Configure Cisco Meeting Server and CUCM Ad hoc Conferences

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Configure CMS
Configure the CUCM
Verify
Troubleshoot

Introduction

This document describes the steps to configure ad hoc conferences with Cisco Meeting Server (CMS) and Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CMS deployment and configuration
- CUCM endpoint registration and trunk creation
- Signed Certificates

Components Used

- CUCM
- CMS Server 2.0.X and above
- Webadmin and Call Bridge components must be already configured on CMS
- Internal Domain Name System (DNS) records for Call Bridge & Webadmin, resolvable to CMS Server IP address
- Internal Certificate authority (CA) in order to sign the certificate with Enhanced key usage of Web Server and Web Client authentication
- Signed Certificates for Transport Layer Security (TLS) communication

> **Note**: Self signed certificates are not supported for this deployment because they need the Web Server and Web Client authentication that is not possible to add in self signed certificates

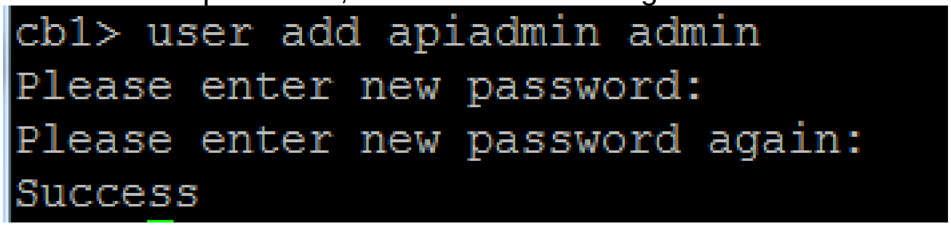
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command. This document is not restricted to specific software and hardware versions, however the minimum software version requirements must be met.

Configure

Configure CMS

Step 1. Create an administrator user account with Application Program Interface (API) privileges.

- Open a Secure Shell (SSH) session to the Mainboard Management Processor (MMP)
- In order to add an admin level user account run the command **user add <username> <role>**
- Enter the password, as shown in the image.



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

Step 2. Generate the certificates.

- Run the command **pki csr <file name> CN:<common name> subjectAltName:<subject alternative names>**
- Use the information according to your requirements

File name	certall
CN	tptac9.com
subjectAltName	cmsadhoc.tptac9.com,10.106.81.32

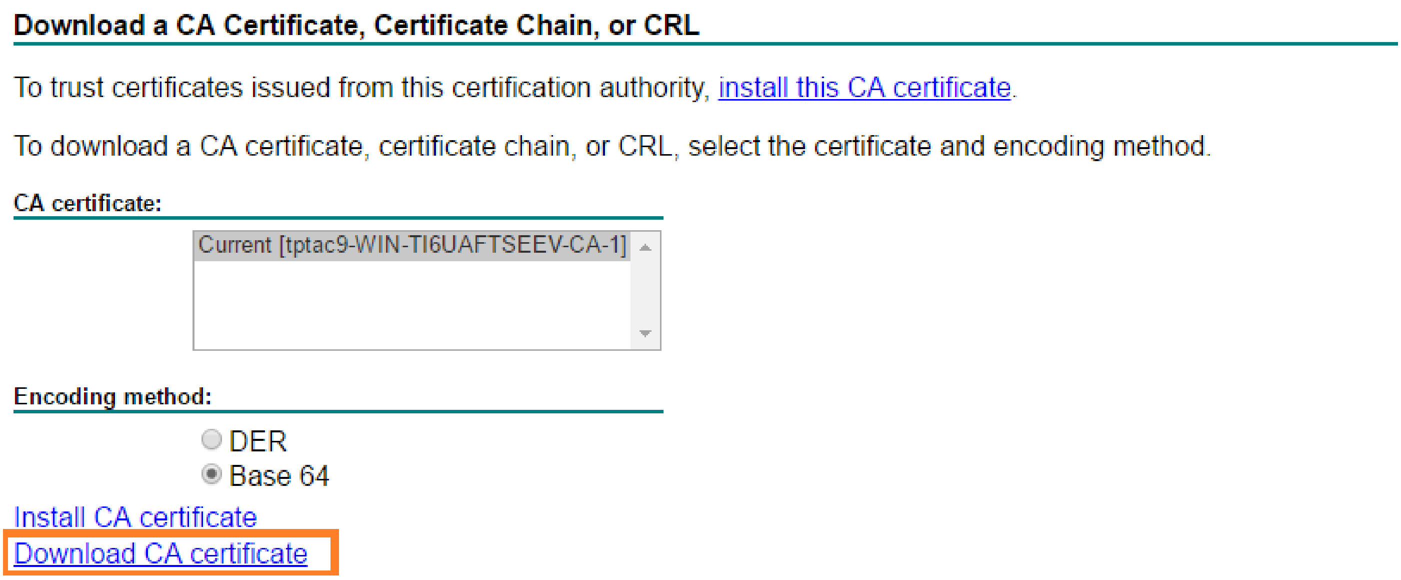
- Do not use wildcards to generate the certificate. A certificate with wildcards is not supported by CUCM
- Ensure the certificate is signed with Enhanced key usage Web Server and Web Client authentication

> **Note**: To use the same certificate for all the services, the Common Name (CN) must be the domain name and the name of the other CMS services must be included as Subject Alterntive Name (SAN). In this case the IP address is also signed by the certificate and is trusted by any machine that has the Root certificate installed.

Configure the CUCM

Step 1. Upload the the certificates to the CUCM trusted store.

