Configurar as conferências do Cisco Meeting Server e CUCM Ad hoc

Contents

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

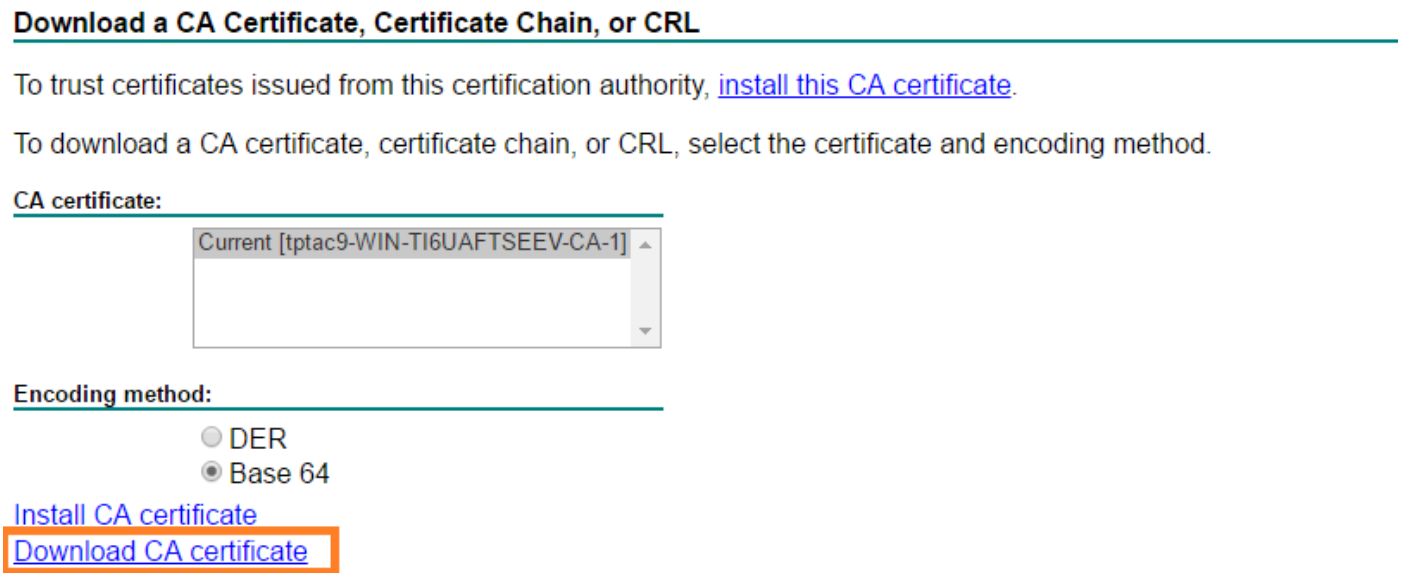
- Não use caracteres curinga para gerar o certificado. Um certificado com caracteres curinga não é suportado pelo CUCM
- Certifique-se de que o certificado esteja assinado com a autenticação de servidor da Web e um cliente da Web de uso de chave avançado

> **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.

