CMS einzeln konfigurieren und integrieren

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration und Integration von Cisco Meeting Server (CMS) Single Combined.

Zu konfigurierende Services sind Call Bridge, Webadmin, Web Bridge, Extensible Messaging and Presence Protocol (XMPP) und Lightweight Directory Access Protocol (LDAP).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Communications Manager (CUCM)
- Active Directory (AD)
- Zertifizierungsstelle (Certificate Authority, CA)
- SFTP-Client (Secure File Transfer Protocol)
- DNS-Server (Domain Name Service)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt 1: Zugriff auf CMS

- Wenn Sie sich zum ersten Mal bei CMS anmelden, wird das Willkommen auf dem Bildschirm angezeigt und Sie werden aufgefordert, sich anzumelden.
- Die Standardanmeldeinformationen sind:

Benutzer: Administrator

Kennwort: Administrator

- Nachdem die Anmeldeinformationen eingegeben wurden, fordert der Server Sie zur Eingabe eines neuen Kennworts auf.

```
Welcome to the CMS VM
acano login: admin
Please enter password:
Password has expired
Please enter new password:
Please enter new password again:
Failed logins since last successful login 0
acano>
acano> _
```

- Es wird empfohlen, einen neuen Admin-Benutzer zu erstellen. Dies ist eine gute Vorgehensweise, wenn Sie das Passwort für ein Konto verlieren.
- Geben Sie den Befehl ein: **Benutzer fügt <Benutzername> admin hinzu**
- Geben Sie ein neues Kennwort ein, und bestätigen Sie das neue Kennwort.

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

Schritt 2: Ändern des Hostnamens

- Diese Änderung ist optional.
- Führen Sie den Befehl **hostname <name> aus**
- Server neu starten
- Führen Sie den Befehl **reboot aus**

```
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...
```

Schritt 3: Netzwerkeinstellungen konfigurieren

- Um die aktuellen Einstellungen anzuzeigen, führen Sie den Befehl **ipv4 a**
- IPv4-Konfiguration hinzufügen
- Führen Sie den Befehl **ipv4 <interface> add <ipaddress>/<subnetzmask> <gateway> aus.**

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

- Zeitzone konfigurieren
- Führen Sie den Befehl **timezone <timezoneName> aus.**
- Um alle verfügbaren Zeitzonen anzuzeigen, führen Sie den Befehl **timezone list aus.**
- NTP-Server (Network Time Protocol) hinzufügen
- Führen Sie den Befehl **ntp server add <ipaddress> aus.**

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

- DNS-Server hinzufügen
- Führen Sie den Befehl **dns add forwardZone <domain> <dnsip> aus.**

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

Hinweis: Eine bestimmte Domäne kann für die DNS-Suche konfiguriert werden. Wenn jedoch eine Domäne vom DNS aufgelöst werden kann, verwenden Sie einen Punkt als Domäne.

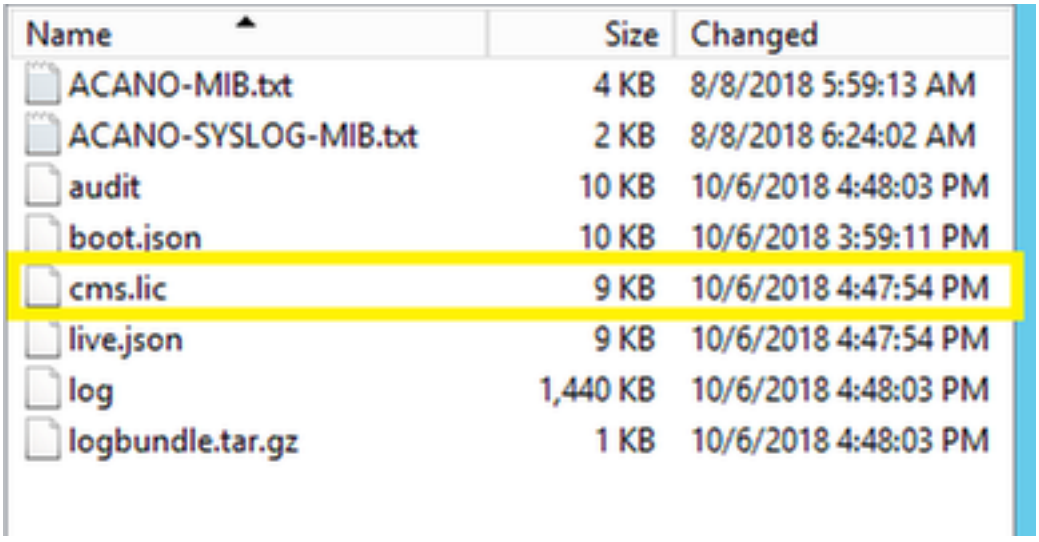
Schritt 4: Lizenzierung des CMS

- Für die Konfiguration der CMS-Dienste muss eine Lizenz installiert sein.
- Um die Lizenz zu generieren und zu installieren, ist die MAC-Adresse (Media Access Control) erforderlich, da die Lizenzen mit ihr abgeglichen werden.
- Führen Sie den Befehl **interface a**
- Kopieren der **MAC-Adresse**
- Wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine Lizenz zu erstellen.

Hinweis: Der Vorgang zum Generieren der Lizenz wird in diesem Dokument nicht behandelt.

```
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>
```

- Benennen Sie die Datei nach dem Speichern der Lizenzdatei in **cms.lic um.**
- Verwenden Sie WinSCP oder einen anderen SFTP-Client, um die Datei auf den CMS-Server hochzuladen.



- Führen Sie nach dem Hochladen der Datei die **Befehlslizenz** aus.
- Server neu starten
- Führen Sie den Befehl **reboot aus**

```
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...
```

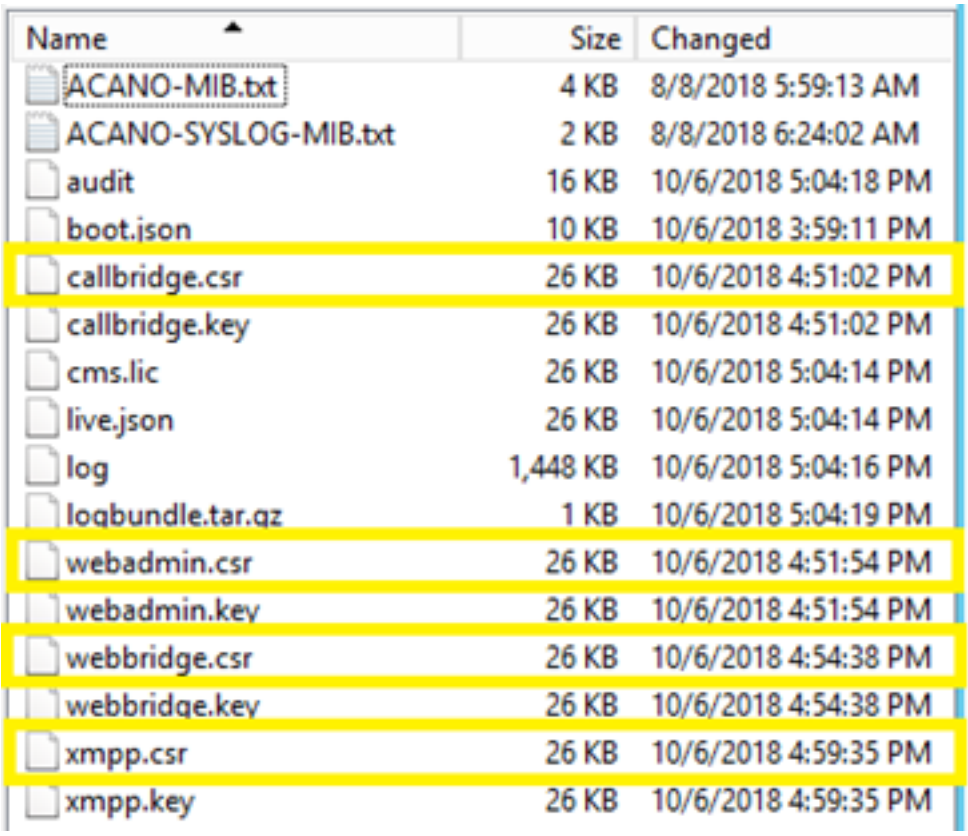
Schritt 5: Erstellen und Installieren von Zertifikaten