- The root certificate can be downloaded from internal Certificate Authority web interface



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:

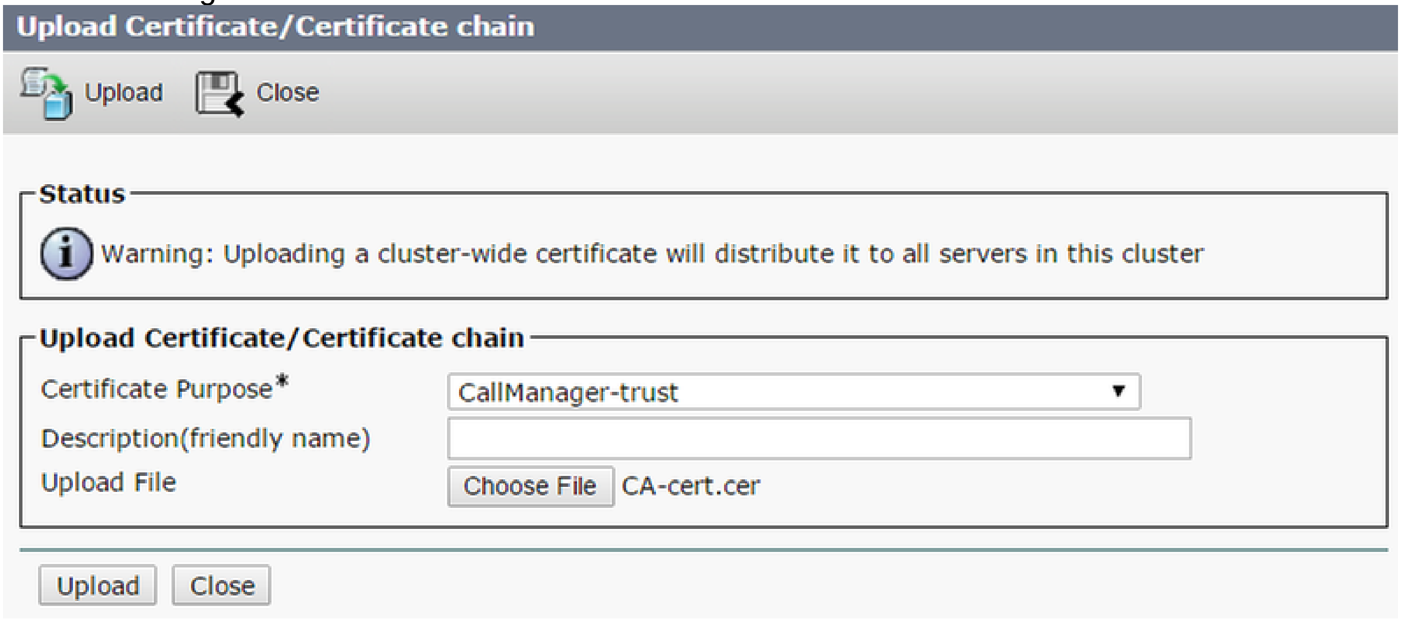
Current [tptac9-WIN-TI6UAFTSEEV-CA-1]

Encoding method:

○ DER
● Base 64

Install CA certificate
Download CA certificate

- Add the Call Bridge certificate and bundle certificate (intermediate and root) to the CallManager-trust store



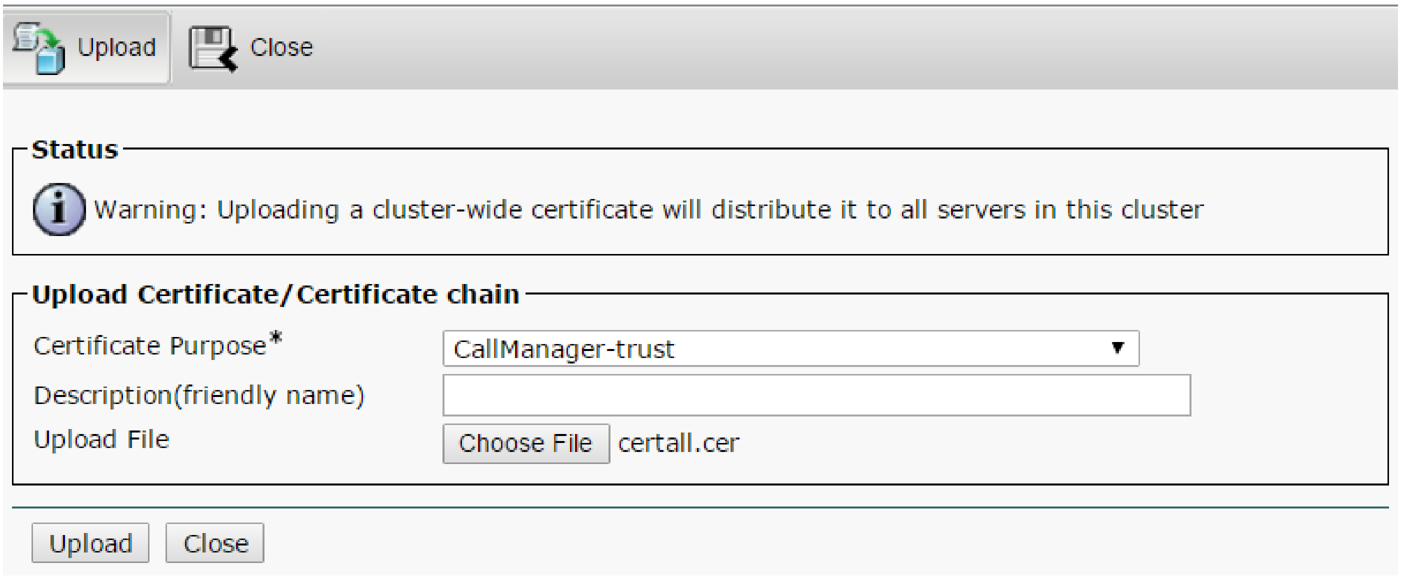
Upload Certificate/Certificate chain

Status

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

Upload Certificate/Certificate chain

Certificate Purpose*	CallManager-trust
Description(friendly name)	
Upload File	Choose File CA-cert.cer



Status

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

Upload Certificate/Certificate chain

Certificate Purpose*	CallManager-trust
Description(friendly name)	
Upload File	Choose File certall.cer

If you have separate certificates for Call Bridge and Webadmin please ensure to upload:

- The Webadmin, Call Bridge and Root certificates to Call Manager trust store on CUCM

