



Video Conferencing & Recording Using Cisco BE6000

Cisco Validated Design Guide

July 2017

© 2017 Cisco Systems, Inc. All rights reserved.





Contents

Preface	3
Scope	3
Proficiency	4
Comments and Questions	4
Disclaimer	4
Whats new in this version	4
Introduction	5
Technology Use Case	5
Use Case: Video Collaboration with Desktop and Multipurpose Room Systems	5
Design Overview	6
Cisco Preferred Architecture	6
Network Considerations	7
Solution Details	7
Cisco Unified Communications Manager	9
Cisco Video and TelePresence Endpoints	9
Cisco Meeting Server	9
Cisco TelePresence Management Suite	9
Dial Plan	10
Deployment Details	11
Installing Cisco Meeting Server	12
Installing TelePresence Management Suite	21
Configuring Cisco Meeting Server	33
Configuring Cisco TelePresence Management Suite	60
Configuring Cisco Unified Communications Manager	66
Configuring Endpoints	79
Initiating Conferences	81
Recording Conferences	87
Appendix A: Product List	88

Preface

Documentation for Cisco Validated Designs

The following types of documentation for Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs and ensure faster, more reliable, and fully predictable deployment:

[Cisco Preferred Architecture \(PA\) Design Overview](#) guides help customers and sales teams select the appropriate architecture based on an organization's business requirements, understand the products that are used within the architecture, and obtain general design best practices. These guides support sales processes.

[Cisco Validated Design \(CVD\)](#) guides provide detailed steps for deploying the Cisco Preferred Architectures. These guides support planning, design, and implementation of the Preferred Architectures.

[Cisco Collaboration Solution Reference Network Design \(SRND\)](#) guides provide detailed design options for Cisco Collaboration. The SRND should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

Related PA Guides

[Cisco Preferred Architecture for Midmarket Collaboration Design Overview](#)

[Cisco Preferred Architecture for Video Design Overview](#)

Related CVD Guides

[Unified Communications Using Cisco Business Edition 6000 CVD](#)

To view the related CVD guides, click the titles or visit the following site:
<http://www.cisco.com/go/cvd/collaboration>

Scope

Organizations want to reap the budgetary and productivity gains that a remote workforce allows, without compromising the benefits of face-to-face interaction. They need a solution that is fast to deploy and easy to manage from a central location, without replicating costly components at their remote sites.

This document details **Video Collaboration with Desktop and Multipurpose Room Systems**. It covers the following areas of technology and products:

- Video call agent
- Desktop video endpoints
- Multipurpose room systems
- Video Conference Bridge
- Video Conference Management Systems
- Video Conference Scheduling Systems



- Video Recording and Streaming
- Session Initiation Protocol (SIP) signaling

For more information, see the *Design Overview* section in this guide.

Proficiency

This guide is for people with technical proficiencies—or equivalent experience in CCNA Collaboration—1 to 3 years in designing, installing, and troubleshooting voice and unified communications applications, devices, and networks.

Comments and Questions

If you would like to comment on a guide or ask questions, please email collab-mm-cvd@external.cisco.com.

Disclaimer

The IP address scheme used in this document is for representational purposes only.

Whats new in this version

- Cisco Meeting Server as the Conferencing Bridge
- Cisco Meeting Server as the Recording Platform
- Cisco TelePresence Server and Cisco Conductor has been removed
- Cisco TelePresence Content Server has been removed



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

Introduction

Businesses around the world are struggling with escalating travel costs. Growing corporate expense accounts reflect the high price of travel, but travel also takes a toll on the health and well being of employees and their families. Often, the only way to solve a difficult problem is to fly an expert to the location to see the issue and discuss it with the people at the site. When an expert cannot see what is being described, the resolution of a complex problem often takes much longer.

Workers at remote sites often feel isolated from their departments because they do not spend enough face time with their peers and they feel disconnected from the decision-making process. This isolation can lead to lower job performance and less job satisfaction from employees who do not work at the organization's main location.

Hiring process can be very lengthy and costly, especially when candidates are located in other cities or when multiple people are involved in the interview process. Organizations with video conferencing systems in their offices can reduce expenses and time by bringing candidates into the nearest facility and allowing interviews to be conducted both in person and over video.

Technology Use Case

The face-to-face interaction during video collaboration meetings helps to boost information retention, promotes increased attention span, and reduces participant confusion. The nonverbal cues experienced in a visual meeting are sometimes more important than what is actually spoken.

Use Case: Video Collaboration with Desktop and Multipurpose Room Systems

Organizations want to reap the budgetary and productivity gains that a remote workforce allows—without compromising the benefits of face-to-face interaction. They want to allow the flexibility for an employee to work across remote sites while still maintaining the familiar in-person contact of their peers and managers. They also want to enrich the collaboration experience in their meeting rooms, boardrooms, auditoriums and other shared environments. A solution is needed that is fast to deploy and easy to manage from a central location without replicating costly components at their remote sites.

This design guide enables the following capabilities:

- Single cluster centralized design to simplify deployment and management while saving on infrastructure components.
- URI and numeric dialing to allow video-enabled IP phones to call room systems.
- Provisioning the videoconference bridge for the site.
- Conference resource optimization, management and scheduling.
- Instant, Personal and Scheduled Conferences on Cisco Meeting Server Spaces.
- Recording and Streaming of Conferences.

- Captures video and presentations for live streaming and video-on-demand (VoD) viewing.