- Erstellen einer CSR-Anfrage (Certificate Signing Request) für Callbridge, Webadmin, Webbridge und xmpp
- Führen Sie zu diesem Zweck den Befehl **pki csr <service> CN:<serviceefqdn> aus**.

```
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
```

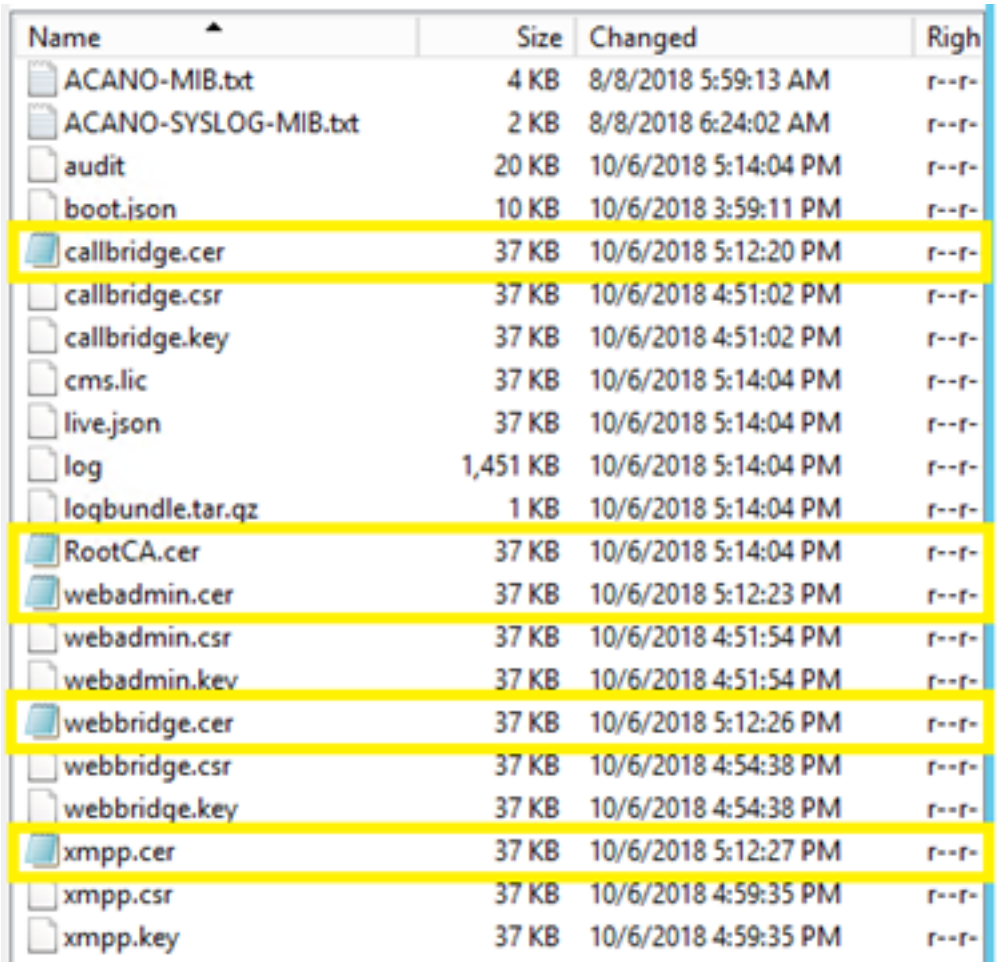
> **Hinweis**: In diesem Beispiel wird für jeden Server ein einzelnes Zertifikat erstellt. Für alle Dienste können Sie ein Zertifikat erstellen. Weitere Informationen zum Erstellen von Zertifikaten finden Sie im Leitfaden zum Erstellen von Zertifikaten.

- Nach Ausführung des Befehls werden zwei Dateien generiert: .**csr**-Datei und eine .**key-**Datei. mit dem Namen des Dienstes, den Sie in den vorherigen Schritten zugewiesen haben.
- Laden Sie die CSR-Dateien vom CMS-Server herunter. Verwenden Sie hierzu WinSCP oder einen anderen SFTP-Client.



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

- Signieren Sie den CSR mit einer Zertifizierungsstelle.
- Stellen Sie sicher, dass Sie eine Vorlage verwenden, die **Webclient-** und **Webserverauthentifizierung** enthält.
- Hochladen des signierten Zertifikats auf den CMS-Server
- Stellen Sie sicher, dass Sie die **Root CA** und jedes **Zwischenzertifikat** hochladen, das die Zertifikate signiert hat.



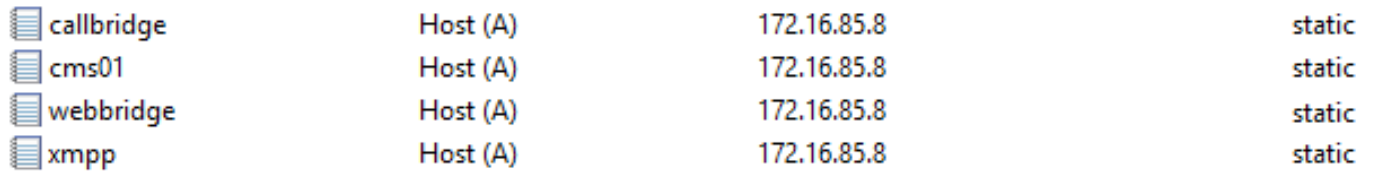
Name	Size	Changed	Righ
ACANO-MIB.txt	4 KB	8/8/2018 5:59:13 AM	r--r-
ACANO-SYSLOG-MIB.txt	2 KB	8/8/2018 6:24:02 AM	r--r-
audit	20 KB	10/6/2018 5:14:04 PM	r--r-
boot.json	10 KB	10/6/2018 3:59:11 PM	r--r-
callbridge.cer	37 KB	10/6/2018 5:12:20 PM	r--r-
callbridge.csr	37 KB	10/6/2018 4:51:02 PM	r--r-
callbridge.key	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-

- Um zu überprüfen, ob alle Zertifikate in CMS aufgeführt sind, führen Sie den Befehl **pki** aus.

```
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>
```

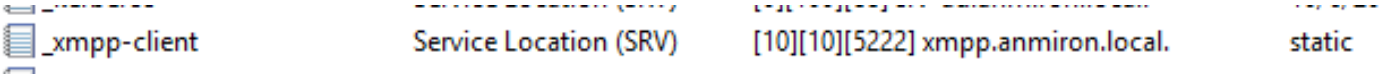
Schritt 6: DNS-Einträge

- Erstellen Sie die DNS-Adressprotokolle (A) für callbridge, xmpp, webadmin und webbridge.
- Stellen Sie sicher, dass alle Datensätze auf die CMS-IP-Adresse zeigen.