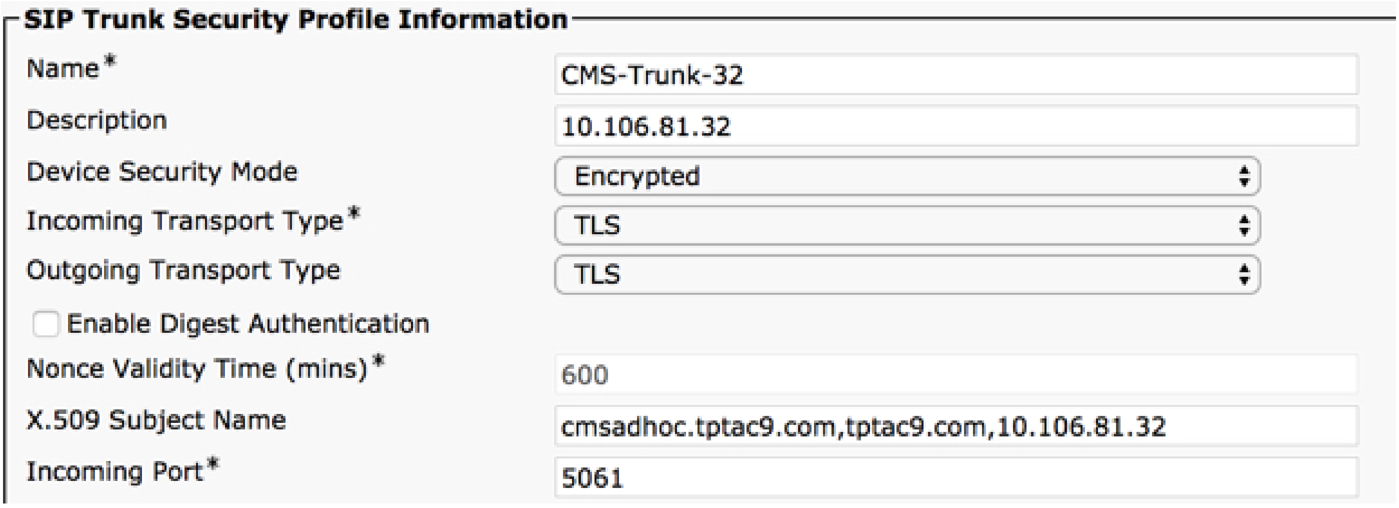
  Note: The CUCM SIP trunk can be created as a Non-Secure SIP trunk, if that is the case, it is not required to upload the Call Bridge certificate to the CallManager-trust store, but it is required to upload the Root certificate that signed the webadmin certificate to the CallManager-trust store.

Step 2. Configure a secure SIP trunk Profile.

- Open the CUCM web interface
- Navigate to **System > Security > SIP Trunk Security Profile**
- Select **Add New**
- Enter the values with the proper information

Name	Enter a name, for example CMS-Trunk-32
Device Security Mode	Select Encrypted
Incoming Transport Type	Select TLS
Outgoing Transport Type	Select TLS
X.509 Subject Name	Enter the CN of the Call Bridge certificate, separete names with comas
Incoming Port	Enter the port to receive TLS requests. The default is 5061

- Select **Save**



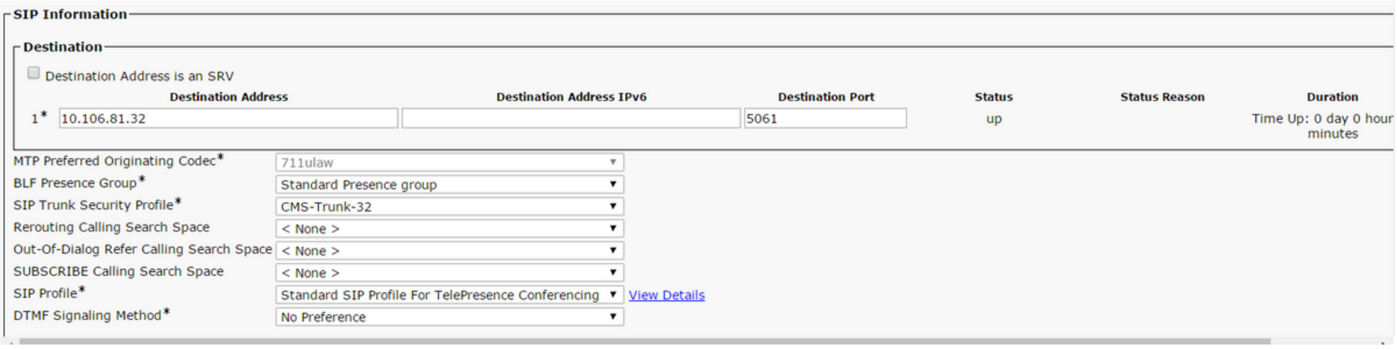
SIP Trunk Security Profile Information

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

Step 3. Create SIP trunk

- Navigate to **Device >Trunk**
- Select **Add New**
- Select **SIP Trunk** for the **Trunk Type**
- Select **Next**
- Enter the applicable values

Device Name	Enter a name for the SIP Trunk, for example **CMS-Abhishek-32**
Destination Address	Enter the CMS IP address or the Call Bridge FQDN, for example **10.106.81.3**
Destination Port	Enter the port where the CMS listens TLS communication, for example **5061**
SIP Trunk Security Profile	Select the Secure Profile created in the step 2, **CMS-Trunk-32**
SIP Profile	Select **Standard SIP Profile for TelePresence Conferencing**



