Configurar e integrar o CMS único e combinado

Contents

Introduction

Este documento descreve como configurar e integrar o Cisco Meeting Server (CMS) único e combinado.

os serviços usados para configuração são o Call Bridge, Webadmin, Web Bridge, Extensible Messaging and Presence Protocol (XMPP) e Lightweight Directory Access Protocol (LDAP)

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- Cisco Unified Communications Manager (CUCM)
- Active Directory (AD)
- autoridade de certificado (CA)
- Cliente Secure File Transfer Protocol (SFTP)
- Protocolo DNS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CMS versão 2.3.7
- CUCM versão 11.5.1
- Google Chrome versão 69.0.3497
- WinSCP versão 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.

Configurar

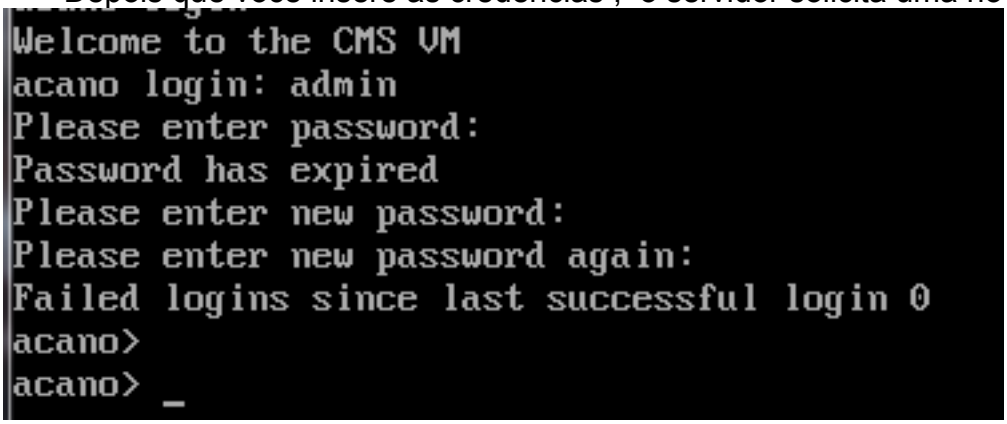
Etapa1. CMS de acesso

- Na primeira vez que você fizer logon no CMS, são mostradas Boas-vindas na tela de solicitação do Logon
- As credenciais padrão são:

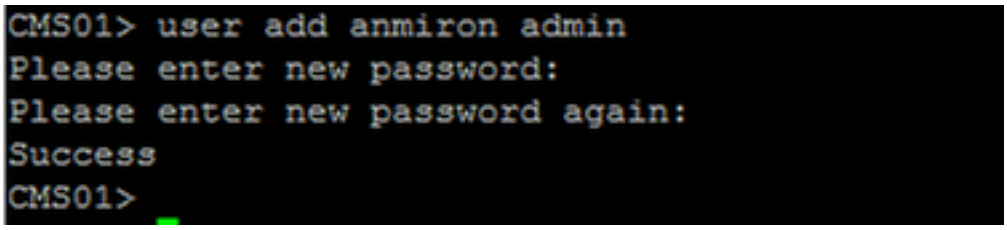
Usuário: admin

Senha: admin

- Depois que você insere as credencias , o servidor solicita uma nova senha



- Recomenda-se a criação de um novo usuário administrador, o que é uma boa prática, caso você perca a senha de uma conta.
- Insira o comando: **user add <username> admin**
- Insira uma nova senha e confirme-a



Etapa 2. Alterar o nome do host

- Essa alteração é opcional
- Execute o comando hostname <name>

- Reinicie o servidor.
- Execute o comando 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...
```

Etapa 3. Definir configurações de rede

- Para exibir as configurações atuais execute o comando **ipv4 a**
- Adicionar configuração de ipv4
- Execute o comando **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>
```

- Configure o fuso horário
- Execute o comando **timezone <timezoneName>**
- Para ver todos os fusos horários disponíveis, execute o comando timezone list
- Adicionar um Servidor Network Time Protocol (NTP)
- Execute o comando 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> _
```

- Adicionar um servidor DNS
- Execute o comando **dns add forwardzone <domain> <dnsip>**

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

> **Note**: Um domínio específico pode ser configurado para pesquisa de DNS, no entanto se qualquer domínio puder ser resolvido com o DNS, então use um ponto como o domínio

Etapa 4. Licença do CMS

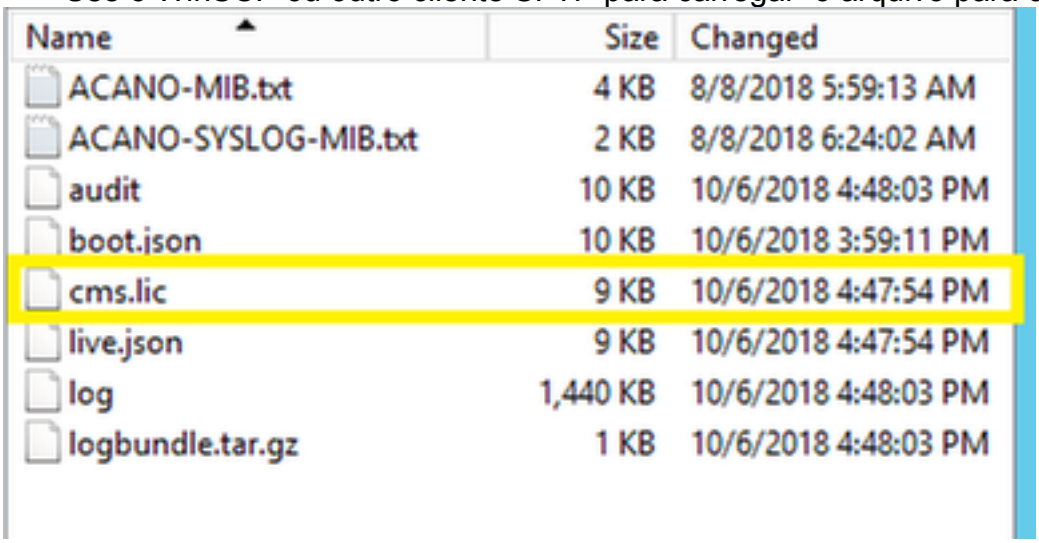
- É necessário instalar uma licença para configurar os serviços de CMS

- Para gerar e instalar a licença, é necessário o endereço do Media Access Control (MAC), já que as licenças serão comparadas a ele.
- Execute o comando **iface a**
- Copie o **Endereço MAC**
- Entre em contato com o representante de vendas para que uma licença seja gerada.

Note: O processo para gerar a licença não é abordado neste documento.