- Erstellen eines Service Record (SRV) für **xmpp-client**
- Das Format des Service-Datensatzes ist

Service _xmpp-Client
Protokoll _tcp
Port 522
Ziel Geben Sie den XMPP FQDN ein, z. B. **xmpp.anmiron.local.**



Schritt 7: Servicekonfiguration

Konfigurieren Sie die Callbridge:

- Geben Sie den Befehl **callbridge listen listen <interface> ein.**
- Geben Sie den Befehl **callbridge certs <callbridge-key-file> ein. <crt-Datei> [<cert-bündel>]**
- Die **Schlüsseldatei** ist der Schlüssel, der bei der Erstellung des CSR erstellt wird.
- Das **Zertifizierungspaket** ist das Paket der **Root CA** und eines anderen Zwischenzertifikats.

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

Hinweis: Die Call Bridge Listen-Schnittstelle darf nicht auf einer Schnittstelle eingerichtet werden, die so konfiguriert ist, dass sie Network Address Translation (NAT) für eine andere IP-Adresse verwendet.

Webadmin konfigurieren:

- Führen Sie den Befehl **webadmin listen <interface> <port> aus.**
- Führen Sie den Befehl **webadmin certs <key-file> <crt-file> [<cert-bündel>] aus.**

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

Hinweis: Wenn der Webadmin und die Webbridge auf demselben Server konfiguriert sind, müssen sie auf verschiedenen Schnittstellen konfiguriert sein oder auf verschiedenen Ports abhören. Die Webbridge muss in Port 443 lauschen. Der Webadmin wird normalerweise in Port 445 konfiguriert.

Konfigurieren von XMPP:

- Führen Sie den Befehl **xmpp listen <interface whitelist> aus.**
- Führen Sie den Befehl **xmpp domain <domain name> aus**
- Führen Sie den Befehl **xmpp certs <key-file> <crt-file> [<crt-bündel>] aus.**

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

Hinweis: Der Domänenname muss mit der Domäne übereinstimmen, in der die DNS-Datensätze erstellt wurden.

Webbridge konfigurieren:

- Führen Sie den Befehl **webbridge listen <interface[:port] whitelist> aus.**
- Führen Sie den Befehl **webbridge certs <key-file> <crt-file> [<crt-bündel>] aus.**
- Führen Sie den Befehl **webbridge trust <crt-Paket> aus.**

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

Hinweis: Das trust **crt-Paket** ist das callbridge-Zertifikat und muss der Webbridge hinzugefügt werden, damit die callbridge der webbridge vertrauen kann. Dadurch wird die **Join-as-a-Guest-**Funktion aktiviert.

- Führen Sie den Befehl **callbridge restart aus.**
- Führen Sie den Befehl **wbeadmin enable aus.**
- Führen Sie den Befehl **xmpp enable aus**
- Führen Sie den Befehl **webbridge enable aus**

```
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>
```

Hinweis: Der Server muss **ERFOLG** für alle Services zurückgeben, wenn er **FEHLER** zurückgibt, die vorherigen Schritte überprüfen und alle Konfigurationen auf ihre Richtigkeit überprüfen.

Damit die Call Bridge sicher auf den XMPP-Dienst zugreifen kann, muss ein **Komponentenname** bereitgestellt werden, der für die Authentifizierung mit dem XMPP-Dienst für die Call Bridge verwendet wird.

- Führen Sie den Befehl **xmpp callbridge add <Komponentenname> aus.**
- Das Ergebnis zeigt ein Secret (Geheim), wie im Bild gezeigt.

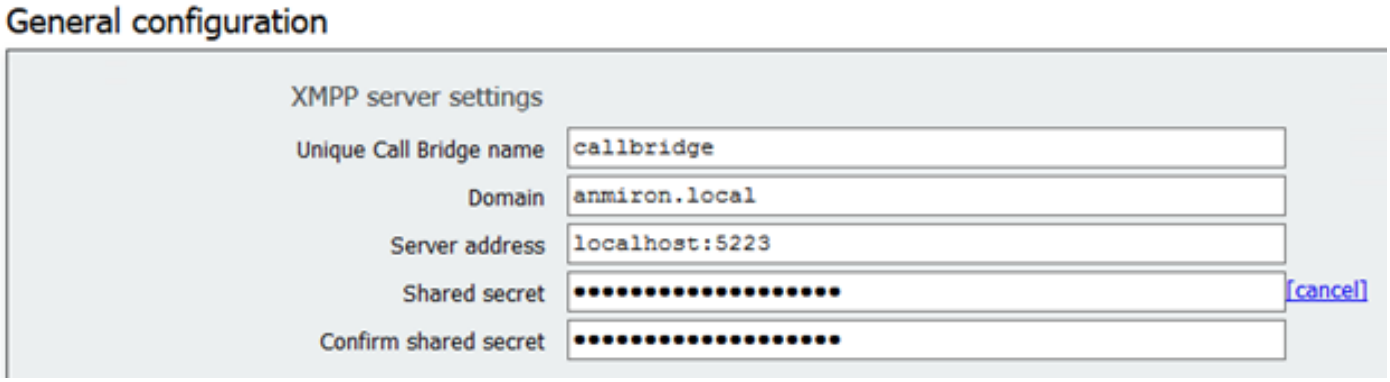
```
CMS01> xmpp callbridge add callbridge
Success             : true
Callbridge : callbridge
Domain     : anmiron.local
Secret     : 6DwNANabpumutI4pAb1
CMS01>
```

- Kopieren des Werts "**Geheime**"
- Zugriff auf die CMS-Webschnittstelle
- Navigieren Sie zu **Konfiguration > Allgemein.**
- Geben Sie die Informationen ein.

Eindeutiger Name der Anrufbrücke	Geben Sie den Namen der erstellten Callbridge ein, z. B. **callbridge**
Domäne	Geben Sie den Domänennamen ein, z. B. **anmiron.local.**

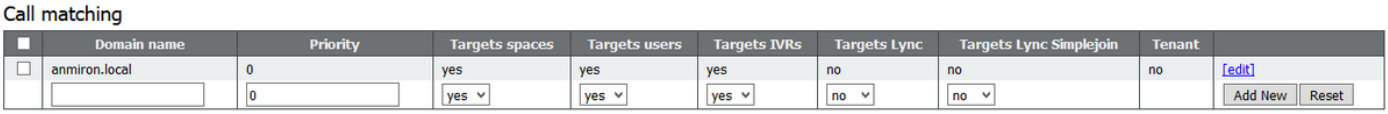
Serveradresse	Legen Sie die CMS-IP-Adresse fest, z. B. **localhost:5223.**
Gemeinsamer geheimer Schlüssel	Geben Sie den im vorherigen Schritt erstellten geheimen Schlüssel ein, z. B. **6DwNANabpumut14pAb1.**

- Wählen Sie **Senden**



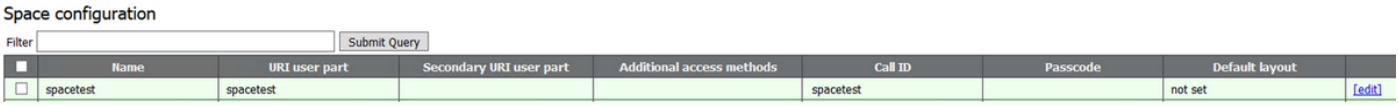
- Erstellen einer **Regel für die Übereinstimmung eingehender Anrufe** für eingehende Anrufe
- Navigieren Sie zu **Konfiguration > Eingehende Anrufe.**
- Geben Sie die Informationen ein.