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

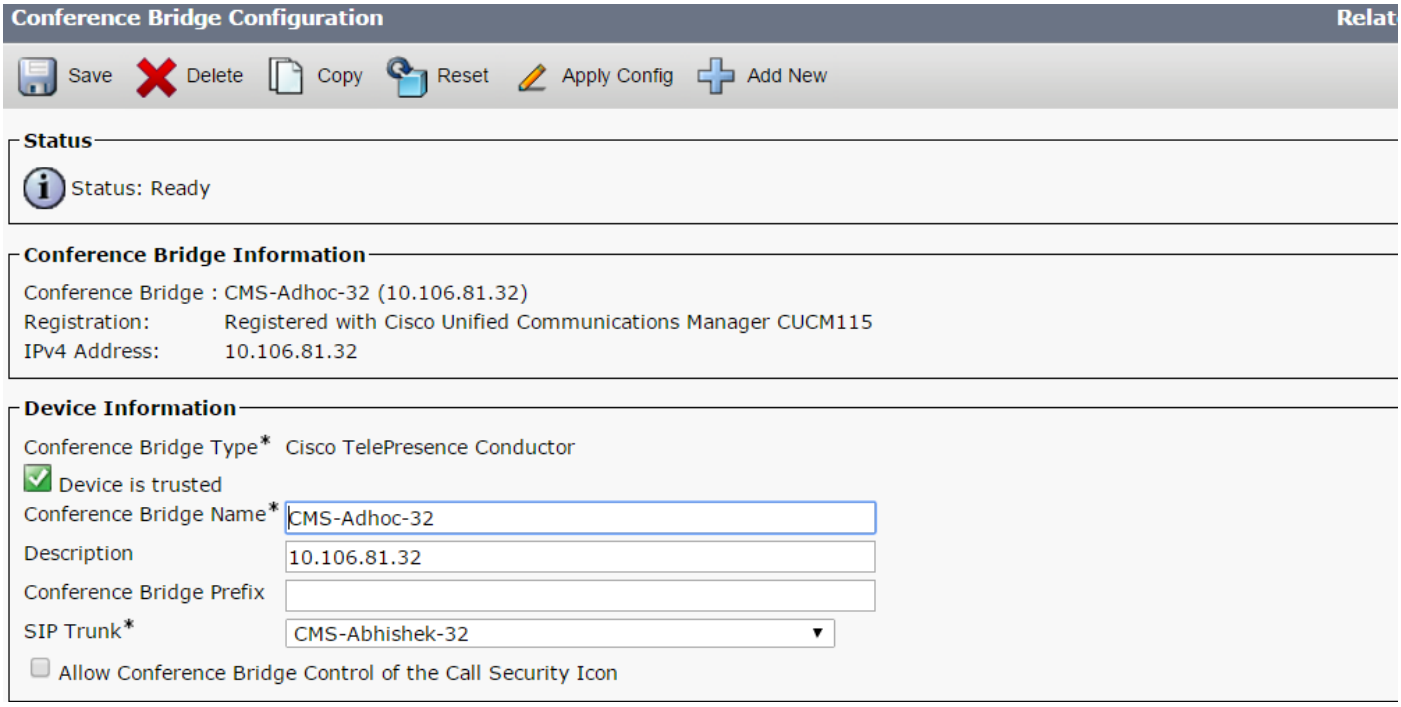
Step 4. Create the Conference Bridge

- Navigate to **Media Resources > Conference Bridge**
- Select Add New
- Select **Cisco TelePresence Conductor** from the **Conference Bridge** drop-down menu

Note: From CUCM version 11.5.1 SU3, the **Cisco Meeting Server** option is available to be selected as **Conference Bridge Type** in the drop-down menu

- Enter the proper information

Conference Bridge Name	Enter a name for this device, for example **CMS-Adhoc-32**
Description	Enter a description for this Conference Bridge, for exampl **10.106.81.32**
SIP Trunk	Select the SIP Trunk created in step 3, **CMS-Abhishek-32**
Override SIP Trunk Destination as HTTP Address	Check this box in case a different name is required
Hostname/IP Address	Enter the Hostname or IP address of the CMS, for exampl **10.106.81.32**
Username	Enter the user created in CMS with API privileges, for exa **admin**
Password	Enter the password of the API user
Confirm Password	Enter the password one more time
Use HTTPS	Check the box, this is required for CMS connection
HTTP Port	Enter the CMS webadmin port, for example **443**



Status

Status: Ready

Conference Bridge Information

Conference Bridge : CMS-Adhoc-32 (10.106.81.32)

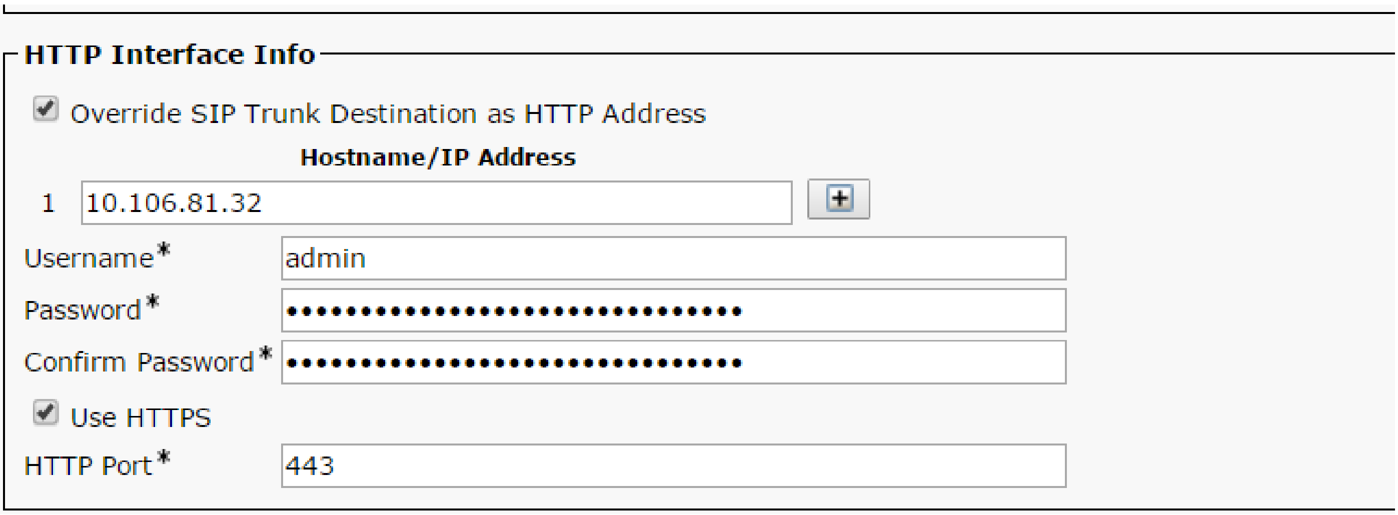
Registration: Registered with Cisco Unified Communications Manager CUCM115