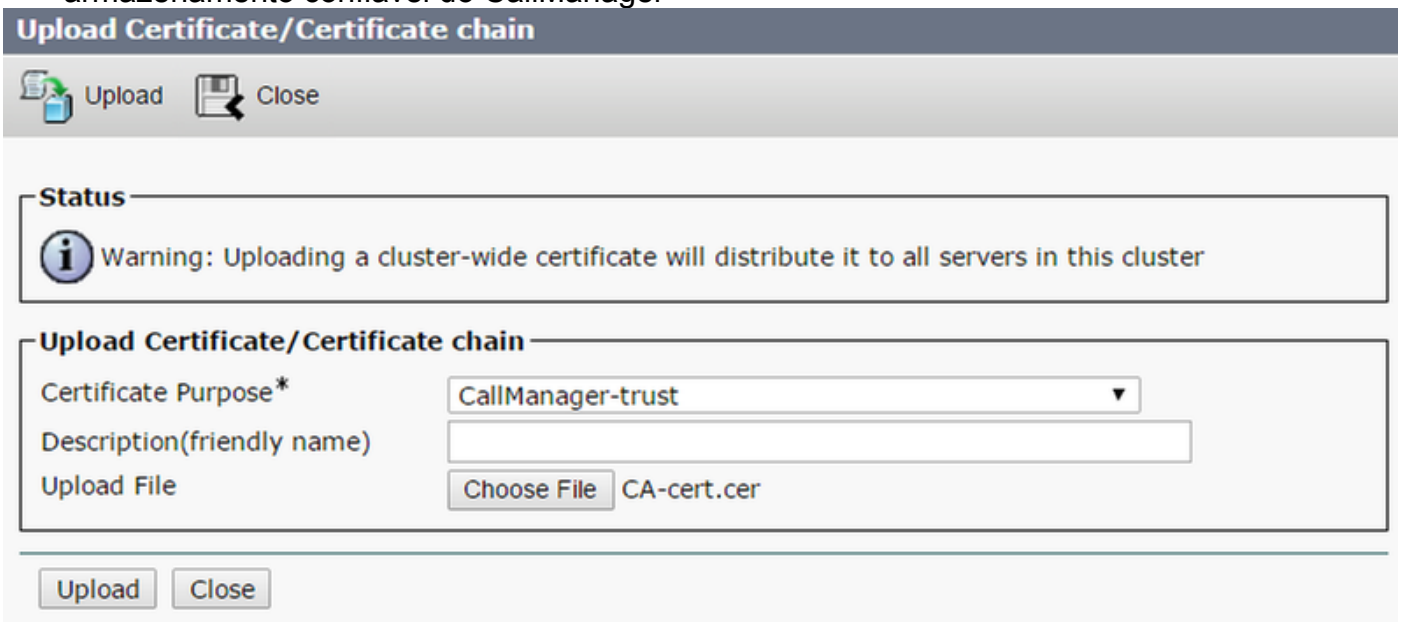
Configurar o CUCM

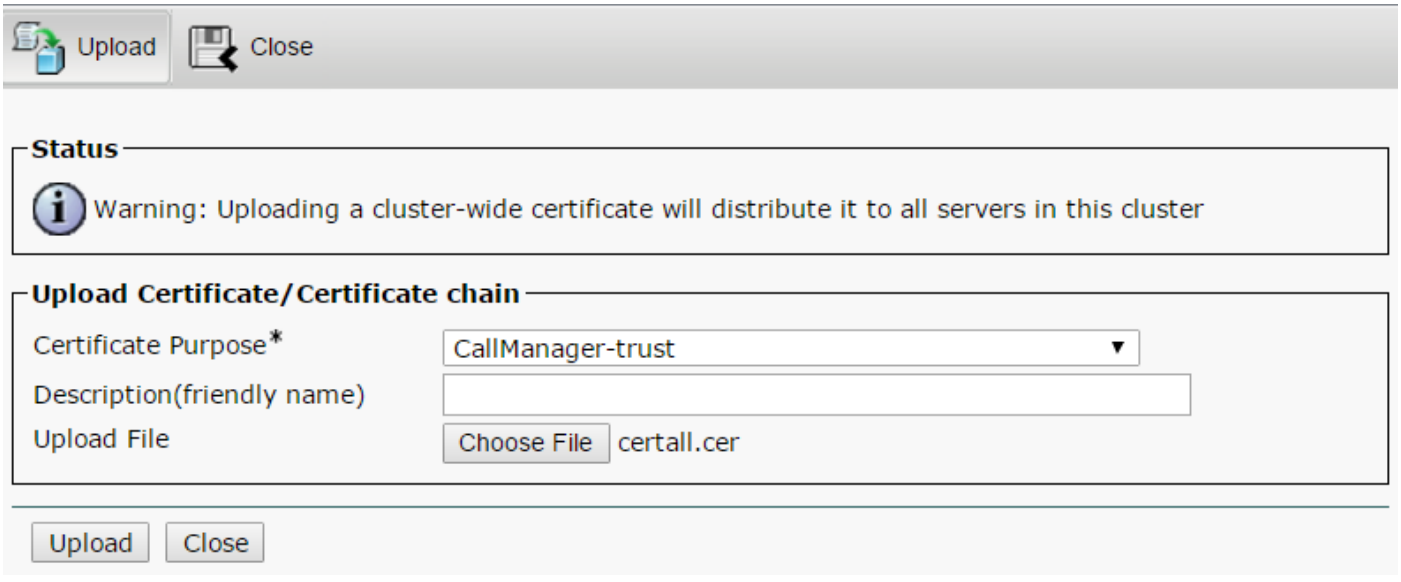
Etapa 1. Carregue os certificados no repositório confiável do CUCM.

