Configurer et intégrer le serveur de réunion Cisco (CMS) unique et combiné

Contenu

Introduction

Ce document décrit comment configurer et intégrer le serveur de réunion Cisco (CMS) unique et combiné.

les services à configurer sont le pont d'appel, Webadmin, Web Bridge, le protocole Messagerie et présence extensibles (XMPP) et l'intégration du protocole LDAP (Lightweight Directory Access Protocol).

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les sujets suivants :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Active Directory (AD)
- Autorité de certification (CA)
- Client du protocole de transfert de fichier sécurisé (SFTP)

- Serveur de service de noms de domaine (Domain Name Service, DNS)

Components Used

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

- CMS version 2.3.7
- CUCM version 11.5.1
- Google Chrome version 69.0.3497
- WinSCP version 5.7.7
- Windows Server 2012

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

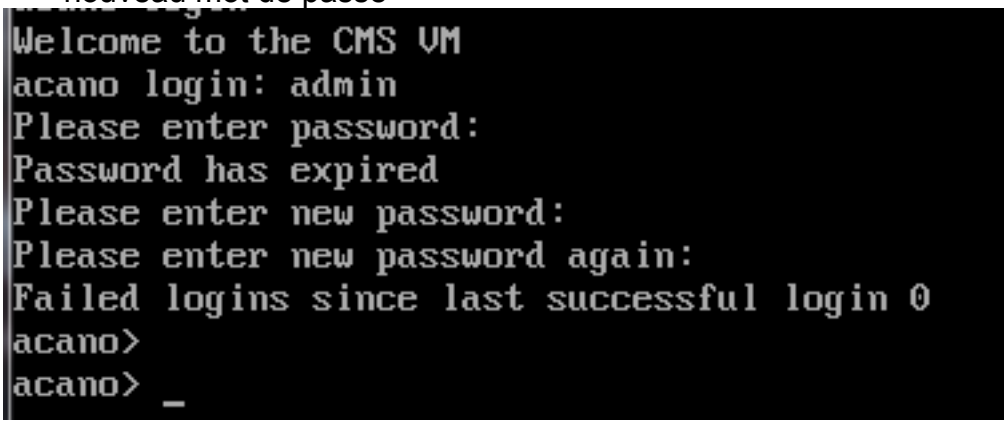
Étape 1. Accéder à CMS

- La première fois que vous vous connectez sur CMS, le message de bienvenue s'affiche à l'écran et vous invite à vous connecter
- Les informations d'authentification par défaut sont les suivantes :

Utilisateur : admin

Mot de passe : admin

- Une fois que les informations d'authentification sont entrées, le serveur vous demande un nouveau mot de passe



- Il est recommandé qu'un nouvel utilisateur administrateur soit créé puisqu'il s'agit d'un bon exercice au cas où vous perdiez le mot de passe d'un compte.
- Saisissez la commande : **user add <username> admin**
- Entrez un nouveau mot de passe et confirmez le nouveau mot de passe

```
CMS01> user add anmiron admin
Please enter new password:
Please enter new password again:
Success
CMS01>
```

Étape 2. Modifier le nom d'hôte

- Ce changement est facultatif
- Exécutez la commande **hostname <name>**
- Redémarrez le serveur
- Exécutez la commande **reboot**

```
acano> hostname CMS01
A reboot is required for the change to take effect
acano>
acano> reboot
Waiting for server to stop...
Waiting for server to stop...
Waiting for server to stop...
Waiting for server to stop...
Waiting for server to stop...
Rebooting...
```

Étape 3. Configurer les paramètres réseau

- Afin d'afficher les paramètres actuels, exécutez la commande **ipv4a**
- Ajouter une configuration IPv4
- Exécutez la commande **ipv4 <interface> add <ipaddress>/<subnetmask> <gateway>**

```
CMS01> ipv4 a add 172.16.85.8/27 172.16.85.1
Only interface enabled: setting gateway as default egress route
CMS01>
```

- Configurer le fuseau horaire
- Exécutez la commande **timezone <timezoneName>**
- Afin de voir tous les fuseaux disponibles, exécutez la commande timezone list
- Ajoutez un serveur de protocole NTP (Network Time Protocol)
- Exécutez la commande **ntp server add <ipaddress>**

```
CMS01> ntp server add 10.88.246.254
CMS01>
CMS01> timezone America/Mexico_City
Reboot the system to finish updating the timezone
CMS01>
CMS01> _
```

- Ajouter un serveur DNS
- Exécutez la commande **dns add forwardzone <domain> <dnsip>**

```
CMS01> dns add forwardzone . 172.16.85.2
CMS01>
```

Note: Un domaine spécifique peut être configuré pour la recherche de DNS, cependant, si le DNS peut mener à n'importe quel domaine, utilisez un point en tant que domaine

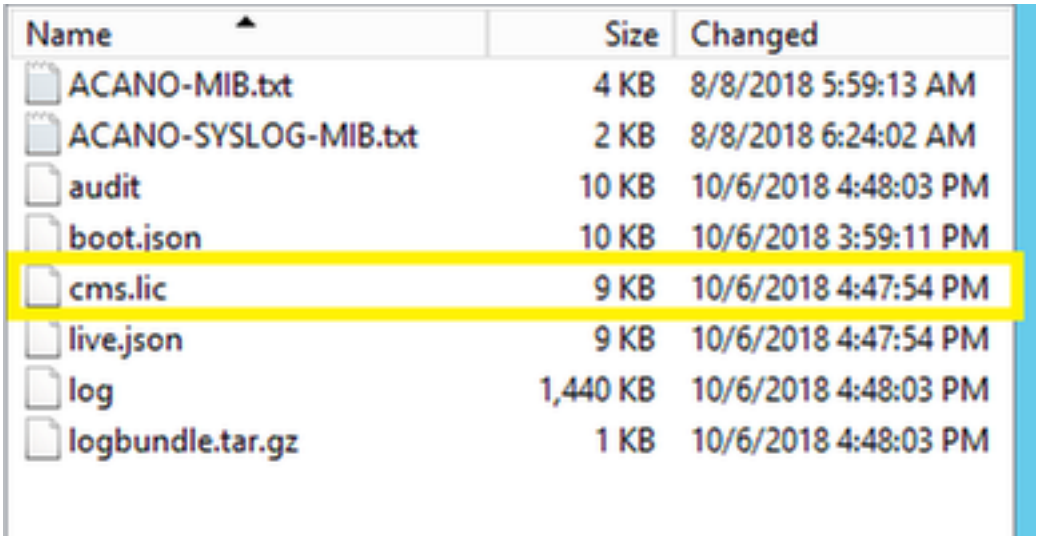
Étape 4. Licence du CMS

- Afin de configurer les services de CMS, une licence doit être installée
- Afin de générer et d'installer la licence, l'adresse MAC (Media Access Control) est requise, puisque les licences y seront rattachées.
- Exécutez la commande **iface a**
- Copiez l'**adresse MAC**
- Communiquez avec votre représentant commercial afin de pouvoir générer une licence.

