Configurar e integrar CMS individual con servicios combinados

Contenido

Introducción

En este documento se describe cómo configurar e integrar Cisco Meeting Server (CMS) individual con servicios combinados.

Los servicios que se deben configurar e integrar son Call Bridge, Webadmin, WebBridge, Extensible Messaging and Presence Protocol (XMPP) y Lightweight Directory Access Protocol (LDAP).

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Cisco Unified Communications Manager (CUCM)
- Active Directory (AD)
- Autoridad de certificación (CA)
- Cliente Secure File Transfer Protocol (SFTP)

- Servidor de servicio de nombres de dominios (DNS)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CMS, versión 2.3.7
- CUCM, versión 11.5.1
- Google Chrome, versión 69.0.3497
- WinSCP, versión 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

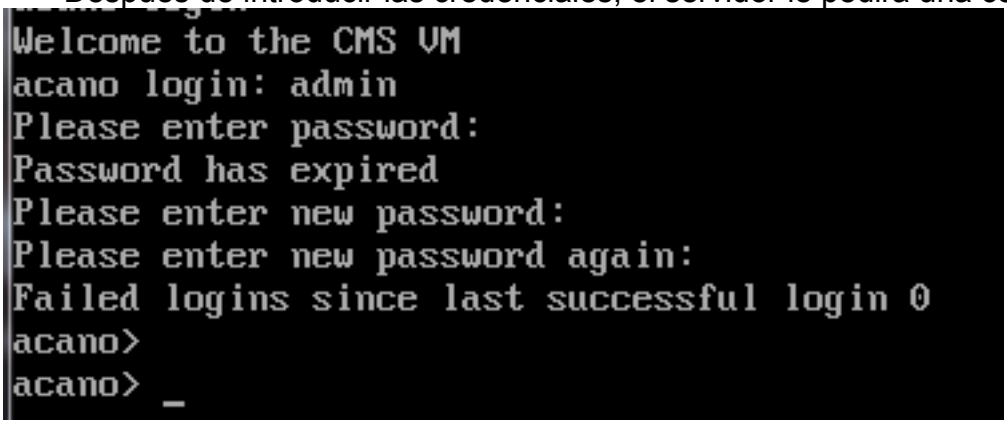
Paso 1. Acceso a CMS

- La primera vez que inicie sesión en CMS, en la pantalla aparecerá la bienvenida y se le pedirá que inicie sesión.
- Estas son las credenciales predeterminadas:

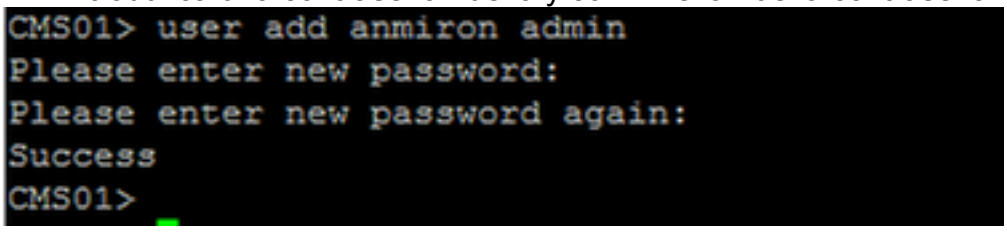
Usuario: admin

Contraseña admin

- Después de introducir las credenciales, el servidor le pedirá una contraseña nueva.



- Es recomendable que cree un nuevo usuario administrador; esta es una medida adecuada por si pierde la contraseña de una cuenta.
- Introduzca el comando: **Nombre de usuario: admin**
- Introduzca una contraseña nueva y confirme la nueva contraseña.



Paso 2. Cambiar el nombre de host

- Este cambio es opcional.
- Ejecute el comando hostname <name>.
- Reinicie el servidor.
- Ejecute el 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...
```

Paso 3. Configuración de los parámetros de red

- Para ver los ajustes actuales, ejecute el comando **ipv4 un.**
- Agregue la configuración de ipv4.
- Ejecute el 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 la zona horaria.
- Ejecute el comando **timezone <timezoneName>.**
- Para poder ver todas las zonas horarias disponibles, ejecute el comando timezone list.
- Agregue un servidor Network Time Protocol (NTP).
- Ejecute el comando command 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> _
```

- Agregue un servidor DNS.
- Ejecute el comando **dns add forwardzone <domain> <dnsip>.**

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

Nota: Se puede configurar un dominio específico para búsqueda de DNS; sin embargo, si el DNS puede resolver cualquier dominio, utilice un punto como el dominio.

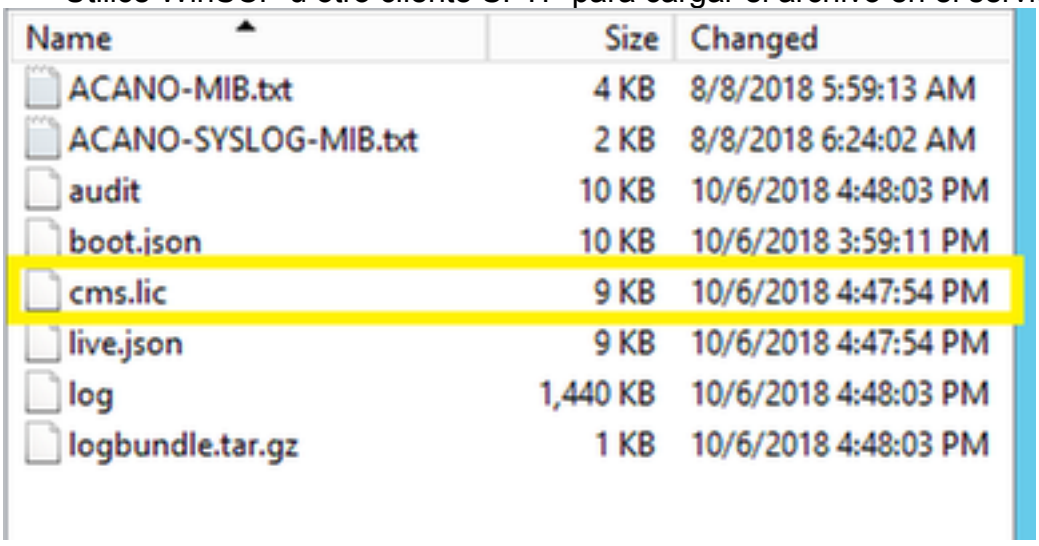
Paso 4. Licencia de CMS

- Para configurar los servicios de CMS, se debe instalar una licencia.
- Para poder generar e instalar la licencia, es necesaria la dirección MAC (control de acceso a los medios), ya que las licencias se asociarán con ella.
- Ejecute el comando **iface un.**
- Copie la **dirección MAC.**
- Póngase en contacto con su representante de ventas para generar una licencia.

Nota: En este documento, no se aborda el proceso para generar la licencia.

```
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>
```

- Una vez que tenga el archivo de licencia, cámbiele el nombre por **cms.lic.**
- Utilice WinSCP u otro cliente SFTP para cargar el archivo en el servidor CMS.