Domäne	Geben Sie den Domänennamen des CMS-Servers ein, z. B. **anmiron.local.**
Priorität	Geben Sie einen Wert für die Priorität ein, z. B. **0**
Zielbereiche Ja auswählen	



- Erstellen Sie einen Leerzeichen für den Test.
- Navigieren Sie zu **Konfiguration > Leerzeichen**
- Geben Sie die Informationen ein.

Name	Geben Sie einen Namen für das Leerzeichen ein, z. B. **Leerzeichen.**
URI-Benutzerteil	Geben Sie einen URI für den zu benennenden Leerzeichen ein, z. B. **Leerzeichen**
Anruf-ID	Geben Sie die Anruf-ID ein, um diesen Bereich von webbridge aus anzuschließen, z. B. **Leerzeichen.**
Passcode	Geben Sie eine Zahl ein, wenn Sie den Zugriff auf das Leerzeichen zulassen möchten, v dies erforderlich ist.



> **Hinweis**: Der **URI-Benutzerteil** ist das, was die Anrufer in der Domäne wählen müssen, die in der **Regel für die Übereinstimmung eingehender Anrufe** konfiguriert ist, z. B. muss der Anrufer **spacetest@anmiron.local** wählen.

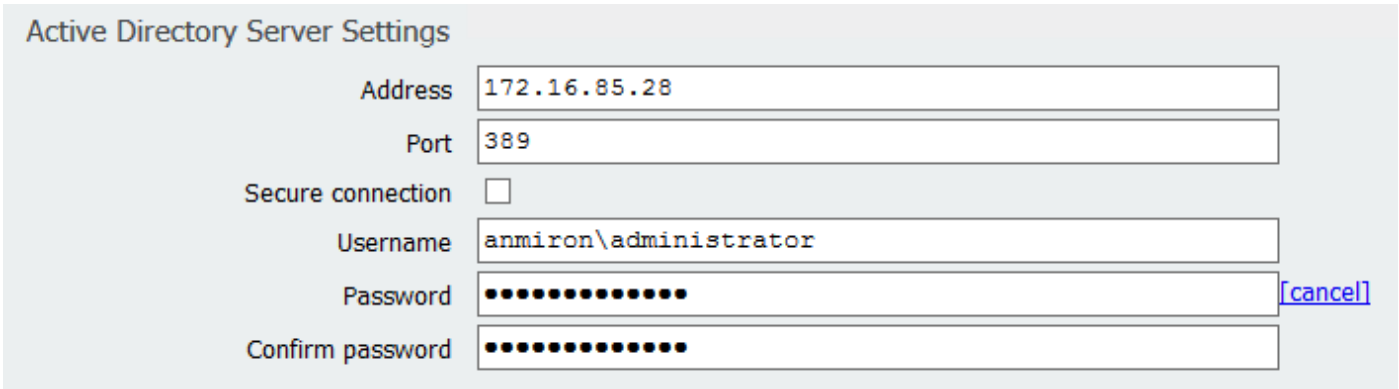
- Navigieren Sie zu **Konfiguration > Allgemein > Webbridge-Einstellungen.**
- Geben Sie die Informationen ein.

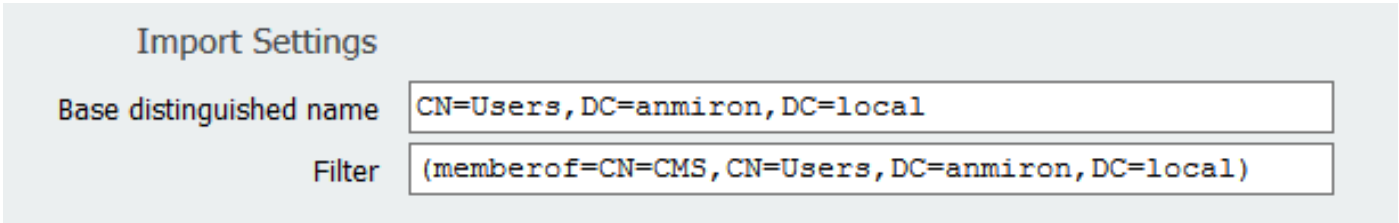
URL des Gastkontos	Dies ist die Webbridge-Webschnittstelle, z. B. https://webbridge.anmiron.loc
JID-Domäne des Gastkontos	Die konfigurierte Domäne in CMS, z. B. **anmiron.local**
Gastzugriff über Hyperlink	Auswahl **zulässig**

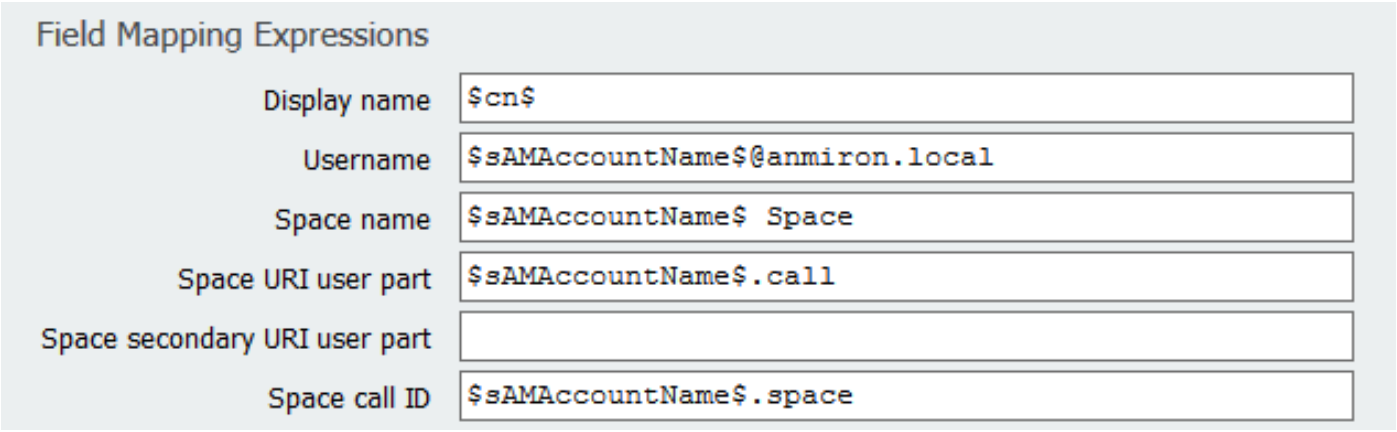
Schritt 8: LDAP integrieren

- Öffnen Sie die CMS-Webschnittstelle.
- Navigieren Sie zu **Konfiguration > Active Directory.**
- Geben Sie die Informationen ein.