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



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





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

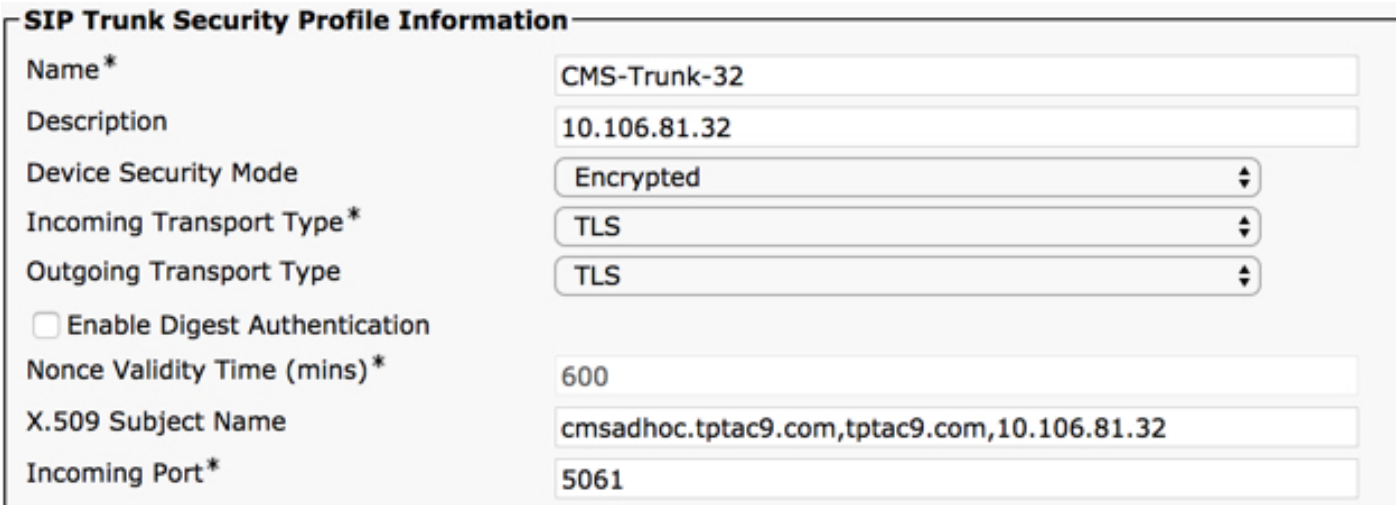
> **Note**: O tronco SIP do CUCM pode ser criado como um tronco SIP não seguro, se for esse o caso, não é necessário fazer o upload do certificado de Call Brdge para o armazenamento confiável do CallManager, mas é necessário fazer o upload do certificado raiz que assinou o certificado webadmin para o 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 vírgul
Porta de entrada	Insira a porta para receber solicitações TLS. O padrão é 5061

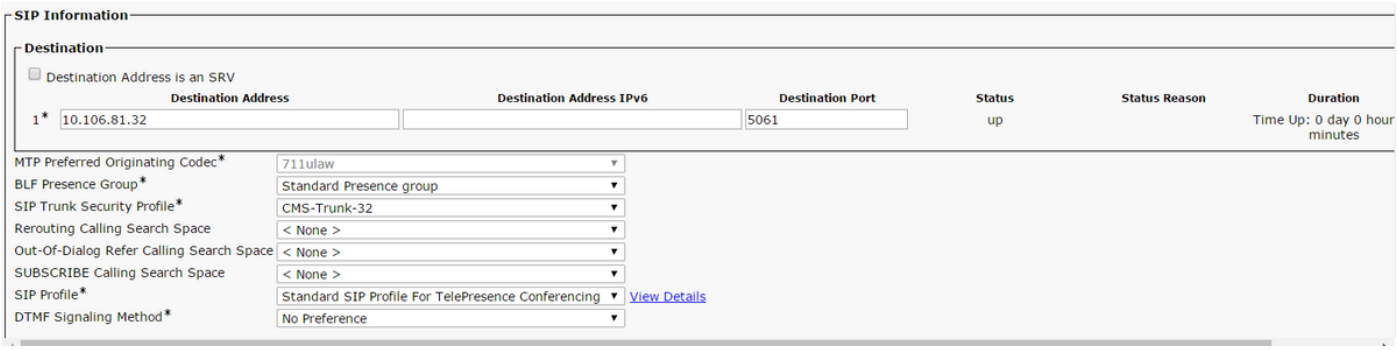
- Selecione **Salvar**



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 **5**
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**