Note: Le processus de création de la licence est hors de la portée de ce document.

```
CMS01> iface a
Mac address 00:50:56:96:CD:2A
Configured values:
Auto-negotiation:   default
Speed:              default
Duplex:             default
MTU:                1500
Observed values:
Speed:              10000
Duplex:             full
CMS01>
CMS01>
```

- Une fois que vous avez le fichier de licence, renommez le fichier à **cms.lic**
- Utilisez WinSCP ou un autre client SFTP afin de téléverser le fichier dans le serveur CMS



- Une fois que le fichier est téléversé, exécutez la commande **licence**

- Redémarrez le serveur
- Exécutez la commande **reboot**

```
CMS01> license
Feature: callbridge status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: turn status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: webbridge status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: recording status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: personal status: Activated expiry: 2019-Jan-04 (88 days remain)
Feature: shared status: Activated expiry: 2019-Jan-04 (88 days remain)
CMS01>
CMS01> reboot
Waiting for server to stop...
```

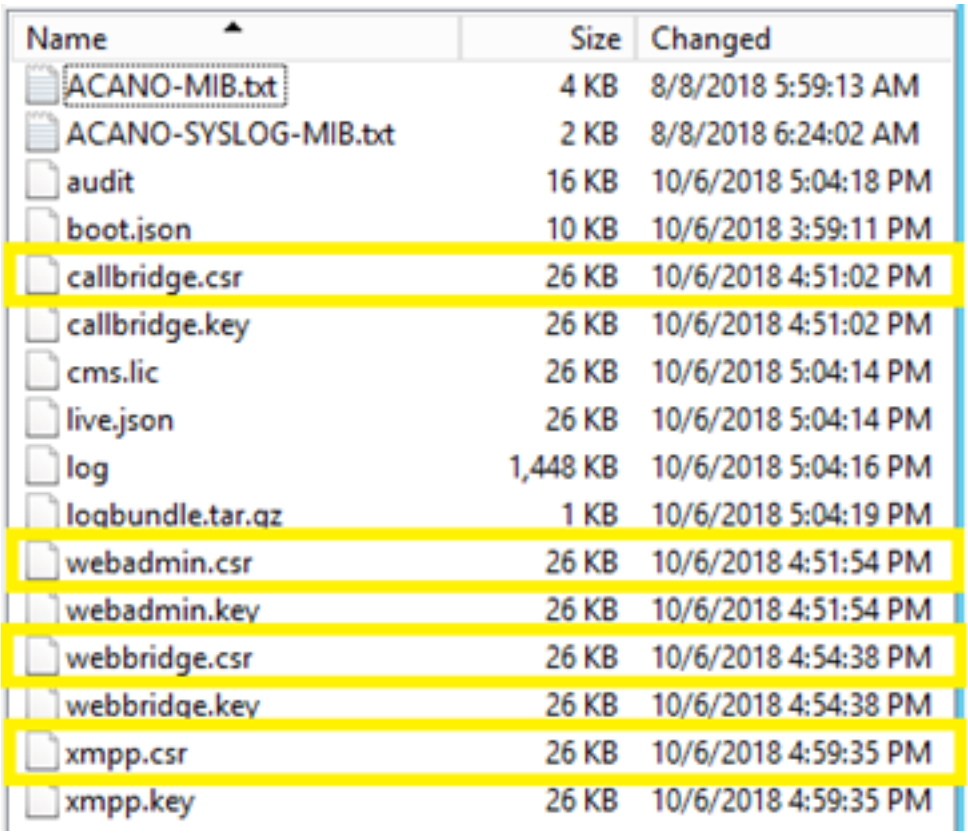
Étape 5. Générer et installer des certificats

- Générer une requête de signature de certificat (CSR) pour le pont d'appel, webadmin, webbridge et XMPP
- Exécutez la commande **pki csr <service> CN:<servicefqdn>** à cette fin.

```
CMS01> pki csr callbridge CN:callbridge.anmiron.local
.....................................
.....................
Created key file callbridge.key and CSR callbridge.csr
CSR file callbridge.csr ready for download via SFTP
CMS01>
CMS01> pki csr webadmin CN:cms01.anmiron.local
.......
.....................................
Created key file webadmin.key and CSR webadmin.csr
CSR file webadmin.csr ready for download via SFTP
CMS01> pki csr webbridge CN:webbridge.anmiron.local
.......
.................
Created key file webbridge.key and CSR webbridge.csr
CSR file webbridge.csr ready for download via SFTP
CMS01>
CMS01> pki csr xmpp CN:xmpp.anmiron.local
............
...
Created key file xmpp.key and CSR xmpp.csr
CSR file xmpp.csr ready for download via SFTP
```

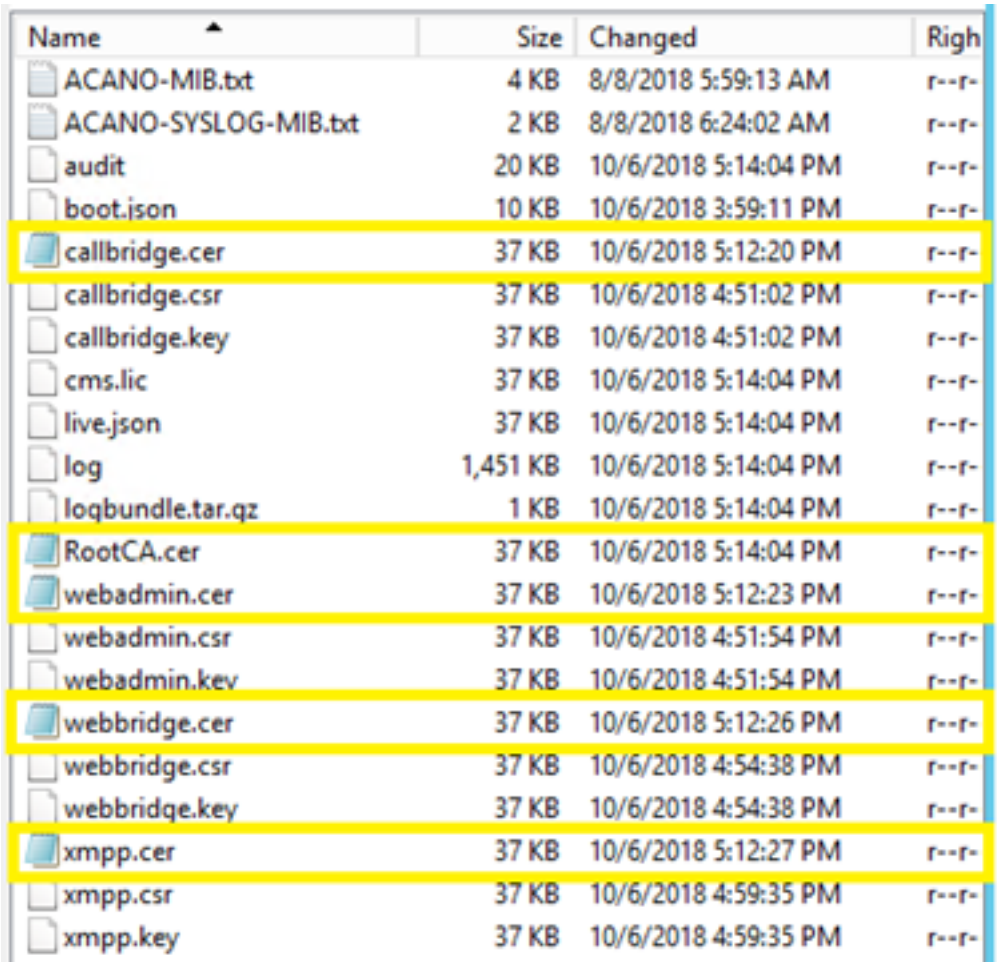
> **Note**: Dans cet exemple, un certificat unique pour chaque serveur est créé; vous pouvez créer un certificat pour tous les services. Pour plus d'informations sur la création de certificats, passez en revue le guide de création de certificats

- Deux fichiers sont générés après l'exécution de la commande : un fichier .csr et un fichier .key. avec le nom du service que vous avez affecté dans les étapes précédentes.
- Téléchargez les fichiers CSR à partir du serveur CMS. Utilisez WinSCP ou autre client SFTP dans ce but.



