

# Configuración de conferencias de Cisco Meeting Server y CUCM ad hoc

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración de CMS](#)

[Configuración de CUCM](#)

[Verificación](#)

[Troubleshoot](#)

## Introducción

En este documento se describen los pasos para configurar conferencias ad hoc con Cisco Meeting Server (CMS) y Cisco Unified Communications Manager (CUCM).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración e implementación de CMS
- Registro de terminales y creación de enlaces troncales en CUCM
- Certificados firmados

### Componentes Utilizados

- CUCM
- Servidor CMS 2.0.X y versiones superiores
- Es posible que los componentes WebAdmin y Call Bridge ya estén configurados en CMS
- Registros del sistema de nombres de dominio (DNS) internos para WebAdmin y Call Bridge, que pueden establecer un vínculo con la dirección IP del servidor CMS
- Autoridad de certificación (CA) interna que firme el certificado con uso mejorado de clave de la autenticación de servidor web y cliente web
- Certificados firmados para la comunicación de Seguridad de la capa de transporte (TLS)

**Nota:** No se admiten certificados autofirmados en esta implementación porque necesitan la autenticación de servidor web y cliente web que no se puede agregar a certificados autofirmados.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando. La información que se presenta en este documento no se limita a versiones de software y hardware específicas; no obstante, se deben cumplir los requisitos de versión mínimos de software.

## Configurar

### Configuración de CMS

Paso 1. Cree una cuenta de usuario de administrador con privilegios de interfaz de programa de aplicaciones (API).

- Abra una sesión de Shell seguro (SSH) en el procesador de administración de Mainboard (MMP).
- Para agregar una cuenta de usuario de nivel de administrador, ejecute el comando `user add <username> <role>`.
- Introduzca la contraseña, como se muestra en la imagen.

```
cb1> user add apiadmin admin
Please enter new password:
Please enter new password again:
Success
```

Paso 2. Genere los certificados.

- Ejecute el comando `pki csr <nombre de archivo> CN:<nombre común> subjectAltName:<nombre alternativo del asunto>`
- Utilice la información de acuerdo con sus requisitos.

Nombre del archivo                      certall

CN    tptac9.com

Nombre alternativo del sujeto cmsadhoc.tptac9.com,10.106.81.32

- No utilice caracteres comodines para generar el certificado. CUCM no admite un certificado con caracteres comodines.
- Asegúrese de que el certificado esté firmado con la autenticación de servidor web y cliente web del uso mejorado de clave.

**Nota:** Si desea utilizar el mismo certificado para todos los servicios, el nombre común (CN) debe ser el nombre de dominio y el nombre de los otros servicios CMS debe estar incluido como nombre alternativo del sujeto (SAN). En este caso, la dirección IP también está firmada por el certificado y todo equipo que tenga instalado el certificado raíz confía en ella.

### Configuración de CUCM

Paso 1. Cargue los certificados en el almacén de confianza de CUCM.

- Se puede descargar el certificado raíz interno de interfaz web de entidad emisora de certificados.

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [tptac9-WIN-TI6UAFTSEEV-CA-1] ▲

Encoding method:

- DER  
 Base 64

[Install CA certificate](#)


[Download CA certificate](#)

- Agregue el certificado de Call Bridge y el certificado de agrupamiento (intermedio y raíz) al almacén de CallManager-trust

### Upload Certificate/Certificate chain



 Upload  Close

#### Status


 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

#### Upload Certificate/Certificate chain

Certificate Purpose\*  ▼  
 Description(friendly name)   
 Upload File  CA-cert.cer

 Upload  Close

#### Status

 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

#### Upload Certificate/Certificate chain

Certificate Purpose\*  ▼  
 Description(friendly name)   
 Upload File  certall.cer

Si dispone de certificados independientes para Call Bridge y Webadmin, asegúrese de cargar:

- Certificados Webadmin, Call Bridge y Root al almacén de confianza de Call Manager en CUCM