```
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>
```

- Assim que você tiver o arquivo de licença, renomeie-o como **cms.lic**
- Use o WinSCP ou outro cliente SFTP para carregar o arquivo para o servidor do CMS



- Depois que o arquivo for carregado execute a licença de comando
- Reinicie o servidor.
- Execute o comando 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...
```

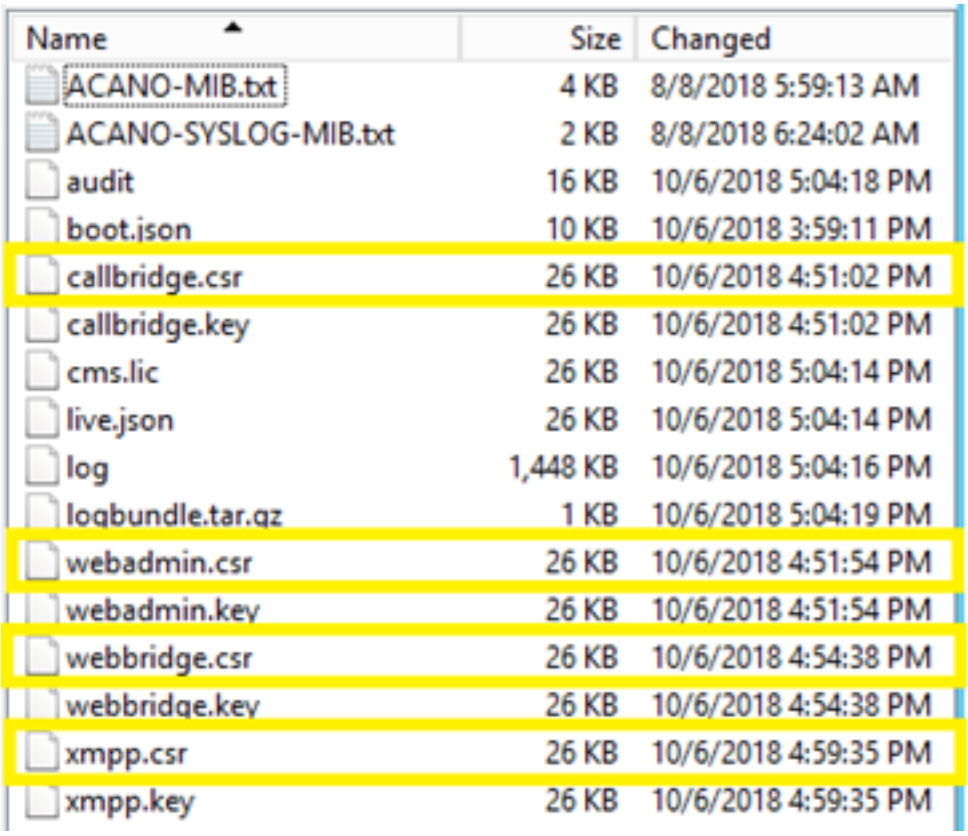
Etapa 5. Gerar e instalar certificados

- Gere uma solicitação de assinatura de certificado (CSR) para callbridge, webadmin, webbridge e xmpp
- Execute o comando **pki csr <service> CN:<servicefqdn>** para esse fim.

```
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
```

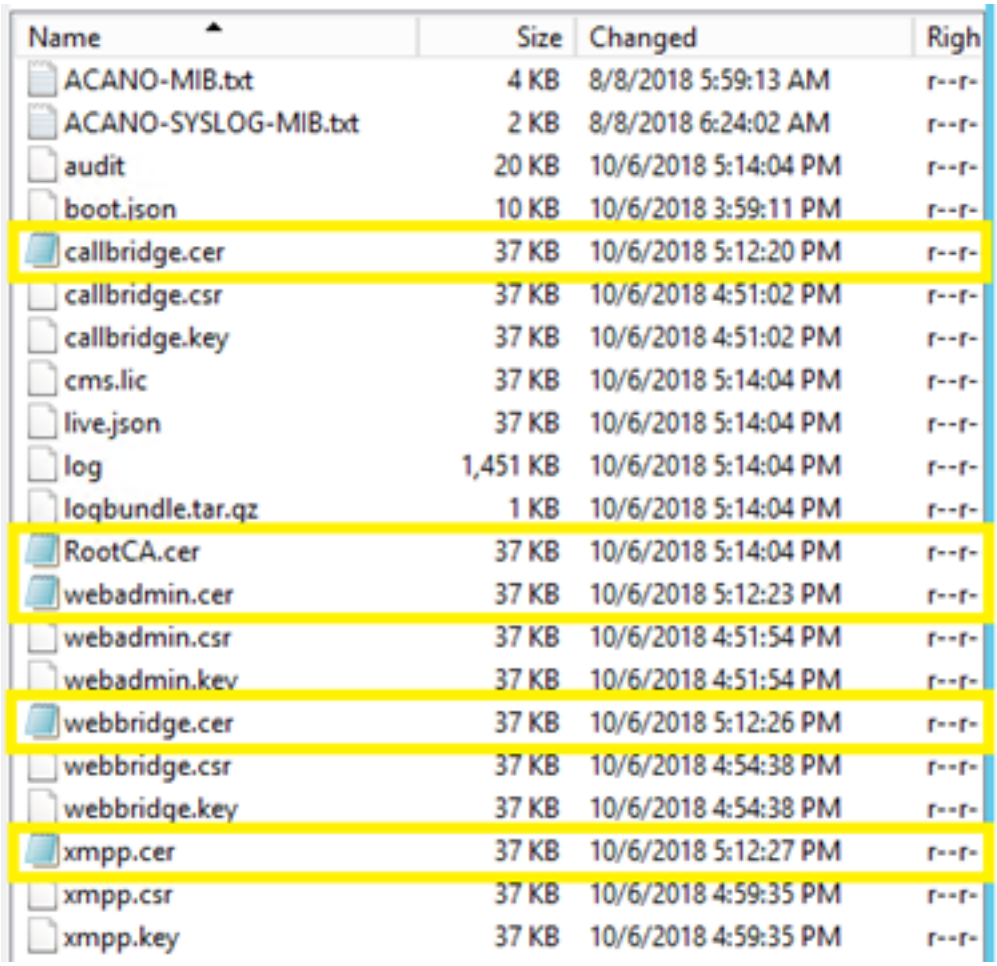
Note: Neste exemplo, é criado um único certificado para cada servidor, porém é possível criar um certificado para todos os serviços. Para obter mais informações sobre a criação de certificados, revise o Guia de criação do certificado

- Dois arquivos gerados após a execução do comando: arquivo .csr e arquivo .key. com o nome do serviço atribuído em etapas anteriores.
- Baixe os arquivos CSR do servidor CMS. Use WinSCP ou outro cliente SFTP para essa finalidade.



