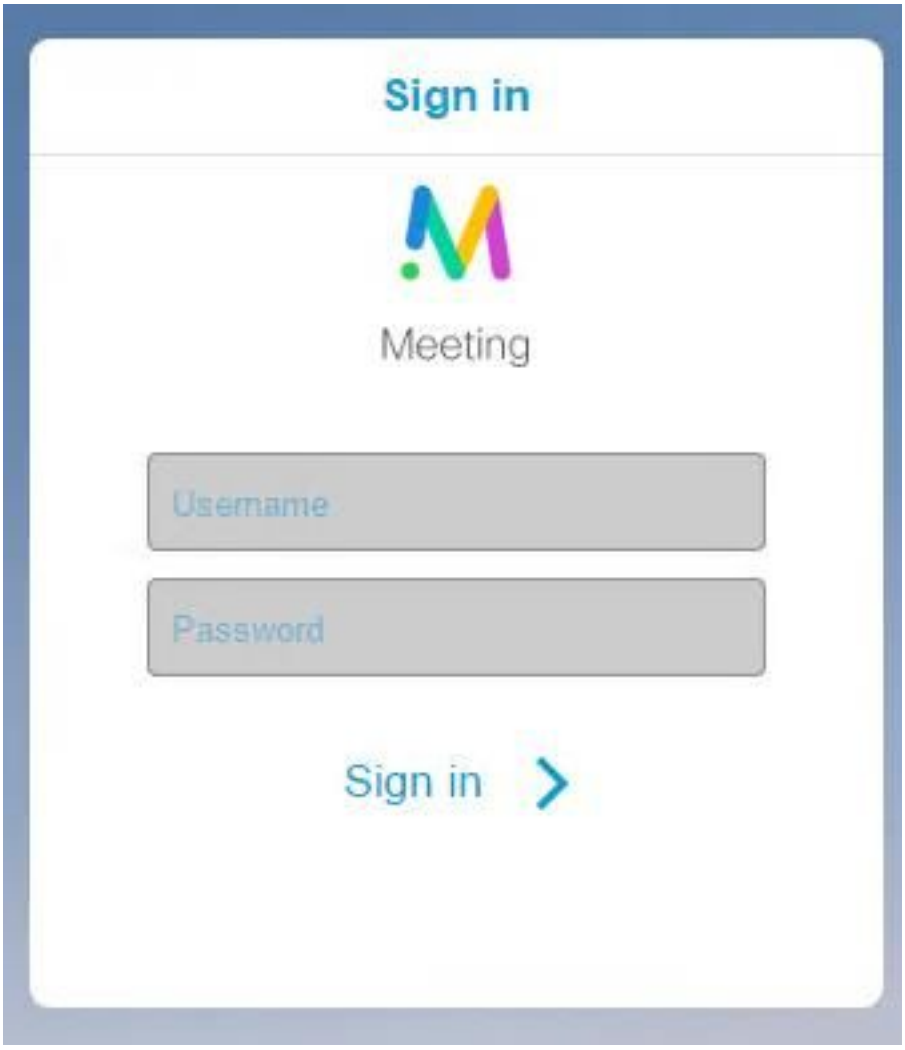
Étape 4. Rejoignez un autre périphérique et vous devez voir les deux périphériques connectés à la conférence comme indiqué dans l'image.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Le bouton Join Call n'est pas affiché

Le bouton **Joindre l'appel** n'est pas affiché lorsque vous ouvrez la page du pont Web et que vous voyez l'erreur affichée dans la deuxième image lorsque vous accédez à la page Web du CMS comme indiqué dans l'image.



Fault conditions

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

Le problème se produit lorsque le pont Web ne communique pas correctement avec le pont d'appel.