Design Overview

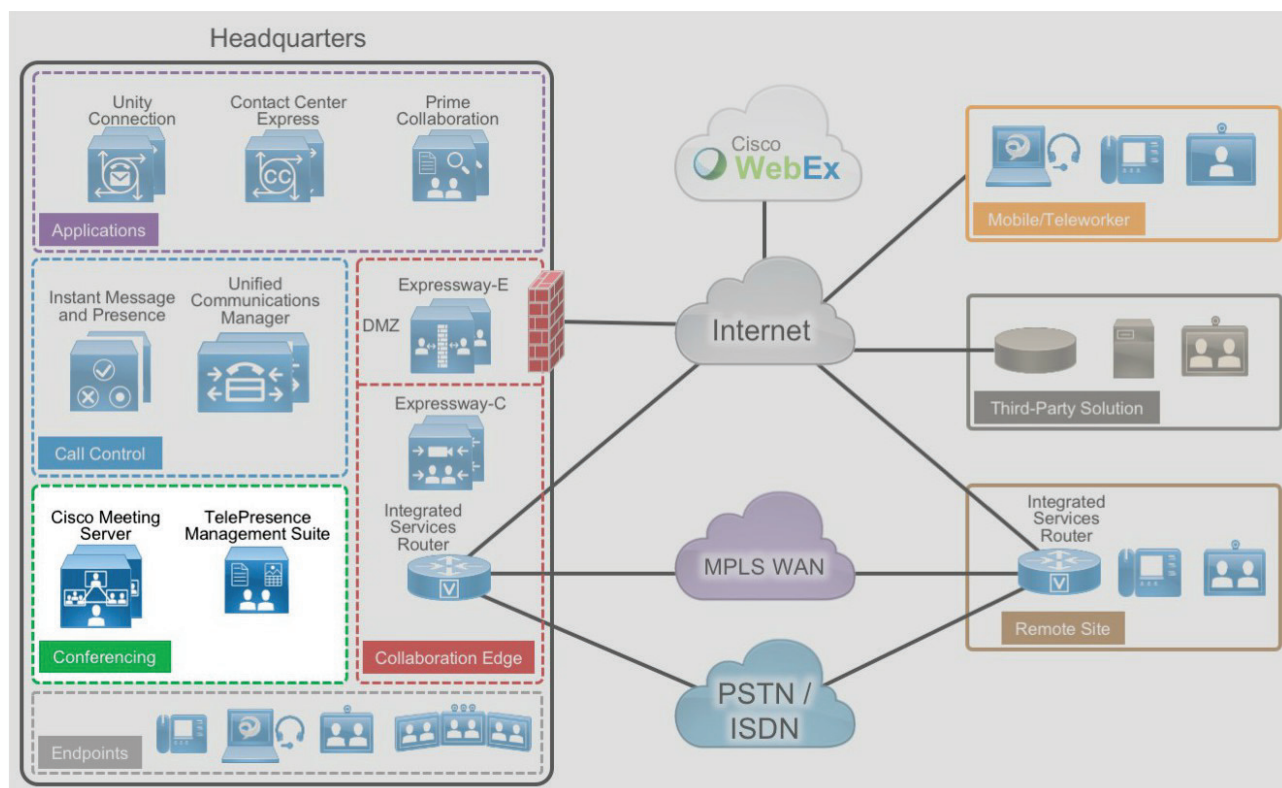
An end-to-end video-collaboration solution incorporates a full suite of endpoints, infrastructure components, and centralized management tools.

Cisco Preferred Architecture

Cisco Preferred Architectures provide recommended deployment models for specific market segments based on common use cases. They incorporate a subset of products from the Cisco Collaboration portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive, out-of-the-box, and built to scale with an organization as its business needs change. This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

The Cisco Preferred Architecture (PA) delivers capabilities that enable organizations to realize immediate gains in productivity and add value to their current voice deployments.

Figure 1. High-Level Block Diagram





Network Considerations

If you already have an IP network in place for voice, your natural next step is to deploy video over IP. Many organizations run video systems in a mixed environment as they move from older systems to newer ones, based on IP. As older systems migrate off of ISDN, significant quality improvements and cost savings will be seen.

Unified communications running over IP offers lower costs, easier management, remote monitoring, and control from across the network. It also provides higher bandwidth for calls, enabling superior audio and video quality while providing tighter integration into the corporate IT mainstream.

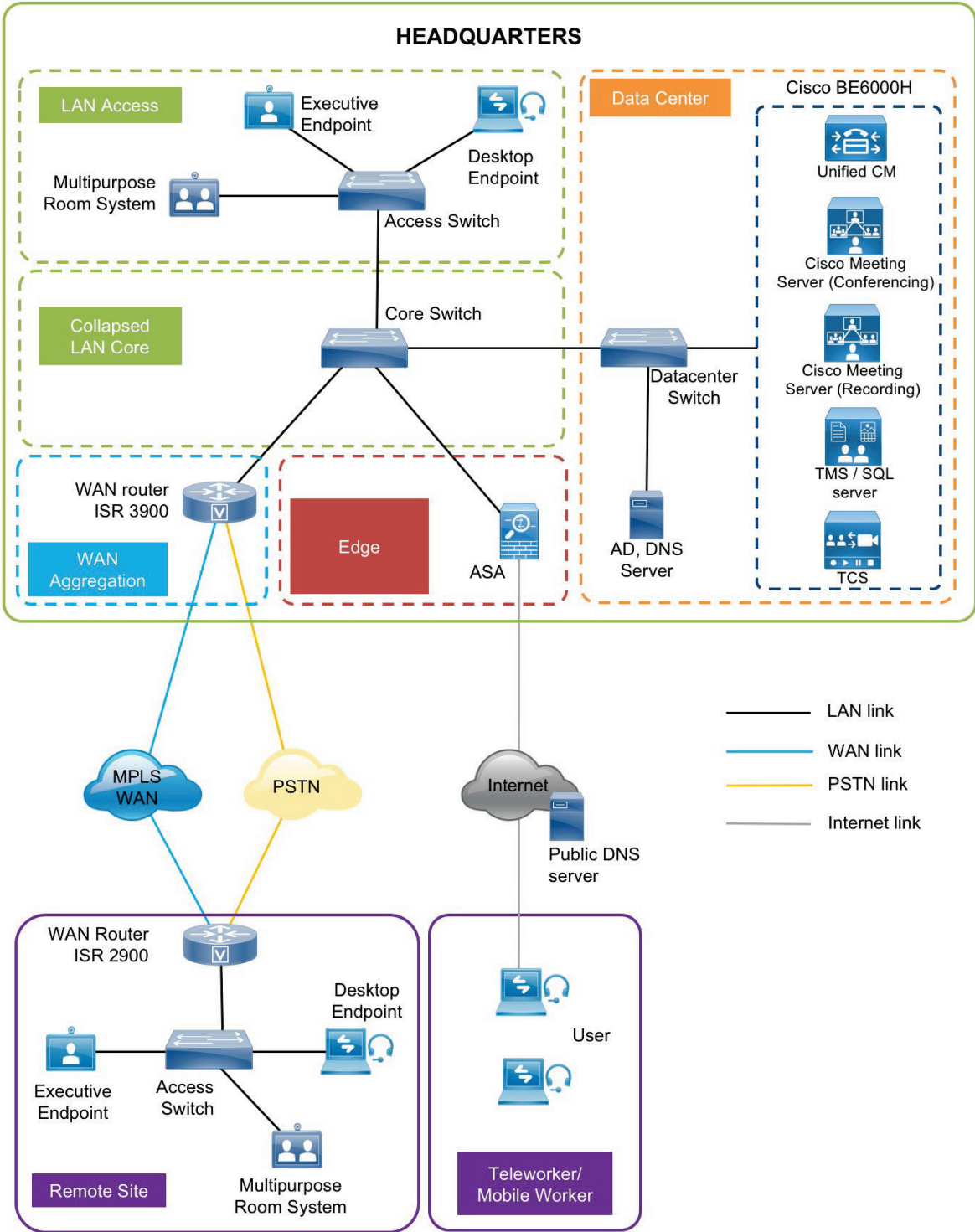
With an IP network, the ongoing costs of running video calls are minimal because you only have to pay for maintenance and technical support. When return on investment (ROI) for the initial deployment is met, any additional costs are essentially free. Because there is no incremental cost involved, employees and managers are more likely to use the technology. As usage goes up, payback times go down, further boosting the ROI.