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

- Conecte-se ao CSR com uma Certificate Authority
- Certifique-se de usar um modelo que contenha **cliente Web e autenticação do servidor da Web**
- Carregue o certificado assinado para o servidor do CMS
- Certifique-se de carregar **CA raiz e qualquer certificado intermediário** que assinou os certificados



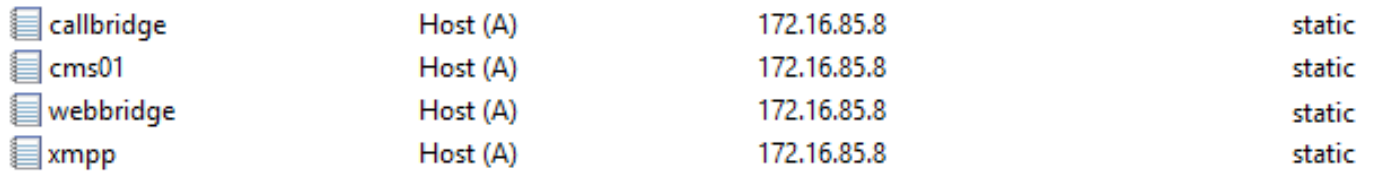
Name	Size	Changed	Righ
ACANO-MIB.txt	4 KB	8/8/2018 5:59:13 AM	r--r-
ACANO-SYSLOG-MIB.txt	2 KB	8/8/2018 6:24:02 AM	r--r-
audit	20 KB	10/6/2018 5:14:04 PM	r--r-
boot.json	10 KB	10/6/2018 3:59:11 PM	r--r-
callbridge.cer	37 KB	10/6/2018 5:12:20 PM	r--r-
callbridge.csr	37 KB	10/6/2018 4:51:02 PM	r--r-
callbridge.key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

