

# Configurar as conferências do Cisco Meeting Server e CUCM Ad hoc

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurar o CMS](#)

[Configurar o CUCM](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Este documento descreve as etapas para configurar as conferências ad hoc com Cisco Meeting Server (CMS) e Cisco Unified Communications Manager (CUCM).

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração e implantação do CMS
- Criação de tronco e registro de endpoint do CUCM
- Certificados assinados

## Componentes Utilizados

- CUCM
- Servidor do CMS 2.0.X e posterior
- Os componentes WebAdmin e Call Bridge já devem estar configurados no CMS
- Registros de Domain Name System (DNS) internos para Call Bridge & Webadmin, resolvível para o Endereço IP de servidor do CMS
- Autoridade de certificado (CA) interna para assinar o certificado com uso avançado de chave de autenticação de servidor da Web e um cliente da Web
- Certificados assinados para a comunicação de segurança de camada de transporte (TLS)

**Note:** Certificados assinados automaticamente não são suportados para essa implantação, porque precisam do servidor da Web e autenticação de cliente da Web, que não é possível adicionar nos certificados assinados automaticamente

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando. Este documento não está restrito a versões específicas de software e hardware, no entanto, os requisitos mínimos de versão de software devem ser atendidos.

## Configurar

### Configurar o CMS

Etapa 1. Crie uma conta de usuário administrador com privilégios de API (Application Program Interface, Interface de programa de aplicativos).

- Abra uma sessão Secure Shell (SSH) para o processador de gerenciamento de placa-mãe (MMP)
- Para adicionar uma conta de usuário de nível de administrador, execute o comando `user add <username> <role>`
- Digite a nova senha, conforme mostrado na imagem:

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

Etapa 2. Gerar os certificados.

- Execute o comando `pki csr <nome do arquivo> CN:<nome comum> subjectAltName:<nomes alternativos do assunto>`
- Use as informações de acordo com seus requisitos

Nome do arquivo certall

CN tptac9.com

subjectAltName cmsadhoc.tptac9.com,10.106.81.32

- Não use caracteres curinga para gerar o certificado. Um certificado com caracteres curinga não é suportado pelo CUCM
- Certifique-se de que o certificado esteja assinado com a autenticação de servidor da Web e um cliente da Web de uso de chave avançado

**Note:** Para usar o mesmo certificado para todos os serviços, o Nome comum (CN) deve ser o nome do domínio e o nome dos outros serviços do CMS deve ser incluído como Nome alternativo de assunto (SAN). Nesse caso, o Endereço IP também é assinado pelo certificado e é confiável em qualquer computador que tenha o certificado raiz instalado.

### Configurar o CUCM

Etapa 1. Carregue os certificados no repositório confiável do CUCM.

- O certificado raiz poderá ser baixado na interface da Web da autoridade de certificado

### 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](#)

- Adicione o certificado Call Bridge e o certificado do pacote (intermediário e raiz) ao armazenamento confiável do CallManager

**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

Se você tiver certificados separados para Call Bridge e Webadmin, faça o upload:

- Os certificados Webadmin, Call Bridge e Root para o armazenamento confiável do Call Manager no CUCM

**Note:** O tronco SIP do CUCM pode ser criado como um tronco SIP não seguro, se for esse o caso, não é necessário fazer o upload do certificado de Call Bridge para o armazenamento confiável do CallManager, mas é necessário fazer o upload do certificado raiz que assinou o certificado webadmin para o armazenamento confiável do CallManager.

Etapa 2. Configure um perfil de tronco SIP seguro.

- Abra a interface da Web do CUCM
- Navegue até **Sistema > Segurança > Perfil de segurança do tronco SIP**
- Selecione **Adicionar novo**
- Insira os valores com as informações apropriadas

**Nome** Insira um nome, por exemplo CMS-tronco-32  
**Modo de segurança do dispositivo** Selecione Criptografado  
**Tipo de transporte de entrada** Selecione TLS  
**Tipo de transporte de saída** Selecione TLS  
**Nome do assunto X.509** Insira os CN do certificado de Call Bridge, separe os nomes por vírgula  
**Porta de entrada** Insira a porta para receber solicitações TLS. O padrão é 5061

- Selecione **Salvar**

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

Etapa 3. Criar tronco SIP

- Navegue até **Dispositivo > Tronco**
- Selecione **Adicionar novo**
- Selecione **Tronco SIP para Tipo de tronco**
- Selecione **Próximo**
- Informe os valores.