Name	Size	Changed
ACANO-MIB.txt	4 KB	8/8/2018 5:59:13 AM
ACANO-SYSLOG-MIB.txt	2 KB	8/8/2018 6:24:02 AM
audit	16 KB	10/6/2018 5:04:18 PM
boot.json	10 KB	10/6/2018 3:59:11 PM
callbridge.csr	26 KB	10/6/2018 4:51:02 PM
callbridge.key	26 KB	10/6/2018 4:51:02 PM
cms.lic	26 KB	10/6/2018 5:04:14 PM
live.json	26 KB	10/6/2018 5:04:14 PM
log	1,448 KB	10/6/2018 5:04:16 PM
logbundle.tar.gz	1 KB	10/6/2018 5:04:19 PM
webadmin.csr	26 KB	10/6/2018 4:51:54 PM
webadmin.key	26 KB	10/6/2018 4:51:54 PM
webbridge.csr	26 KB	10/6/2018 4:54:38 PM
webbridge.key	26 KB	10/6/2018 4:54:38 PM
xmpp.csr	26 KB	10/6/2018 4:59:35 PM
xmpp.key	26 KB	10/6/2018 4:59:35 PM

- Signez le CSR avec une Autorité de certification
- Assurez-vous d'utiliser un modèle qui contient l'authentification du **client Web et du serveur Web**
- Téléversez le certificat signé sur le serveur CMS
- Assurez-vous de téléverser l'**autorité de certification racine et tout certificat intermédiaire** qui avaient signé les certificats



Name	Size	Changed	Righ
ACANO-MIB.txt	4 KB	8/8/2018 5:59:13 AM	r--r-
ACANO-SYSLOG-MIB.txt	2 KB	8/8/2018 6:24:02 AM	r--r-
audit	20 KB	10/6/2018 5:14:04 PM	r--r-
boot.json	10 KB	10/6/2018 3:59:11 PM	r--r-
callbridge.cer	37 KB	10/6/2018 5:12:20 PM	r--r-
callbridge.csr	37 KB	10/6/2018 4:51:02 PM	r--r-
callbridge.key	37 KB	10/6/2018 4:51:02 PM	r--r-
cms.lic	37 KB	10/6/2018 5:14:04 PM	r--r-
live.json	37 KB	10/6/2018 5:14:04 PM	r--r-
log	1,451 KB	10/6/2018 5:14:04 PM	r--r-
logbundle.tar.gz	1 KB	10/6/2018 5:14:04 PM	r--r-
RootCA.cer	37 KB	10/6/2018 5:14:04 PM	r--r-
webadmin.cer	37 KB	10/6/2018 5:12:23 PM	r--r-
webadmin.csr	37 KB	10/6/2018 4:51:54 PM	r--r-
webadmin.key	37 KB	10/6/2018 4:51:54 PM	r--r-
webbridge.cer	37 KB	10/6/2018 5:12:26 PM	r--r-
webbridge.csr	37 KB	10/6/2018 4:54:38 PM	r--r-
webbridge.key	37 KB	10/6/2018 4:54:38 PM	r--r-
xmpp.cer	37 KB	10/6/2018 5:12:27 PM	r--r-
xmpp.csr	37 KB	10/6/2018 4:59:35 PM	r--r-
xmpp.key	37 KB	10/6/2018 4:59:35 PM	r--r-

- Afin de vérifier tous les certificats qui sont affichés sur CMS, exécutez la commande **pki list**

```
CMS01> pki list
User supplied certificates and keys:
callbridge.key
callbridge.csr
webadmin.key
webadmin.csr
webbridge.key
webbridge.csr
xmpp.key
xmpp.csr
callbridge.cer
webadmin.cer
webbridge.cer
xmpp.cer
RootCA.cer
CMS01>
```

Étape 6. Enregistrements DNS

- Créer les enregistrements d’adresse DNS (A) pour le pont d’appel, XMPP, webadmin et webbridge
- Assurez-vous que tous les enregistrements pointent vers l’adresse IP de CMS

callbridge	Host (A)	172.16.85.8	static
cms01	Host (A)	172.16.85.8	static
webbridge	Host (A)	172.16.85.8	static
xmpp	Host (A)	172.16.85.8	static

- Créez un enregistrement SRV pour **xmpp-client**
- Le format de l'enregistrement SRV est

Service _xmpp-client
Protocol _tcp
Port 5222
Target Entrez le FQDN XMPP, par exemple **xmpp.anmiron.local**

_xmpp-client	Service Location (SRV)	[10][10][5222] xmpp.anmiron.local.	static

Étape 7. Configuration du service

Configurez le pont d'appel :

- Entrez la commande **callbridge listen <interface>**
- Entrez la commande **callbridge certs <callbridge-key-file> <fichier_crt> [<bundle_cert>]**
- Le fichier **key-file (fichier de clé) est la clé créée lors de la création du CSR.**
- L'ensemble **cert-bundle (ensemble de certificats) est l'ensemble comprenant l'autorité de certification racine et tout autre certificat intermédiaire**

```
CMS01> callbridge listen a
CMS01>
CMS01> callbridge certs callbridge.key callbridge.cer RootCA.cer
CMS01>
```

Note: L'interface de réception du pont d'appel ne doit pas être définie sur une interface qui est configurée pour utiliser la traduction d'adresses réseau (NAT) vers une autre adresse IP

Configurez webadmin :

- Exécutez la commande **webadmin listen <interface> <port>**
- Exécutez la commande **webadmin certs <key-file> <crt-file> [<cert-bundle>]**

```
CMS01> webadmin listen a 445
CMS01>
CMS01> webadmin certs webadmin.key webadmin.cer RootCA.cer
CMS01>
```

Note: Si le webadmin et le webbridge sont configurés dans le même serveur, ils doivent être configurés sur différentes interfaces ou recevoir dans différents ports; le webbridge doit recevoir dans le port 443. Le webadmin est généralement configuré dans le port 445.

Configurez XMPP :

- Exécutez la commande **xmpp listen <interface whitelist>**

- Exécutez la commande **xmpp domain <domain name>**
- Exécutez la commande **xmpp certs <key-file> <crt-file> [<crt-bundle>]**

```
CMS01> xmpp listen a
CMS01>
CMS01> xmpp domain anmiron.local
CMS01>
CMS01> xmpp certs xmpp.key xmpp.cer RootCA.cer
CMS01>
```

Note: Le nom de domaine doit correspondre au domaine où les enregistrements DNS ont été créés.

Configurez webbridge :

- Exécutez la commande **webbridge hear <liste blanche interface[:port]>**
- Exécutez la commande **webbridge certs <key-file> <crt-file> [<crt-bundle>]**
- Exécutez la commande **webbridge trust <crt-bundle>**

```
CMS01> webbridge listen a
CMS01>
CMS01> webbridge certs webbridge.key webbridge.cer RootCA.cer
CMS01>
CMS01> webbridge trust callbridge.cer
CMS01>
```

Note: L'ensemble de confiance **crt-bundle est le certificat du pont d'appel et doit être ajouté au webbridge afin que le pont d'appel fasse confiance au webbridge, ce qui permettra la fonctionnalité Join as a Guest (se joindre en tant qu'invité).**

- Exécutez la commande **callbridge restart**
- Exécutez la commande **wbeadmin enable**
- Exécutez la commande **xmpp enable**
- Exécutez la commande **webbridge enable**

```
CMS01> callbridge restart
SUCCESS: listen interface configured
SUCCESS: Key and certificate pair match
SUCCESS: certificate verified against CA bundle
CMS01>
CMS01> webadmin enable
SUCCESS: TLS interface and port configured
SUCCESS: Key and certificate pair match
SUCCESS: certificate verified against CA bundle
CMS01>
CMS01> xmpp enable
SUCCESS: Callbridge activated
SUCCESS: Domain configured
SUCCESS: Key and certificate pair match
SUCCESS: certificate verified against CA bundle
SUCCESS: XMPP server enabled
CMS01>
CMS01> webbridge enable
SUCCESS: Key and certificate pair match
SUCCESS: certificate verified against CA bundle
SUCCESS: Webbridge enabled
CMS01>
```

Note: Le serveur doit renvoyer **SUCCESS pour tous les services; s'il renvoie FAILURE**, passez en revue les étapes précédentes et validez que toute la configuration est correcte

Pour permettre au pont d'appel d'accéder au service XMPP en toute sécurité, il est nécessaire de fournir un **nom du composant que le pont d'appel peut utiliser pour l'authentification avec le service XMPP.**

- Exécutez la commande **xmpp callbridge add <component name>**
- Le résultat affiche un Secret, comme illustré dans l'image