IPv4 Address: 10.106.81.32

Device Information

Conference Bridge Type*	Cisco TelePresence Conductor
☑ Device is trusted	
Conference Bridge Name*	CMS-Adhoc-32
Description	10.106.81.32
Conference Bridge Prefix	
SIP Trunk*	CMS-Abhishek-32

☐ Allow Conference Bridge Control of the Call Security Icon



HTTP Interface Info

☑ Override SIP Trunk Destination as HTTP Address

Hostname/IP Address

1 10.106.81.32

Username*	admin
Password*	••••••••••••••••••••••••••••••••
Confirm Password*	••••••••••••••••••••••••••••••••

☑ Use HTTPS

HTTP Port*	443

- Select **Save**

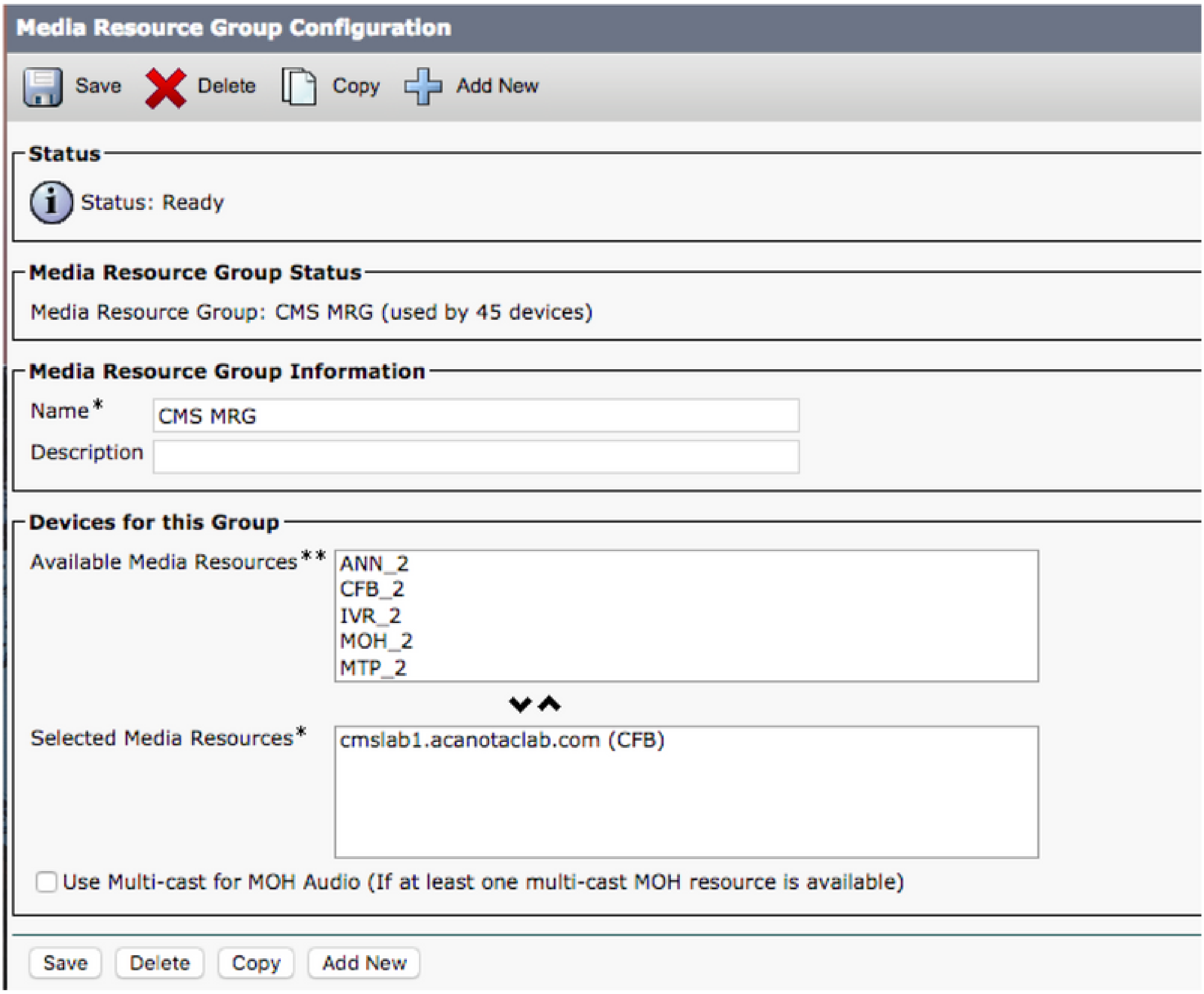
  Note: The **Hostname (FQDN of CMS) and/or IP address** field, must be included in the Webadmin certificate, in the **Common Name** or in the **Subject Alternative Name** field in order to allow secure connection

- After the Conference Bridge creation, open the **Cisco Unified Serviceability** section
- Navigate to **Tools > Control Center - Feature Services**
- From the drop-down menu, select the CUCM publisher node
- Select **Go**
- Select the **Cisco CallManager service**
- Select **Restart**

  Caution: When the CallManager service is restarted, the connected calls remain but some features are not available during this restart. No new calls are possible. The service restart takes around 5 to 10 minutes, depending on the CUCM workload. Perform this action with caution and ensure to do it during a maintenance window.