Solution Details

The Video Conferencing CVD includes the following components:

- Cisco Unified Communications Manager (Unified CM), for call control and SIP endpoint registrations
- Desktop (Cisco 8800 series IP phones, Cisco Jabber and Cisco Desktop Collaboration Experience DX series) and multipurpose (Cisco TelePresence SX 10 and 20 Quick Set) systems for placing and receiving calls
- Cisco Meeting Server for reservation-less, instant conference (formerly ad-hoc conference), personal conference (formerly rendezvous/static conference)
- Cisco TelePresence Management Suite (TMS) for scheduled conference
- Cisco Meeting Server for conference recording
- Network Time Protocol (NTP) server for logging consistency

Figure 2. High-Level Network Diagram





Contents | Technology Use Case | Design Overview | Deployment Details | Product List

Cisco Unified Communications Manager

Unified CM serves as the software-based, call-processing component of Cisco Unified Communications. Additional data, voice, and video services, such as unified messaging, rich media conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified Communications Manager open-telephony application program interface (API).

Unified CM is the primary call agent in this CVD. Unified CM supports session initiation protocol (SIP), and the configurations in this document use SIP as the signaling protocol for endpoints.

Cisco Video and TelePresence Endpoints

Cisco video endpoints provide IP video telephony features and functions similar to IP voice telephony, enabling users to make point to point and multipoint video calls. Cisco video endpoints are classified into families based on the features they support, hardware screen size, and environments where the endpoints are deployed.

There are two types of endpoints mentioned in this document:

- **Desktop & Mobile Video endpoints**—Cisco Jabber software-based clients, such as Cisco Jabber for Windows/Mac/Android/IOS and the Cisco 8800 series IP phones are capable of transmitting video by means of the built-in front-facing camera. The Cisco TelePresence System DX70 and 80 endpoints take the personal desktop solution to the next level of experience with support for content sharing, mobile and remote access.
- **Multipurpose Endpoints**—The Cisco TelePresence SX10 and SX20 Quick Sets are flexible integrators that can turn any display into a powerful Cisco TelePresence system. SX20 Quick Sets are designed for HD video and multiparty conferencing, with the flexibility to accommodate various room sizes.

Cisco Meeting Server

The Cisco Meeting Server is an innovative software solution enabling high-quality standards-based conferencing for mobile, webRTC based clients, desktop and immersive endpoints. It can have instant, personal and scheduled conferences hosted on Spaces. It also enables Recording and streaming of the conferences. It is available in both appliance based offering and can also be installed on a specs based vmware hardware.

Spaces are always-on virtual spaces that have a fixed video address. Users can call in to that address at any time to start a meeting.

Cisco TelePresence Management Suite

Cisco TelePresence Management Suite (Cisco TMS) enables a variety of scheduling features and management functionality within Cisco Unified Communications for the Scheduled Conferences.



Dial Plan

This design uses, single-cluster, centralized call processing. The endpoints use a seven-digit phone number for dialing, which preserves the capability to receive calls from devices that only support only numeric dialing. The numbers are in the following pattern:

- **800xxxx**

For URI dialing the endpoints are assigned the URI in the following pattern:

- **800xxxx@mmcvd.ciscolabs.com**

The domain used in this document is **mmcvd.ciscolabs.com**.

As your solution grows, you may need to acquire a security certificate from a public certification authority. Choose a domain name in this step with a valid Internet domain suffix (.com, .edu etc) to ensure that your system is ready for this requirement.

For instant conferences, Cisco Meeting Server is added as a media resource on the Unified CM.

For personal Spaces, Cisco Meeting Server is SIP trunked to Unified CM. Personal Spaces can have both numbers and URIs. In this document, every user has a dedicated number and URI configured on the Cisco Meeting Server imported via Active Directory. The Space numbers and URIs used in the following pattern:

- **851xxxx**
- **<user>.space@mmcvd.ciscolabs.com** e.g. **abdey.space@mmcvd.ciscolabs.com**

For scheduled conferences, Cisco Meeting Server is SIP trunked to Unified CM. In this document, the same SIP trunk referenced above is used. Whenever a user schedules a conference; a number, from a configured range in TMS, is assigned to the scheduled conference for the users to dial in. The scheduled conference numbers are used in the following pattern:

- **821xxxx**

For recording, Cisco Meeting Server is SIP-trunked to Unified CM. User can press a number to start and stop a recording. In this document, the same SIP trunk referenced above is used. For self-video recording the user has to be the only participant in the space and record the space.



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

Deployment Details

This guide is divided into multiple sections: server installations and deploying Spaces. Each section has procedures and steps needed to configure the system from the ground up.

For customers who want to deploy both conferencing and recording in their environments, please follow all the procedures in all the process boxes.

For customers who want to deploy only conferencing without the recording capability, please skip the procedures labelled as (recording only).

For customers who want to deploy only recording without the conferencing capability, please follow the procedures labelled as (recording only).

For the installation of Cisco Unified Communications Manager (Unified CM), refer to the Installing the Cisco Unified CM process in the [Installation Guide for Cisco Business Edition 6000](#).

Easy Access Configuration Sheet

General Networking Parameters		
Element	CVD Configuration	Site-Specific Configuration
Domain name	mmcvd.ciscolabs.com	
DNS server	10.106.170.130	
NTP server	10.106.170.130	



Installing Cisco Meeting Server

Easy Access Configuration Sheet

Cisco Meeting Server Installation Requirements		
Element	CVD Configuration	Site-Specific Configuration
Cisco Meeting Server Name	cms1	
Cisco Meeting Server IP Address for Conferencing	10.106.170.214	
Cisco Meeting Server IP Address for Recording and Streaming	10.106.170.215	
Cisco Meeting Server Subnet Masks	255.255.255.128	
Cisco Meeting Server Default Gateway	10.106.170.129	

Cisco Meeting Server Configuration Requirements		
Element	CVD Configuration	Site-Specific Configuration
User for API access	apiadmin	

We would need two instances of Cisco Meeting Servers installed. One for Conferencing and the second for Recording and Streaming.

PROCESS

1. [Configure Cisco Business Edition 6000 Connectivity to LAN](#)
2. [Deploy OVA to Host for Conferencing](#)
3. [Deploy OVA to Host for Recording and Streaming](#)
4. [Configure the VM Guest for Conferencing](#)
5. [Configure the VM Guest for Recording](#)
6. [Apply Licenses on Cisco Meeting Server](#)

This process guides you through installing the Cisco Meeting Server.

Procedure 1

Configure Cisco Business Edition 6000 Connectivity to LAN

The Cisco Business Edition 6000 is connected to a switch in the data center.

- Step 1.** Using the user account that has the ability to make configuration changes, log in to the data center switch.

Step 2. If there is a previous configuration on the switch port where BE6000 is connected, bring the port back to its default state by issuing a no in front of each command.