- Una vez que se carga el archivo, ejecute el comando license.
- Reinicie el servidor.
- Ejecute el 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...
```

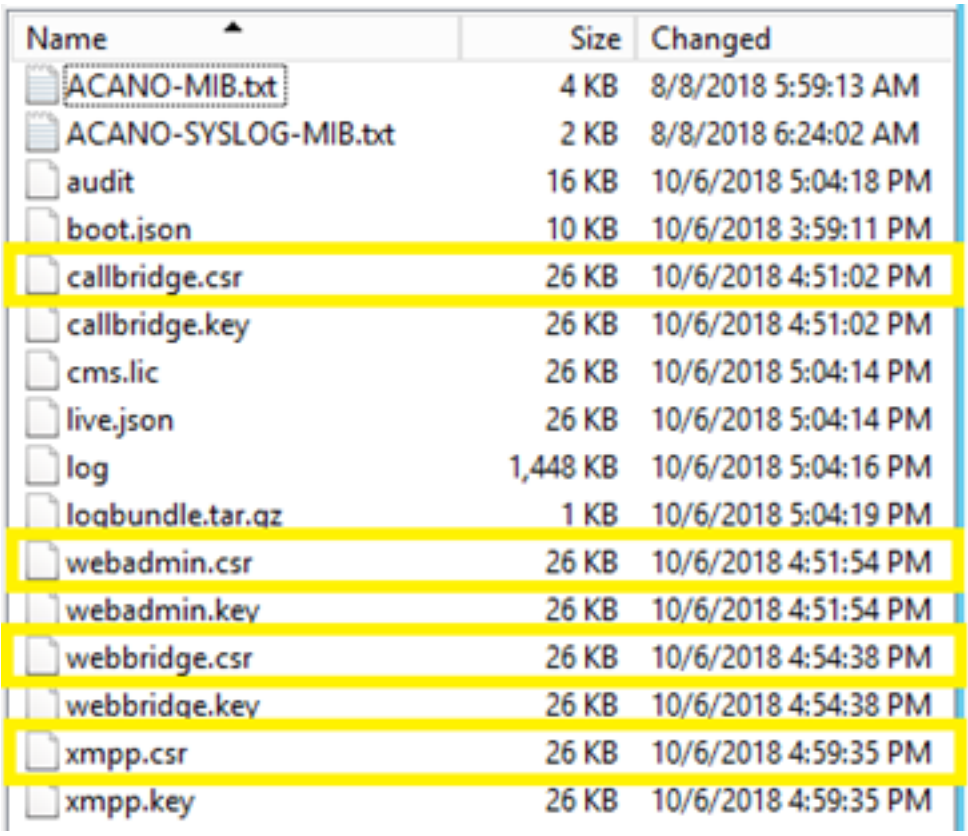
Paso 5. Generar e instalar certificados

- Genere una solicitud de firma de certificado (CSR) para callbridge, webadmin, webbridge y xmpp.
- Ejecute el comando **pki csr <service> CN:<servicefqdn>** para este 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
```

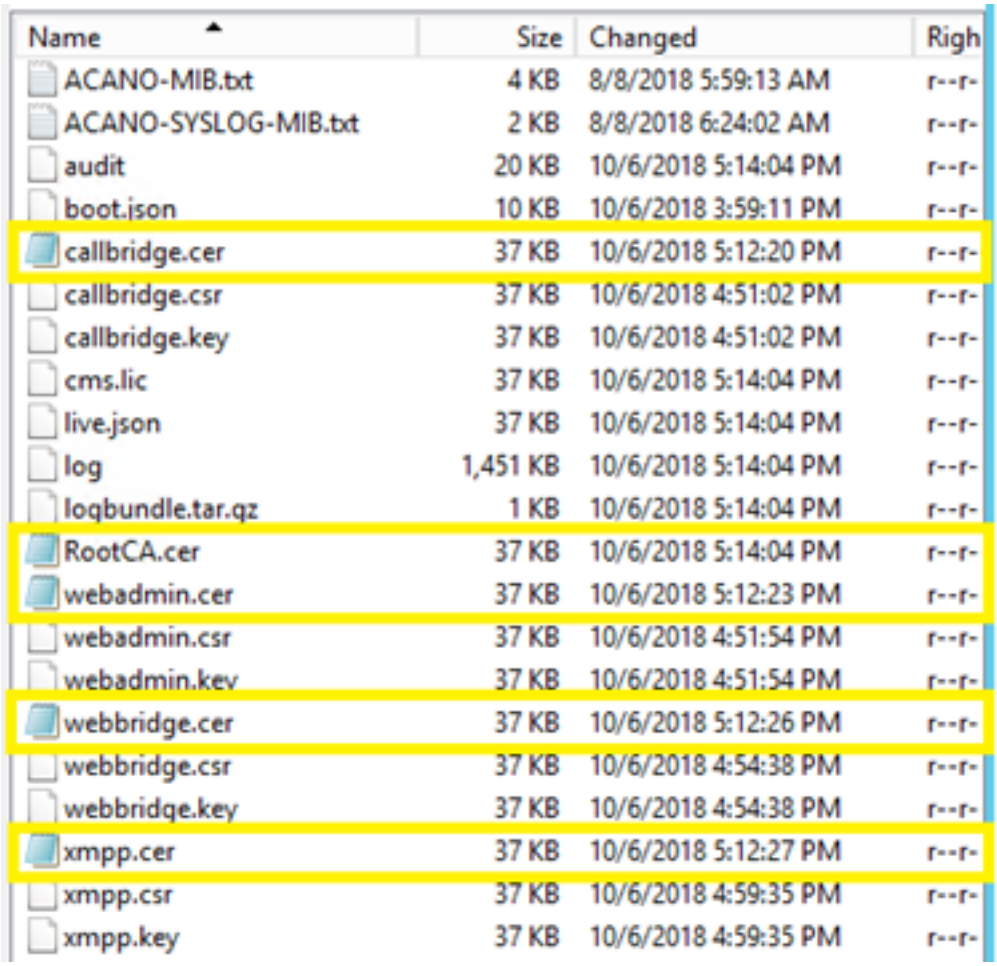
Nota: En este ejemplo, se crea un único certificado para cada servidor; usted puede crear un certificado para todos los servicios. Para obtener más información sobre la creación de certificados, revise la Guía de creación de certificados.

- Se generan dos archivos después de ejecutar el comando: un archivo .csr y un archivo .key con el nombre del servicio que asignó en los pasos anteriores.
- Descargue los archivos de CSR desde el servidor CMS. Utilice WinSCP u otro cliente SFTP para este fin.



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

- Firme el archivo de CSR con una autoridad de certificación.
- Asegúrese de usar una plantilla que contenga **cliente web y autenticación de servidor web.**
- Cargue el certificado firmado en el servidor CMS.
- Asegúrese de cargar la **CA raíz y cualquier certificado intermedio** que haya firmado los certificados.