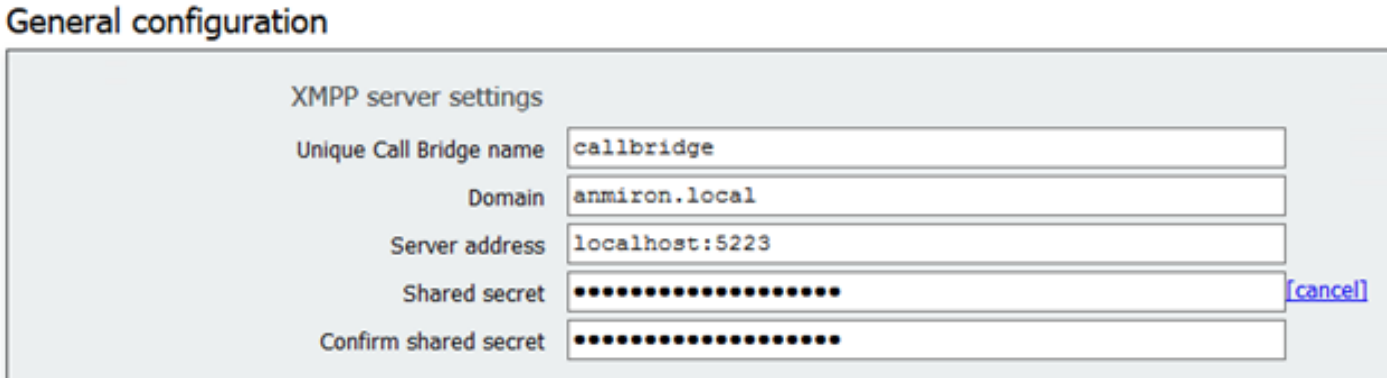
```
CMS01> xmpp callbridge add callbridge
Success              : true
Callbridge : callbridge
Domain     : anmiron.local
Secret     : 6DwNANabpumutI4pAb1
CMS01>
```

- Copiez la valeur du **Secret**
- Accédez à l'interface Web de CMS
- Naviguez jusqu'à **Configuration > General (Configuration > Générale)**
- Entrez l'information

Nom unique de pont d'appel	Entrez le nom du pont d'appel créé, par exemple **callbridge**
Domaine	Entrez le nom du domaine, par exemple **anmiron.local**
Adresse du serveur	Définissez l'adresse IP CMS, par exemple **localhost:5223**

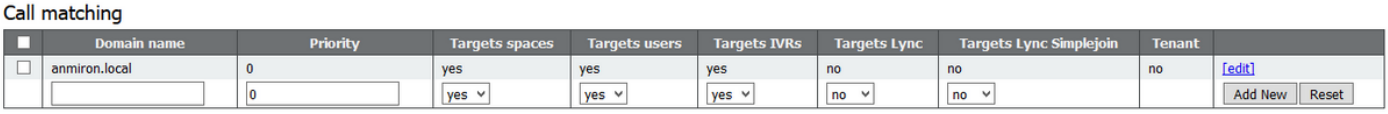
Secret partagé	Entrez le Secret créé à l'étape précédente, par exemple **6DwNANabpumut14pAb1**

- Sélectionnez **Submit (soumettre)**



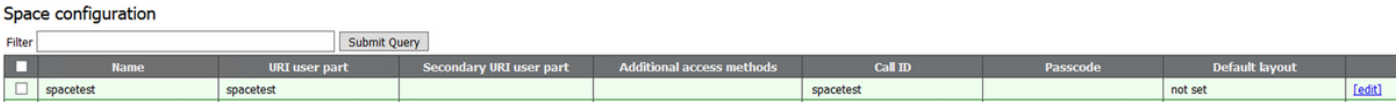
- Créer une **Règle de correspondance des appels entrants pour les appels entrants**
- Naviguez jusqu'à **Configuration > Incoming calls (Configuration > Appels entrants)**
- Entrez l'information

Domaine	Entrez le nom de domaine du serveur CMS, par exemple **anmiron.local**
Priorité	Entrez une valeur pour la priorité, par exemple **0**
Espaces cibles	Sélectionnez **oui**



- Créez un espace pour faire des tests
- Naviguez jusqu'à **Configuration > Spaces (Configuration > Espaces)**
- Entrez l'information

Name (nom)	Entrez un nom pour l'espace, par exemple **spacetest**
Partie de l'utilisateur URI	Entrez une URI à donner comme nom pour cet espace, par exemple **spacetest**
ID de l'appel	Entrez l'ID de l'appel qui se joindra à cet espace à partir de webbridge, par exemp **spacetest**
Mot de passe	Entrez un numéro si c'est nécessaire pour permettre l'accès à l'espace

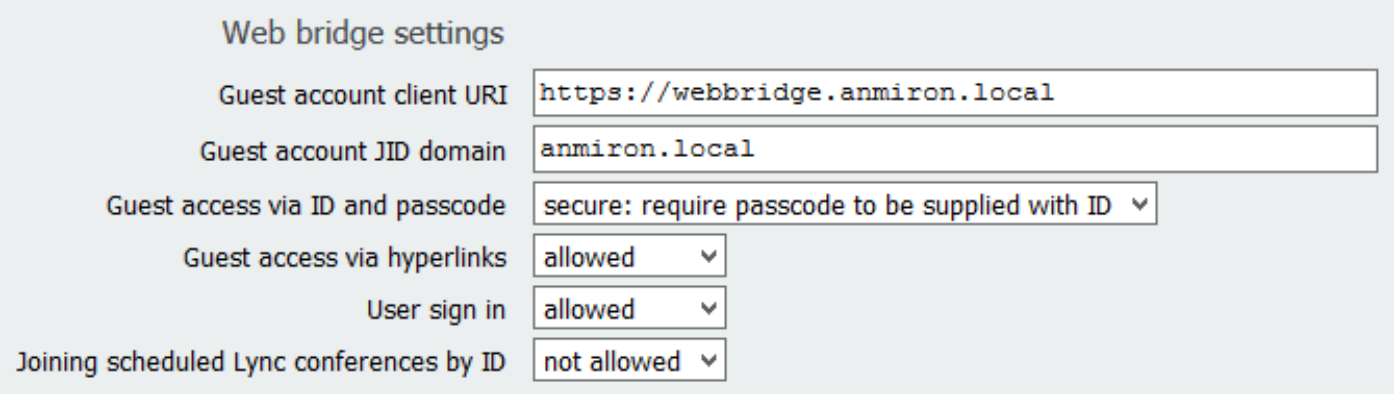


> **Note**: La **partie de l'utilisateur URI est ce que les appelants doivent composer au domaine configuré sur la Règle de correspondance des appels entrants**, par exemple, l'appelant doit composer **spacetest@anmiron.local**

- Naviguez jusqu'à **Configuration > General > Web bridge settings (Configuration > Générale > Configuration Web bridge)**
- Entrez l'information

URI de client du compte invité	Il s'agit de l'interface Web de webbridge, par exemple https://webbridge.anmiron.local
Domaine JID du compte invité	Le domaine configuré dans CMS, par exemple **anmiron.local**
Accès de l'invité par lien	Sélectionnez **allowed (autorisé)**