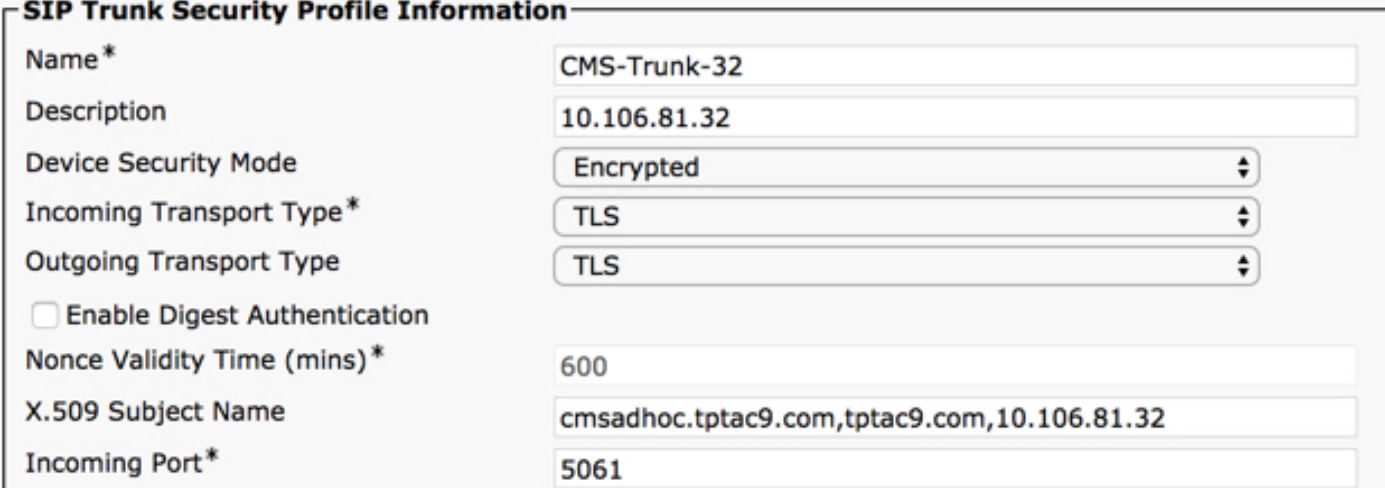
**Nota:** Se pueden crear el enlace troncal SIP de CUCM como un enlace troncal SIP no seguro. Si es así, no es necesario cargar el certificado de CallBridge en el almacén de confianza de CallManager, pero sí es necesario cargar el certificado raíz que firmó el certificado de webadmin en el almacén de confianza de CallManager.

Paso 2. Configure un perfil de troncal SIP seguro.

- Abra la interfaz web de CUCM.
- Vaya a **System > Security > SIP Trunk Security Profile (Sistema > Seguridad > Perfil de seguridad de enlace troncal SIP)**.
- Seleccione **Add New (Agregar nuevo)**.
- Introduzca los valores con la información correcta.

<b>Nombre</b>	Introduzca un nombre; por ejemplo, CMS-Trunk-32.
<b>Modo de seguridad del dispositivo</b>	Seleccione Encrypted (Cifrado)
<b>Tipo de transporte de entrada</b>	Seleccione TLS
<b>Tipo de transporte de salida</b>	Seleccione TLS
<b>Nombre del sujeto X.509</b>	Introduzca el CN del certificado de Call Bridge; separe los nombres con comas
<b>Puerto de entrada</b>	Introduzca el puerto para recibir solicitudes de TLS; el valor predeterminado es 5061

- Seleccione **Save (Guardar)**.



**SIP Trunk Security Profile Information**

Name*	CMS-Trunk-32
Description	10.106.81.32
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	cmsadhoc.tptac9.com,tptac9.com,10.106.81.32
Incoming Port*	5061

Paso 3. Crear tronco SIP

- Vaya a **Device > Trunk (Dispositivo > Enlace troncal)**
- Seleccione **Add New (Agregar nuevo)**.
- Seleccione **SIP Trunk (Enlace troncal SIP)** en Trunk Type (Tipo de enlace troncal).
- Seleccione Next (Siguiente).
- Introduzca los valores correspondientes.