Step 3. Configure the port as an access port.

```
interface GigabitEthernet1/14
description BE6000
switchport access vlan 20
switchport host
```

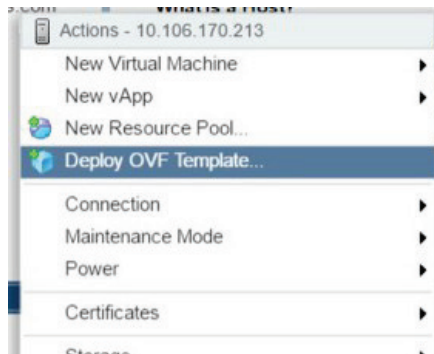
Procedure 2

Deploy OVA to Host for Conferencing

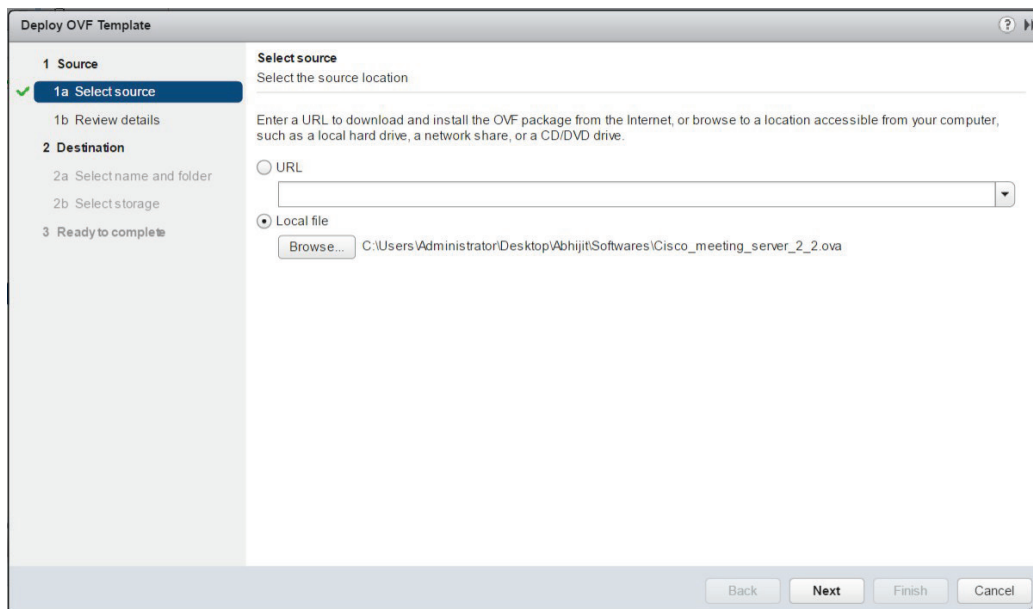
This procedure represents a typical installation. The Deploy OVF Template wizard dynamically changes to reflect host configuration, so your steps may vary.

Step 1. Log in to vSphere in order to access the ESXi Host.

Step 2. Select **File > Deploy OVF Template**.



Step 3. Click **Browse**, find the location of the ova file, click **Open**, and then click **Next**.



Step 4. On the OVF Template Details page, click **Next**.

Step 5. If an End User License Agreement page appears, read it, click **Accept**, then **Next**.

Step 6. On the Name and Location page, enter **cms1** and the Inventory Location where the virtual machine will reside.

Step 7. If the Host Cluster page appears, select the host or cluster you want to run the deployed virtual machine, and then click **Next**.

Step 8. If the Resource Pool page appears, select the resource pool with which you want to run the deployed virtual machine, and then click **Next**.

Step 9. If the Storage page appears, select the datastore onto which the Cisco Meeting Server Virtual Machine Guest will be deployed, and then click **Next**.

Step 10. On the Disk Format page, ensure that the default disk format of **Thick Provision Lazy Zeroed** is selected and then click **Next**.

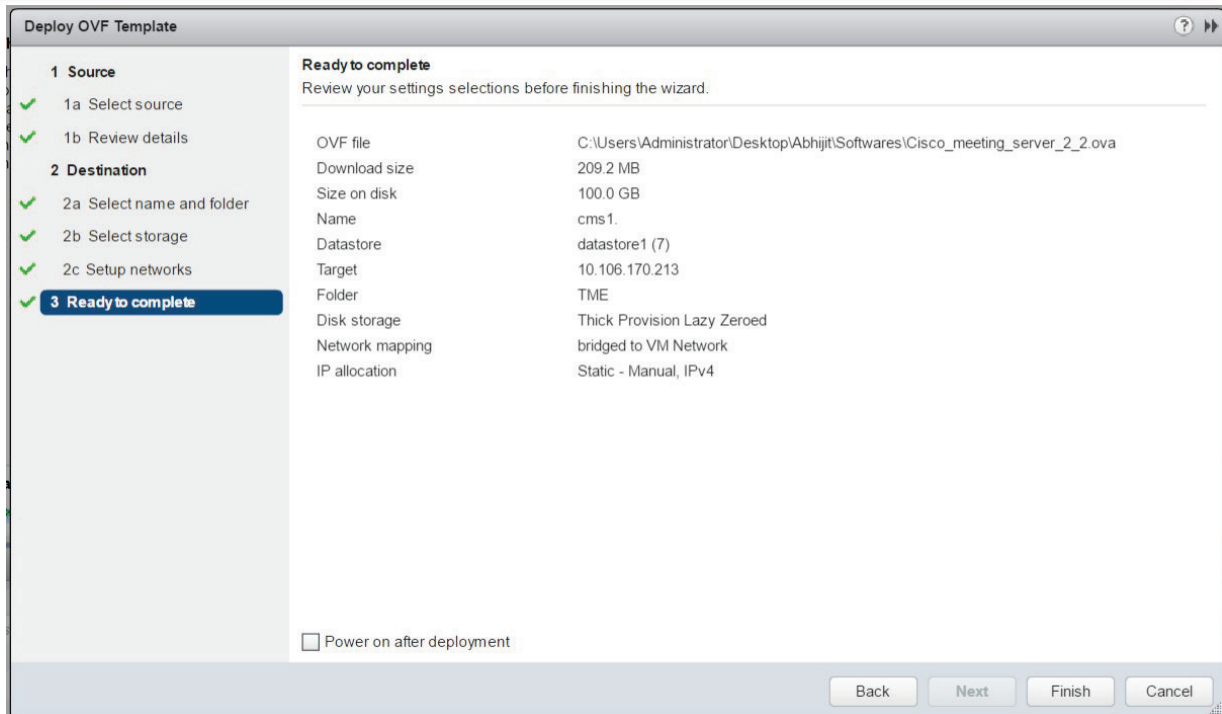
Name	Capacity	Provisioned	Free	Type	Storage DRS
datastore1 (7)	1.90 TB	223.07 GB	1.69 TB	VMFS	

i Tech Tip

Because VM performance may degrade during the resizing of a partition, Thin Provision is not recommended.

Step 11. If Network Mapping is listed, configure it and select the network mapping that applies to your infrastructure (the default is VM Network), and then click **Next**.

Step 12. On the Ready to Complete page, confirm your deployment Setting, do not select **Power on after deployment**, and click **Finish**.



Step 13. Right-click the **cms1** virtual machine and click **Edit Settings**.

Step 14. Set the **CPU** to **8**, **Memory** to **8 GB** and click **OK**.

cms1 - Edit Settings

Virtual Hardware | VM Options | SDRS Rules | vApp Options

- CPU: 8
- Memory: 8192 MB
- Hard disk 1: 100 GB
- SCSI controller 0: LSI Logic Parallel
- Network adapter 1: VM Network Connected
- Video card: Specify custom settings
- VMCI device
- Other Devices
- Upgrade: Schedule VM Compatibility Upgrade...