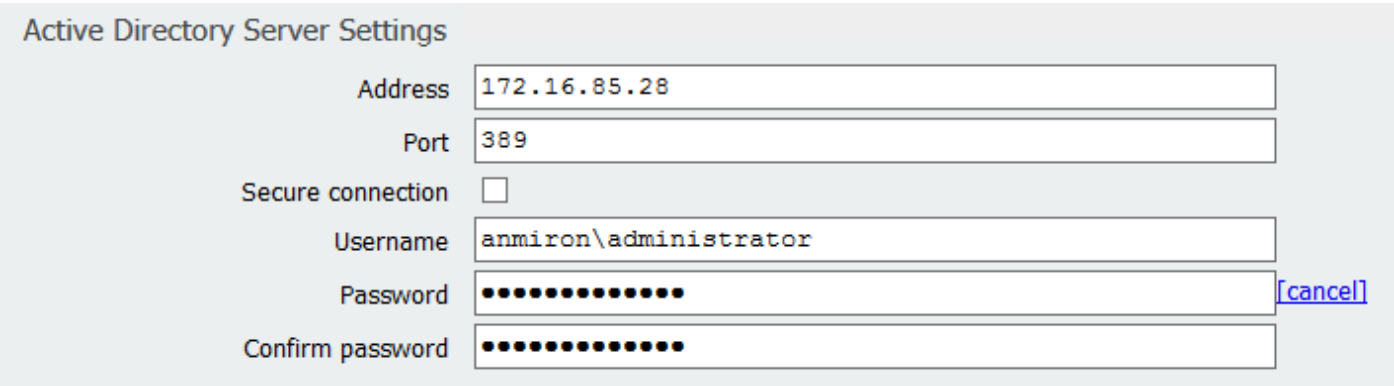
hypertexte

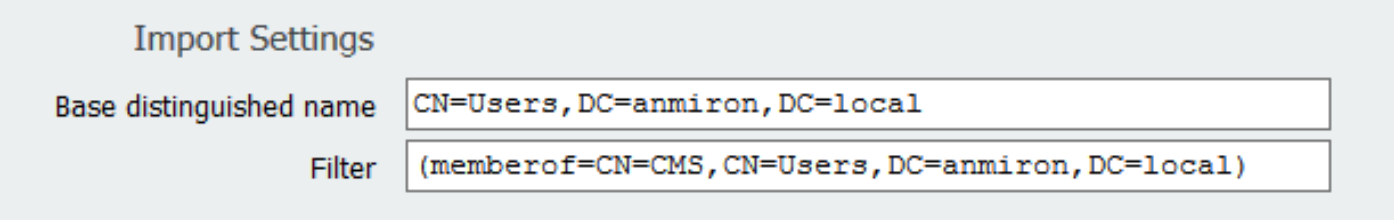


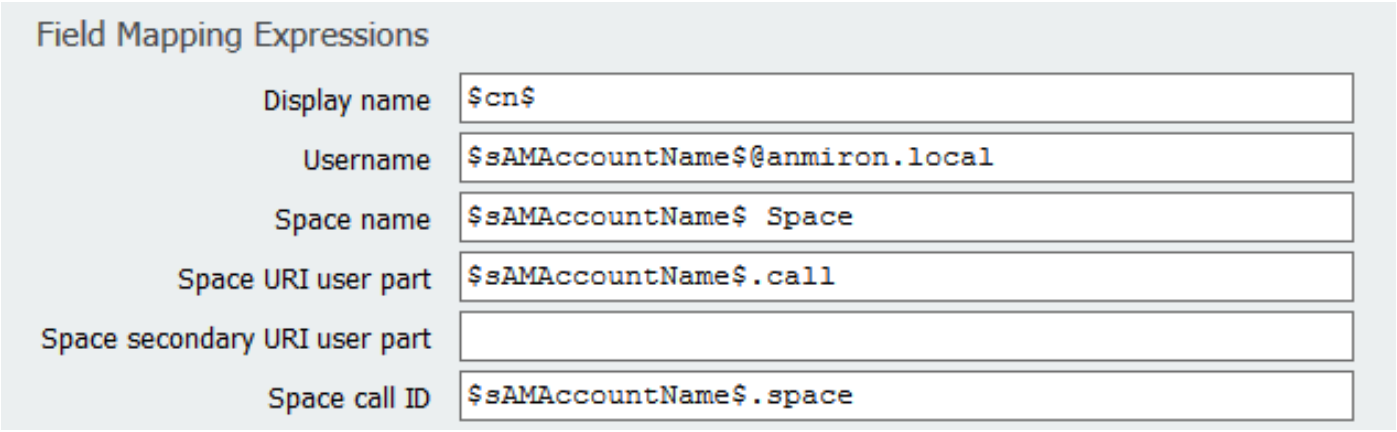
Étape 8. Intégrer LDAP

- Ouvrez l'interface Web de CMS
- Naviguez jusqu'à **Configuration > Active Directory (Configuration > Active Directory)**
- Entrez l'information

Adresse	L'adresse IP du serveur LDAP, par exemple **172.16.85.28**
Port	Il s'agit de **389 si vous utilisez une connexion non sécurisée et de 636 si une connexion sécurisée est requise**
Nom d'utilisateur	Entrez un administrateur pour le serveur LDAP, par exemple **anmiron\adminis**
Mot de passe	Entrez le mot de passe de l'utilisateur administrateur
Nom distinctif de base	Il s'agit d'un paramètre d'Active directory, par exemple **CN=Users, DC=anmir DC=local**
Filtre	Il s'agit d'un paramètre d'Active directory, par exemple **(memberof=CN=CMS, CN=Users, DC=anmiron, DC=local)**
Nom d'affichage	La façon dont le nom d'utilisateur est affiché, par exemple **cn**
Nom d'utilisateur	ID de connexion de l'utilisateur, par exemple **$sAMAccountName$@anmiron.**
Nom de l'espace	Comment l'espace est affiché, par exemple **$sAMAccountName$ Space**
Partie de l'utilisateur URI de l'espace	L'URI à laquelle composer, par exemple **$sAMAccountName$.call**
ID d'appel de l'espace	L'ID d'appel à être utilisée à partir de webbridge, par exemple **$sAMAccountName$.space**



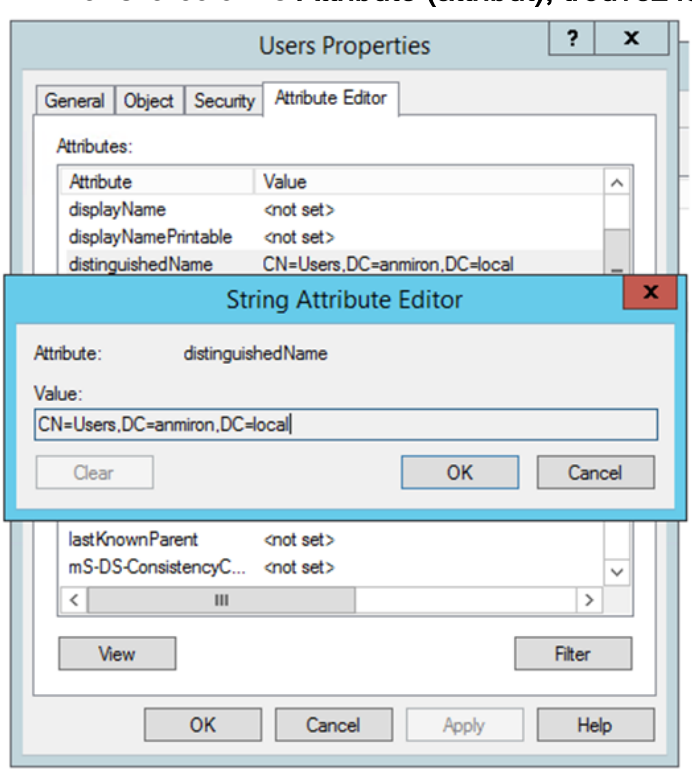


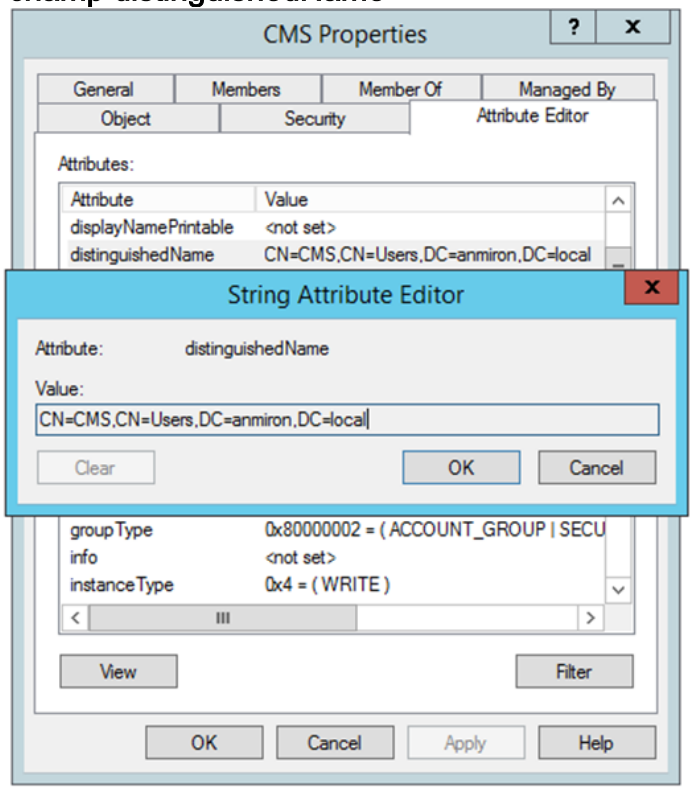


- Sélectionnez **Submit (soumettre)**
- Sélectionnez **Sync now (synchroniser maintenant)**