**Nome de dispositivo** Insira um nome para o tronco SIP, por exemplo **CMS-Abhishek-32**  
**Endereço de destino** Insira o Endereço IP do CMS ou o FQDN da Call Bridge, por exemplo **10.106.81.32**  
**Porta de Destino** Insira a porta onde o CMS escuta a comunicação TLS, por exemplo **5061**  
**Perfil de Segurança de Tronco de SIP** Selecione o perfil seguro criado na etapa 2, **CMS-trunk-32**  
**Perfil SIP** Selecione **Perfil SIP padrão para conferência de TelePresence**

**SIP Information**

**Destination**

Destination Address is an SRV

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

#### Etapa 4. Crie a ponte de conferência

- Navegue até **Recursos de mídia > Conference Bridge**
- Selecione Adicionar novo
- Selecione **Cisco TelePresence Conductor** no menu suspenso **Recurso de conferência**

**Note:** No CUCM versão 11.5.1 SU3, a opção **Cisco Meeting Server** está disponível para seleção como **Tipo de recurso de conferência** no menu suspenso

- Insira as informações apropriadas

**Nome do recurso de conferência**

Insira um nome para este dispositivo, por exemplo **CMS-32**

**Descrição**

Digite uma descrição para este recurso de conferência, por exemplo **10.106.81.32**

**Tronco SIP**

Selecione o tronco SIP criado na etapa 3, **CMS-Abhishek-**

**Substitua o destino do tronco SIP como endereço de HTTP**

Marque esta caixa caso seja necessário um nome diferente

**Nome de host/Endereço IP dos servidores CUCM**

Insira o nome do host ou Endereço IP do CMS, por exemplo **10.106.81.32**

**Nome de usuário**

Insira o usuário criado no CMS com privilégios de API, por exemplo **admin**

**Senha**

Digite a senha do usuário API

**Confirmar senha**

Digite a senha mais uma vez

**Use HTTPS**

Marque a caixa, isso é necessário para conexão do CMS

**Porta HTTP**

Insira a porta de webadmin do CMS, por exemplo **443**

**Conference Bridge Configuration** Relat

Save
 Delete
 Copy
 Reset
 Apply Config
 Add New

---

**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\*

- Selecione **Salvar**

**Note:** O campo Nome de host (FQDN do CMS) e/ou Endereço IP, devem ser incluídos no certificado Webadmin, no Nome comum ou no campo Nome alternativo do assunto para permitir a conexão segura





- Após a criação do recurso de conferência, abra a seção **Cisco Unified Serviceability**
- Navegue até **Ferramentas > Centro de controle - Serviços de recurso**
- No menu suspenso, selecione o nó publisher do CUCM
- Selecione **Ir**
- Selecione o **serviço Cisco CallManager**
- Selecione **Reiniciar**

**Caution:** Quando o serviço CallManager é reiniciado, as chamadas conectadas permanecem, mas algumas funções não estão disponíveis durante essa reinicialização. Não é possível fazer chamadas novas. A reinicialização do serviço demora aproximadamente de 5 a 10 minutos, dependendo da carga de trabalho do CUCM. Execute esta ação com cuidado e durante uma janela de manutenção.


Etapa 5. A ponte CMS foi registrada com êxito no CUCM

- Vá para **Recursos de mídia > rupo de recursos de mídia**
- Clique em **Adicionar novo** para criar um novo grupo de recursos de mídia e insira um nome
- Nesse caso, mova o recurso de conferência (cms) da caixa **Recursos de mídia disponíveis** para a caixa **Recursos de mídia selecionados**
- Clique em **Salvar**

**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\*

Description

---

**Devices for this Group**

Available Media Resources\*\*

ANN\_2  
CFB\_2  
IVR\_2  
MOH\_2  
MTP\_2

▼ ▲

Selected Media Resources\*

cmsglab1.acanotaclab.com (CFB)

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

---

Etapa 6. Adicione os MRGs (Media Resource Groups, grupos de recursos de mídia) às MRGLs (Media Resource Group Lists, listas de grupos de recursos de mídia)