New device: ----- Select ----- Add

Compatibility: ESXi 5.0 and later (VM version 8) OK Cancel

Cisco Meeting Server OVA for Conferencing is now deployed as a guest on the VM Host.

Procedure 3

Deploy OVA to Host for Recording and Streaming

- Step 1.** Follow steps 1 - 5 from Procedure 2 above.
- Step 2.** On the Name and Location page, enter **cms2** and the Inventory Location where the virtual machine will reside.
- Step 3.** Follow steps 7 -12 from Procedure 2 above.
- Step 4.** Right-click the **cms1** virtual machine and select **Edit Settings**.
- Step 5.** Set the **CPU** to **4**, **Memory** to **4 GB** and click **ok**.



[Contents](#) | [Technology Use Case](#) | [Design Overview](#) | [Deployment Details](#) | [Product List](#)

Cisco Meeting Server OVA for Recording and Streaming is now deployed as a guest on the VM Host.

Procedure 4

Configure the VM Guest for Conferencing

- Step 1.** Right-click the VM guest and click **Power -> Power On**.
- Step 2.** Right-click the VM guest and click **Open Console**. The VM guest will take some time to boot. This is the Mainboard Management Processor (MMP) interface.
- Step 3.** When the Acano login prompt appears, log in with the following:
 - Username: **admin**
 - Password: **admin**.
- Step 1.** When the default password expires, create a new password and, The Cisco Meeting Server is now ready for initial configuration.
- Step 4.** At the acano: prompt, **Enter the following to configure a static IP address.**

```
ipv4 a add 10.106.170.214/25 10.106.170.129
```



```
#####
Cisco Systems Inc. Cisco Meeting Server (CMS)
#####

Welcome to the CMS VM
acano login: admin
Please enter password:
Password has expired
Please enter new password:
Please enter new password again:
Failed logins since last successful login 0
acano> ipv4 a add 10.106.170.214/25 10.106.170.129
Only interface enabled: setting gateway as default egress route
acano> ipv4 a
IPv4 configuration:
  address      10.106.170.214
  default      true
  dhcp         false
  enabled      true
  gateway      10.106.170.129
  macaddress   00:50:56:AE:66:F2
  prefixlen    25
IPv4 observed values
Addresses:
10.106.170.214/25
Routes:
  source      destination      gateway      global
  0.0.0.0     10.106.170.214  0.0.0.0     false
  0.0.0.0     10.106.170.128  0.0.0.0     false
  0.0.0.0     10.106.170.128  0.0.0.0     false
  0.0.0.0     10.106.170.255  0.0.0.0     false
  0.0.0.0     0.0.0.0         10.106.170.129  true
acano> _
```

Cisco Meeting Server for Conferencing is now accessible using the configured IP address.

Procedure 5

Configure the VM Guest for Recording

- Step 1.** Follow steps 1 - 3 from Procedure 4 above.
- Step 2.** At the acano: prompt, Enter the following to configure a static IP address.

```
ipv4 a add 10.106.170.215/25 10.106.170.129
```

Cisco Meeting Server for Recording can now be accessed using the configured IP address.



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

Procedure 6

Apply Licenses on the Cisco Meeting Server

For the scenarios covered in this CVD, the following types of licenses can be installed on the Cisco Meeting Server:

- Virtual Machine Activation key for both the servers
- CallBridge key
- Recording and Streaming key
- Personal Multiparty Plus License



Tech Tip

For additional licensing details, refer to the [Cisco Preferred Architecture for Midmarket Collaboration Design Overview](#).

The licenses are included in a single .lic file that must be uploaded to the CMS server.

Two cms.lic files are required. One is for Conferencing server and the other for the Recording and streaming server.

The server for Conferencing will have the activation key and CallBridge key.

The server for Recording and streaming will have activation key and Recording and Streaming key.

Configuration of the Personal Multiparty Plus Licenses is covered in the Configuring Cisco Meeting Server section of this document.

Step 1. If the name of the license file is not cms.lic, you must rename it to **cms.lic**.

Step 2. Transfer the license file to the default folder of Cisco Meeting Server using SFTP.

Step 3. After the file is uploaded, restart the servers.

The required licenses are applied.



Installing TelePresence Management Suite

Easy Access Configuration Sheet

Cisco TMS Installation Requirements		
Element	CVD Configuration	Site-Specific Configuration
TMS Name	TMS on Win Std 2012	
TMS IP Address	10.106.170.203	
TMS Subnet Mask	255.255.255.128	
TMS Default Gateway	10.106.170.129	
Release Key		
IP/ISDN zone name	HQ	
IP/ISDN zone country/region	India	

Cisco TMS Configuration Requirements		
Element	CVD Configuration	Site-Specific Configuration
DN range for scheduled conferences	8211000-8211010	

PROCESS

1. [Install Windows Server](#)
2. [Install TMS on the Windows Server](#)

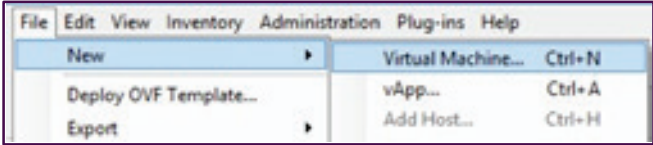
This CVD installs the TMS applications on Windows Server 2012 Standard 64-bit Edition with Microsoft SQL Server 2012 64-bit installed. TMS stores all its customer data in its SQL database.

<i>i</i>	Tech Tip
	The SQL Server can also be installed off-box for resiliency.

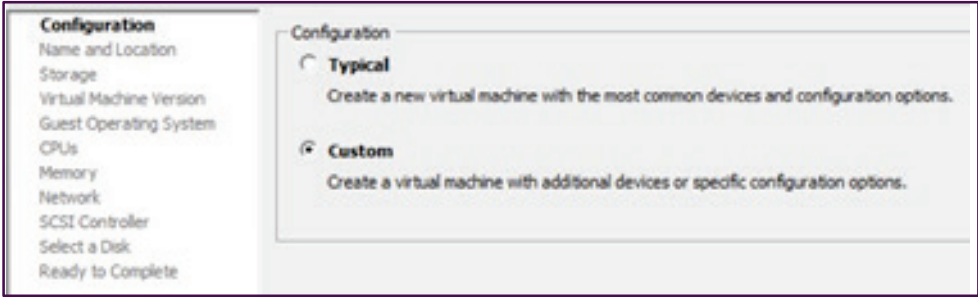
Procedure 1

Install Windows Server

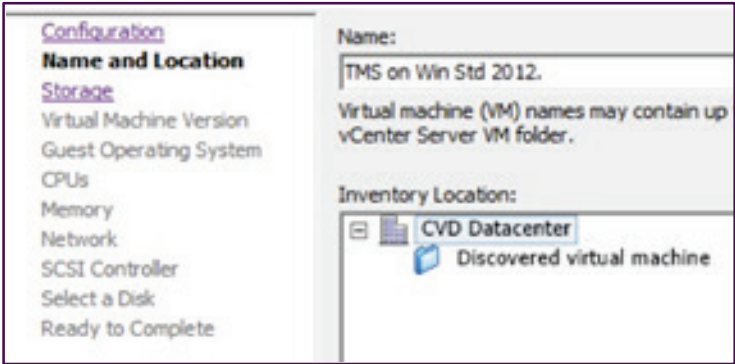
- Step 1.** Log in to vSphere to access the ESXi Host.
- Step 2.** Select **File > New > Virtual Machine**.