Base distinguished name (nom distinctif de base) et Filter (filtre) sont des paramètres d'Active Directory (directoire actif). Cet exemple contient des informations de base pour obtenir les informations avec Attribute editor (éditeur d'attributs) sur Active Directory (directoire actif). Pour ouvrir dans **l'éditeur d'attributs**, activez **Fonctionnalités avancées** sur **Active Directory.** Naviguez jusqu'à **Users and Computers > View (Utilisateurs et ordinateurs > Affichage) et sélectionnez Advanced Features (fonctionnalités avancées)**

- Pour cet exemple, un groupe appelé **CMS est créé**
- Ouvrez la fonctionnalité **Users and Computers (utilisateurs et ordinateurs) sur Active Directory**
- Sélectionnez à droite un **utilisateur et ouvrez les propriétés**
- Naviguez jusqu'à **Attribute Editor**
- Dans la colonne **Attribute (attribut), trouvez le champ distinguishedName**

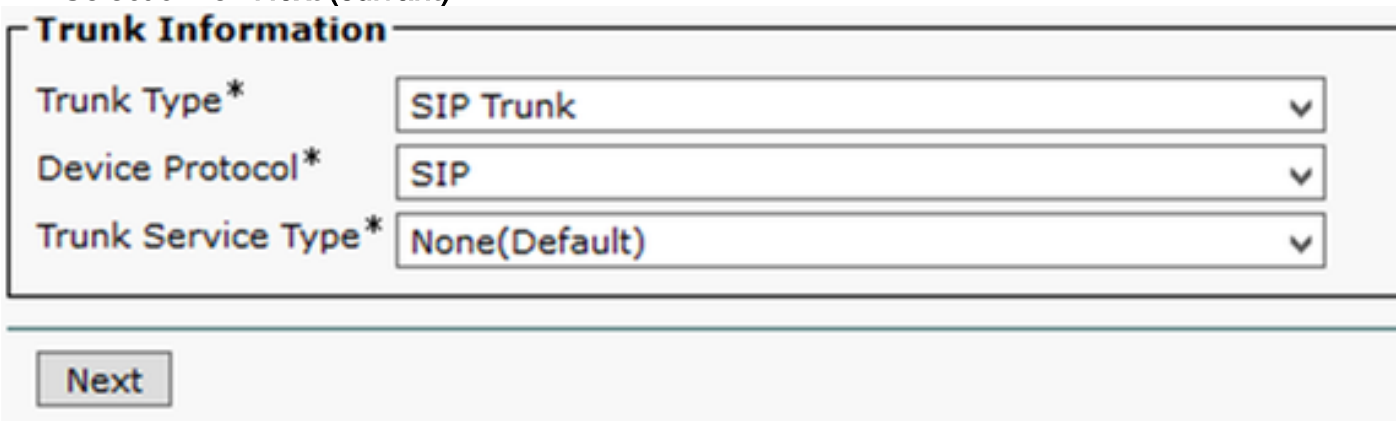




Note: Pour plus d'informations sur les filtres LDAP, consultez le [guide de déploiement de CMS]

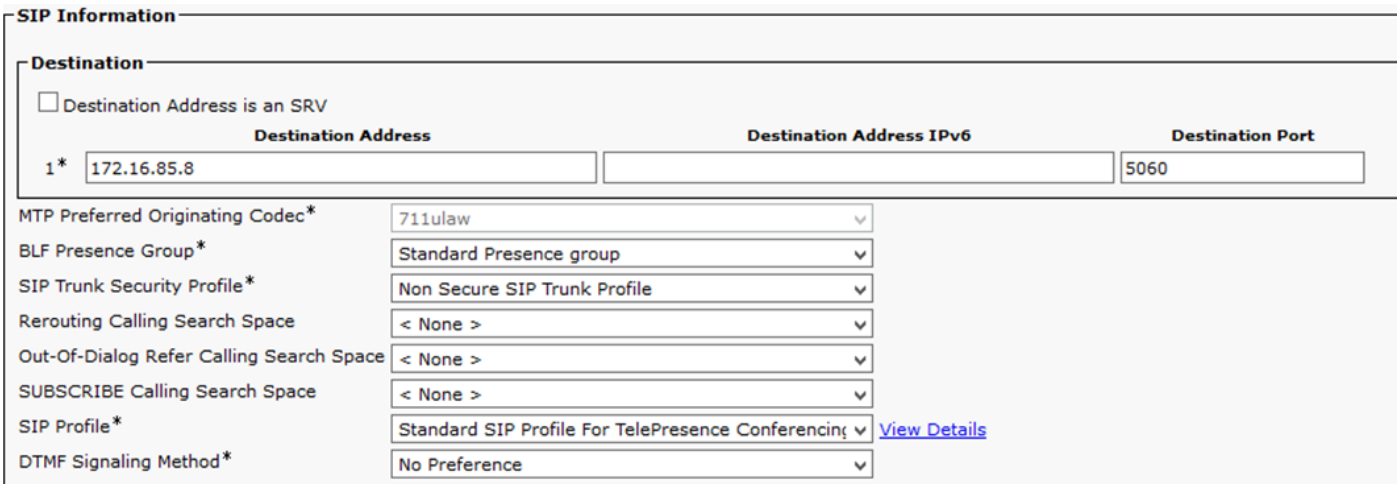
Étape 9. Configurer CUCM

- Ouvrez l'interface Web de CUCM
- Naviguez jusqu'à **Device > Trunks (Périphérique > Lignes principales)**
- Sélectionnez **Add New (ajouter nouveau)**
- Dans le menu déroulant du **type de ligne principale, sélectionnez ligne principale SIP**
- Sélectionnez **Next (suivant)**



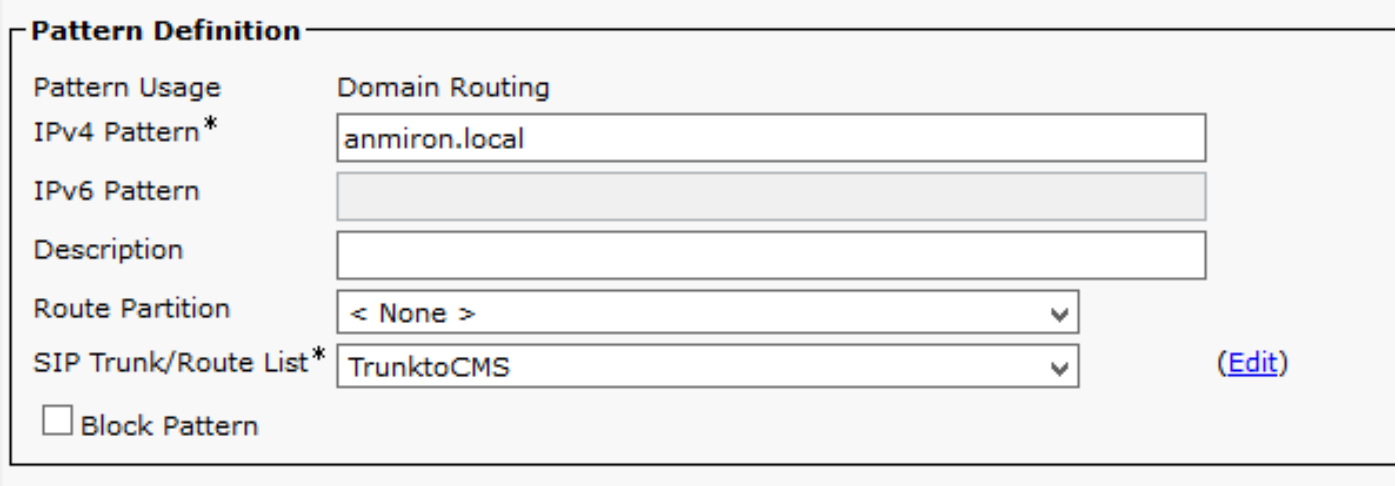
- Entrez l'information

Nom du périphérique	Entrez un nom pour la ligne principale SIP, par exemple **TrunktoCMS**
Adresse de destination	Entrez l'adresse IP CMS ou le FQDN du pont d'appel, par exemple **172.16.8**
Destination Port (port de destination)	Entrez le port où CMS reçoit, par exemple **5060**
Profil de sécurité de la ligne principale SIP	Sélectionnez le profil de sécurité, par exemple **Non Secure SIP TrunkProfile (profil non sécurisé de la ligne principale SIP)**
Profil SIP	Sélectionnez **Standard SIP Profile for TelePresence Conferencing (profil SIP standard pour TelePresence Conferencing)**