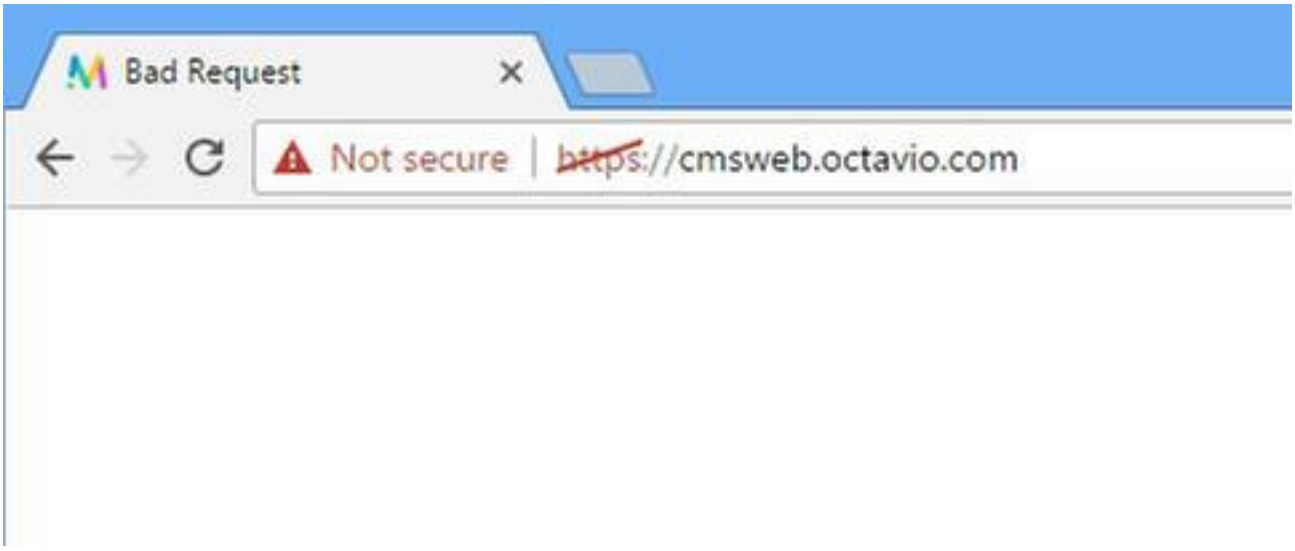
Solution

- Vérifiez que l'URL du pont Web est correctement configurée sur la page Web de l'administrateur CMS. Accédez à **Configuration > General** à cette fin.
- Le pont Web et le pont d'appel doivent se faire confiance, vérifiez que le bundle d'approbation est ajouté à la configuration de webbridge comme indiqué dans les images :

```
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>
```

Note: L'ensemble d'approbation est le certificat de pont d'appel.

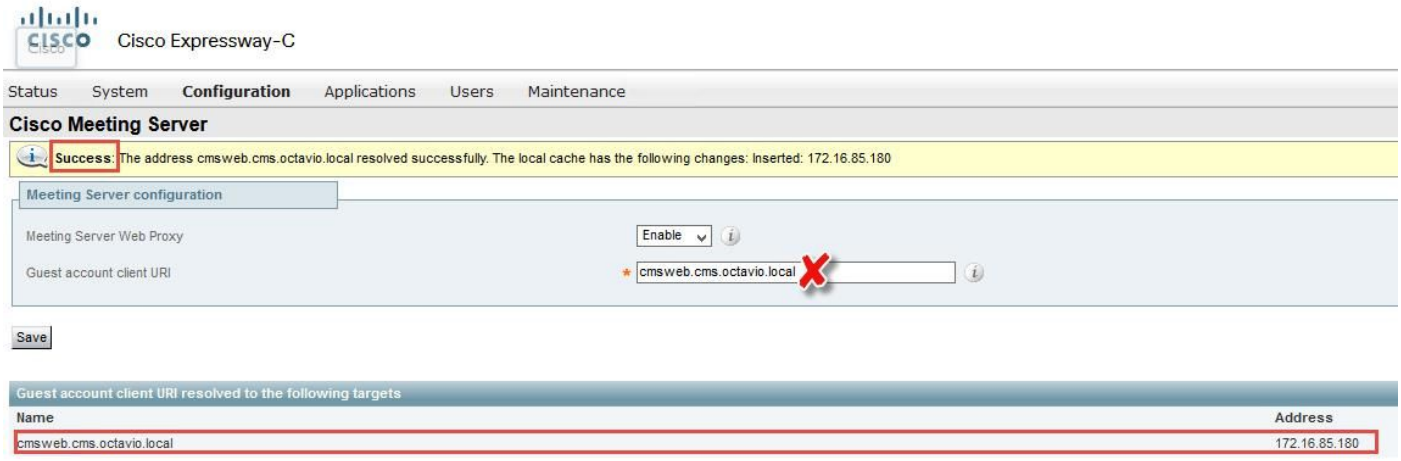
La page WebRTC affiche la 'mauvaise demande'