Step 3. On the Configuration page select **Custom**, and click **Next**.



Step 4. On the Name and Location page, enter **Name** as **TMS on Win Std 2012**, select Inventory Location and click **Next**.



Step 5. On the Storage page select the datastore and click **Next**.

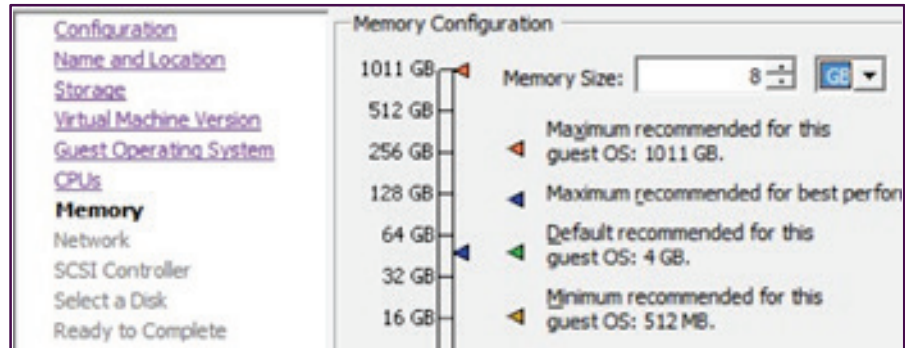
Step 6. On the Virtual Machine Version page, select **Virtual Machine Version: 8** and click **Next**.

Step 7. On the Guest Operating System page, select **Windows** under Guest Operating System, select **Microsoft Windows Server 2012 (64-bit)** and click **Next**.

Step 8. On the CPUs page, select the following and click **Next**:

- Number of Virtual sockets: 1
- Number of cores per virtual: 1

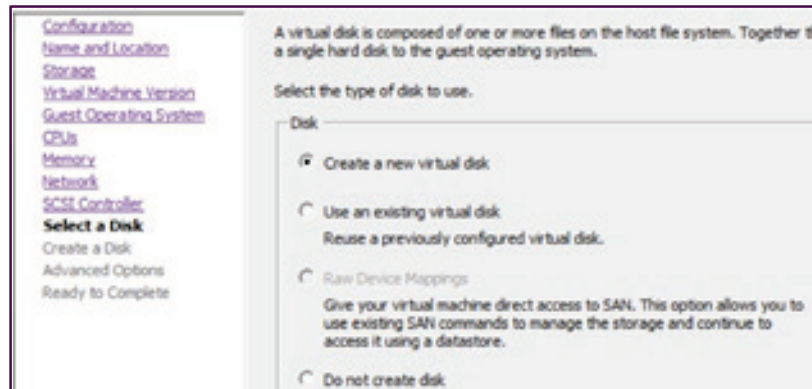
Step 9. On the Memory page, select Memory Size as **8 GB** and click **Next**.



Step 10. On the Network page, select the How many NICs do you want to connect as 1 and click **Next**.

Step 11. On the SCSI Controller page, select the appropriate settings and click **Next**.

Step 12. On the Select a disk page, select **Create a new virtual disk**, click **Next**.



Step 13. On the Create a Disk page, select Disk Size as **60 GB**, Disk Provisioning as **Thick Provision Lazy Zeroed** and click **Next**.

The screenshot shows the 'Create a Disk' configuration page. On the left, there is a navigation menu with links for Configuration, Name and Location, Storage, Virtual Machine Version, Guest Operating System, CPUs, Memory, Network, SCSI Controller, Select a Disk, Create a Disk, Advanced Options, and Ready to Complete. The 'Create a Disk' section is currently active. On the right, the 'Capacity' section shows 'Disk Size' set to '60 GB'. The 'Disk Provisioning' section has three radio button options: 'Thick Provision Lazy Zeroed' (selected), 'Thick Provision Eager Zeroed', and 'Thin Provision'. The 'Location' section has two radio button options: 'Store with the virtual machine' (selected) and 'Specify a datastore or datastore cluster:'.



Tech Tip

Because VM performance may degrade during the resizing of a partition, Thin provision is not recommended.

Step 14. On the Advanced Options page, select appropriate options and click **Next**.

Step 15. On the Ready to Complete page, confirm your deployment settings and click **Finish**.

Step 16. Once the VM is created, right-click the newly created VM, select **Power** and click **Power On**.

Step 17. Install Windows Server 2012 Standard on this newly created VM.

Step 18. To configure the IP information, enter the following in the relevant fields. (Configure other entries as required):

- o IP address: **10.106.170.203**
- o Subnet mask: **255.255.255.128**
- o Default gateway: **10.106.170.129**
- o DNS server: **10.106.170.130**

Step 19. Complete all critical Windows updates, close all open applications and disable virus-scanning and other software that may prevent an installation from completing.



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

i Tech Tip

Depending on windows components needing to be added, you may be prompted to reboot the server more than once during the installation. The installer automatically resumes after the server boots.

The Windows server is now installed.

Step 20. Install SQL Server 2012 on the Windows Server.

Procedure 2

Install TMS on the Windows Server

For the scenarios covered in this CVD, following are the type of licenses installed on the TMS:

- Cisco TelePresence Management Suite Base License
- Cisco TMS - additional 100 systems

i Tech Tip

For additional licensing details, refer the [Cisco Preferred Architecture for Midmarket Collaboration Design Overview](#).

Step 1. Download the Cisco TMS.zip file from Cisco.com.

Step 2. Extract the .zip file.