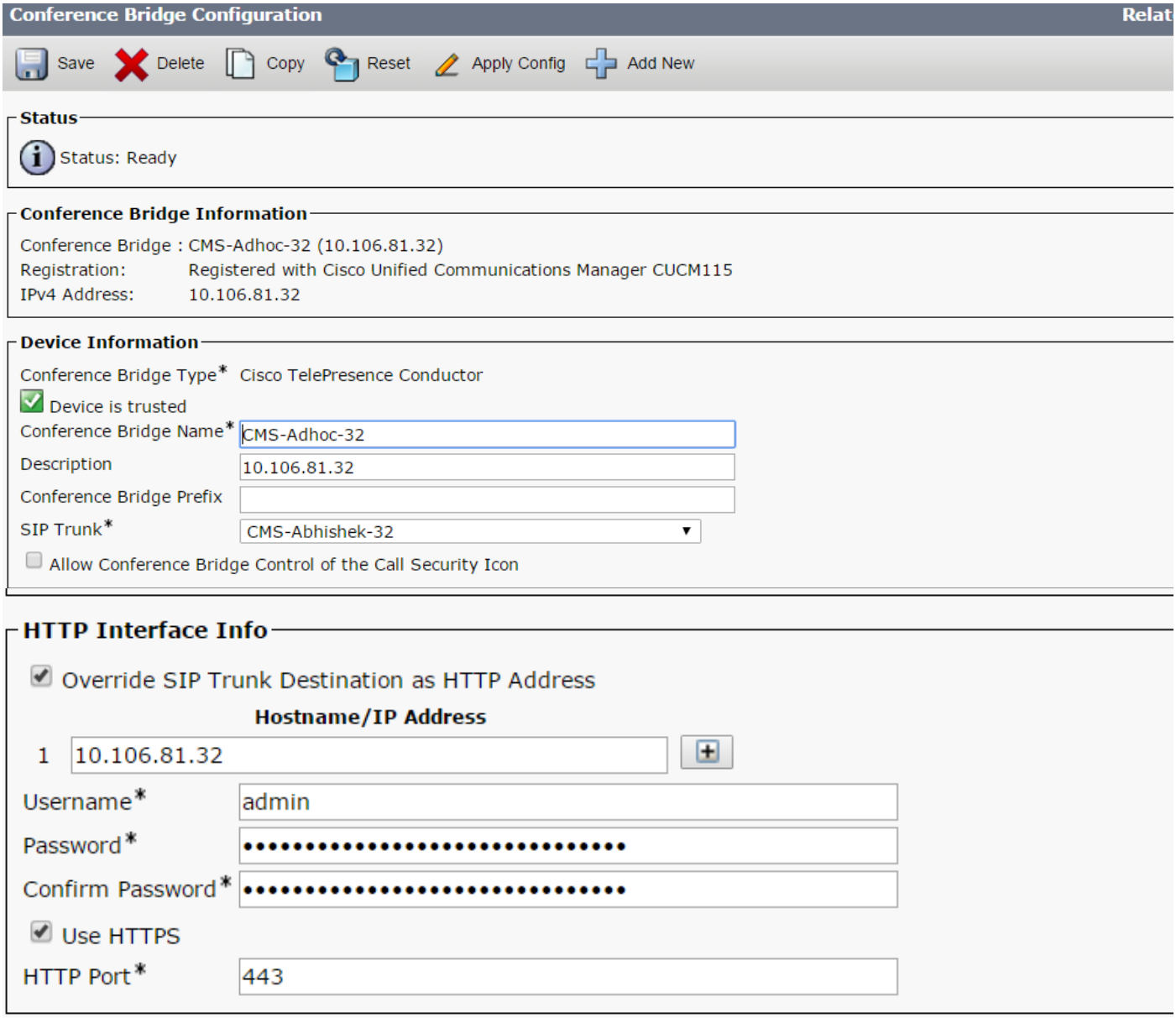
Etapa 4. Crie a ponte de conferência

- 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-A 32**
Descrição	Digite uma descrição para este recurso de conferência, po 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 diferent
Nome de host/Endereço IP dos servidores CUCM	Insira o nome do host ou Endereço IP do CMS, por exemp **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**