- Vá para **Recursos de mídia > Lista de grupos de recursos de mídia**
- Clique em **Adicionar nova** para criar uma nova lista de grupos de recurso de mídia e insira um nome, ou selecione uma MRGL existente e clique para editá-la.
- Mova um ou mais grupos de recurso de mídia criados na caixa **Grupos de recurso de mídia disponíveis** para **Grupos de recurso de mídia selecionados**
- Clique em **Salvar**

**Media Resource Group List Configuration**

Save Delete Copy Add New

**Status**  
Status: Ready

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

**Media Resource Group List Information**  
Name\* CMS MRGL

**Media Resource Groups for this List**

Available Media Resource Groups  
CMS Cluster 1 MRGL  
CMS Cluster 2 MRGL  
CMS Cluster 3 MRGL  
CMS Cluster MRG  
softwareBridge

Selected Media Resource Groups  
CMS MRG

Save Delete Copy Add New

Etapa 7: Adicione a MRGL a um pool de dispositivos ou dispositivo

Dependendo da implementação, um pool de dispositivos pode ser configurado e aplicado aos endpoints, ou um dispositivo individual (um endpoint) pode ser atribuído a uma MRGL específica. Se uma MRGL é aplicada ao pool de dispositivos e a um endpoint, as configurações de endpoint terão precedência.

- Vá para **Sistema >> Pool de dispositivos**
- Crie um novo Pool de dispositivos ou use um pool de dispositivos existente. Clique em **Adicionar Novo**



### Device Pool Configuration

Save

Status: Ready

---

#### Device Pool Information

Device Pool: New

---

#### Device Pool Settings

Device Pool Name\* CMS-Adhoc-DevicePool

Cisco Unified Communications Manager Group\* Default

Calling Search Space for Auto-registration < None >

Adjunct CSS < None >

Reverted Call Focus Priority Default

Intercompany Media Services Enrolled Group < None >

---

#### Roaming Sensitive Settings

Date/Time Group\* CMLocal

Region\* Default

Media Resource Group List CMS MRGL

Etapa 8: adicionar o pool de dispositivos ao endpoint e adicionar MRGL ao endpoint

- Vá para **Dispositivo > Telefones**
- Clique em **Localizar** e selecione o dispositivo para alterar as configurações do Pool de dispositivos
- Aplique o Pool de dispositivos e a MRGL criados nas etapas acima
- **Salvar, Aplicar configuração e redefinição**

O endpoint reinicializará e será registrado

### Phone Configuration

Save Delete Copy Reset Apply Config Add New

Modify Button Items

1 Line [1] - 6000 (no partition)

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\* 0896AD2D9DB2

Description SPARK KIT

Device Pool\* CMS-Adhoc-DevicePool [View Details](#)

Common Device Configuration < None > [View Details](#)

Phone Button Template\* Standard Cisco Spark Room Kit

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

Calling Search Space < None >

AAR Calling Search Space < None >

Media Resource Group List CMS MRGL

Etapa 9: Configuração em um endpoint

- Login para web-gui do endpoint
- Vá para **Configurar > Configuração > Conferência > Modo multiponto**
- Selecione **CUCMMediaResourceGroupList**

Multipoint Mode

CUCMMediaResourceGroupList ⇅

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- Abra a interface da Web do CUCM
- Navegue até **Dispositivo > Troncos**
- Selecione o tronco SIP que aponta para CMS
- Certifique-se de que os troncos estejam em estado **Serviço completo**
- Navegue até **Recurso de mídia > Recurso de conferência**
- Selecione o recurso de conferência do CMS
- Certifique-se ele esteja registrado com CUCM

Faça uma chamada ad-hoc

- Chamada de EndpointA registrada ao CUCM (MRGL adicionada) para outro EndpointB
- No EndpointA, clique em **Adicionar**, disque EndpointC
- O EndpointA ficará em espera
- Clique em **Mesclar**
- Confirme que as chamadas estão conectadas ao CMS
- Abra a interface da Web do CMS
- Navegue até **Status > Calls (Status > Chamadas)**

Para testar, 3 endpoints foram usados para áudio/videoconferência 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

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