- Para verificar se todos os certificados estão listados no CMS, execute o comando **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>
```

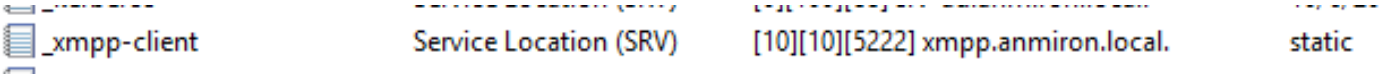
Etapa 6. Registros de DNS

- Crie os registros de endereço DNS (A) para callbridge, xmpp, webadmin e webbridge
- Certifique-se de que todos os registros apontem para o endereço IP do CMS



- Crie um registro de serviço (SRV) para **xmpp-client**
- O formato de registro de serviço é

Serviço _xmpp-client
Protocolo TCP
Porta 5222
Destino Digite o FQDN XMPP, por exemplo **xmpp.anmiron.local**



Passo 7. Configuração do serviço

Configure o callbridge:

- Digite o comando **callbridge listen <interface>**
- Digite o comando **callbridge certs <callbridge-key-file> <crt-file> [<cert-bundle>]**
- O **key-file é a chave criada quando o CSR é criado**
- O **cert-pacote é o pacote do CA raiz e qualquer outro certificado intermediário**

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

Note: A interface de escuta do Call Bridge não deve ser definida em uma interface que está configurada para usar o Network Address Translation (NAT) para outro Endereço IP

Configure o webadmin:

- Execute o comando **webadmin listen <interface> <port>**
- Execute o comando **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: Se o webadmin e webbridge estiverem configurados no mesmo servidor, eles devem ser configurados em interfaces distintas ou para ouvirem em portas diferentes. O webbridge precisa ouvir na porta 443. O webadmin é normalmente configurado na porta 445.

Configure XMPP:

- Execute o comando **xmpp listen <interface whitelist>**
- Execute o comando **xmpp domain <domain name>**

- Execute o comando **xmppcerts <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: O nome do domínio deve corresponder ao domínio onde os registros DNS foram criados.

Configure o webbridge:

- Execute o comando **webbridge Listen <interface[:port] whitelist>**
- Execute o comando **webbridge certs <key-file> <crt-file> [<crt-bundle>]**