- Selecione **Salvar**

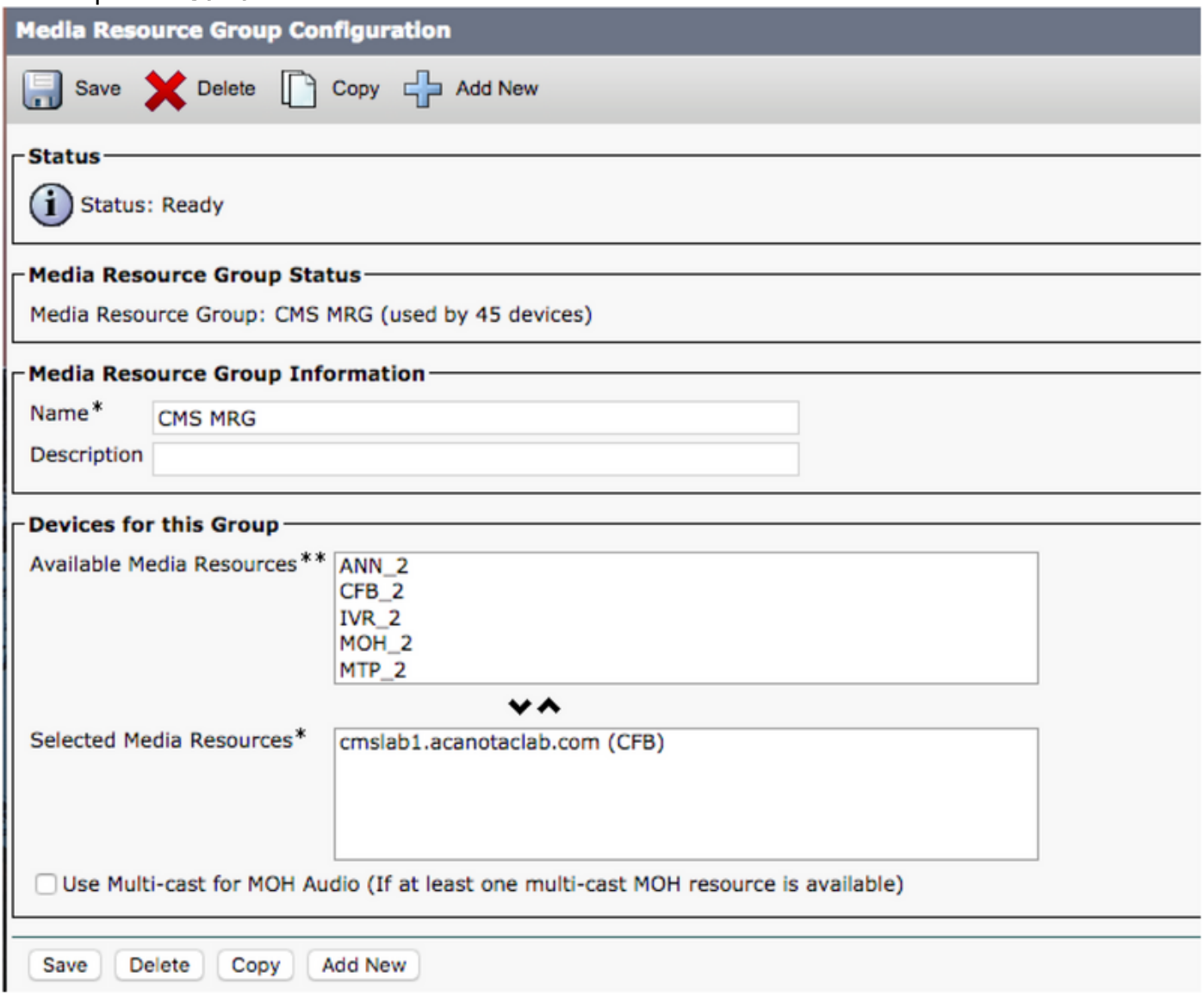
Note: O campo **Nome de host (FQDN do CMS) e/ou Endereço IP, devem ser incluídos no certificado Webadmin, no Nome comum ou no campo Nome alternativo do assunto para permitir a conexão segura**

- 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.

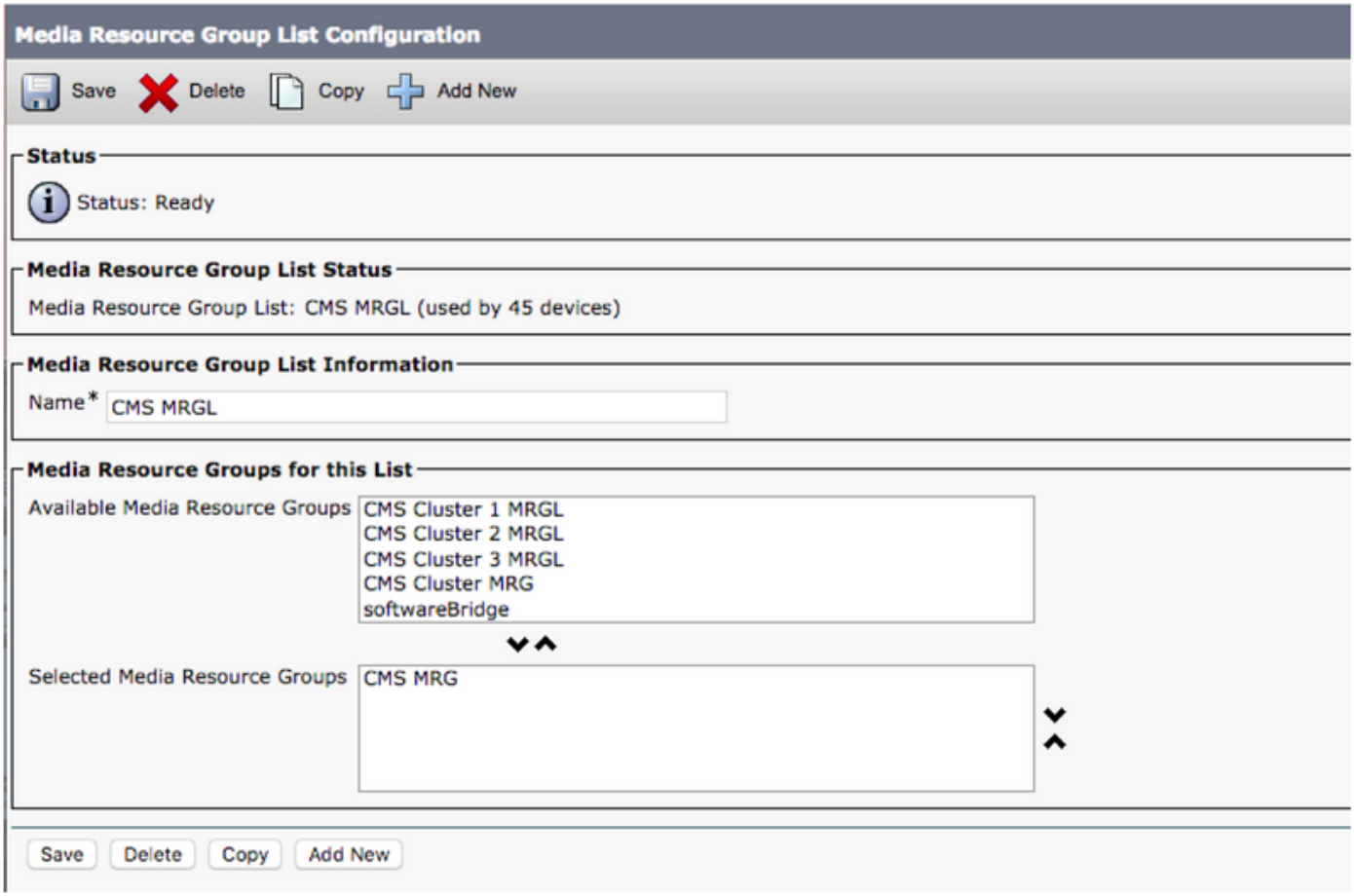
Etapa 5. A ponte CMS foi registrada com êxito no CUCM