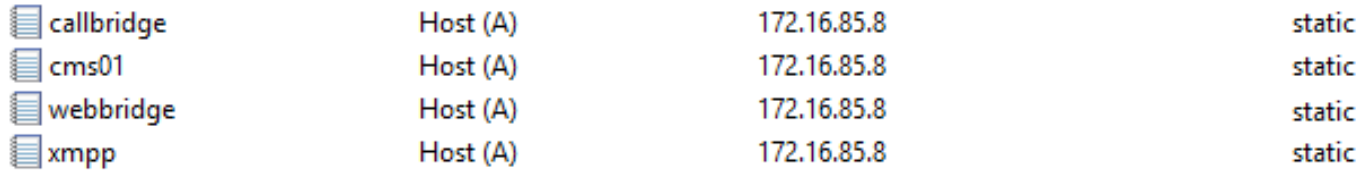
Name	Size	Changed	Righ
ACANO-MIB.txt	4 KB	8/8/2018 5:59:13 AM	r--r-
ACANO-SYSLOG-MIB.txt	2 KB	8/8/2018 6:24:02 AM	r--r-
audit	20 KB	10/6/2018 5:14:04 PM	r--r-
boot.json	10 KB	10/6/2018 3:59:11 PM	r--r-
callbridge.cer	37 KB	10/6/2018 5:12:20 PM	r--r-
callbridge.csr	37 KB	10/6/2018 4:51:02 PM	r--r-
callbridge.key	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 comprobar que todos los certificados aparezcan en CMS, ejecute el 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>
```

Paso 6. Registros DNS

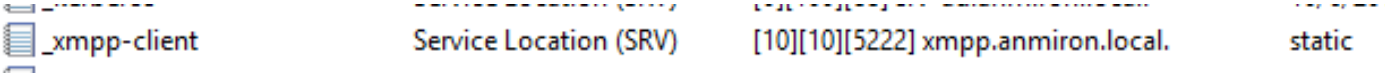
- Cree los registros de dirección DNS (A) para callbridge, xmpp, webadmin y webbridge.
- Asegúrese de que todos los registros apunten a la dirección IP de CMS.



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

- Cree un registro de servicio (SRV) para **xmpp-client.**
- Este es el formato de registro del servicio:

Servicio cliente _xmpp
Protocolo TCP
Puerto 5222
Objetivo Introduzca el FQDN XMPP; por ejemplo, **xmpp.anmiron.local.**



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

Paso 7. Configuración de servicio

Configuración de callbridge:

- Introduzca el comando **callbridge listen <interface>.**
- Ingrese el comando **callbridge certs <callbridge-key-file> <crt-file> [<cert-bundle>]**
- El archivo **key-file es la clave que se genera cuando se crea la CSR.**
- El archivo **cert-bundle es el paquete de la CA raíz y cualquier otro certificado intermedio.**

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

Nota: La interfaz de escucha del servicio Call Bridge no debe establecerse en una interfaz que esté configurada para utilizar la Traducción de direcciones de red (NAT) a otra dirección IP.

Configuración de webadmin:

- Ejecute el comando **webadmin listen <interface> <port>.**
- Ejecute el 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>
```

Nota: Si los servicios webadmin y webbridge están configurados en el mismo servidor, deben configurarse en interfaces diferentes o escuchar en puertos diferentes; el servicio webbridge debe escuchar en el puerto 443. El servicio webadmin normalmente se configura en el puerto 445.

Configuración de XMPP:

- Ejecute el comando **xmpp listen <interface whitelist>.**
- Ejecute el comando **xmpp domain <domain name>.**
- Ejecute el comando **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>
```

Nota: El nombre de dominio debe coincidir con el dominio donde se crearon los registros de DNS.

Configuración de webbridge:

- Ejecute el comando **webbridge hear <interface[:port] whitelist>**
- Ejecute el comando **webbridge certs <key-file> <crt-file> [<crt-bundle>].**
- Ejecute el 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>
```

Nota: El archivo **crt-bundle confiable es el certificado de callbridge y se debe agregar a**

webbridge para que callbridge confíe en webbridge, esto habilitará la función para unirse como invitado.