- Execute o comando **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: A relação de confiança **crt-pacote é o certificado de callbridge e deve ser adicionado ao webbridge na ordem para a callbridge confiar no webbridge, isso ativará o recurso Ingressar como Convidado.**

- Execute o comando **callbridge restart**
- Execute o comando **wbeadmin enable**
- Execute o comando **xmpp enable**
- Execute o comando **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: O servidor deve retornar **SUCCESS para todos os serviços, se ele retornar FAILURE**, revise as etapas anteriores e valide se toda a configuração está correta

Para permitir que a Call Bridge acesse o serviço XMPP com segurança, é necessário fornecer um **nome do componente para a Call Bridge usar para autenticação com o serviço XMPP.**

- Execute o comando **xmpp callbridge ads <component name>**
- O resultado mostra um Segredo, como mostrado na imagem

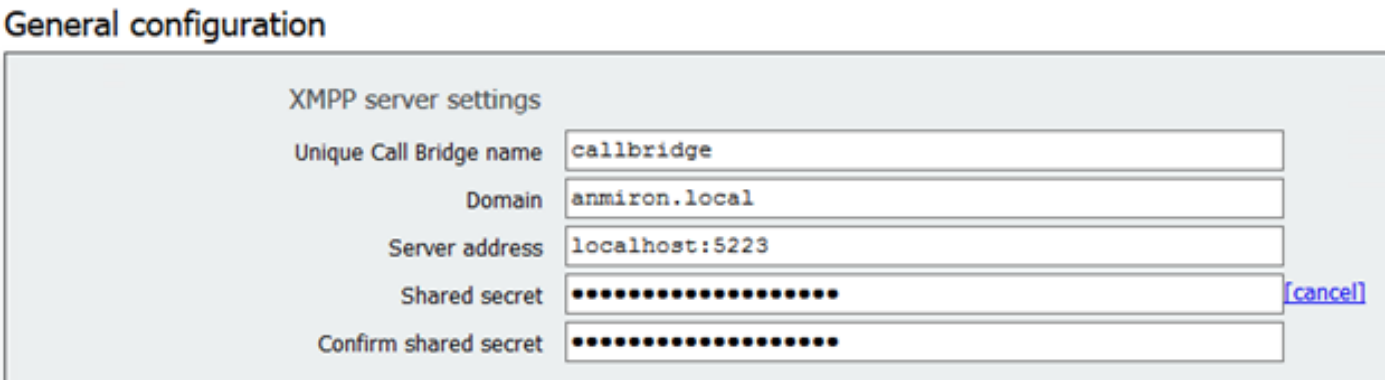
```
CMS01> xmpp callbridge add callbridge
Success              : true
Callbridge : callbridge
Domain     : anmiron.local
Secret     : 6DwNANabpumutI4pAb1
CMS01>
```

- Copie o **Valor secreto**
- Acesso à interface da Web do CMS
- Navegue até **Configuração > Geral**
- Inserir informações

Nome da Call Bridge exclusivo	Digite o nome da callbridge criada, por exemplo **callbridge**
domínio	Insira o nome do domínio, por exemplo **anmiron.local**
Endereço do servidor	Defina o Endereço IP do CMS, por exemplo **localhost:5223**
Shared secret	Digite o segredo criado na etapa anterior, por

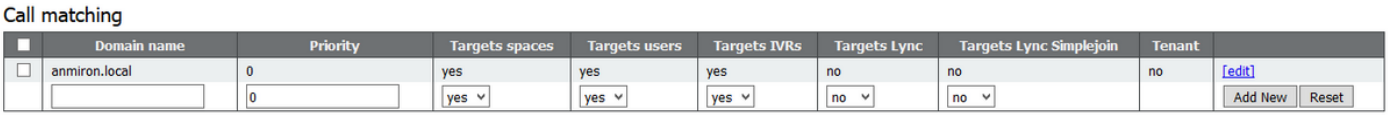
exemplo **6DwNANabpumut14pAb1**

- Selecionar**Enviar.**



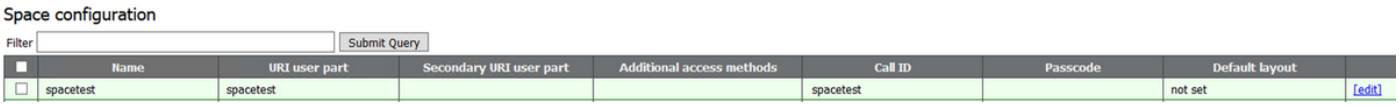
- Criar uma **Regra de correspondência de chamada recebida para as chamadas recebidas**
- Navegue até **Configuração > Chamadas recebidas**
- Inserir informações

domínio	Insira o nome do domínio do servidor CMS, por exemplo **anmiron.local**
Prioridade	Insira um valor para a prioridade, por exemplo **0**
Espaços de destino	Selecione **sim**