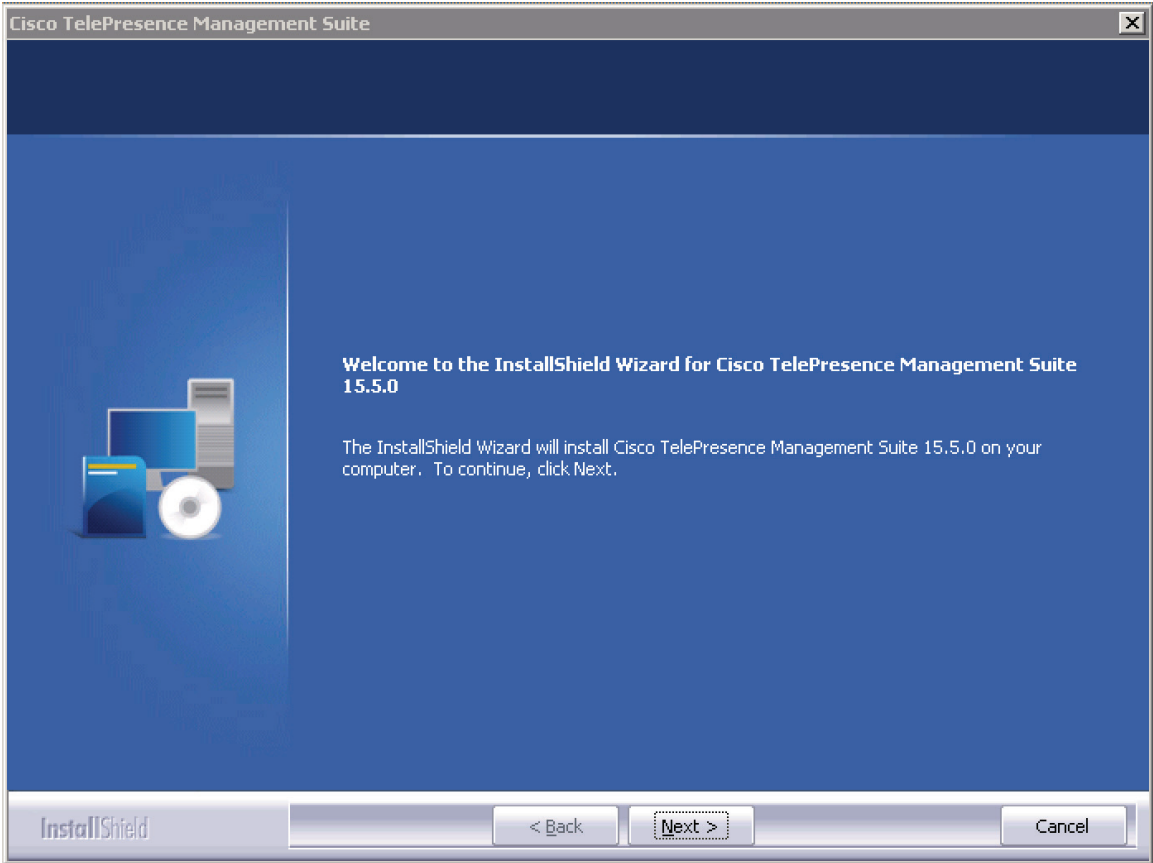
Step 3. Run the Cisco TMS executable as administrator.

The installer checks the hardware and software configuration of the server. A warning or error message may be displayed, depending on your server's configuration. Follow the prompts and install any missing Windows server components.

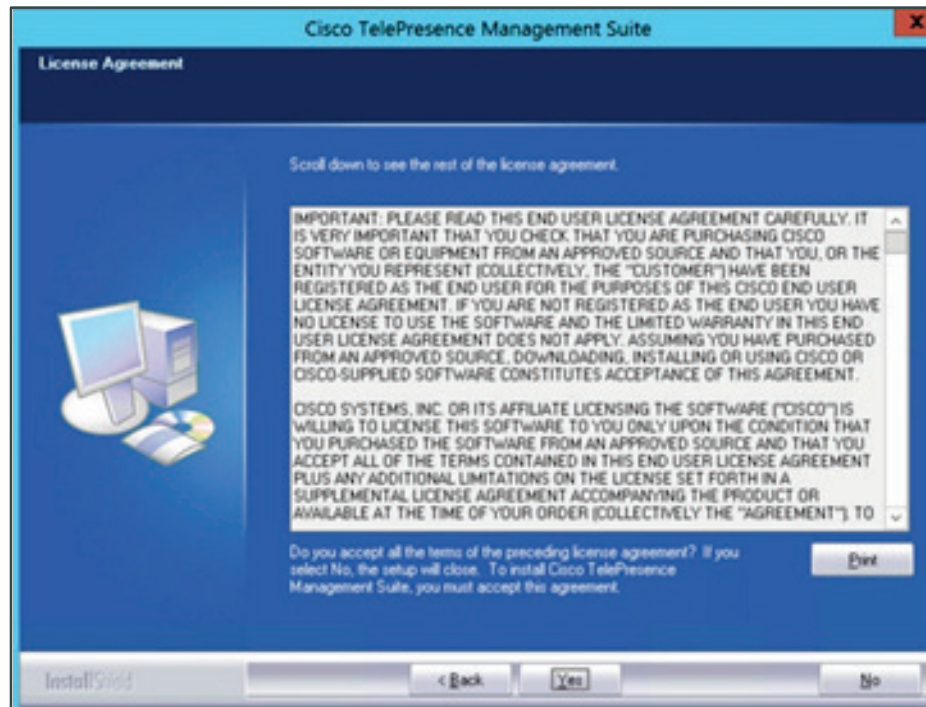
Step 4. Click **Yes** to continue.



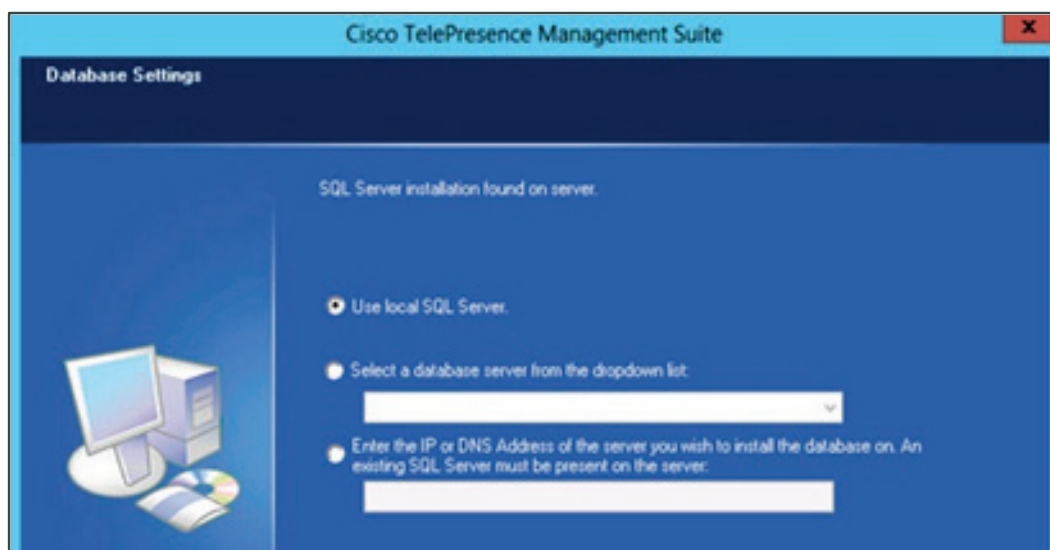
Step 5. On the welcome screen, click **Next**.



Step 6. On the License Agreement page, click **Yes**.



Step 7. On the Database Settings page, select **Use local SQL Server**, enter the username, password to allow the installer to create a new database, and click **Next**.



i Tech Tip

The SQL Server can also be installed off-box for resiliency.

Step 8. On the Release and Option Keys page, enter the release key and click **Next**.