Adresse	Die IP-Adresse des LDAP-Servers, z. B. **172.16.85.28**
Port	Dies ist **389**, wenn Sie eine nicht sichere Verbindung verwenden, und **636**, wenn eine sichere Verbindung erforderlich ist.
Benutzername	Geben Sie einen Administrator des LDAP-Servers ein, z. B. **Anmiron\Administrator.**
Kennwort	Geben Sie das Kennwort des Administratorbenutzers ein.
Identifizierter Basisname	Dies ist eine Einstellung aus dem Active Directory, z. B. **CN=Users, DC=anmiron, DC=**
Filtern	Dies ist eine Einstellung aus Active Directory, z. B. **(member of=CN=CMS, CN=Users, DC=anmiron, DC=local).**
Anzeigename	Wie wird der Benutzername angezeigt, z. B. **cn**
Benutzername	Die Anmelde-ID für den Benutzer, z. B. **$sAMAccountName$@anmiron.local**
Leerzeichen	Wie der Speicherplatz angezeigt wird, z. B. **$sAMAccountName$ Space**
Space URI-Benutzerteil	Der auszuwählende URI, z. B. **$sAMAccountName$.call**
Leerlaufanruf-ID	Die Anruf-ID, die von webbridge verwendet wird, z. B. **$sAMAccountName$.space**



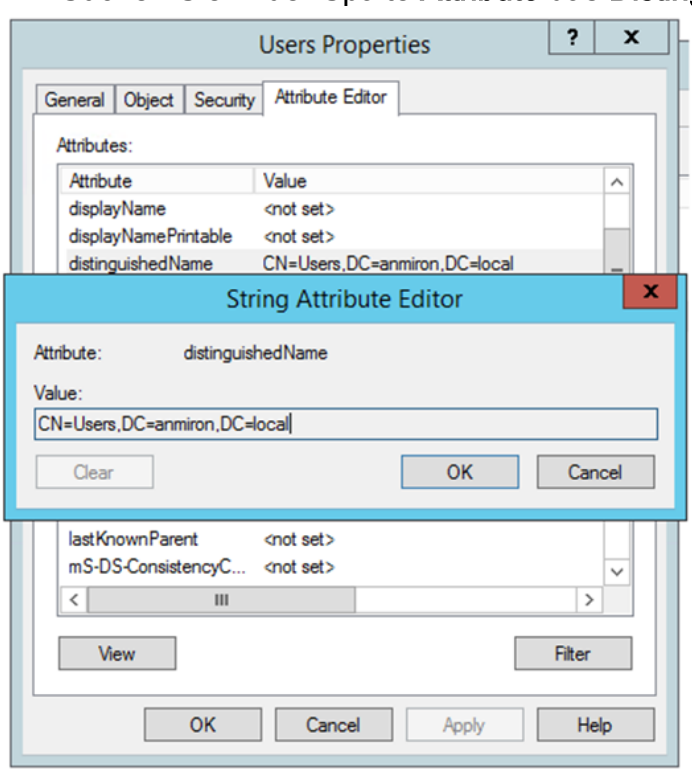


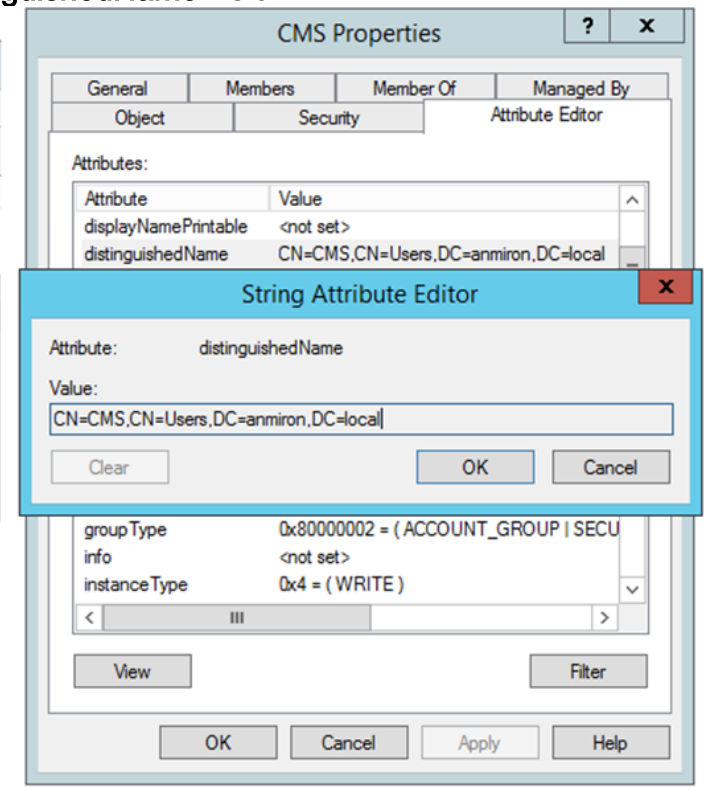


- Wählen Sie **Senden**
- **Jetzt synchronisieren**

Baseline Distinguished Name und Filter sind Einstellungen aus dem Active Directory. Dieses Beispiel enthält grundlegende Informationen zum Abrufen der Informationen mit dem Attribute-Editor in Active Directory. Zum Öffnen Aktivieren Sie im **Attribute-Editor Erweiterte Funktionen** in **Active Directory.** Navigieren Sie zu **Benutzer und Computer > Ansicht**, und wählen Sie **Erweiterte Funktionen aus.**

- In diesem Beispiel wird eine Gruppe mit dem Namen **CMS** erstellt.
- Öffnen Sie die Funktion **Benutzer und Computer** auf AD.
- Wählen Sie den richtigen **Benutzer aus**, und öffnen Sie die Eigenschaften.
- Navigieren zum **Attribut-Editor**
- Suchen Sie in der Spalte **Attribute** das **DistinguishedName**-Feld.

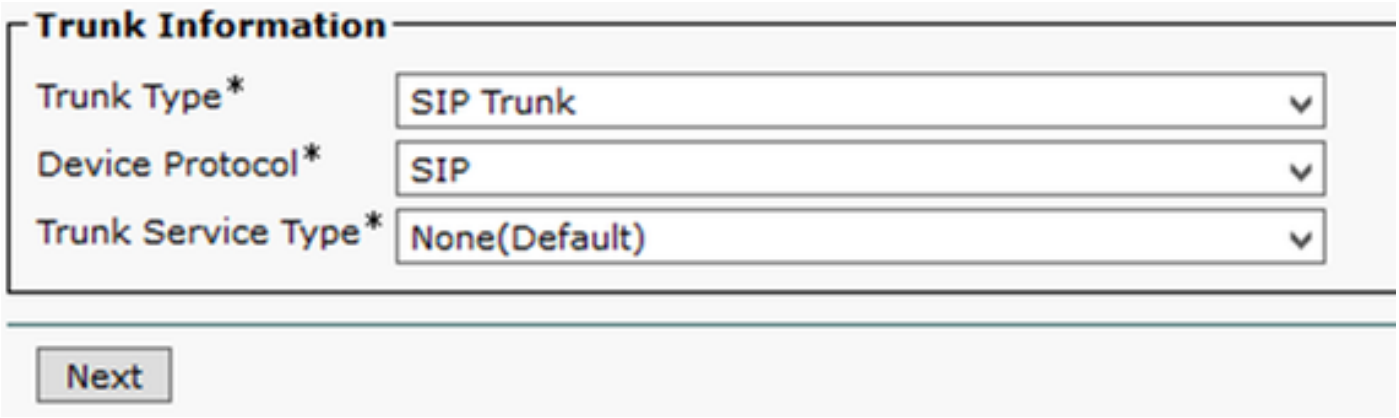




Hinweis: Weitere Informationen zu den LDAP-Filtern finden Sie im [CMS-Bereitstellungsleitfaden.]