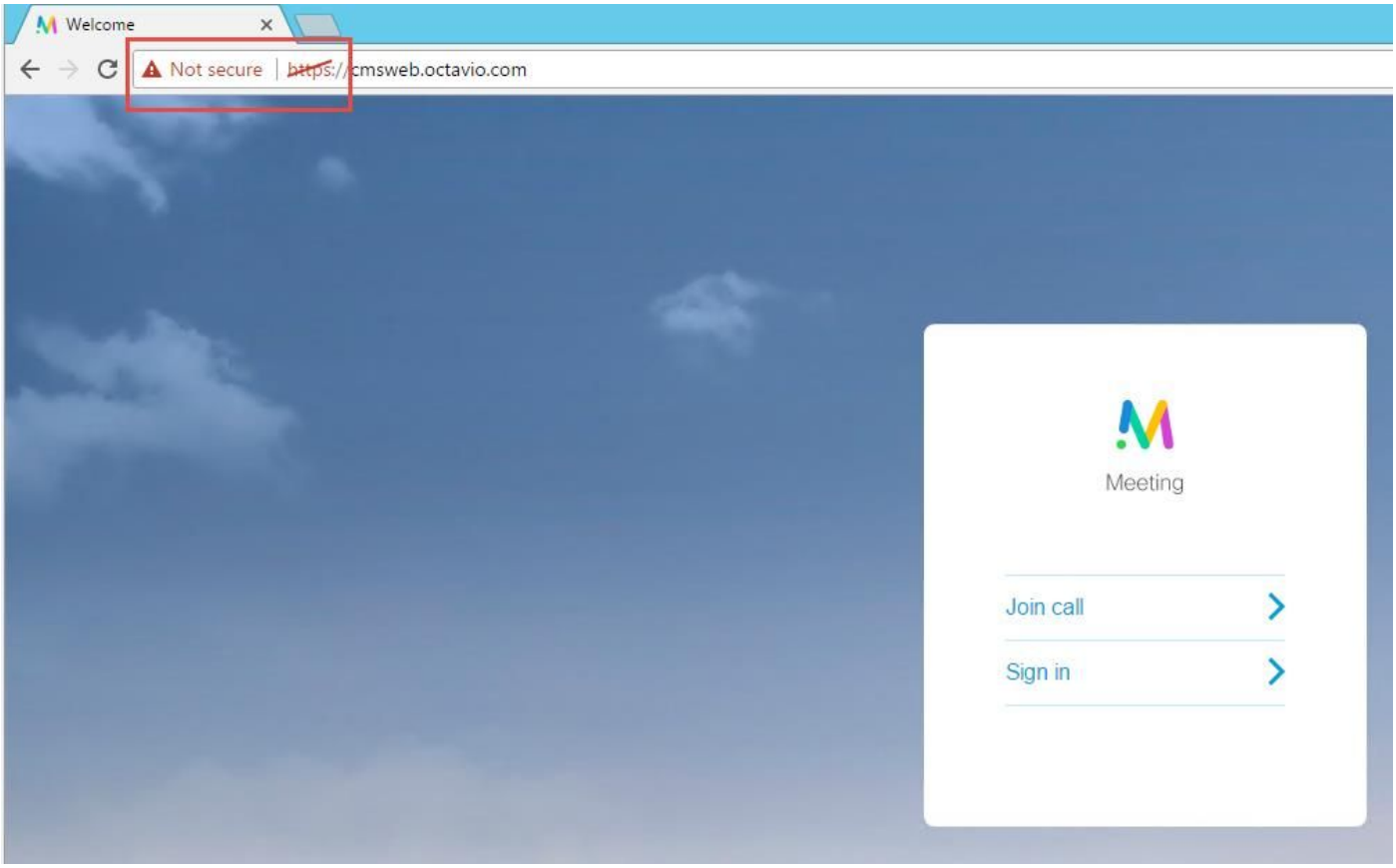
Solution

- Vérifiez que l'URI du client de compte invité correct est configuré sur Expressway-C. Accédez à **Configuration > Unified Communication > Cisco Meeting Server** à cette fin.

Si l'URL interne est configurée dans l'URL du client de compte invité, l'Expressway-C la résoudra puisqu'il y a un enregistrement créé sur le serveur DNS, mais cela peut provoquer le message d'erreur « mauvaise demande » dans le navigateur Web. Dans cet exemple, l'URL interne est configurée afin d'afficher l'erreur comme indiqué dans l'image.