Step 5. CMS bridge is successfully registered to the CUCM

- Go to **Media Resources** > **Media Resource Group**
- Click **Add New** to create a new media resource group and enter a name
- Move the conference bridge (cms) in this case from the **Available Media Resources** box to **Selected Media Resources** box
- Click **Save**



Media Resource Group Configuration

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

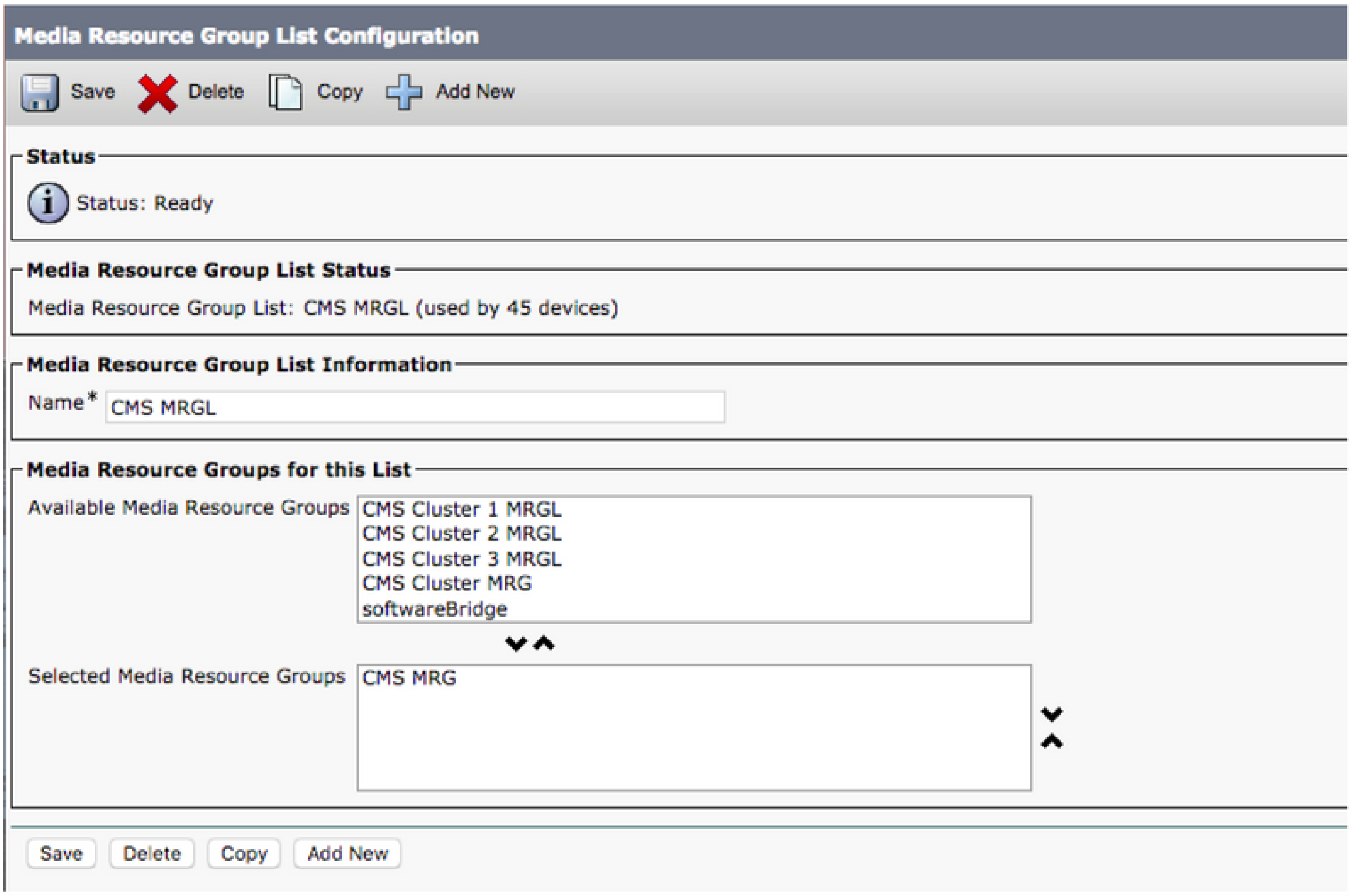
Available Media Resources** ANN_2
CFB_2
IVR_2
MOH_2
MTP_2

Selected Media Resources* cmslab1.acanotaclab.com (CFB)

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

Step 6. Add the Media Resource Groups (MRGs) to the Media Resource Group Lists (MRGLs)

- Go to **Media Resources** > **Media Resource Group List**
- Click **Add New** to create a new media resource group list and enter a name, or select an existing MRGL and click on it to edit it.
- Move one or more of the Media Resource Groups created from the **Available Media Resource Groups** box to the **Selected Media Resource Groups**
- Click **Save**