- Ejecute el comando **callbridge restart.**
- Ejecute el comando **wbeadmin enable.**
- Ejecute el comando **xmpp enable.**
- Ejecute el 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>
```

Nota: El servidor debe arrojar el resultado **SUCCESS (éxito) para todos los servicios; si arroja FAILURE** (error), revise los pasos anteriores y asegúrese de que no haya errores en la configuración.

Para permitir que Call Bridge acceda al servicio XMPP de forma segura, es necesario proporcionar un **nombre de componente para Call Bridge que se utilizará para su autenticación con el servicio XMPP.**

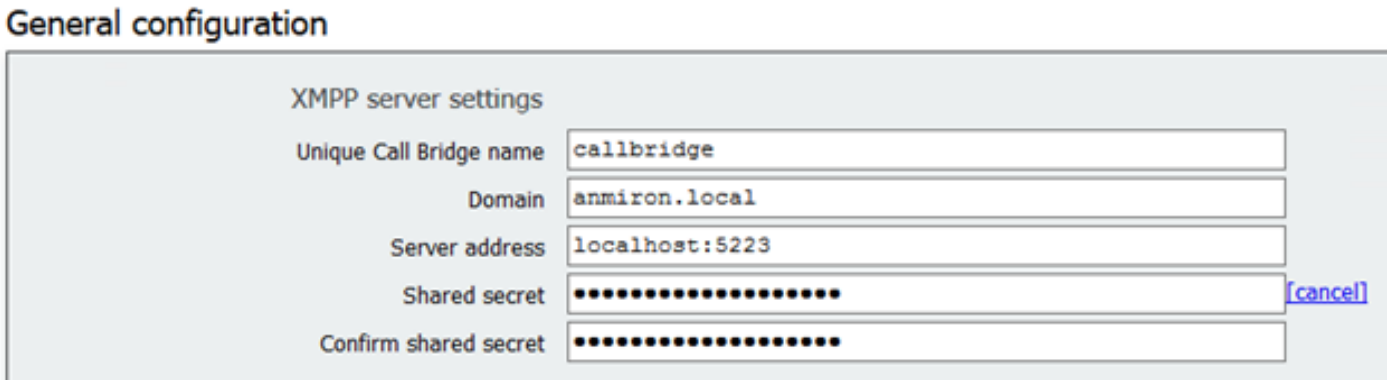
- Ejecute el comando **xmpp callbridge add <nombre del componente>.**
- El resultado muestra un valor secreto, como se muestra en la imagen.

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

- Copie el **valor secreto.**
- Acceda a la interfaz web de CMS.
- Vaya a **Configuration > General (Configuración > General).**
- Introduzca la información.

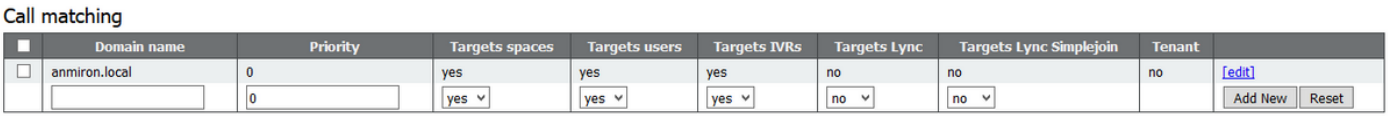
Nombre único de Call Bridge	Introduzca el nombre del servicio callbridge creado; por ejemplo, **callbridge.**
Dominio	Introduzca el nombre de dominio; por ejemplo, **anmiron.local.**
Dirección del servidor	Configure la dirección IP de CMS; por ejemplo, **localhost:5223.**
Secreto compartido	Introduzca el valor secreto creado en el paso anterior; por ejemplo, **6DwNANabpumut14pAb1.**

- Seleccione **Submit (Enviar).**



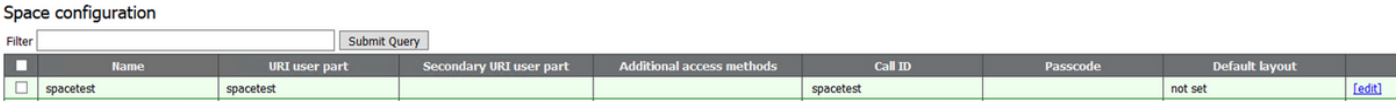
- Cree una **regla de coincidencia de llamadas entrantes para las llamadas entrantes.**
- Vaya a **Configuration > Incoming calls (Configuración > Llamadas entrantes).**
- Introduzca la información.