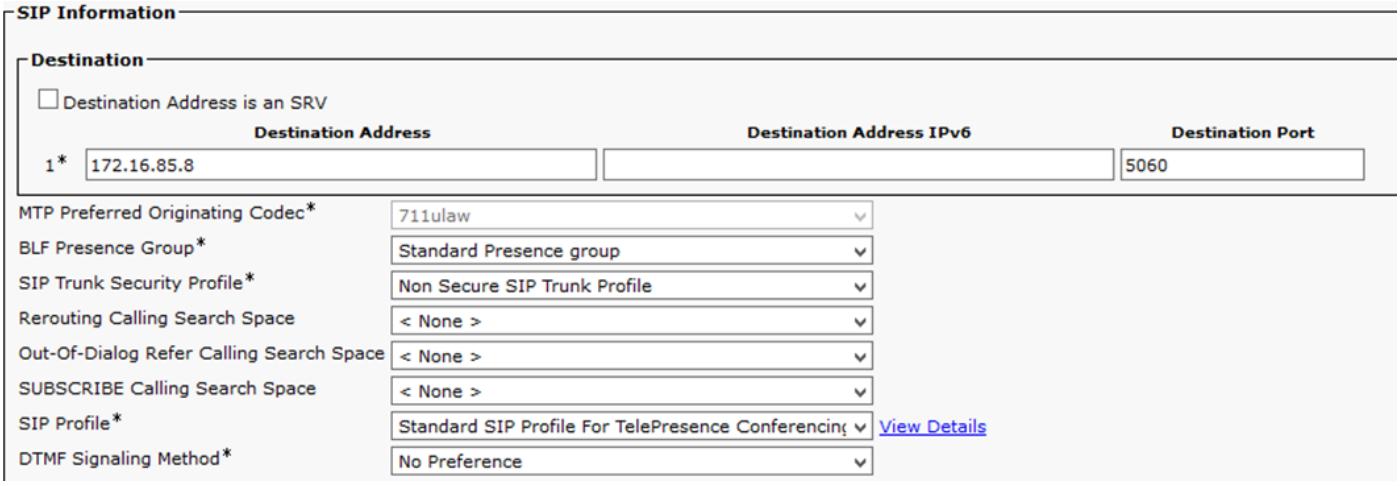
Schritt 9: Konfigurieren von CUCM

- Öffnen Sie die Webschnittstelle von CUCM.
- Navigieren Sie zu **Gerät > Trunks.**
- Wählen Sie **Neu hinzufügen aus**
- Wählen Sie im Dropdown-Menü **Trunk-Typ** die Option **SIP-Trunk aus.**
- **Weiter** auswählen



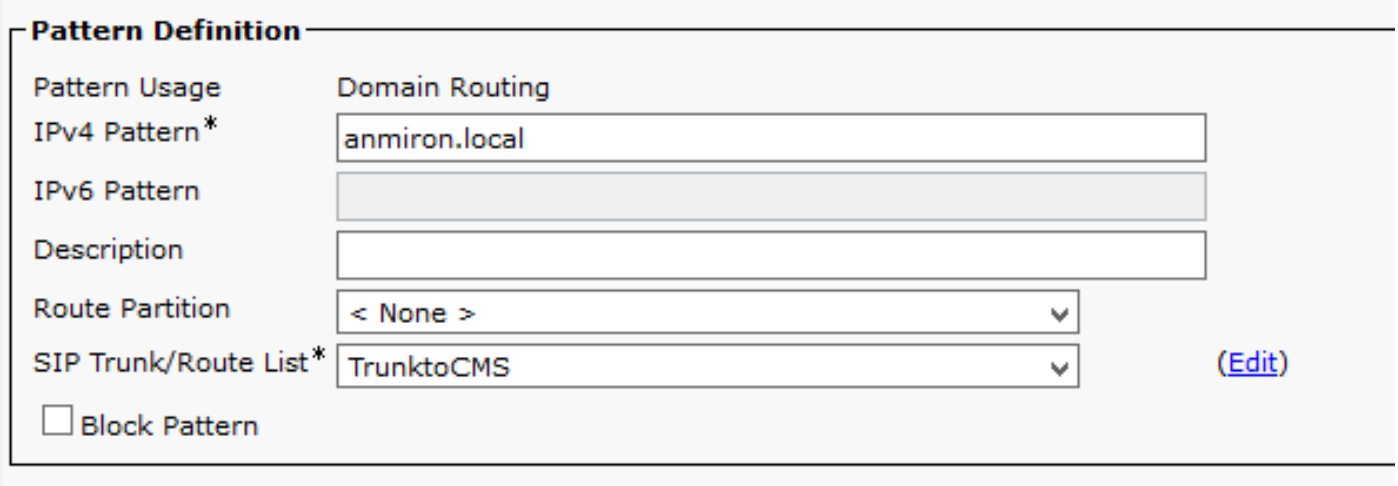
- Geben Sie die Informationen ein.

Gerätename	Geben Sie einen Namen für den SIP-Trunk ein, z. B. **TrunktoCMS.**
Zieladresse	Geben Sie die CMS-IP-Adresse oder den Call Bridge FQDN ein, z. B. **172.16.**
Zielport	Geben Sie den Port ein, an dem das CMS lauscht, z. B. **5060.**
SIP-Trunk-Sicherheitsprofil	Wählen Sie das sichere Profil aus, z. B. **nicht sicheres SIP-Trunk-Profil.**
SIP-Profil	Wählen Sie **Standar-SIP-Profil für TelePresence-Konferenzen aus.**



- Wählen Sie **Speichern**
- Wählen Sie **Zurücksetzen**
- Navigieren Sie zu **Anrufweiterleitung > SIP-Weiterleitungsmuster > Neu hinzufügen > Domänenrouting auswählen.**
- Geben Sie die Informationen ein.

IPv4-Muster	Geben Sie die für CMS konfigurierte Domäne ein, z. B. **anmiron.local.**
SIP-Trunk/Routenliste	Wählen Sie den zuvor erstellten SIP-Trunk, **TrunktoCMS aus.**