- Sélectionnez **Save (enregistrer)**
- Sélectionnez **Reset (réinitialiser)**
- Naviguez jusqu'à **Call routing > SIP Route pattern > Add New > Select Domain Routing (Routage d'appel > schéma de routage SIP > Ajouter nouveau > Sélectionner domaine de routage)**
- Entrez l'information

Schéma IPv4	Entrez le domaine configuré à CMS, par exemple **anmiron.local**
Liste de routage/ligne principale SIP	Sélectionnez la ligne principale SIP précédemment créée, **TrunktoCl**

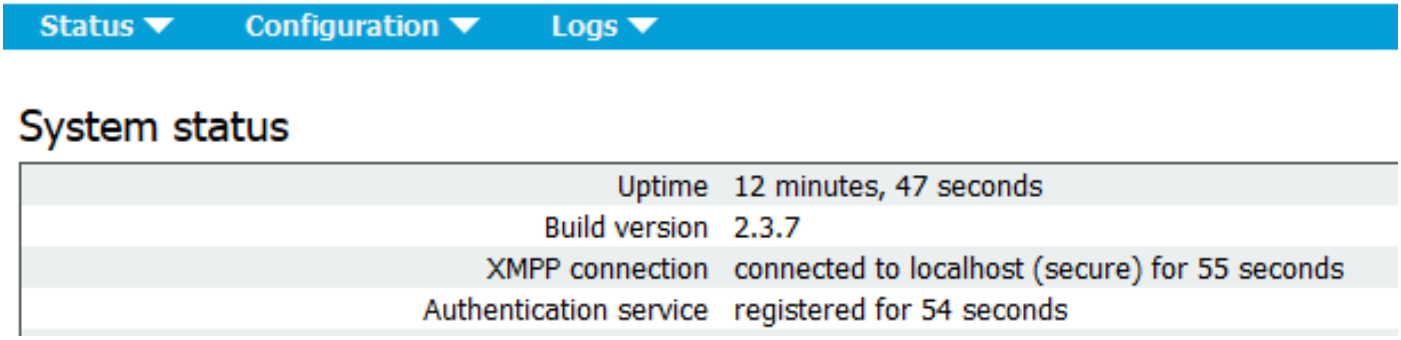


- Sélectionnez **Save (enregistrer)**

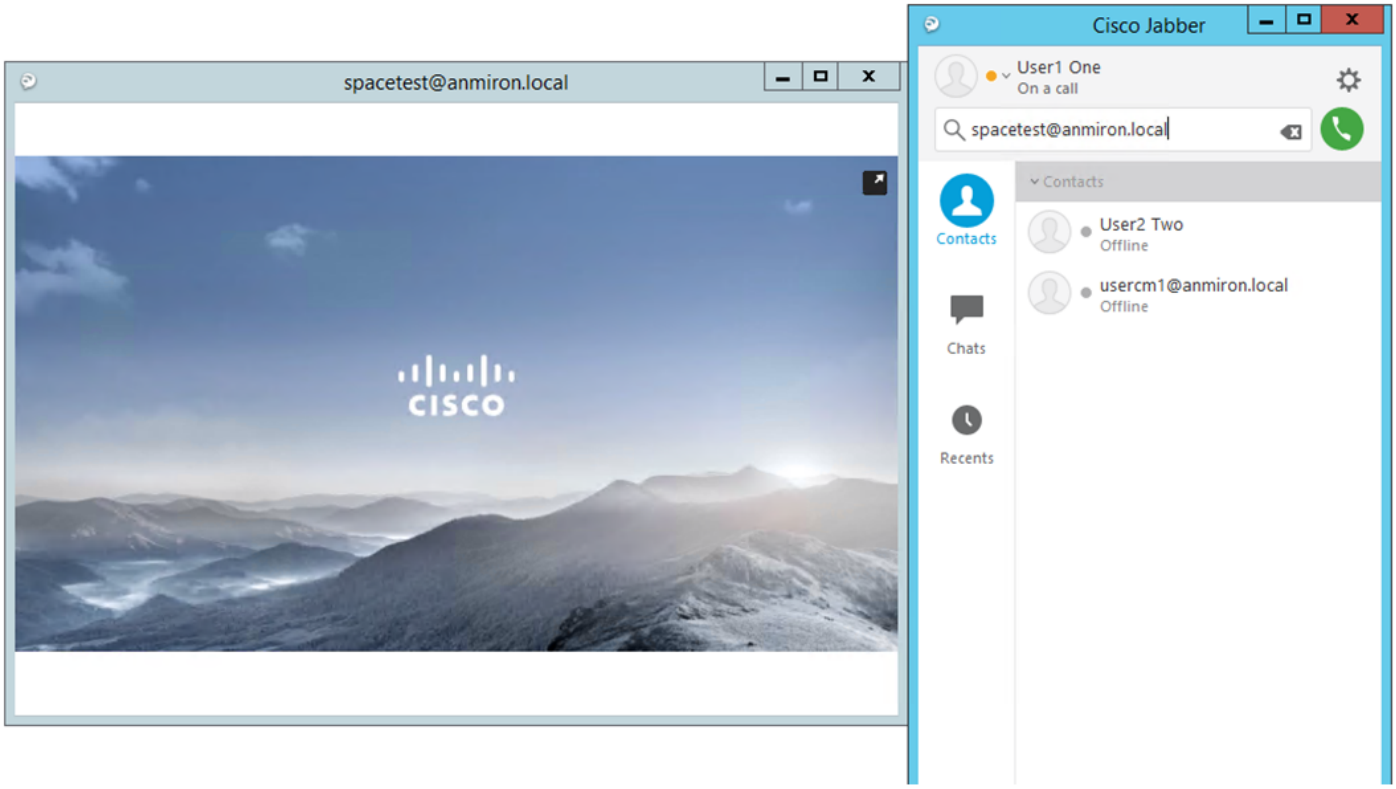
Vérification

Communication du pont d'appel et XMPP

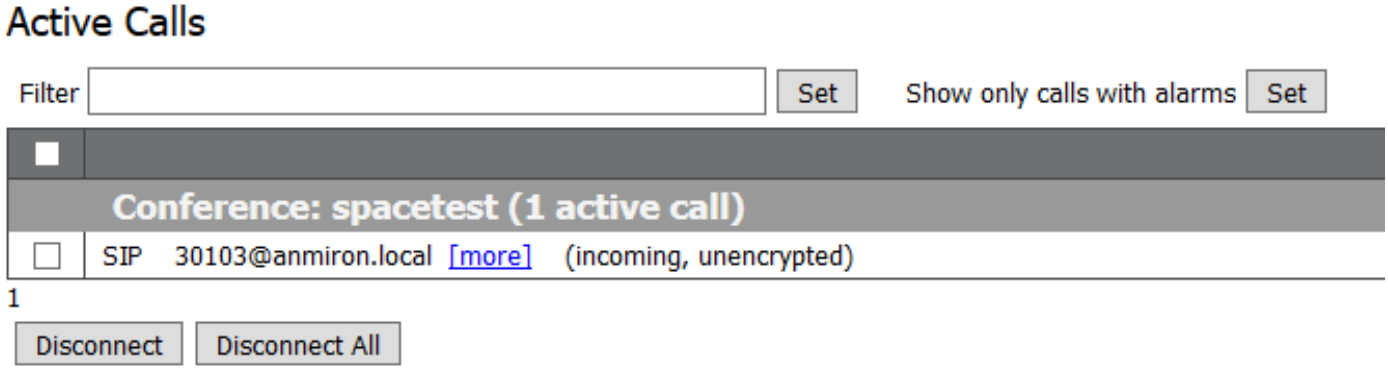
- Ouvrez l'interface Web de CMS
- Naviguez jusqu'à **Status > General (État > Général)**
- L'état de la connexion XMPP doit être connecté à localhost