Dominio	Introduzca el nombre de dominio del servidor CMS; por ejemplo, **anmiron.local.**
Prioridad	Introduzca un valor para la prioridad; para ejemplo, **0.**
Opción Target Spaces (Espacios de destino)	Seleccione **Yes (Sí).**



- Cree un espacio para la prueba.
- Vaya a **Configuration > Spaces (Configuración > Espacios).**
- Introduzca la información.

Nombre	Introduzca un nombre para el espacio; por ejemplo, **spacetest.**
Parte del usuario de URI	Introduzca un URI como nombre para este espacio; por ejemplo, **spacetest.**
ID de llamada	Introduzca el ID de llamada para unirse a este espacio desde webbridge; por ejem **spacetest.**
Código de acceso	Introduzca un número para permitir el acceso al espacio si es necesario.

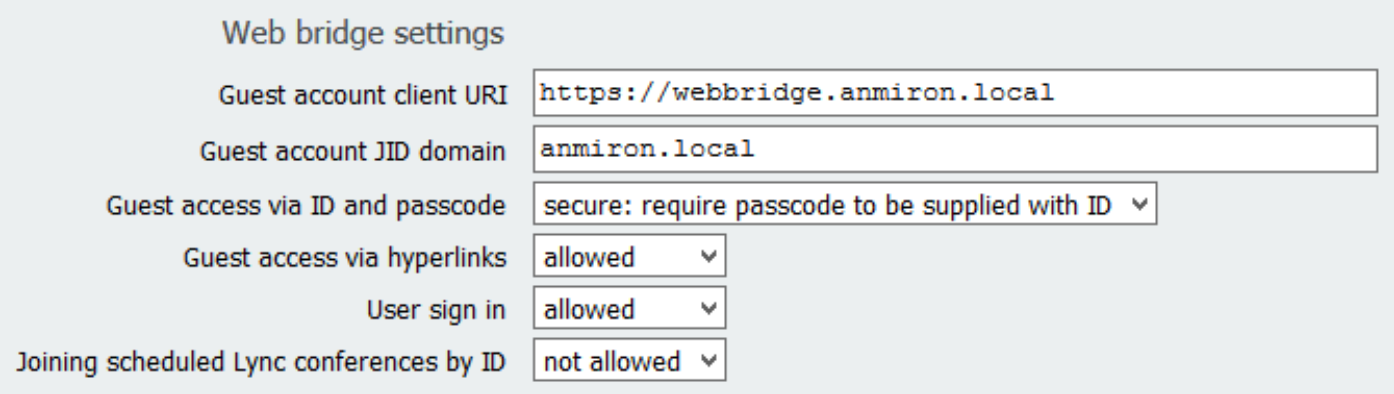


Nota: La **parte del usuario de URI es lo que quienes llaman deben marcar en el dominio**

configurado en la regla de coincidencia de llamadas entrantes; por ejemplo, la persona que llama tiene que marcar **spacetest@anmiron.local.**

- Vaya a **Configuration > General > Web bridgesettings (Configuración > General > Configuración de Web Bridge).**
- Introduzca la información.

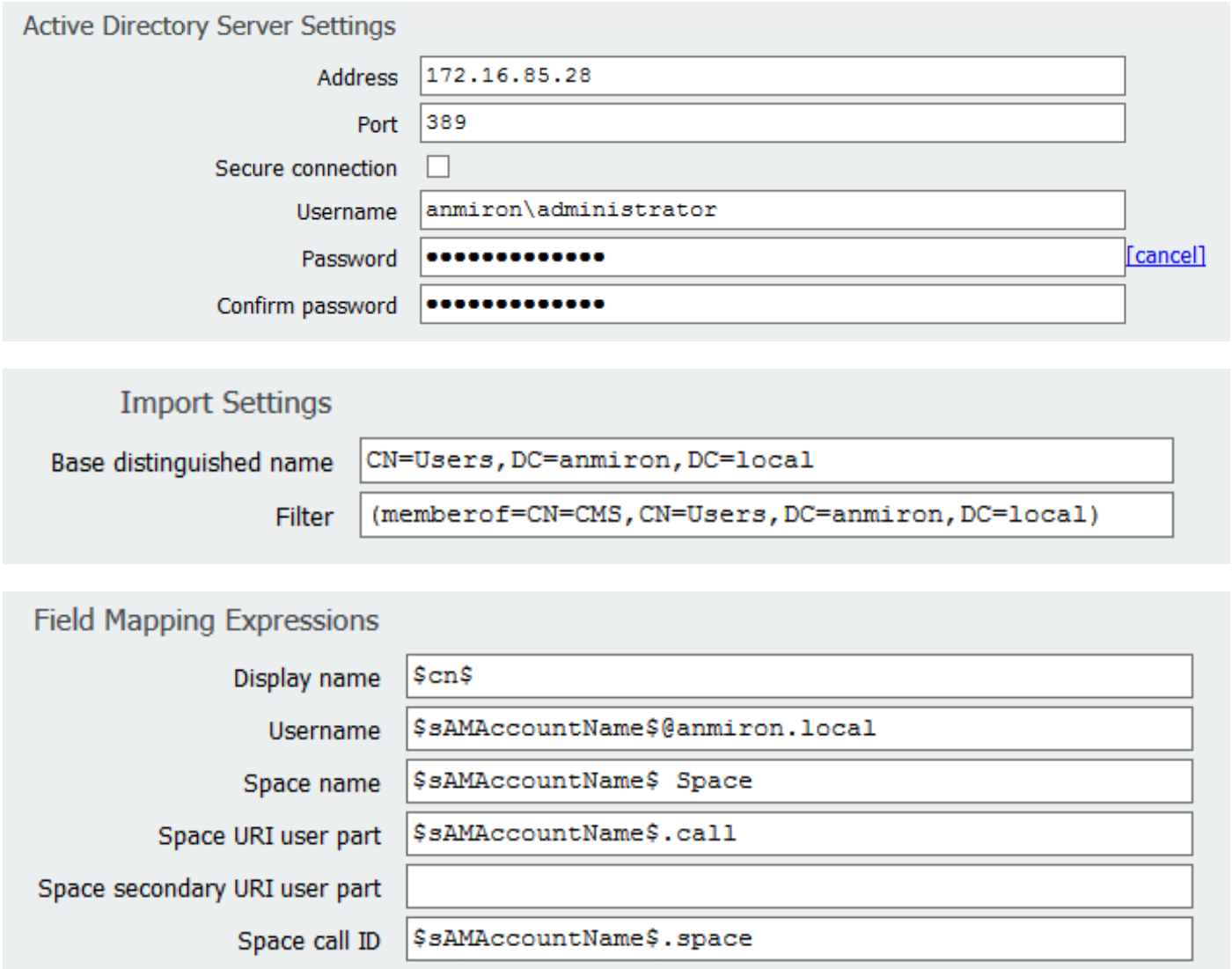
URI de cliente de cuenta de invitado	Se trata de la interfaz web de webbridge; por ejemplo, **https://webbridge.anmiron.local.**
Dominio JID de cuenta de invitado	Este es el dominio configurado en CMS; por ejemplo, **anmiron.local.**
Acceso de invitado mediante hipervínculo	Seleccione **allowed (permitido).**



Paso 8. Integración de LDAP

- Acceda a la interfaz web de CMS.
- Vaya a **Configuration > Active Directory (Configuración > Active Directory).**
- Introduzca la información.