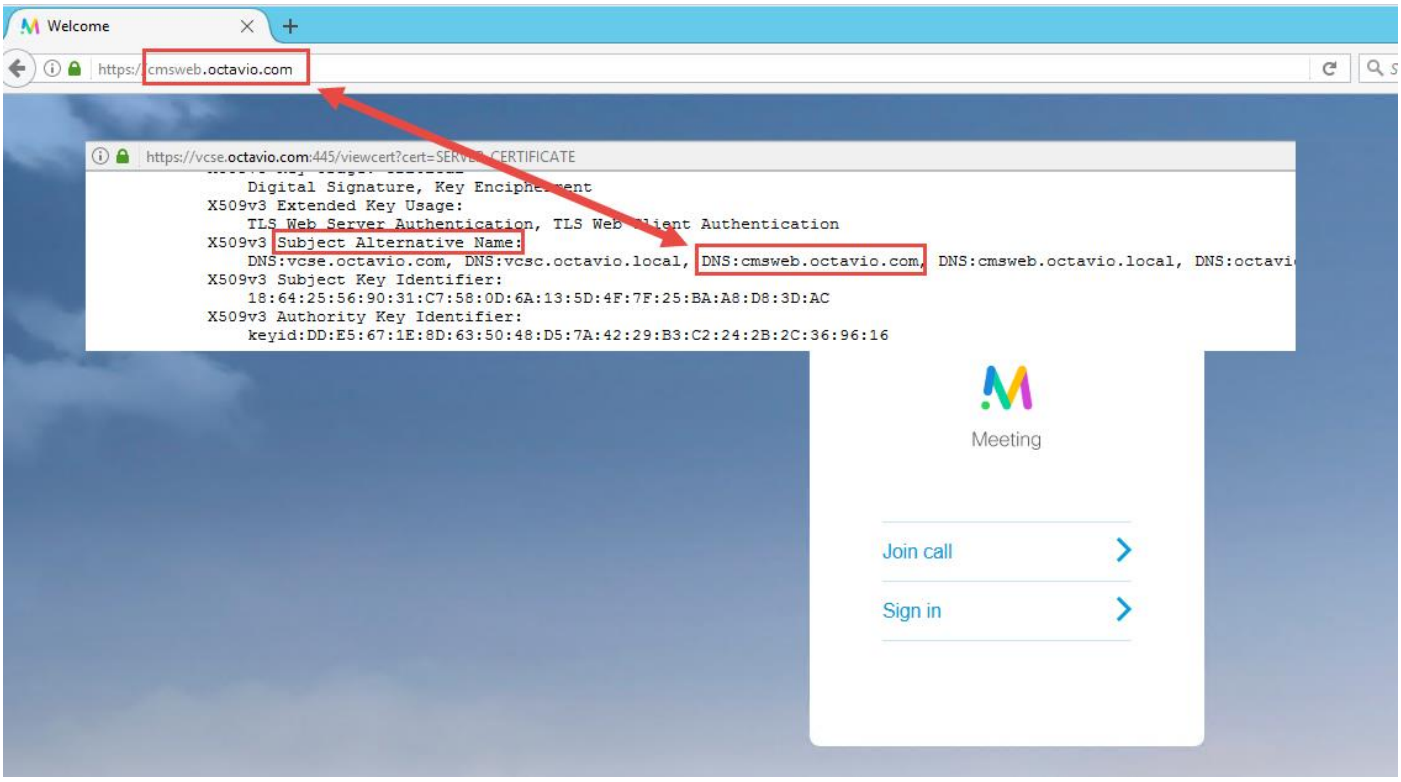


Le client WebRTC affiche une connexion non sécurisée

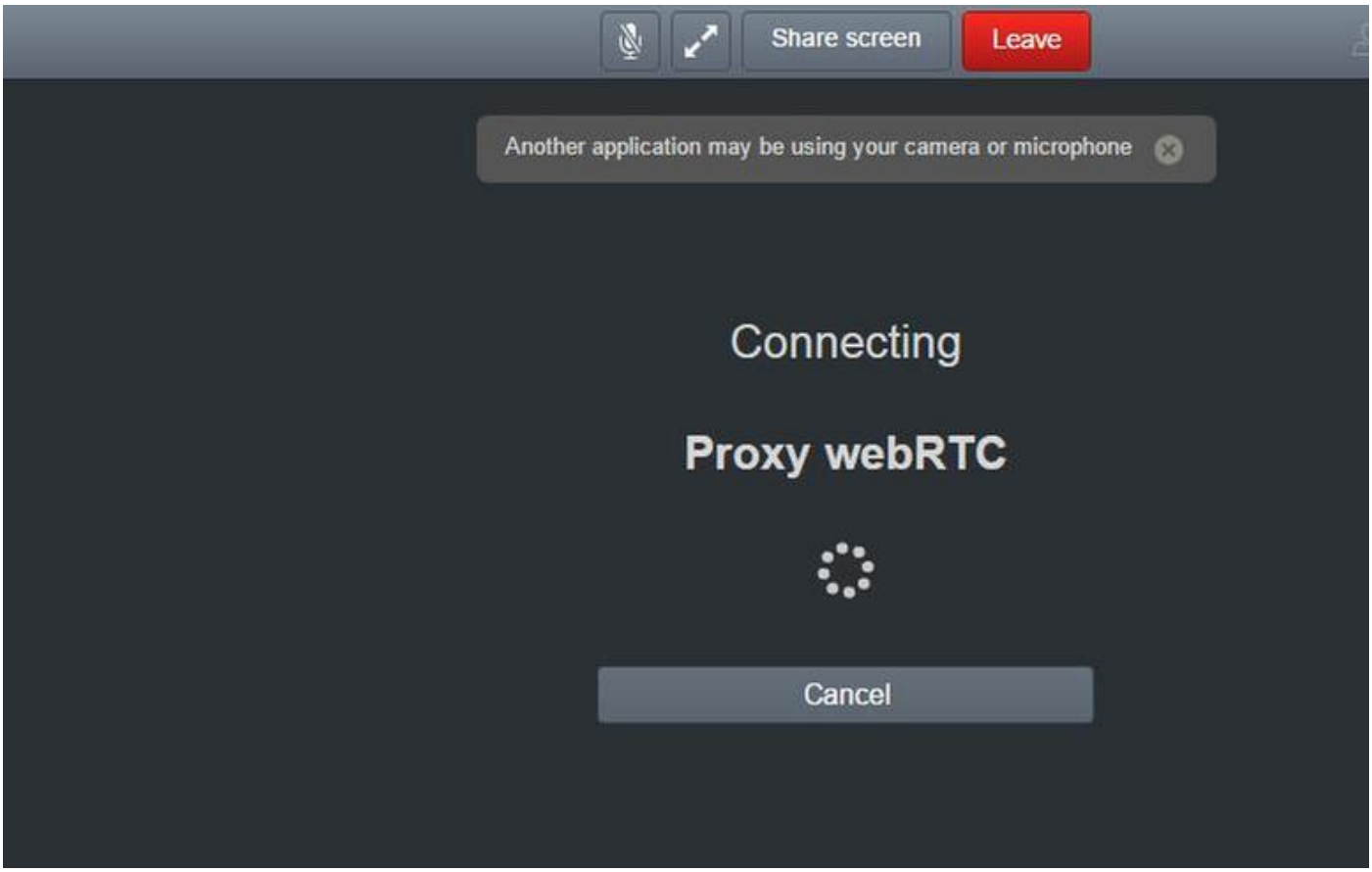


Solution

- Le certificat est auto-signé, ce qui fait que le serveur n'a pas confiance en la source. Remplacez le certificat de l'Expressway-E par une autorité de certification tierce prise en charge.
- Vérifiez que l'URL du pont Web externe est ajoutée en tant que SAN sur le certificat du serveur Expressway-E comme indiqué dans l'image.



Le client WebRTC se connecte mais ne se connecte jamais, puis il a expiré et se déconnecte



Le nom d'utilisateur ou le mot de passe du serveur TURN ne sont pas correctement configurés sur l'autoroute E ou dans le CMS via l'API. Les journaux contiennent les erreurs affichées dans l'image.

2017-05-20	19:43:14.133	Info	web bridge link 3: new guest 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'erreur peut également être confirmée avec une capture de paquets. Exécutez Wireshark sur le PC sur lequel le client WebRTC s'exécute. Une fois que vous avez la capture de paquets, filtrez les paquets par STUN. Vous devez voir les erreurs affichées dans l'image.

Le PC envoie une requête d'allocation et l'adresse NAT d'Expresssway répond par un message d'échec de vérification de l'intégrité.

Solution

Afin de corriger l'erreur, vérifiez le nom d'utilisateur et le mot de passe. Ils doivent être correctement configurés sur les paramètres du serveur TURN comme indiqué dans les images.