- Criar um espaço para teste
- Navegue até **Configuração > Espaços**
- Inserir informações

Nome	Insira um nome para o espaço, por exemplo **spacetest**
Parte de usuário da URI	Insira uma URI para este espaço que pode ser chamado, por exemplo **spacetest**
ID da chamada	Digite a ID de chamada para entrar nesse espaço do webbridge, por exemplo **spacetest**
Senha	Digite um número para permitir o acesso ao espaço, se for necessário



> **Note**: A **parte de usuário da URI é o que os autores da chamada precisam discar no domínio configurado na Regra de correspondência de chamada recebida**, por exemplo, ele deve discar **spacetest@anmiron.local**

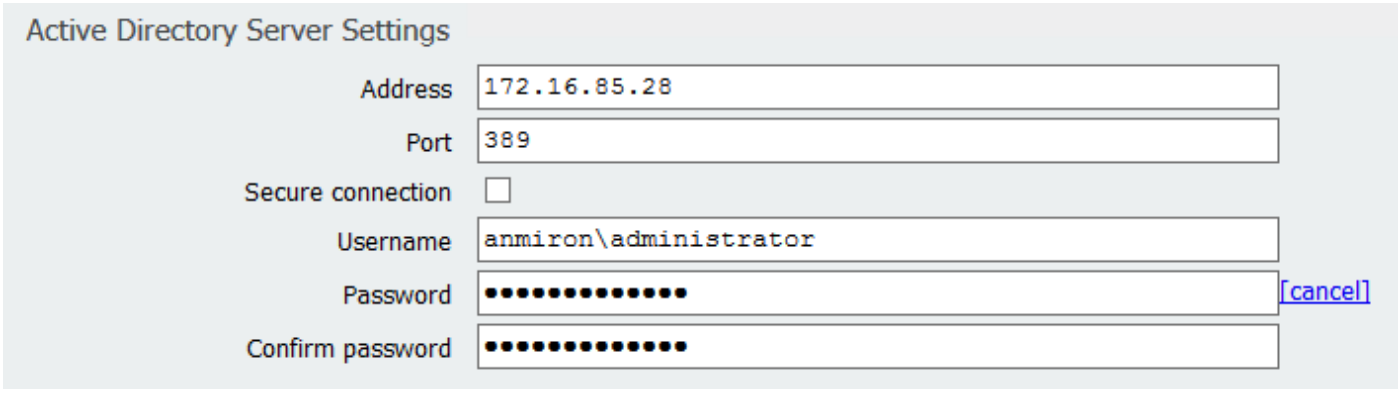
- Navegue até **Configuração > Geral > Configurações de Web bridge**
- Inserir informações

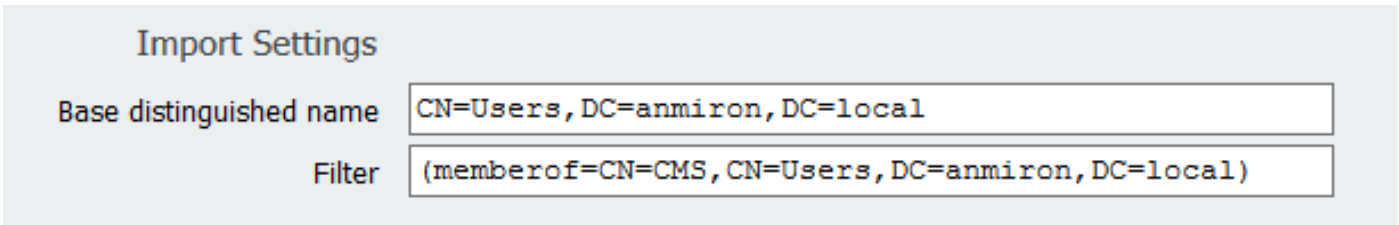
Cliente de conta de convidado URI	Isso é a interface da Web do webbridge, por exemplo https://webbridge.anmiron.local
Domínio de JID de conta de convidado	O domínio configurado no CMS, por exemplo **anmiron.local**
Acesso de convidado por meio do hiperlink	Selecione **permitido**

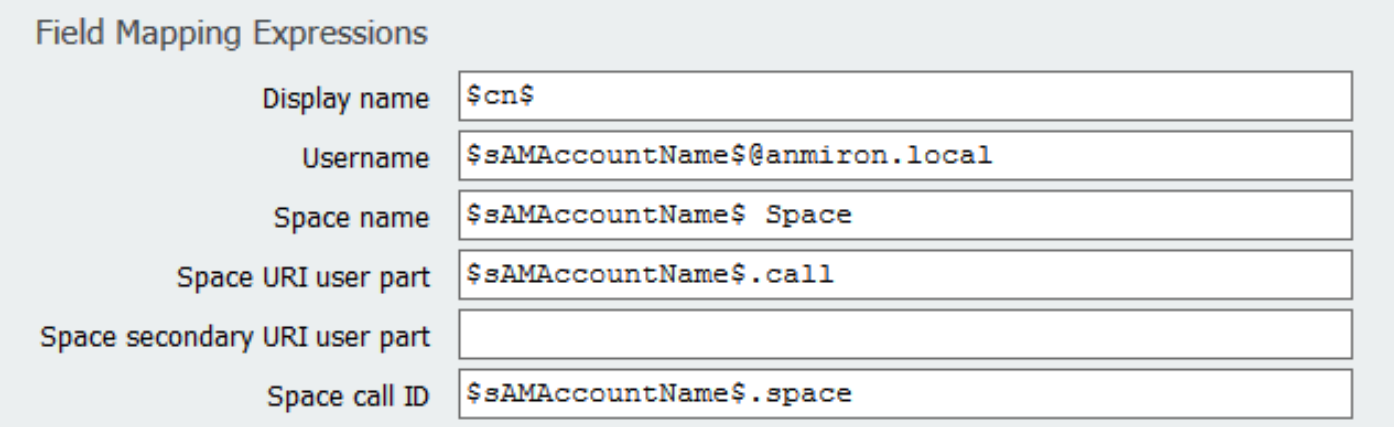
Etapa 8. Integrar LDAP

- Abra a interface da Web do CMS
- Navegue até **Configuração > Active Directory**
- Inserir informações

Endereço	O Endereço IP do servidor LDAP, por exemplo **172.16.85.28**
Porta	Isso é**389 , se você estiver usando uma conexão não segura e 636 , se for necessária uma conexão segura**
Nome de usuário	Insira um administrador do servidor LDAP, por exemplo **anmiron\administrator**
Senha	Digite a senha do usuário Administrador
Nome distinto da base	Essa é uma configuração do Active directory, por exemplo **CN = Users, DC = anmiron, DC = local**
Filtrar	Essa é uma configuração do Active directory, por exemplo **(memberof=CN=CM CN-=Users, DC=anmiron, DC=local)**
Nome de exibição	Como o nome de usuário é mostrado, por exemplo **cn**
Nome de usuário	A ID de login do usuário, por exemplo **$sAMAccountName$@anmiron.local**