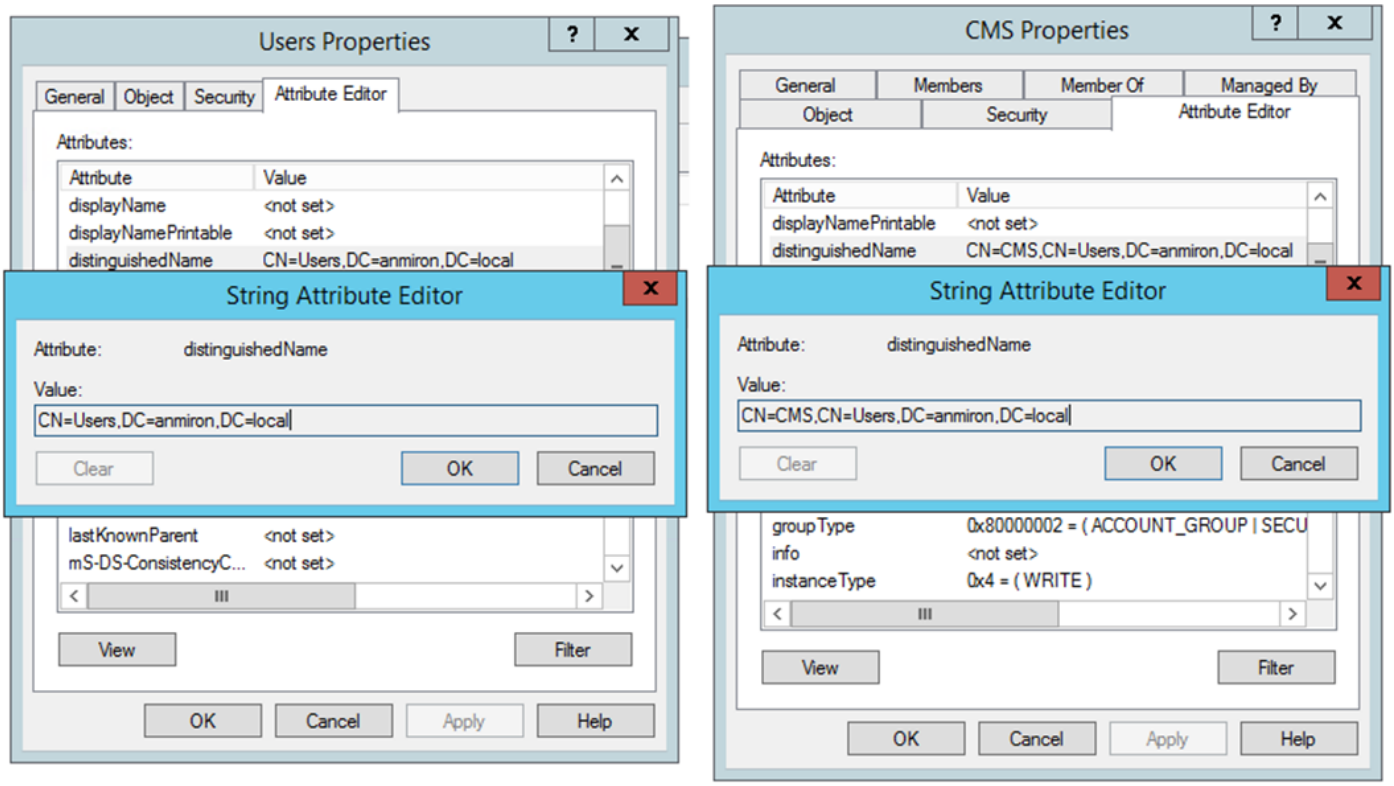
Dirección	La dirección IP del servidor LDAP; por ejemplo, **172.16.85.28.**
Puerto	Es **389 si utiliza una conexión no segura y 636 si se requiere una conexión seg**
Nombre de usuario	Introduzca un administrador del servidor LDAP; por ejemplo, **anmiron\administ**
Contraseña	Introduzca la contraseña del usuario administrador.
Nombre distintivo base	Esta es una configuración de Active directory; por ejemplo, **CN=Users, DC=anmiron, DC=local.**
Filtro	Esta es una configuración de Active directory; por ejemplo, **(memberof=CN=C CN=Users, DC=anmiron, DC=local).**
Mostrar nombre:	Cómo se muestra el nombre de usuario; por ejemplo, **cn$.**
Nombre de usuario	El ID de inicio de sesión para el usuario, por ejemplo **$sAMAccountName$@anmiron.local**
Nombre de espacio	Cómo se muestra el espacio; por ejemplo, **$sAMAccountName$ Space.**
Parte del usuario de URI de espacio	El URI que se debe marcar; por ejemplo, **$sAMAccountName$.call.**
ID de llamada de espacio	El ID de llamada que se utilizará en webbridge; por ejemplo, **$sAMAccountName$.space.**



- Seleccione **Submit (Enviar).**
- Seleccione **Sync now (Sincronizar ahora).**

El nombre distintivo base y el filtro son configuraciones de Active Directory. Este ejemplo contiene información básica para obtener la información con Attribute Editor (Editor de atributo) en Active Directory. Para abrir el **Editor de atributos**, habilite **Funciones avanzadas** en **Active Directory.** Vaya a **Users and Computers > View (Usuarios y equipos > Ver) y seleccione Advanced Features (Funciones avanzadas).**

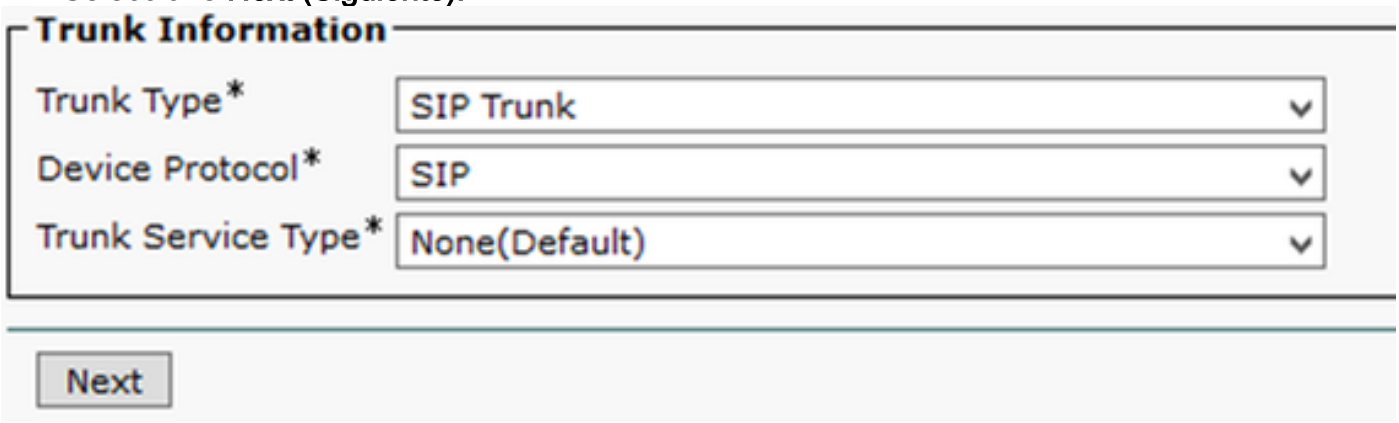
- Para este ejemplo, se crea un grupo llamado **CMS.**