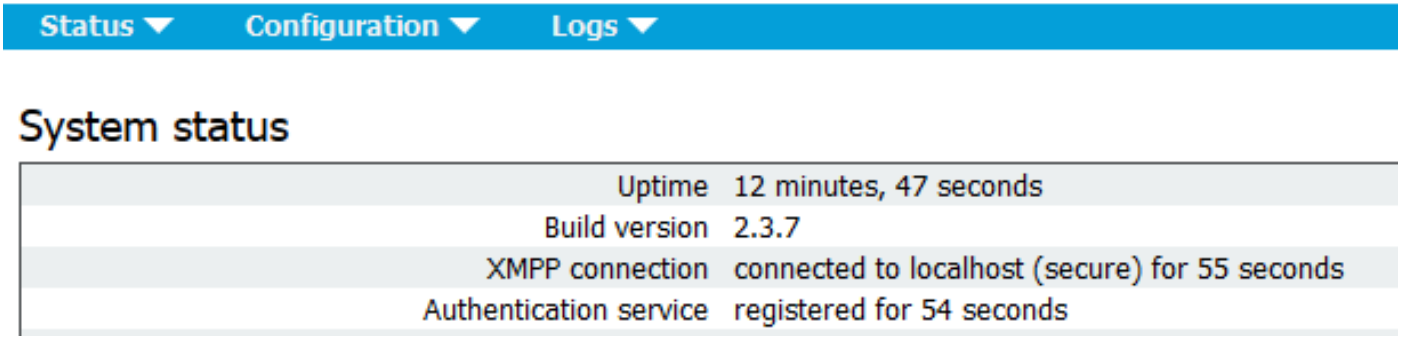


- Wählen Sie **Speichern**

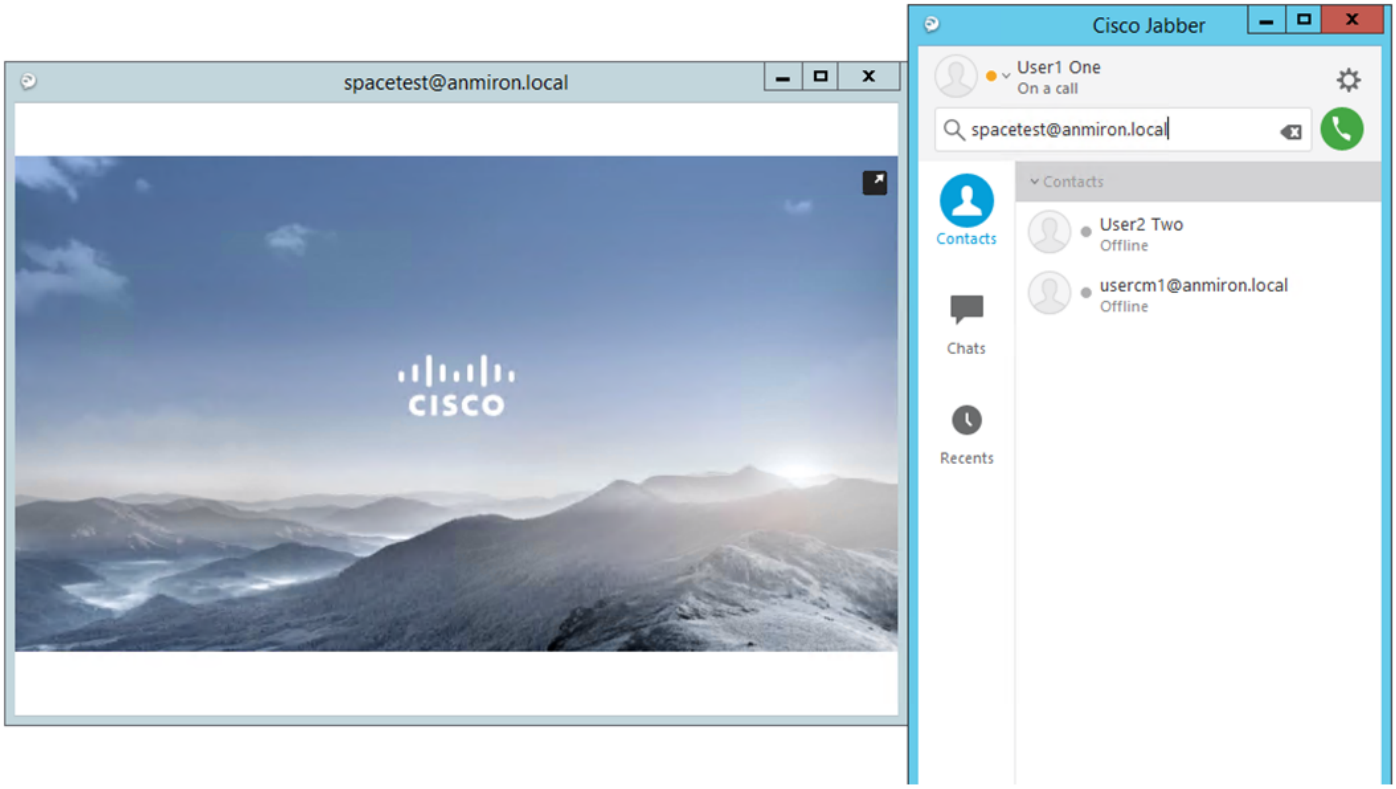
Überprüfen

Callbridge- und XMPP-Kommunikation

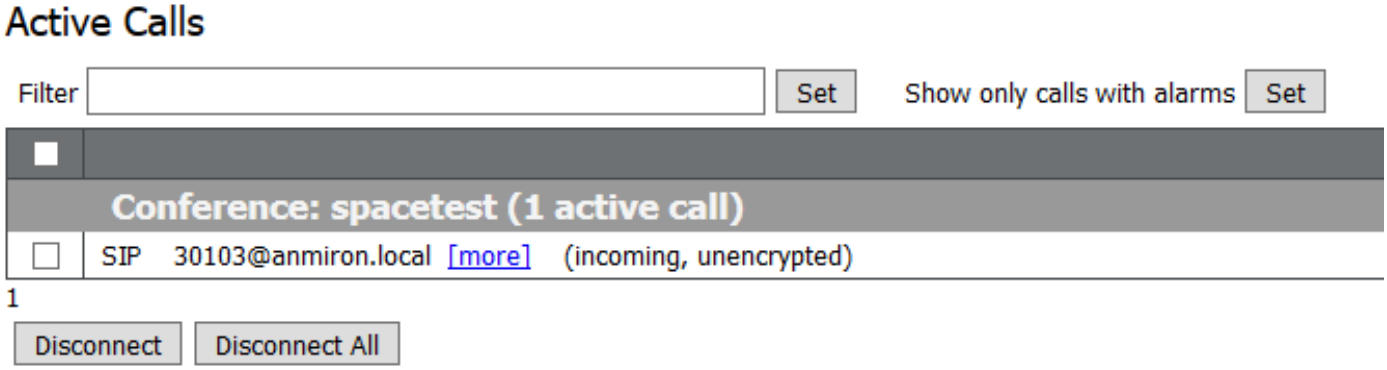
- Öffnen Sie die Webschnittstelle von CMS.
- Navigieren Sie zu **Status > Allgemein.**
- Der XMPP-Verbindungsstatus muss mit localhost verbunden sein.



- Anruf von einem auf CUCM registrierten Gerät tätigen
- Wählen Sie den URI **spacetest@anmiron.local**

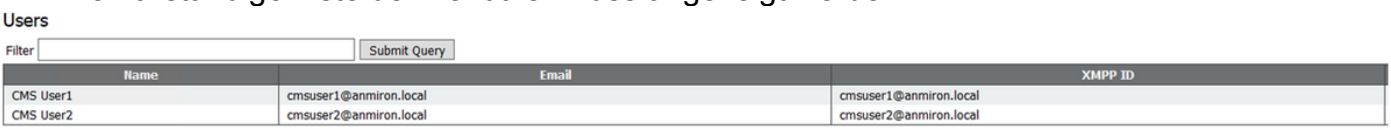


- Öffnen Sie die Webschnittstelle von CMS.
- Navigieren Sie zu **Status > Anrufe.**
- Der Anruf muss als **aktiver Anruf** angezeigt werden.