<b>Nombre del dispositivo</b>	Introduzca un nombre para el enlace troncal SIP; por ejemplo, CMS-Abhishe
<b>Dirección de destino</b>	Introduzca la dirección IP de CMS o el FQDN de Call Bridge; por ejemplo, 10.106.81.32

**Puerto de Destino**

Introduzca el puerto en el que el CMS escucha comunicación TLS; por ejemplo **5061**

**Perfil de seguridad del enlace troncal SIP**

Seleccione el perfil de seguridad creado en el paso 2, **CMS-troncal-32**

**Perfil SIP**

Seleccione **Standard SIP Profile for TelePresence Conferencing (Perfil SIP estándar para conferencias de telepresencia)**

Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1* 10.106.81.32		5061	up		Time Up: 0 day 0 hour minutes

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* CMS-Trunk-32

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* Standard SIP Profile For TelePresence Conferencing [View Details](#)

DTMF Signaling Method\* No Preference

#### Paso 4. Crear el puente de conferencia

- Vaya a **Media Resources > Conference Bridge (Recursos de medios > Dispositivo de conferencia)**.
- Seleccione **Add New (Agregar nuevo)**.
- Seleccione **Cisco TelePresence Conductor** desde el menú desplegable **Conference Bridge (Dispositivo de conferencia)**.

**Nota:** A partir de la versión 11.5.1 SU3 de CUCM, la opción **Cisco Meeting Server** está disponible en el menú desplegable para su selección como **Conference BridgeType** (Tipo de dispositivo de conferencia).

- Introduzca la información correspondiente.

**Nombre del dispositivo de conferencia**

Introduzca un nombre para este dispositivo; por ejemplo, **CMS-ad-hoc-32**

**Descripción**

Introduzca una descripción para este dispositivo de conferencia; por ejemplo, **10.106.81.32**

**Enlace troncal SIP**

Seleccione el enlace troncal SIP creado en el paso 3, **CMS-Abhishek-32**

**Anular el destino del enlace troncal SIP como dirección HTTP**

Marque esta casilla en caso de que se requiera un nombre diferente

**Nombre de host/dirección IP**

Introduzca el nombre de host o la dirección IP de CMS; por ejemplo, **10.106.81.32**

**Nombre de usuario**

Introduzca el usuario creado en CMS con privilegios de API; por ejemplo, **admin**

**Contraseña**

Introduzca la contraseña del usuario de API

**Confirmar contraseña**

Introduzca la contraseña una vez más

**Usar HTTPS**

Marque la casilla; esta opción es obligatoria para la conexión a CMS


**Puerto HTTP**

Introduzca el puerto webadmin de CMS, por ejemplo **443**

**Conference Bridge Configuration** Relat

---

**Status**

 Status: Ready

---

**Conference Bridge Information**

Conference Bridge : CMS-Adhoc-32 (10.106.81.32)  
 Registration: Registered with Cisco Unified Communications Manager CUCM115  
 IPv4 Address: 10.106.81.32

---

**Device Information**

Conference Bridge Type\* Cisco TelePresence Conductor  
 Device is trusted  
 Conference Bridge Name\*   
 Description   
 Conference Bridge Prefix   
 SIP Trunk\*  ▼  
 Allow Conference Bridge Control of the Call Security Icon

---

**HTTP Interface Info**

Override SIP Trunk Destination as HTTP Address

**Hostname/IP Address**

1

Username\*   
 Password\*   
 Confirm Password\*

Use HTTPS  
 HTTP Port\*

- Seleccione **Save (Guardar)**.

**Nota:** Los campos de nombre de host (FQDN de CMS) o de dirección IP deben estar incluidos en el certificado Webadmin, en el campo de nombre común o de nombre alternativo del sujeto para permitir la conexión segura.

- Después de la creación del puente de conferencia, abra la sección **Cisco Unified Serviceability**.
- Vaya a **Tools > Control Center - Feature Services (Herramientas > Centro de control > servicios de funciones)**.
- En el menú desplegable, seleccione el nodo de editor CUCM.
- Seleccione **Go (Ir)**.
- Seleccione **Cisco CallManager service (Servicio de administrador de llamadas de Cisco)**.
- Seleccione **Restart (Reiniciar)**.

**Precaución:** Cuando se reinicie el servicio administrador de llamadas, las llamadas conectadas permanecen, pero algunas funciones no están disponibles durante el reinicio. No se pueden hacer llamadas nuevas. El reinicio del servicio tarda alrededor de 5 a 10 minutos; esto depende de la carga de trabajo de CUCM. Realice esta acción con cuidado y asegúrese de hacerla durante un período de mantenimiento.