- Abra la función **Users and Computers (Usuarios y equipos) en AD.**
- Seleccione a la derecha un **User (Usuario) y abra las propiedades.**
- Vaya a **Attribute Editor (Editor de atributo).**
- En la columna **Attribute (Atributo), busque el campo distinguishedName (nombre distintivo).**



Nota: Para obtener más información sobre los filtros LDAP, consulte la [Guía de implementación de CMS.]

Paso 9. Configuración de CUCM

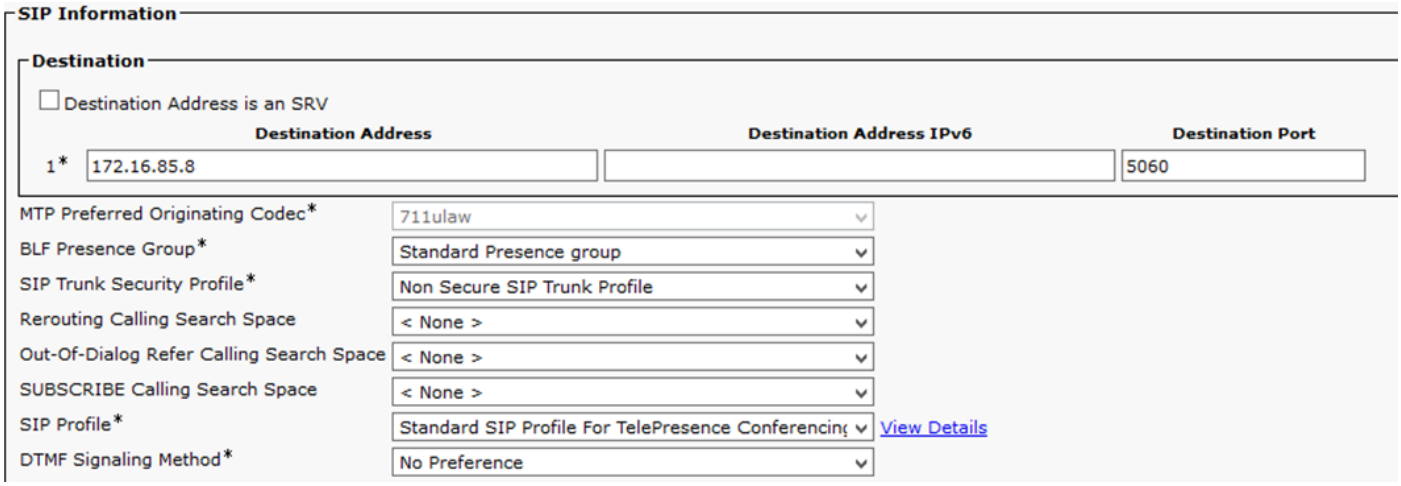
- Abra la interfaz web de CUCM.
- Vaya a **Device > Trunks (Dispositivo > Enlaces troncales).**
- Seleccione **Add New (Agregar nuevo).**
- En el menú desplegable **Trunk Type (Tipo de enlace troncal), seleccione SIP Trunk (Enlace troncal SIP).**
- Seleccione **Next (Siguiente).**



- Introduzca la información.

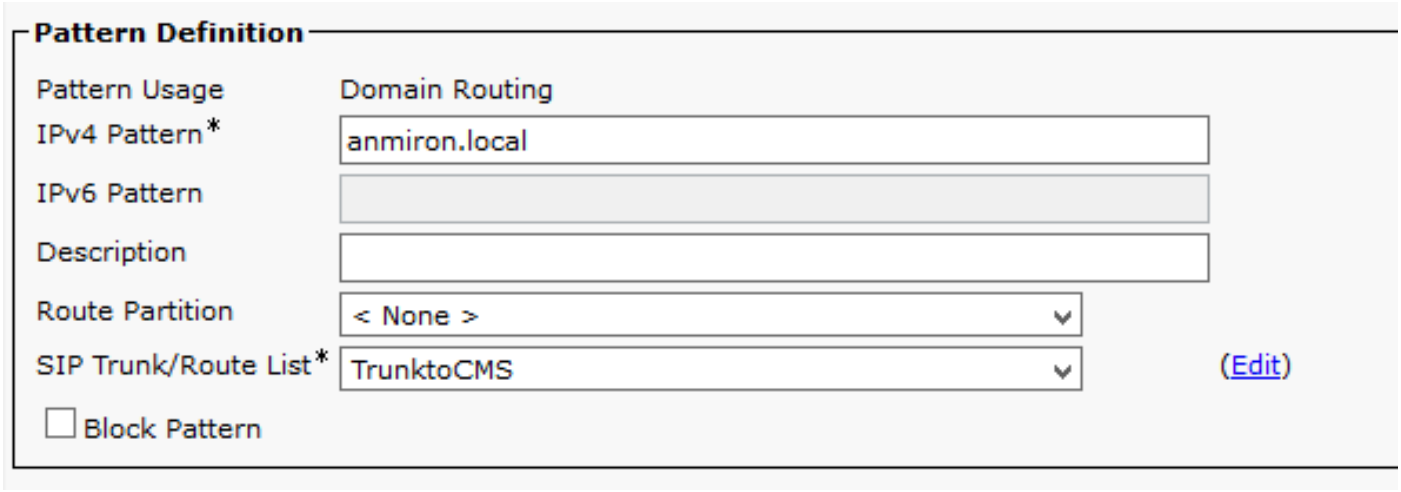
Nombre del dispositivo	Introduzca un nombre para el enlace troncal SIP; por ejemplo, **TrunktoCMS.**
Dirección de destino	Introduzca la dirección IP de CMS o el FQDN de Call Bridge; por ejemplo, **172.16.85.8.**
Puerto de Destino	Introduzca el puerto en el que escucha el CMS; por ejemplo, **5060.**

Perfil de seguridad del enlace troncal SIP	Seleccione el perfil seguro; por ejemplo, **Non Secure SIP Trunk Profi**
Perfil SIP	Seleccione **Standard SIP Profile for TelePresence Conferencing.**



- Seleccione **Save (Guardar).**
- Seleccione **Reset (Restablecer).**
- Vaya a **Call routing > SIP Route pattern > Add New > Select Domain Routing (Routing de llamadas > Patrón de ruta de SIP > Agregar nuevo > Seleccionar routing de dominio).**
- Introduzca la información.

Patrón de IPv4	Especifique el dominio configurado en CMS; por ejemplo, **anmiron.lo**