- 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**



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)

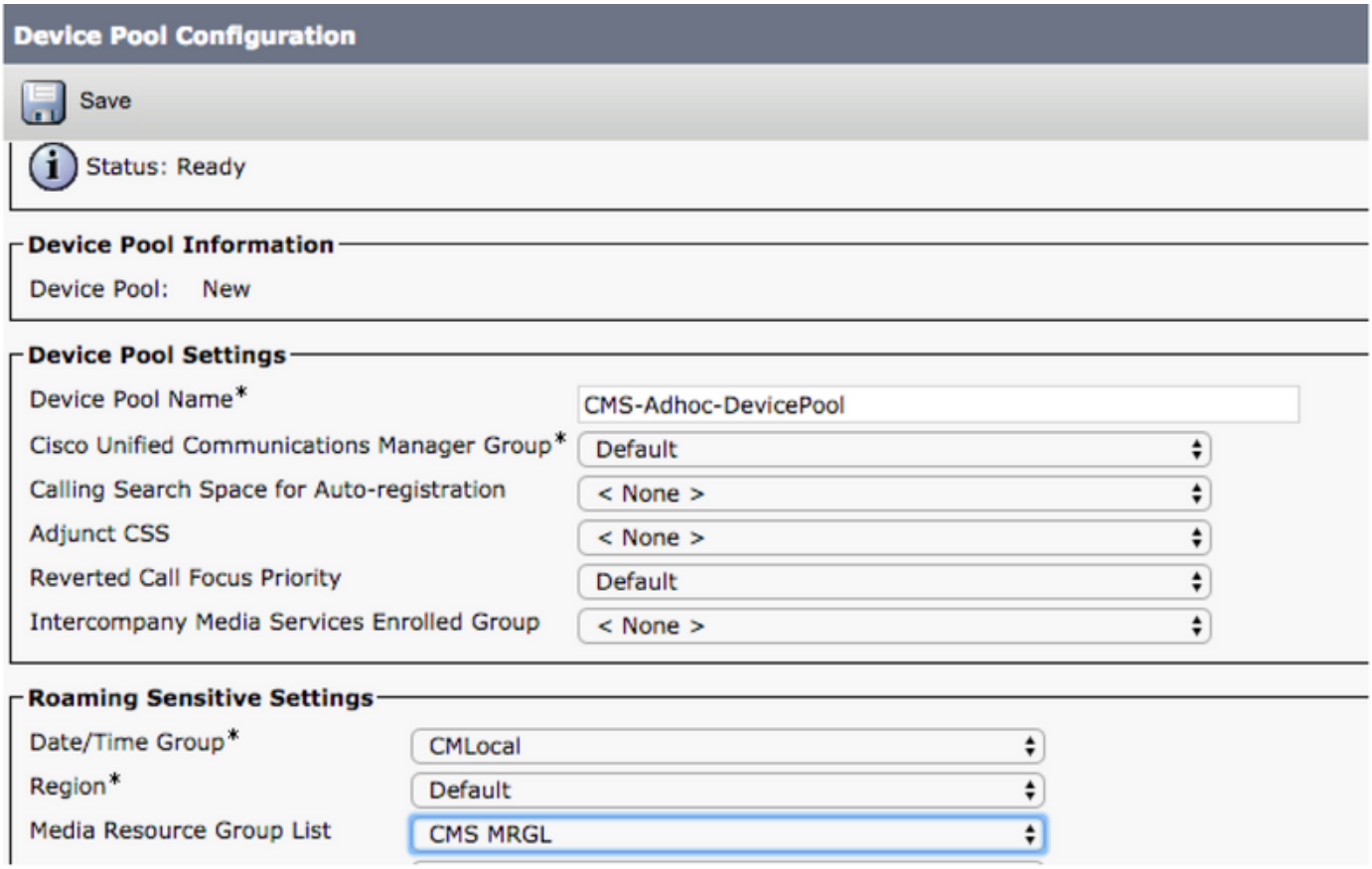
- Vá para **Recursos de mídia > Lista de grupos de recursos de mídia**
- Clique em **Adicionar nova para criar uma nova lista de grupos de recurso de mídia e insira um nome, ou selecione uma MRGL existente e clique para editá-la.**
- Mova um ou mais grupos de recurso de mídia criados na caixa **Grupos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