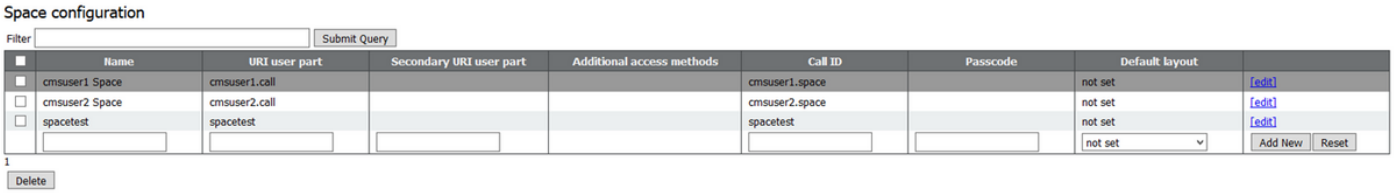


LDAP-Synchronisierung mit CMS

- Öffnen Sie die CMS-Webschnittstelle.
- Navigieren Sie zu **Status > Benutzer.**
- Die vollständige Liste der Benutzer muss angezeigt werden.

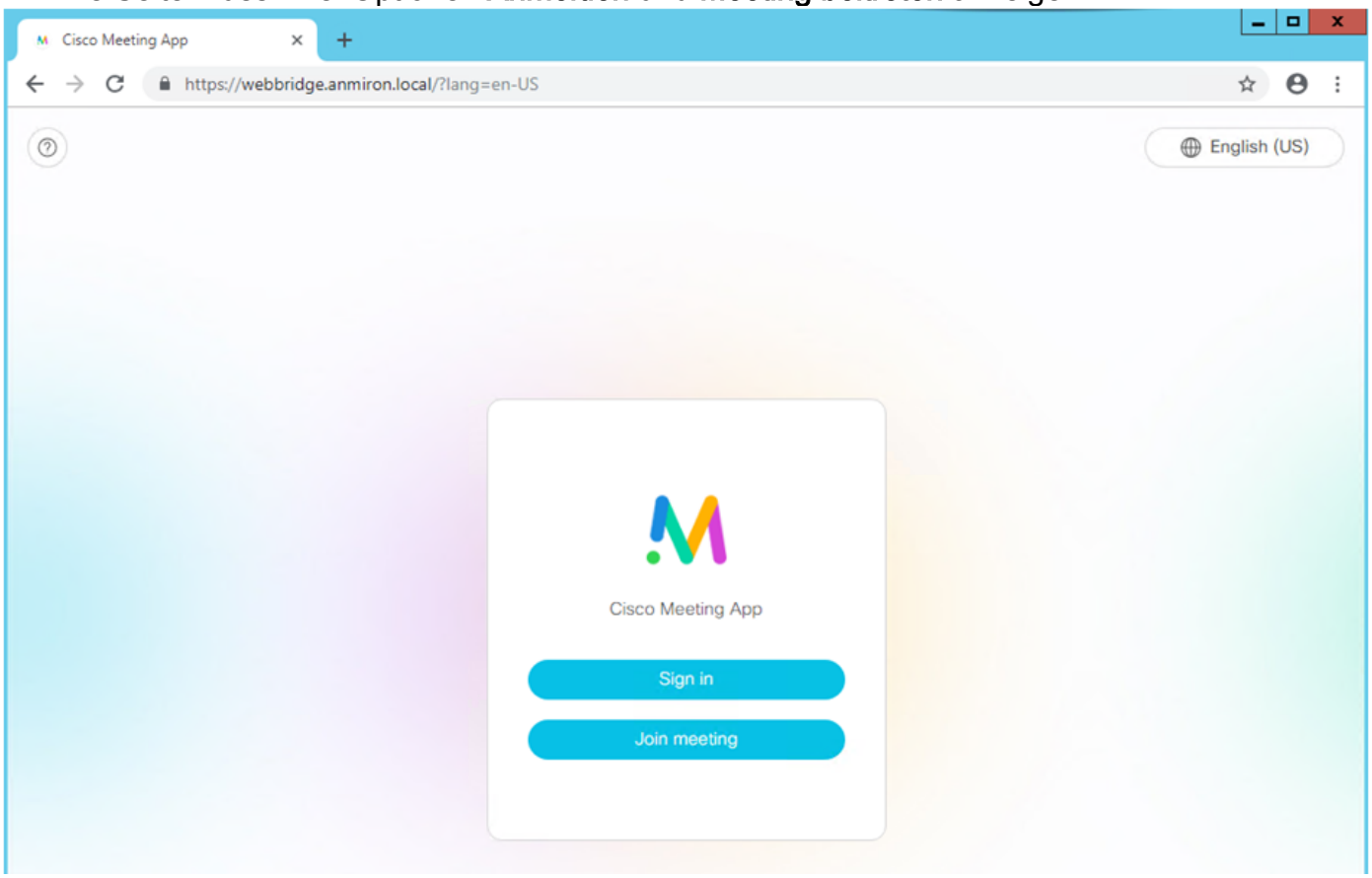


- Navigieren Sie zu **Konfiguration > Leerzeichen**
- Stellen Sie sicher, dass jeder Benutzer über einen eigenen Speicherplatz verfügt.

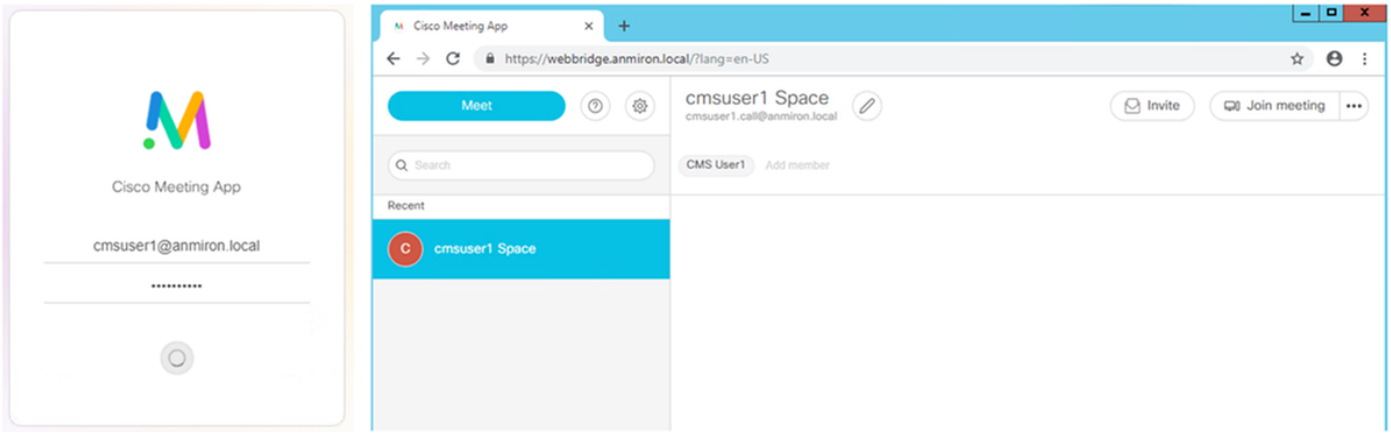


Zugriff auf Webbridge

- Verwenden Sie den Webbrowser, um auf die für den Webbridge-Dienst konfigurierte Webseite zuzugreifen: https://webbridge.anmiron.local
- Die Seite muss zwei Optionen **Anmelden** und **Meeting beitreten** anzeigen



- Die zuvor von AD integrierten Benutzer müssen sich anmelden können.
- Wählen Sie **Anmelden**
- Geben Sie den **Benutzernamen** und das **Kennwort ein.**
- Der Benutzer muss sich **anmelden** können, wie im Bild gezeigt.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.