- Passez un appel à partir d'un appareil enregistré sur CUCM
- Composez à l'URI **spacetest@anmiron.local**



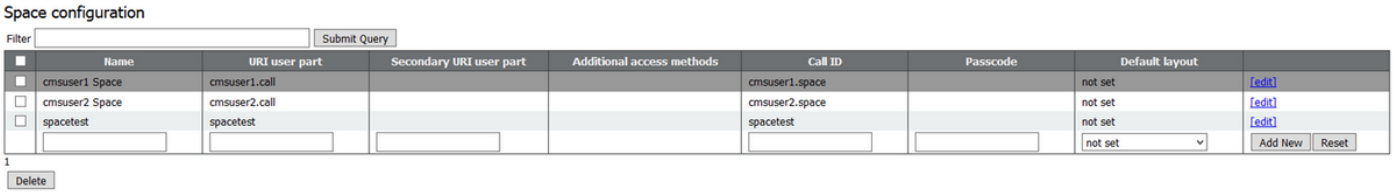
- Ouvrez l'interface Web de CMS
- Naviguez jusqu'à **Status > Calls (État > Appels)**
- L'appel doit être affiché en tant qu'**Active Call (appel actif)**



Syncronization LDAP avec CMS

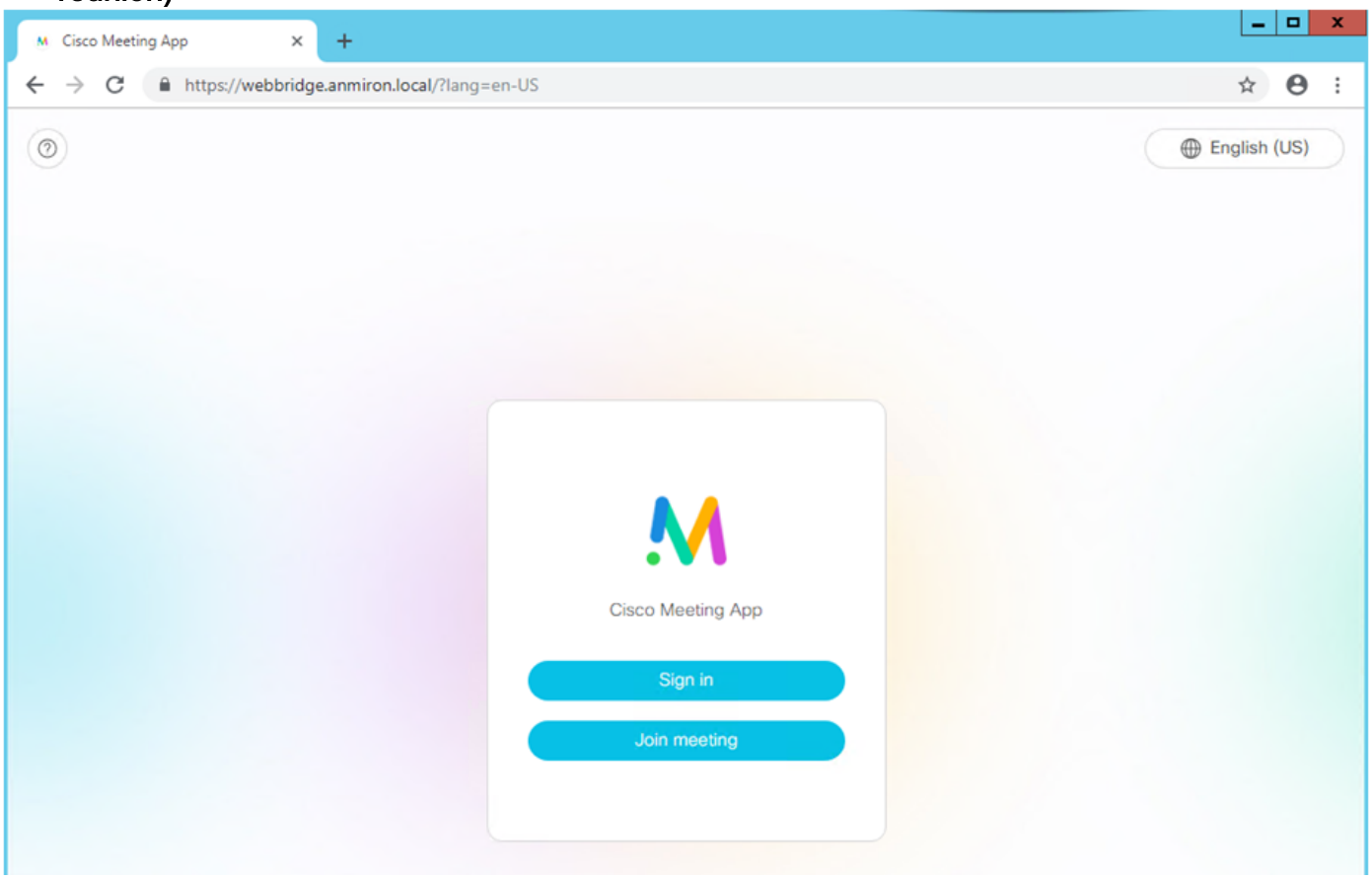
- Ouvrez l'interface Web de CMS
- Naviguez jusqu'à **Status > Users (État > Utilisateurs)**
- La liste complète des utilisateurs doit être affichée.

- Naviguez jusqu'à **Configuration > Spaces (Configuration > Espaces)**
- Assurez-vous que chaque utilisateur possède un espace créé qui lui est propre

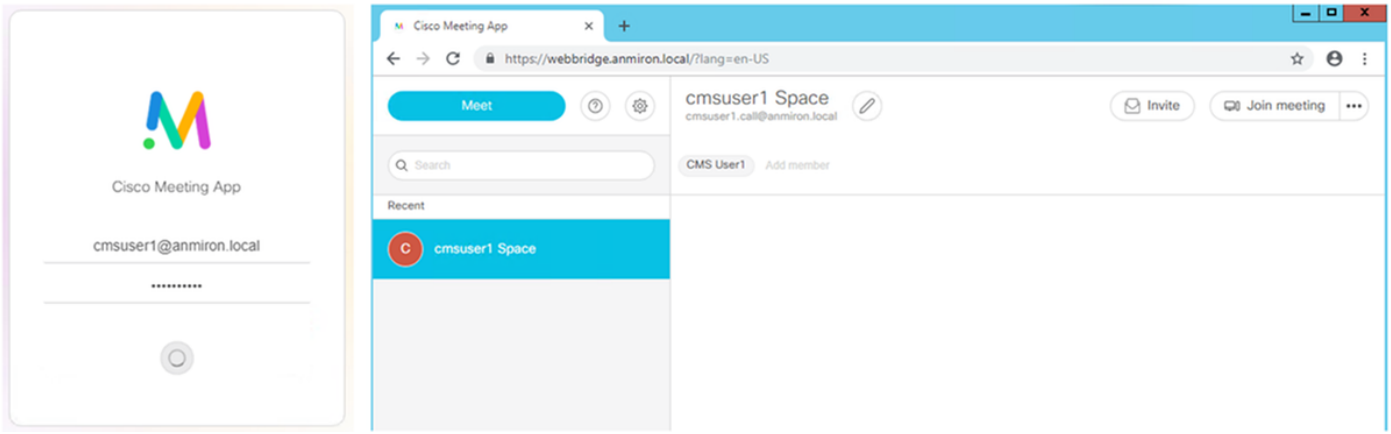


Accès à Webbridge

- Utilisez le navigateur Web pour accéder à la page Web configurée pour le service webbridge, https://webbridge.anmiron.local
- La page doit afficher deux options, **Sign in (se connecter) et Join meeting (se joindre à la réunion)**



- Les utilisateurs précédemment intégrés à partir d'Active Directory doivent être capables de se connecter
- Sélectionnez **Sign in (se connecter)**
- Entrez le **nom d'utilisateur et le mot de passe**
- L'utilisateur doit être en mesure de **se connecter**, comme illustré dans l'image



Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.