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
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.

```
cbl> 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 Alternative 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
Add the Call Bridge certificate and bundle certificate (intermediate and root) to the CallManager-trust store.

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
  
<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name, for example CMS-Trunk-32</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Security Mode</td>
<td>Select Encrypted</td>
</tr>
<tr>
<td>Incoming Transport Type</td>
<td>Select TLS</td>
</tr>
<tr>
<td>Outgoing Transport Type</td>
<td>Select TLS</td>
</tr>
<tr>
<td>X.509 Subject Name</td>
<td>Enter the CN of the Call Bridge certificate, separete names with commas</td>
</tr>
<tr>
<td>Incoming Port</td>
<td>Enter the port to receive TLS requests. The default is 5061</td>
</tr>
</tbody>
</table>

**Select Save**

![SIP Trunk Security Profile Information](image)

**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
  
<table>
<thead>
<tr>
<th>Device Name</th>
<th>Enter a name for the SIP Trunk, for example <strong>CMS-Abhishek-32</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Address</td>
<td>Enter the CMS IP address or the Call Bridge FQDN, for example <strong>10.106.81.32</strong></td>
</tr>
<tr>
<td>Destination Port</td>
<td>Enter the port where the CMS listens TLS communication, for example <strong>5061</strong></td>
</tr>
<tr>
<td>SIP Trunk Security Profile</td>
<td>Select the Secure Profile created in the step 2, <strong>CMS-Trunk-32</strong></td>
</tr>
<tr>
<td>SIP Profile</td>
<td>Select <strong>Standard SIP Profile for TelePresence Conferencing</strong></td>
</tr>
</tbody>
</table>
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 example 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 example 10.106.81.32
  Username
  Enter the user created in CMS with API privileges, for example 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
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
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
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**
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

Step 9: Configuration on an endpoint
Login to web-gui of the endpoint
Go to Setup > Configuration > Conference > Multipoint Mode
Select 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
Troubleshoot

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