Paso 5. El puente CMS se ha registrado correctamente en CUCM

- Vaya a **Media Resources > Media Resource Group (Recursos de medios > Grupo de recursos de medios)**.
- Haga clic en **Add New (Agregar nuevo)** para crear un nuevo grupo de recursos de medios e introduzca un nombre.
- Mueva el puente de conferencia (cms) en este caso de la casilla **Available Media Resources (Recursos de medios disponibles)** a la casilla **Selected Media Resources (Recursos de medios seleccionados)**.
- Haga clic en **Save (Guardar)**.

**Media Resource Group Configuration**

Save Delete Copy Add New

**Status**  
Status: Ready

**Media Resource Group Status**  
Media Resource Group: CMS MRG (used by 45 devices)

**Media Resource Group Information**  
Name\*: CMS MRG  
Description:

**Devices for this Group**  
Available Media Resources\*\*  
ANN\_2  
CFB\_2  
IVR\_2  
MOH\_2  
MTP\_2  
Selected Media Resources\*  
cmslab1.acanotaclab.com (CFB)

Use Multi-cast for MOH Audio (If at least one multi-cast MOH resource is available)

Save Delete Copy Add New

Paso 6. Agregue los grupos de recursos de medios (MRG) a las listas de grupos de recursos de medios (MRGL)

- Vaya a **Media Resources > Media Resource Group (Recursos de medios > Grupo de recursos de medios)**.
- Haga clic en **Add New (Agregar nuevo)** para crear una nueva lista de grupos de recursos de medios e introduzca un nombre, o bien seleccione una MRGL existente y haga clic en ella para editarla.
- Mueva uno o varios grupos de recursos de medios creados de la casilla **Available Media Resource Groups (Grupos de recursos de medios disponibles)** a la casilla **Selected Media**



## Resource Groups (Grupos de recursos de medios seleccionados).

- Haga clic en **Save (Guardar)**.

The screenshot shows the 'Media Resource Group List Configuration' window. At the top, there is a header bar with the title and a toolbar containing icons for Save, Delete, Copy, and Add New. Below the header, the interface is divided into several sections: 1. 'Status' section: Shows an information icon and the text 'Status: Ready'. 2. 'Media Resource Group List Status' section: Displays 'Media Resource Group List: CMS MRGL (used by 45 devices)'. 3. 'Media Resource Group List Information' section: Contains a text input field labeled 'Name\*' with the value 'CMS MRGL'. 4. 'Media Resource Groups for this List' section: Features two list boxes. The top box, 'Available Media Resource Groups', contains a list of options: 'CMS Cluster 1 MRGL', 'CMS Cluster 2 MRGL', 'CMS Cluster 3 MRGL', 'CMS Cluster MRG', and 'softwareBridge'. Below this list are two arrow icons (down and up). The bottom box, 'Selected Media Resource Groups', contains the selected item 'CMS MRG' and has a down arrow icon to its right. At the bottom of the window, there is a row of buttons for 'Save', 'Delete', 'Copy', and 'Add New'.

### Paso 7: Agregar MRGL a un grupo de dispositivos o dispositivo

En función de la implementación, un grupo de dispositivos se puede configurar y aplicar a los terminales, o un dispositivo individual (un terminal) se puede asignar a una MRGL específico. **Si una MRGL se aplica al grupo de dispositivos y a un terminal, la configuración del terminal prevalecerá.**

- Vaya a **System >> Device Pool (Sistema >> Grupo de dispositivos)**.
- Cree un nuevo grupo de dispositivos o utilice un grupo de dispositivos existente. Haga clic en **Add New (Agregar nuevo)**.