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.**

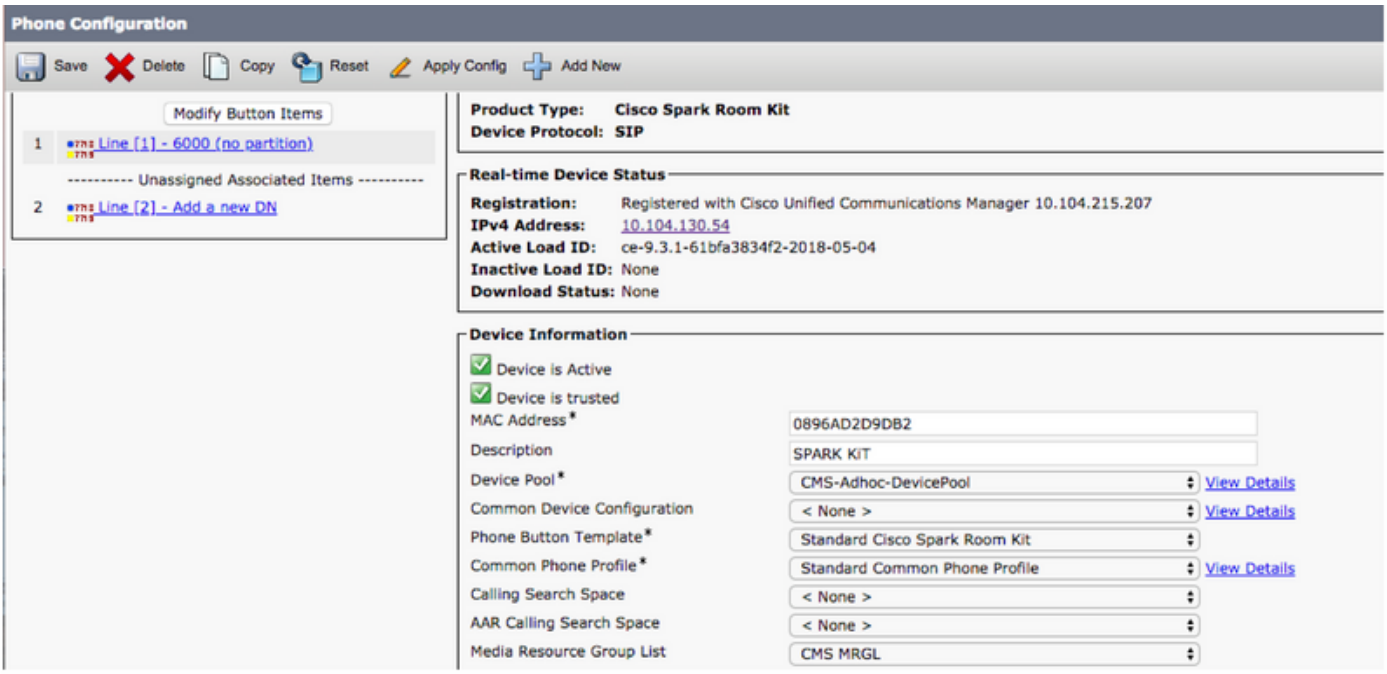
- Vá para **Sistema >> Pool de dispositivos**
- Crie um novo Pool de dispositivos ou use um pool de dispositivos existente. Clique em **Adicionar Novo**