Media Resource Group List Configuration

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

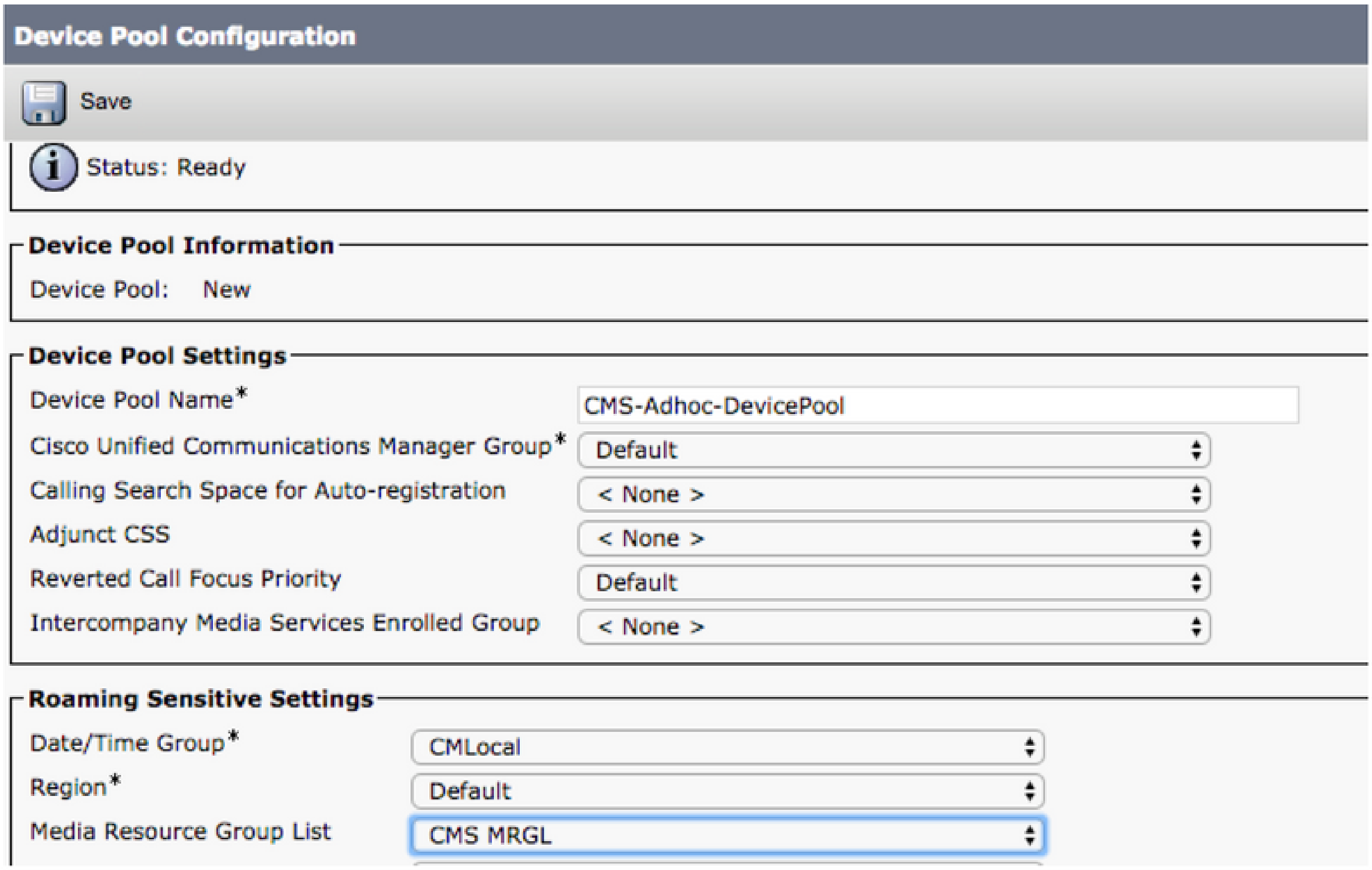
Available Media Resource Groups: CMS Cluster 1 MRGL, CMS Cluster 2 MRGL, CMS Cluster 3 MRGL, CMS Cluster MRG, softwareBridge

Selected Media Resource Groups: CMS MRG

Step 7: Add the MRGL to a Device Pool or Device

Depending on the implementation, either a device pool can be configured and applied to endpoints, or an individual device (an endpoint) can be assigned to a specific MRGL. **If an MRGL is applied to both Device pool and an endpoint, the endpoint settings will take precedence.**

- Go to **System** >> **Device Pool**
- Create a New Device Pool or used an existing device pool. Click **Add New**



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 >

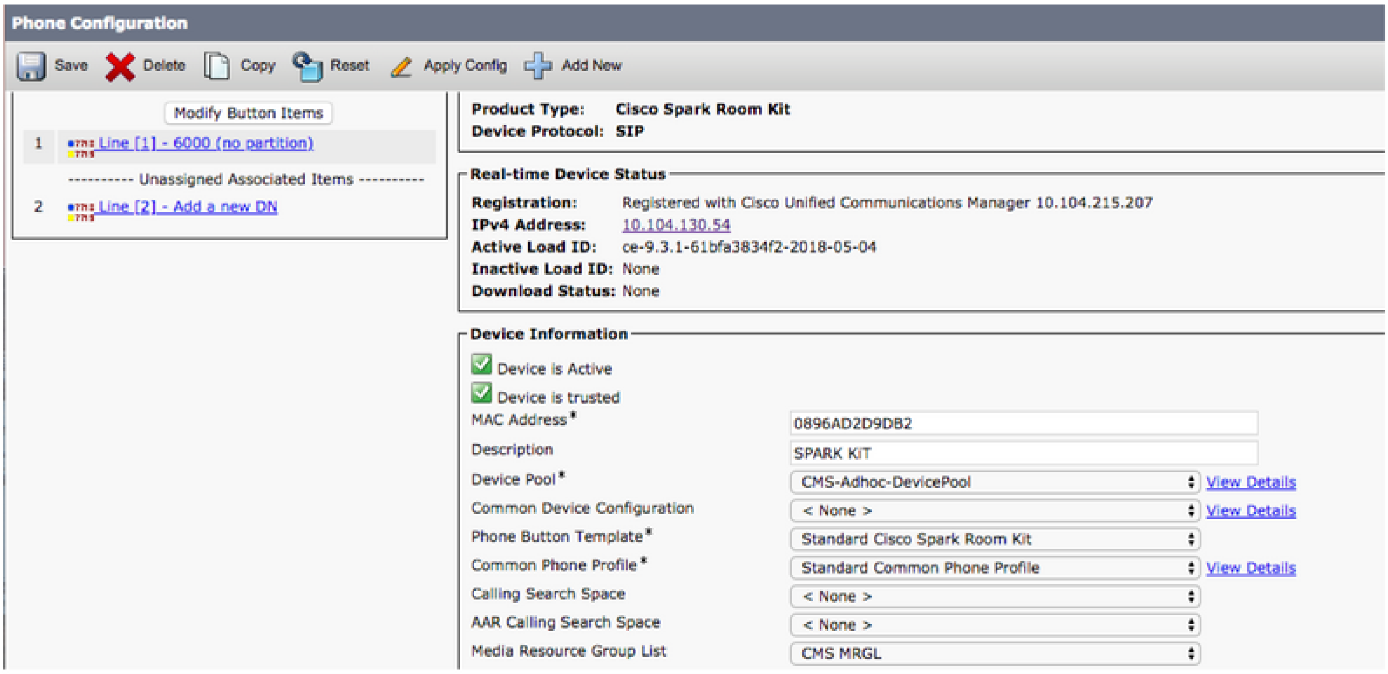
Roaming Sensitive Settings

Date/Time Group*	CMLocal
Region*	Default
Media Resource Group List	CMS MRGL

Step 8: To add Device pool to the endpoint and add MRGL to the endpoint

- Go to **Device**> **Phones**
- Click **Find** and select the device to change the Device Pool settings on
- Apply the created Device Pool and MRGL in above steps
- **Save**, **Apply Config and Reset**