Lista de rutas/enlaces troncales SIP	Seleccione el enlace troncal SIP creado anteriormente, **TrunktoCMS**

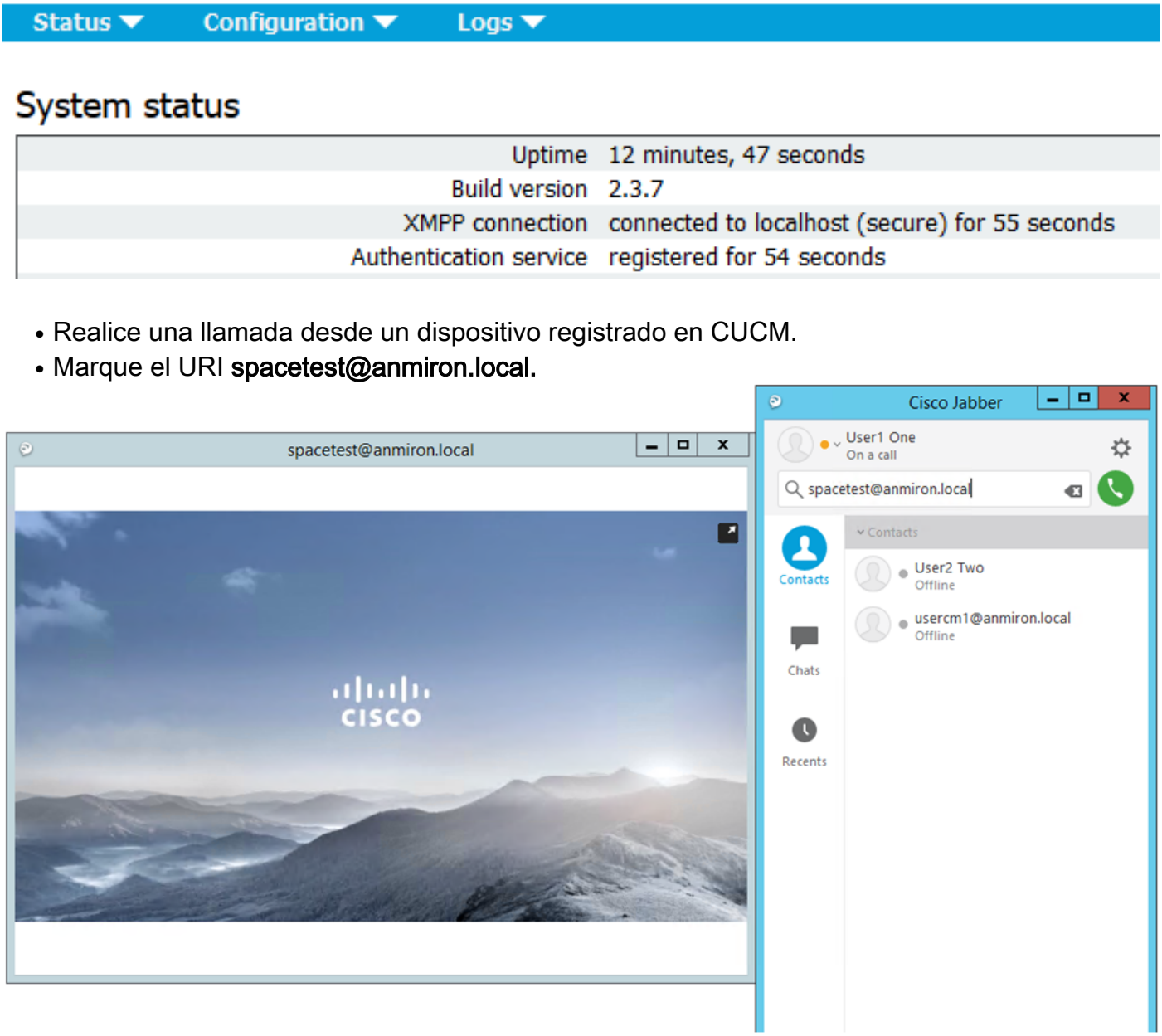


- Seleccione **Save (Guardar).**

Verificación

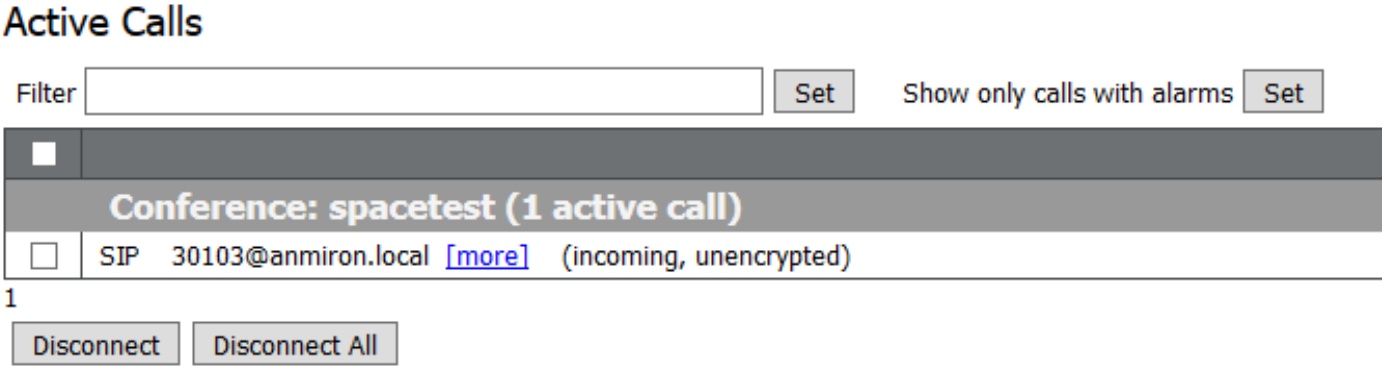
Comunicación de Callbridge y XMPP

- Abra la interfaz web de CMS.
- Vaya a **Status > General (Estado > General).**
- El estado de conexión de XMPP debe ser conectado al host local.



- Realice una llamada desde un dispositivo registrado en CUCM.
- Marque el URI **spacetest@anmiron.local.**

- Abra la interfaz web de CMS.
- Vaya a **Status > Calls (Estado > Llamadas).**
- La llamada debe mostrarse como **Active Call (Llamada activa).**

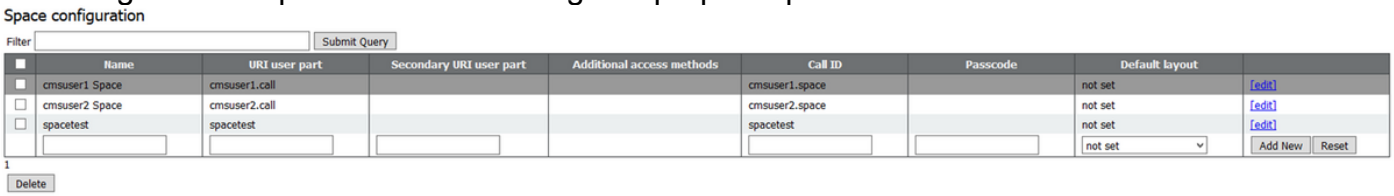


Sincronización de LDAP con CMS

- Acceda a la interfaz web de CMS.
- Vaya a **Status > Users (Estado > Usuarios).**

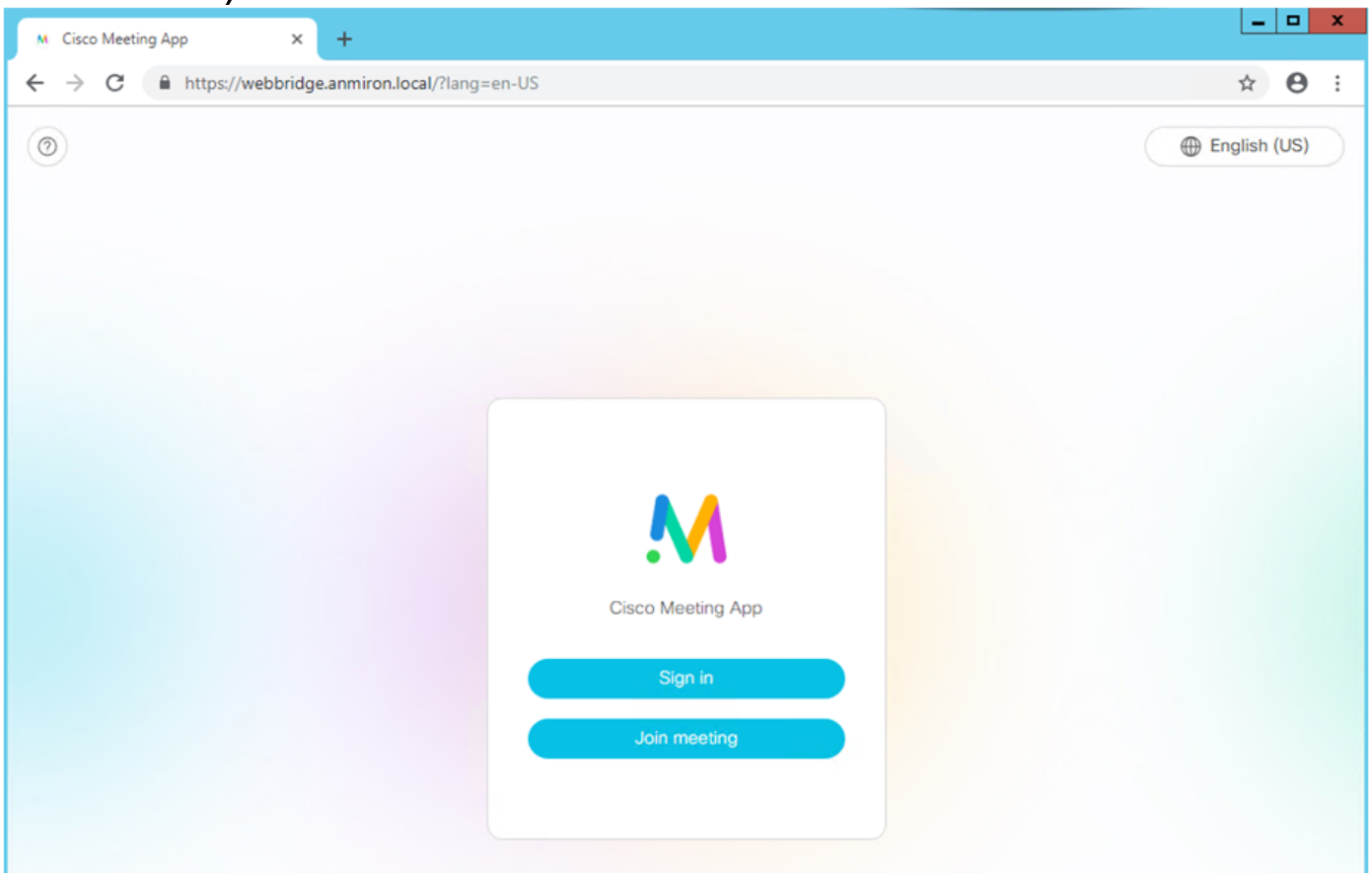
- Debe mostrarse la lista completa de usuarios.

- Vaya a **Configuration > Spaces (Configuración > Espacios).**
- Asegúrese de que cada usuario tenga su propio espacio creado.

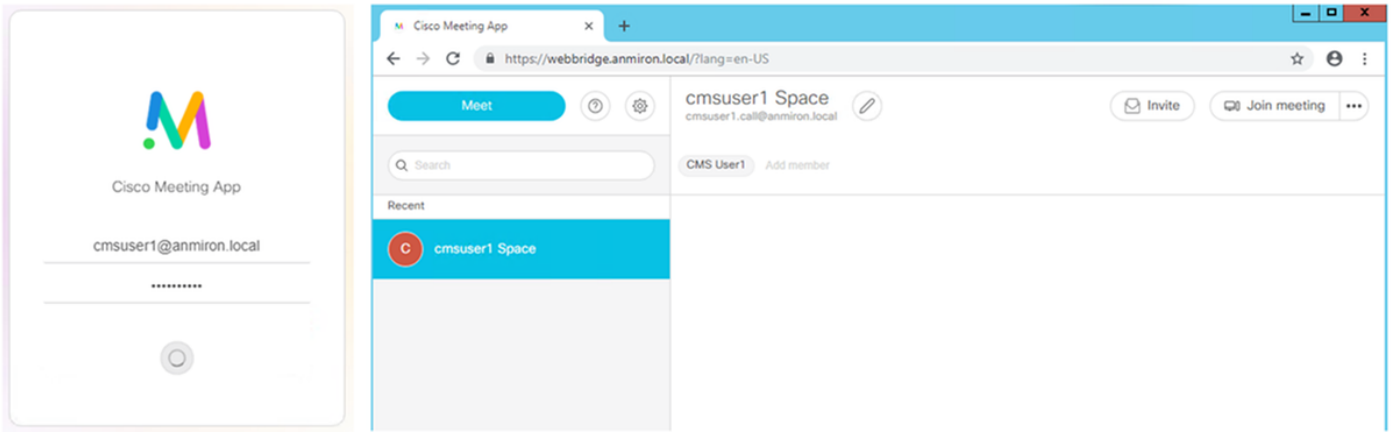


Acceso a Webbridge

- Utilice el navegador web para acceder a la página web configurada para el servicio webbridge, https://webbridge.anmiron.local.
- En la página deben aparecer dos opciones **Sign in (Iniciar sesión) y Join meeting (Unirse a una reunión).**



- Los usuarios que se han integrado anteriormente desde AD deben poder iniciar sesión.
- Seleccione **Sign in (Iniciar sesión).**
- Escriba su **Username (Nombre de usuario) y Password (Contraseña).**
- El usuario debe poder **iniciar sesión**, como se muestra en la imagen



Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.