Nome do espaço	Como o espaço é mostrado, por exemplo **$sAMAccountName$ Space**
Parte de usuário da URI do espaço	A URI a ser discada, por exemplo **$sAMAccountName$.call**
ID de chamada de espaço	A ID de chamada a ser usada em webbridge, por exemplo **$sAMAccountName$.space**



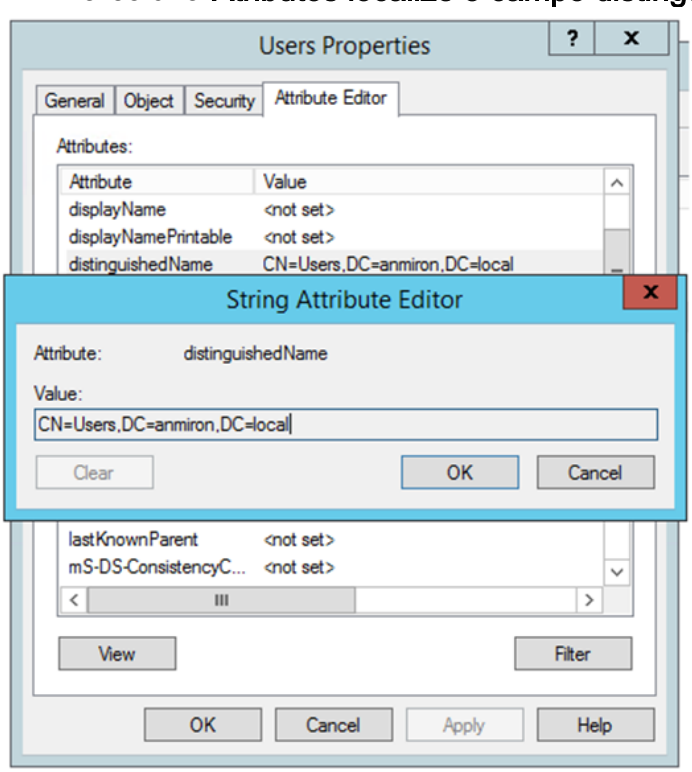


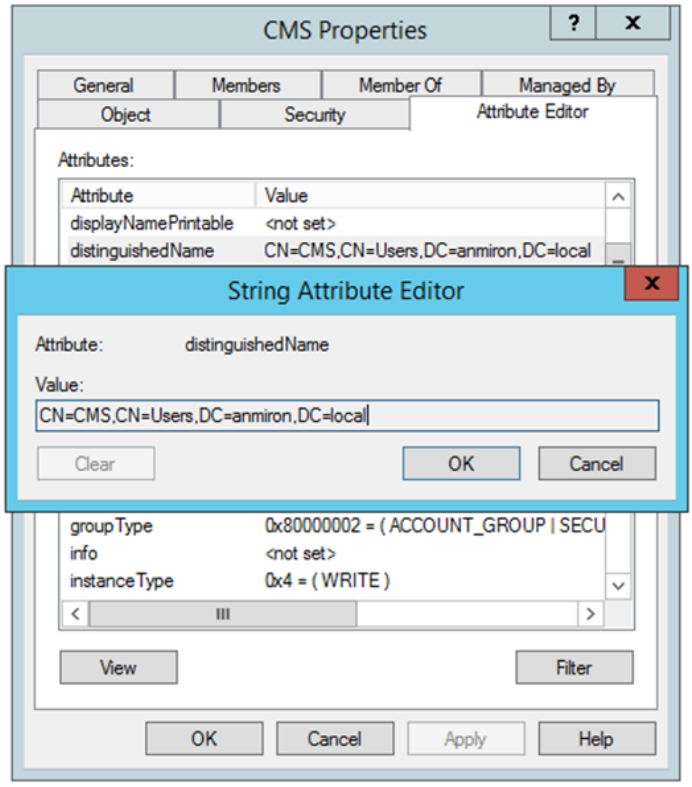


- SelecionarEnviar.
- Selecione Sincronizar agora

Nome distinto da base e Filtro são configurações do Active Directory. Este exemplo contém o básico sobre como obter as informações com Editor de atributos no Active Directory. Para abrir no Editor de atributos, ative Recursos avançados no Ative Diretory. Navegue até Usuários e computadores > Exibição e selecione Recursos avançados

- Para este exemplo, é criado um grupo chamado CMS
- Abra o recurso Usuários e computadores no AD
- Com o botão direito do mouse, selecione um usuário e abra as propriedades
- Navegue até Editor de atributo
- Na coluna Atributos localize o campo distinguishedName

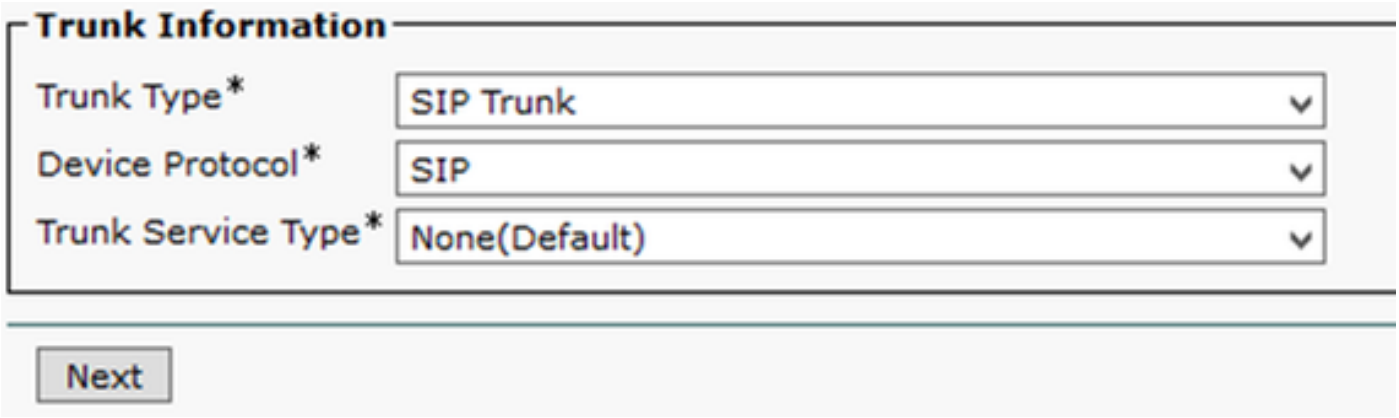




Note: Para obter mais informações sobre os filtros LDAP, acesse o Guia de implantação do CMS

Etapa 9. Configurar CUCM

- Abra a interface da Web do CUCM
- Navegue até **Dispositivo > Troncos**
- Selecione **Adicionar novo**
- Em **Tipo de tronco do menu suspenso, selecione Tronco SIP**
- Selecione **Próximo**



- Inserir informações

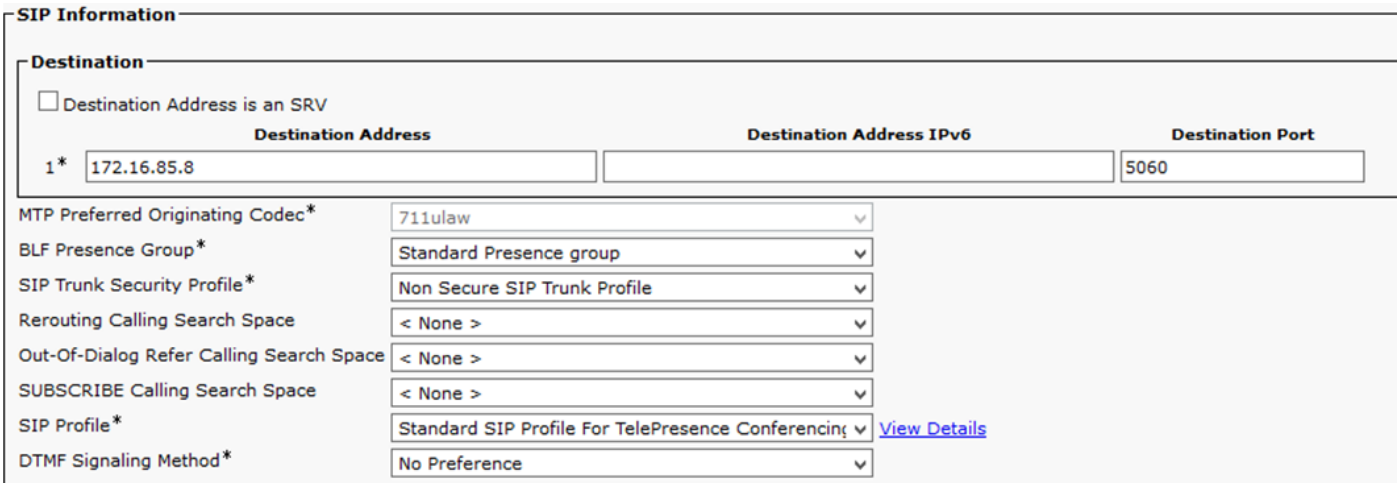
Nome de dispositivo Insira um nome para o tronco SIP, por exemplo **TrunktoCMS**

Endereço de destino Digite o Endereço IP do CMS ou o FQDN de Call Bridge, por exemplo **172.16.85.8**

Porta de Destino Insira a porta onde o CMS escuta, por exemplo **5060**

Perfil de Segurança de Tronco de SIP Selecione o perfil seguro, por exemplo **Perfil de tronco SIP não segur**

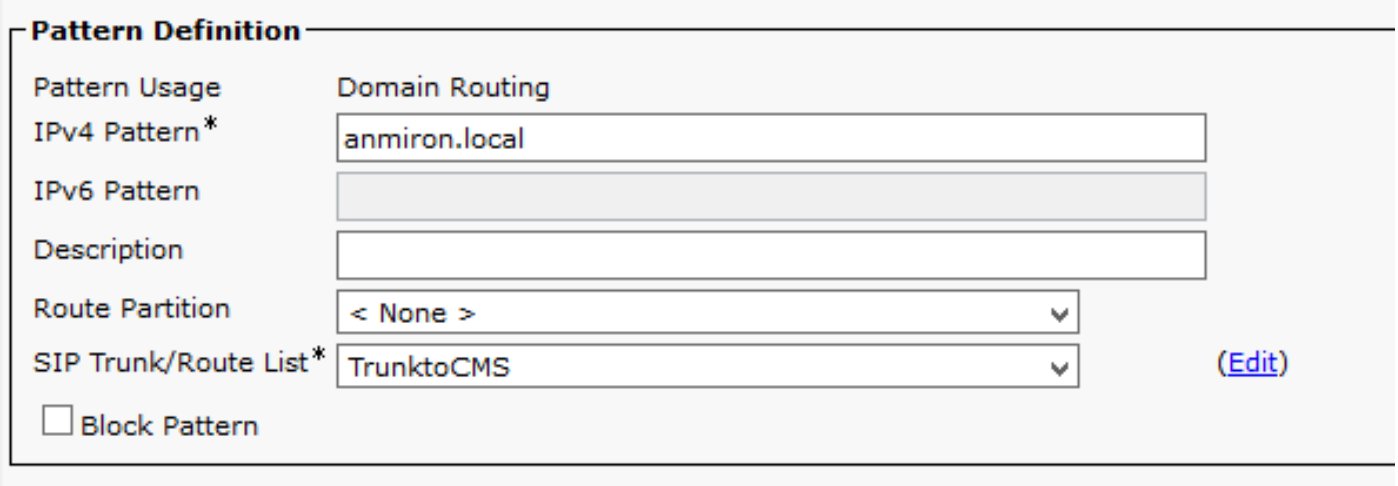
Perfil SIP Selecione **Perfil SIP padrão para conferência de TelePresence**



- Selecione **Salvar**
- Selecione **Redefinir**
- Navegue até **Roteamento de chamada > Padrão de rota SIP > Adicionar novo > Selecionar domínio de roteamento**