Endpoint will reboot and Register



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

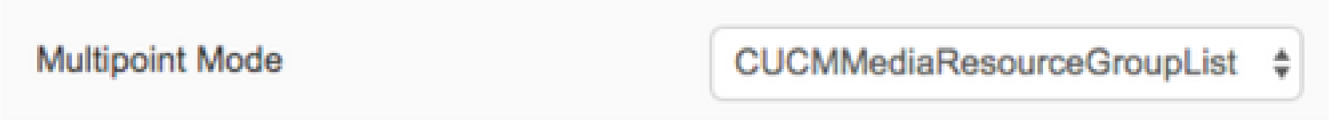
☑ Device is Active

☑ Device is trusted

MAC Address*	0896AD2D9DB2
Description	SPARK KIT
Device Pool*	CMS-Adhoc-DevicePool
Common Device Configuration	< None >
Phone Button Template*	Standard Cisco Spark Room Kit
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	CMS MRGL

Step 9: Configuration on an endpoint

- **Login** to **web-gui** of the endpoint
- Go to **Setup** > **Configuration > Conference > Multipoint Mode**
- Select **CUCMMediaResourceGroupList**



Multipoint Mode CUCMMediaResourceGroupList

Verify

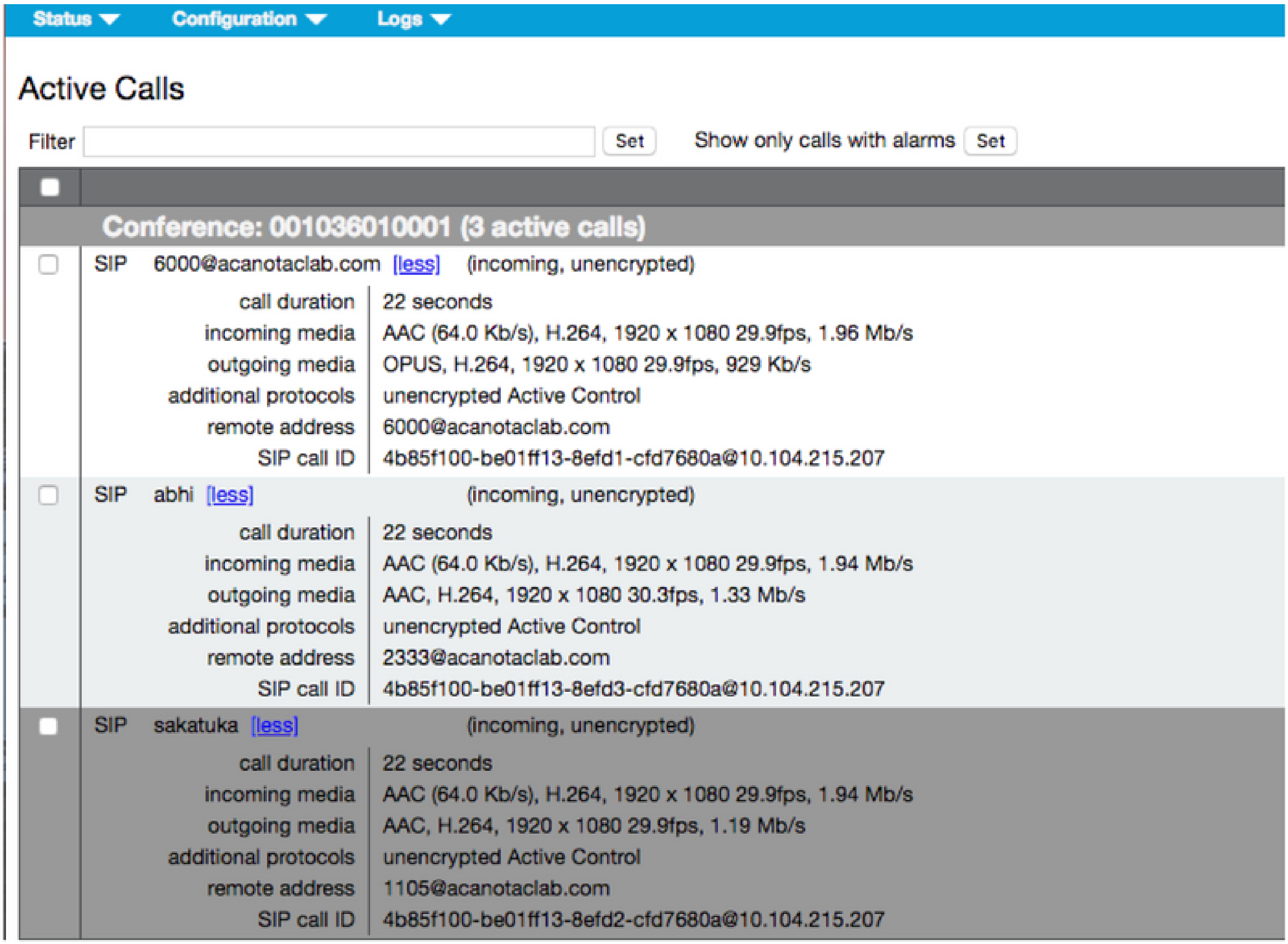
Use this section to confirm that your configuration works properly.

- Open the CUCM web interface
- Navigate to **Device > Trunks**
- Select the SIP Trunk that points to CMS
- Ensure the Trunks is in **Full Service** state
- Navigate to **Media Resource > Conference Bridge**
- Select the CMS conference bridge
- Ensure it is Registered with CUCM

Make an ad-hoc call

- Call from EndpointA registered to CUCM (MRGL added) to another EndpointB
- On EndpointA, Click **Add,** dial EndpointC
- EndpointA will go on hold
- Click **Merge**
- Validate the calls are connected in CMS
- Open the CMS web interface
- Navigate to **Status > Calls**

To test, 3 endpoints were used for ad-hoc audio/video conference



Active Calls

Filter

Show only calls with alarms

□

Conference: 001036010001 (3 active calls)

□ SIP 6000@acanotaclab.com [less] (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

□ SIP abhi [less] (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

□ SIP sakatuka [less] (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

There is currently no specific troubleshooting information available for this configuration.