### Device Pool Configuration

Save

Status: Ready

---

#### Device Pool Information

Device Pool: New

---

#### Device Pool Settings

Device Pool Name\*

Cisco Unified Communications Manager Group\*

Calling Search Space for Auto-registration

Adjunct CSS

Reverted Call Focus Priority

Intercompany Media Services Enrolled Group

---

#### Roaming Sensitive Settings

Date/Time Group\*

Region\*

Media Resource Group List

Paso 8: Para agregar el conjunto de dispositivos al terminal y agregar MRGL al terminal

- Vaya a **Device> Phones (Dispositivo > Teléfonos)**.
- Haga clic en **Find (Buscar)** y seleccione el dispositivo del cual desea cambiar la configuración del grupo de dispositivos.
- Aplique el grupo de dispositivos y la MRGL creados en los pasos anteriores.
- Haga clic en **Save, Apply Config and Reset (Guardar, aplicar configuración y restablecer)**.

El termina se reiniciará y registrará.

### Phone Configuration

Save Delete Copy Reset Apply Config Add New

Modify Button Items

1 [Line \(1\) - 6000 \(no partition\)](#)

----- Unassigned Associated Items -----

2 [Line \(2\) - Add a new DN](#)

---

**Product Type:** Cisco Spark Room Kit  
**Device Protocol:** SIP

---

**Real-time Device Status**

**Registration:** Registered with Cisco Unified Communications Manager 10.104.215.207  
**IPv4 Address:** [10.104.130.54](#)  
**Active Load ID:** ce-9.3.1-61bfa3834f2-2018-05-04  
**Inactive Load ID:** None  
**Download Status:** None

---

**Device Information**

Device is Active  
 Device is trusted

MAC Address\*

Description

Device Pool\*  [View Details](#)

Common Device Configuration  [View Details](#)

Phone Button Template\*

Common Phone Profile\*  [View Details](#)

Calling Search Space

AAR Calling Search Space

Media Resource Group List

Paso 9: Configuración en un terminal

- Inicie sesión en web-gui del terminal.
- Vaya a **Setup > Configuration > Conference > Multipoint Mode** (Configuración > Configuración > Conferencia > Modo multipunto).
- Seleccione **CUCMMediaResourceGroupList**.

Multipoint Mode

CUCMMediaResourceGroupList

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

- Abra la interfaz web de CUCM.
- Vaya a **Device > Trunks (Dispositivo > Enlaces troncales)**.
- Seleccione el enlace troncal SIP que apunta a CMS.
- Asegúrese de que los enlaces troncales estén en el estado **Full Service (Servicio completo)**.
- Vaya a **Media Resources > Conference Bridge (Recursos de medios > Puente de conferencia)**.
- Seleccione el puente de conferencia CMS.
- Asegúrese de que esté registrado en CUCM.

Realizar una llamada ad-hoc

- Realice una llamada del terminal A registrado en CUCM (MRGL agregada) a otro terminal B.
- En el terminal A, haga clic en **Add** (Agregar) y marque terminal C.
- El terminal A pasará a estar en espera.
- Haga clic en Merge (Combinar).
- Corrobore que las llamadas estén conectadas en CMS.
- Acceda a la interfaz web de CMS.
- Vaya a **Status > Calls (Estado > Llamadas)**.

Para la prueba, se utilizaron 3 terminales para audio/videoconferencia ad-hoc.

Status	Configuration	Logs
<b>Active Calls</b>		
Filter	<input type="text"/>	<input type="button" value="Set"/>
Show only calls with alarms <input type="button" value="Set"/>		
<b>Conference: 001036010001 (3 active calls)</b>		
<input type="checkbox"/>	SIP 6000@acanotaclab.com <a href="#">[less]</a> (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.96 Mb/s
	outgoing media	OPUS, H.264, 1920 x 1080 29.9fps, 929 Kb/s
	additional protocols	unencrypted Active Control
	remote address	6000@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd1-cfd7680a@10.104.215.207
<input type="checkbox"/>	SIP abhi <a href="#">[less]</a> (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.94 Mb/s
	outgoing media	AAC, H.264, 1920 x 1080 30.3fps, 1.33 Mb/s
	additional protocols	unencrypted Active Control
	remote address	2333@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd3-cfd7680a@10.104.215.207
<input type="checkbox"/>	SIP sakatuka <a href="#">[less]</a> (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.94 Mb/s
	outgoing media	AAC, H.264, 1920 x 1080 29.9fps, 1.19 Mb/s
	additional protocols	unencrypted Active Control
	remote address	1105@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd2-cfd7680a@10.104.215.207

## Troubleshoot

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