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

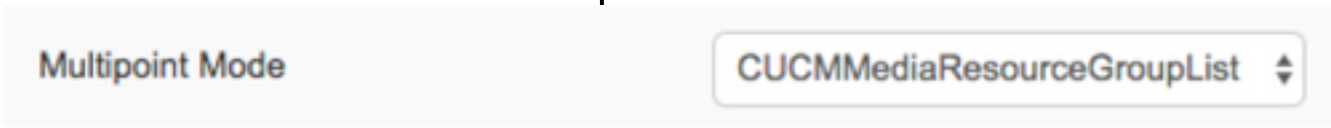
- Vá para **Dispositivo > Telefones**
- Clique em **Localizar e selecione o dispositivo para alterar as configurações do Pool de dispositivos**
- Aplique o Pool de dispositivos e a MRGL criados nas etapas acima
- **Salvar**, **Aplicar configuração e redefinição**

O endpoint reinicializará e será registrado



Etapa 9: Configuração em um endpoint

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



Verificar

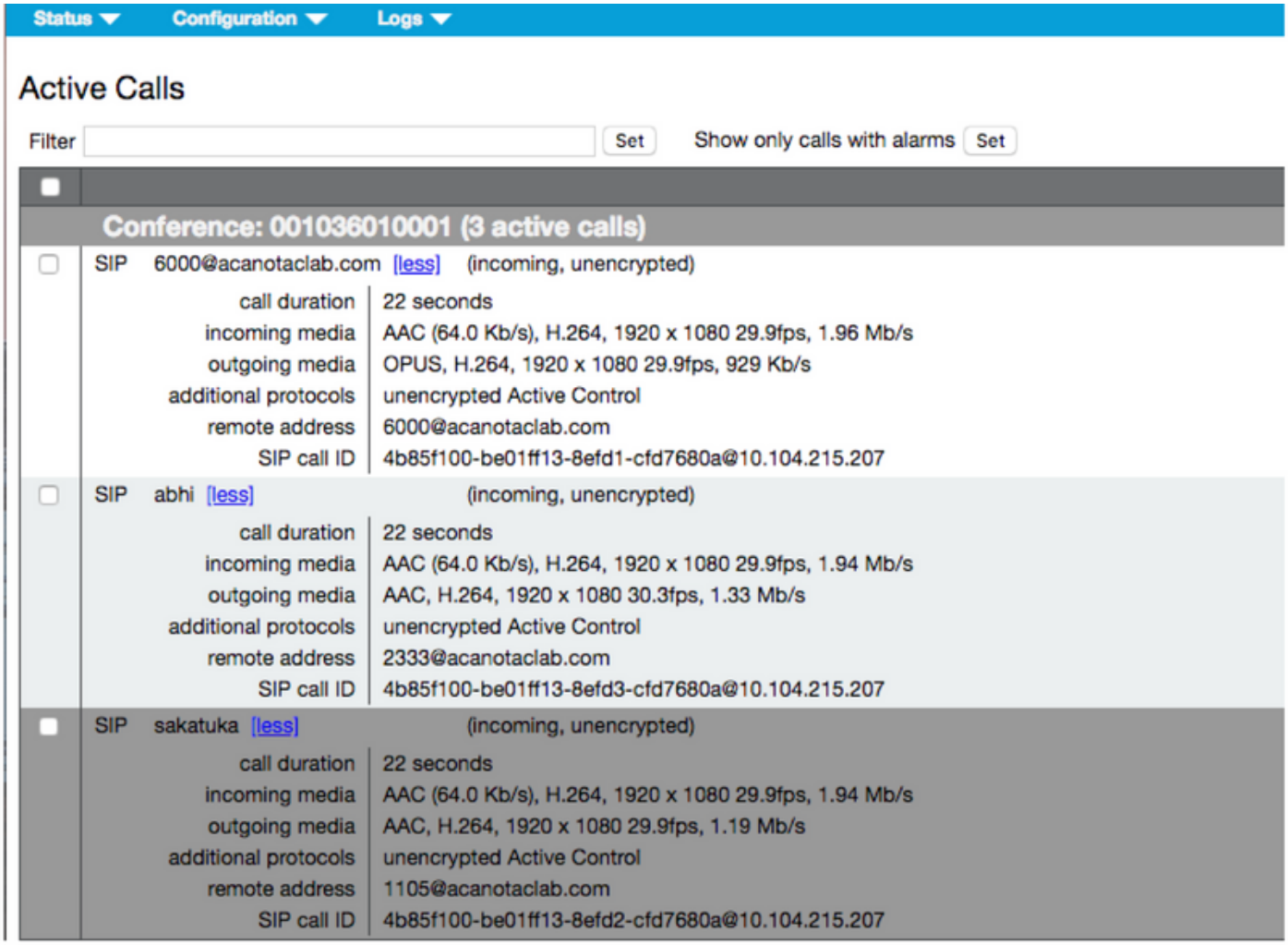
Use esta seção para confirmar se a sua configuração funciona corretamente.

- 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



Troubleshoot

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