- Inserir informações

Padrão de IPv4 Digite o domínio configurado para CMS, por exemplo **anmiron.local**

Lista de rota/tronco SIP Selecione os Troncos SIP criados anteriormente, **TrunktoCMS**

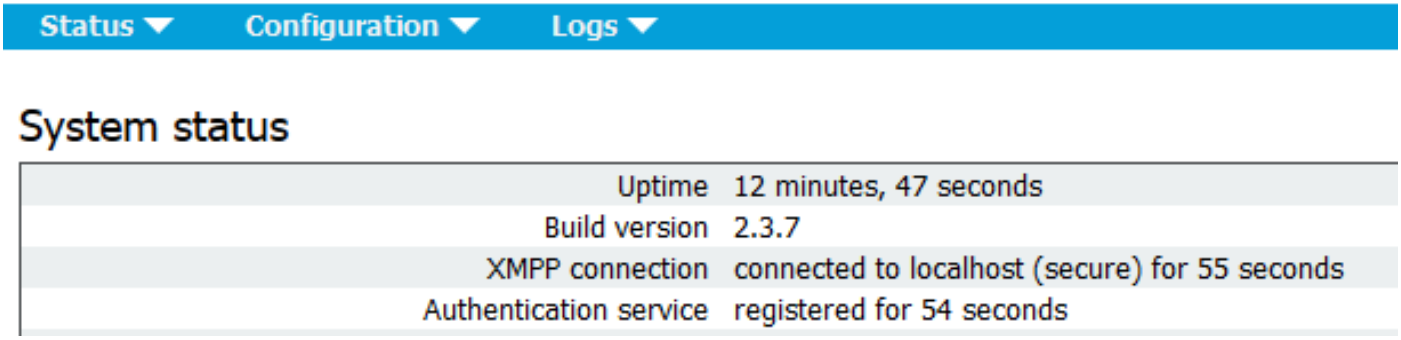


- Selecione **Salvar**

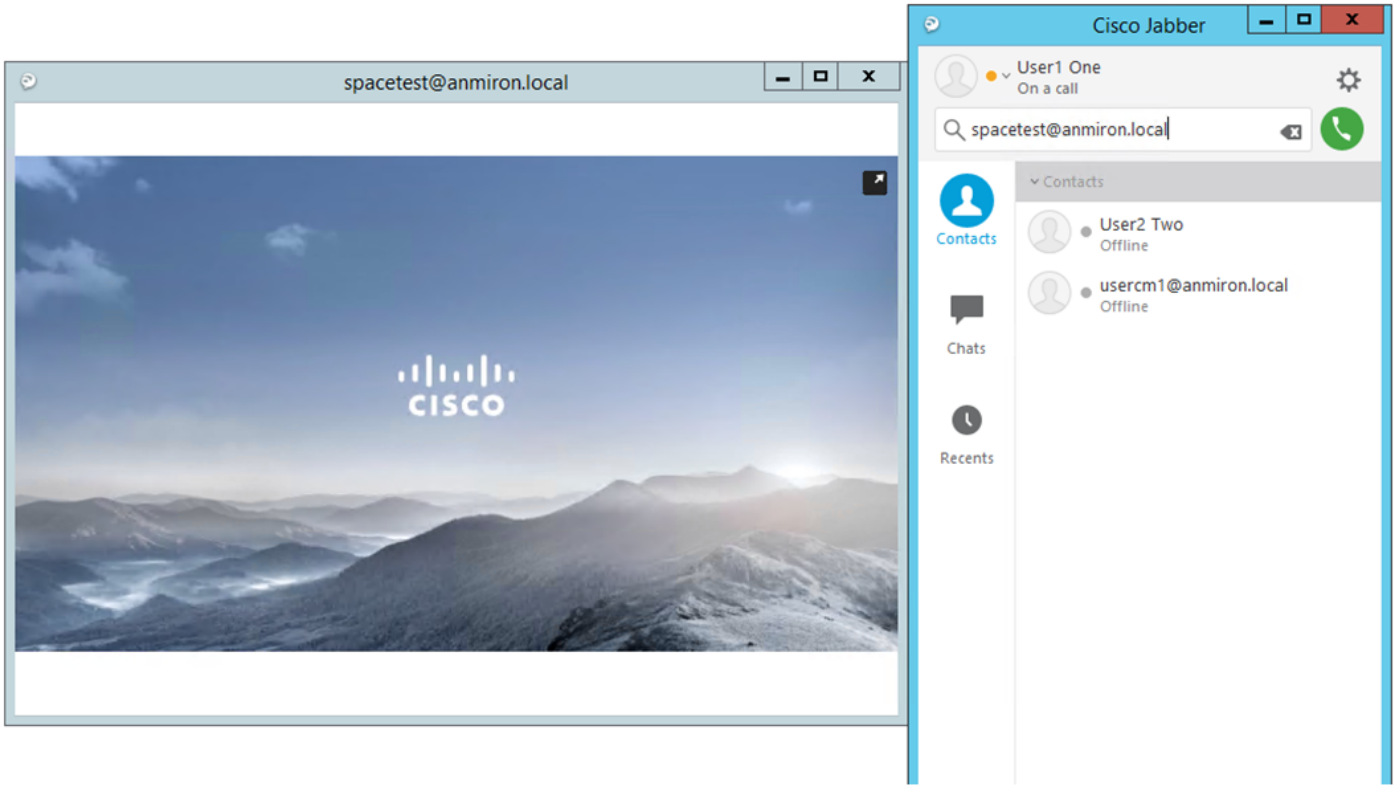
Verificar

Comunicação Callbridge e XMPP

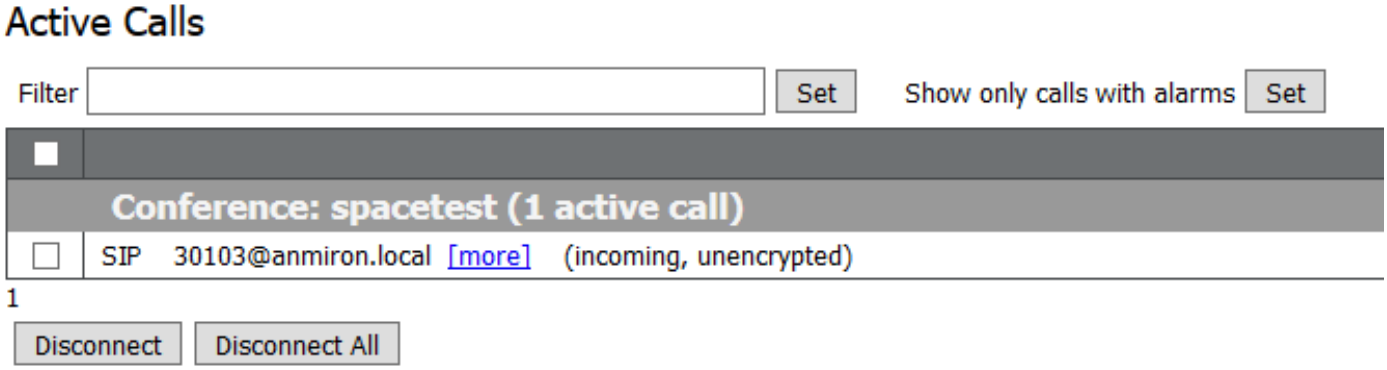
- Abra a interface da Web do CMS
- Navegue até **Status > Geral**
- O status da conexão XMPP deve ser conectado a localhost



- Efetuar uma chamada de um dispositivo registrado no CUCM
- Disque a URI **spacetest@anmiron.local**

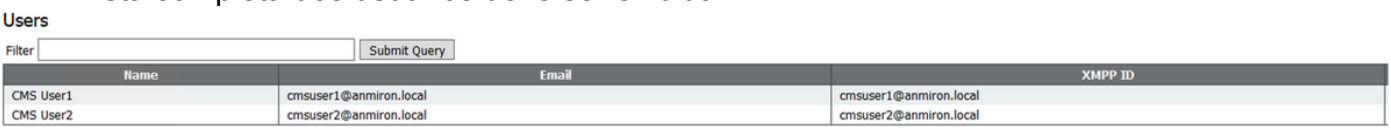


- Abra a interface da Web do CMS
- Navegue até **Status > Calls (Status > Chamadas)**
- A chamada deve ser mostrada como **Chamada ativa**



Sincronização LDAP com CMS

- Abra a interface da Web do CMS
- Navegue até **Status > Usuários**
- A lista completa dos usuários deve ser exibida



- Navegue até **Configuração > Espaços**
- Certifique-se de que cada usuário tenha seu próprio espaço criado

Space configuration

Filter Submit Query

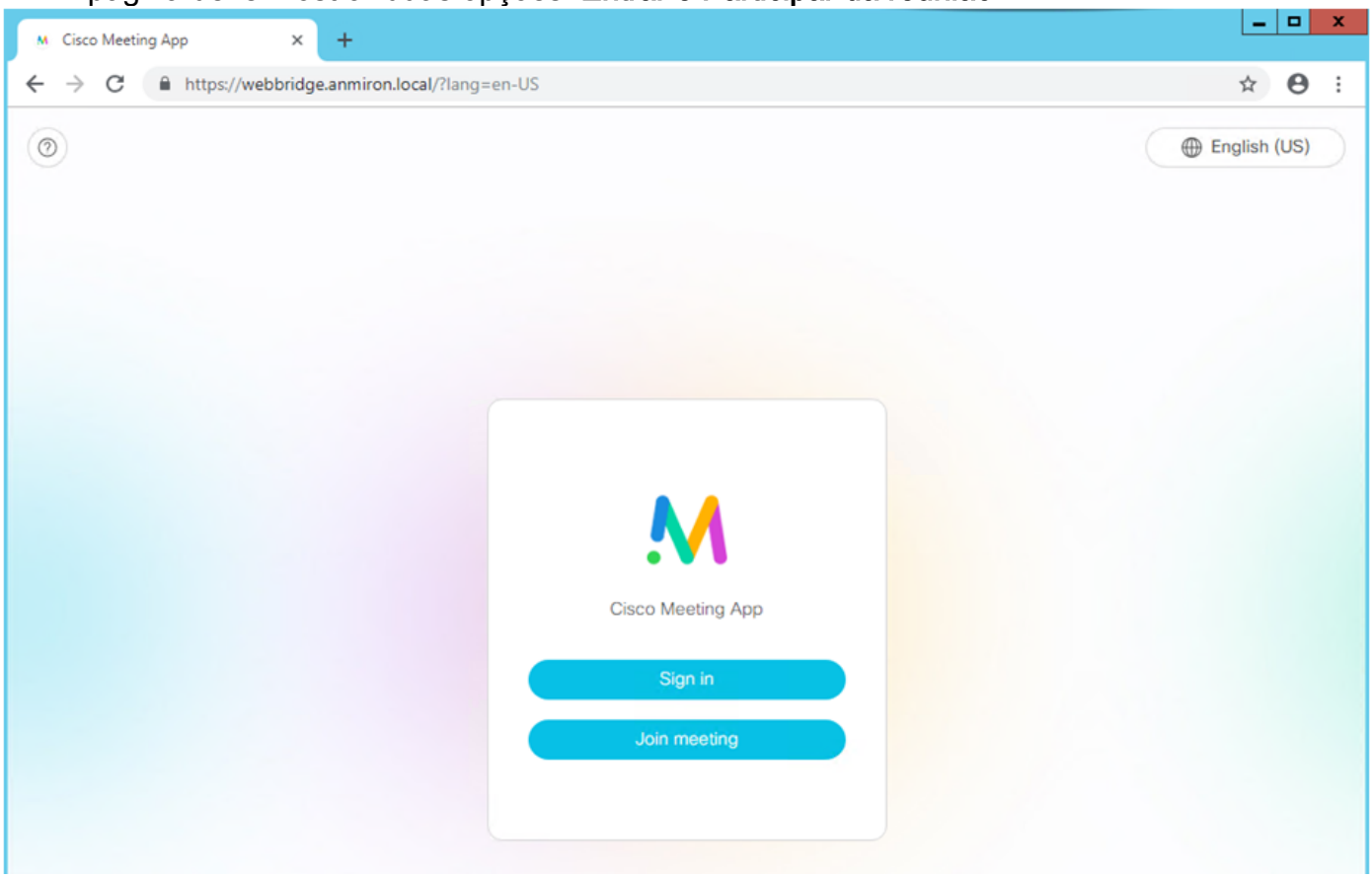
	Name	URI user part	Secondary URI user part	Additional access methods	Call ID	Passcode	Default layout	
	cmsuser1 Space	cmsuser1.call			cmsuser1.space		not set	[edit]
	cmsuser2 Space	cmsuser2.call			cmsuser2.space		not set	[edit]
	spacetest	spacetest			spacetest		not set	[edit]
							not set	Add New Reset

1

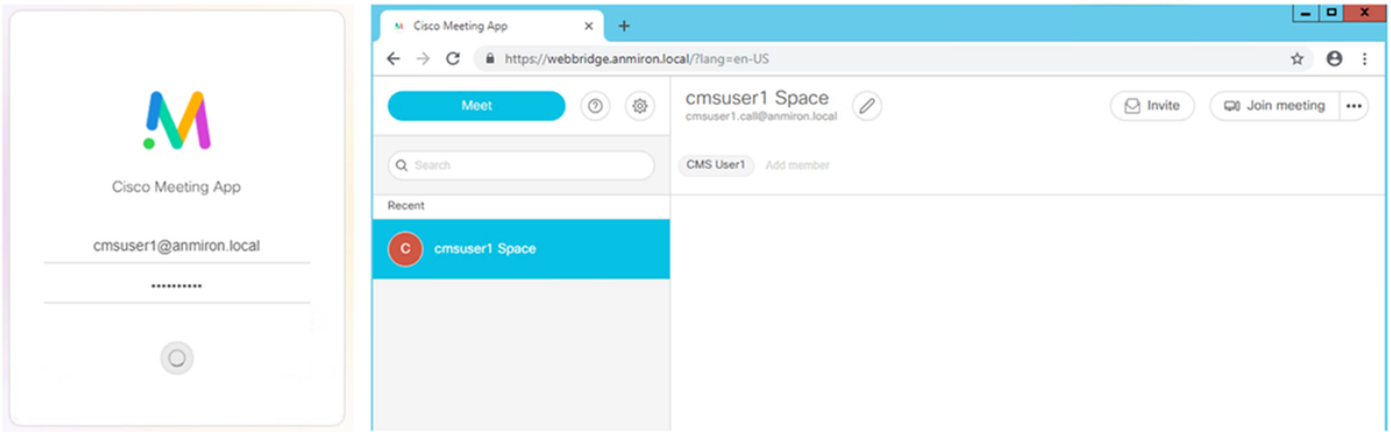
Delete

Acesso ao Webbridge

- Use o navegador da Web para acessar a página da Web configurada para o serviço de webbridge, https://webbridge.anmiron.local
- A página deve mostrar duas opções **Entrar e Participar da reunião**



- Os usuários anteriormente integrados no AD devem ser capazes de iniciar a sessão
- Selecione **Entrar**
- Insira o **Nome de usuário e senha**
- O usuário deve ser capaz de fazer **logon**, conforme mostrado na imagem



Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.