Step 9. On the Network and Settings page, enter the following:

- TMS Server IPv4 Address: **10.106.170.203**
- IP Broadcast/Multicast Addresses for System Discovery: **10.106.170.255**

Cisco TelePresence Management Suite

Network Settings

Server Settings

TMS Server IPv4 Address: 10.106.170.203

TMS Server IPv6 Address:

IP Broadcast/Multicast Addresses for System Discovery: 10.106.170.255

Enable Automatic Registration of Systems in TMS:

E-mail Settings

Sender E-mail Address:

SMTP Server Address:

InstallShield

< Back Next > Cancel

Step 10. Click **Next**.

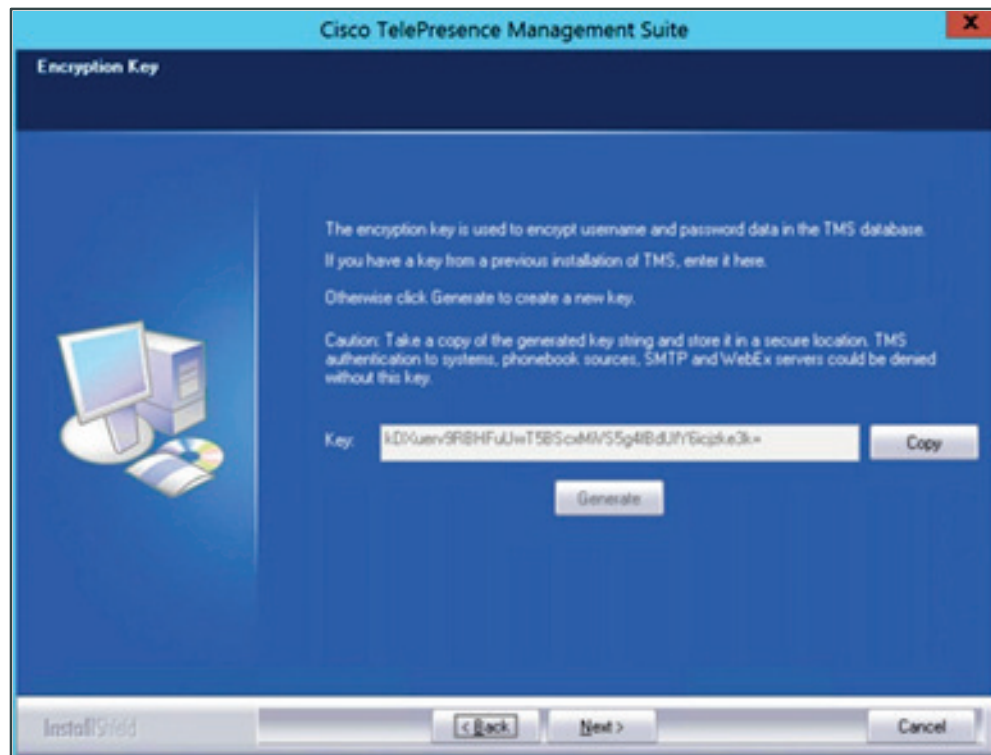
Step 11. On the IP/ISDN Zone page, enter the following:

- Name: **HQ**
- Country/Region: **India**

Step 12. Click **Next**.

Step 13. On the **Folder Settings** page, specify the TMS installation path and click **Next**.

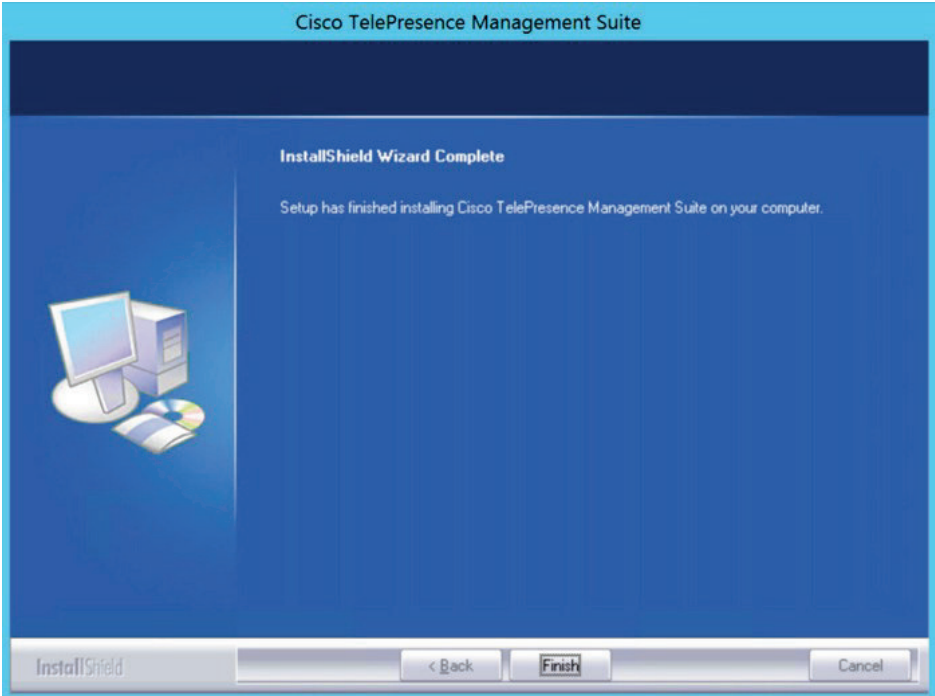
- Step 14.** On the **Encryption Key** page, click **Generate** to generate the new encryption key and click **Copy**.



- Step 15.** Click **Next**.
- Step 16.** On the **Start Copying Files** page, verify all the settings.
- Step 17.** Click **Next**.
- Step 18.** On the **HTTPS for the TMS Website** page, click **Create** to generate a self-signed certificate and click **OK**.



Step 19. Click **Finish**.



The setup wizard is complete and TMS is now installed.



Configuring Cisco Meeting Server

Easy Access Configuration Sheet

Cisco Meeting Server Configuration Requirements		
Element	CVD Configuration	Site-Specific Configuration
API username / password	api / Password	
WebAdmin Listening Port	445	
Recorder Listening Port	8443	
NFS Server IP	10.106.170.84	
XMPP Listening Port	8443	
LDAP Server	10.106.170.130	
LDAP Server Listening Port	389	

PROCESS

1. [Creating a new user for configuring through APIs](#)
2. [Enabling WebAdmin, CallBridge, Recorder, XMPP and WebBridge modules](#)
3. [Setting up CMS to be an ad-hoc resource in CUCCM](#)
4. [Setting up CMS for Personal Spaces](#)
5. [Setting up Personal Multiparty Plus Licenses](#)
6. [Setting up CMS for WebRTC](#)
7. [Setting up CMS for Recording](#)

Procedure 1

Creating a new user for configuring through APIs

A new user account has to be created for configuration throughout the API. This has to be done using the Mainboard Management Processor (MMP) interface in CMS which can be reached by doing SSH into the CMS server.

- Step 1.** SSH into the CMS server using the admin credentials.
- Step 2.** Enter the following command to create an API user named **api**:

```
user add api api
```
- Step 3.** Enter password as api twice when prompted to enter the password.
- Step 4.** Enter the command `user list` to confirm the creation of the user.

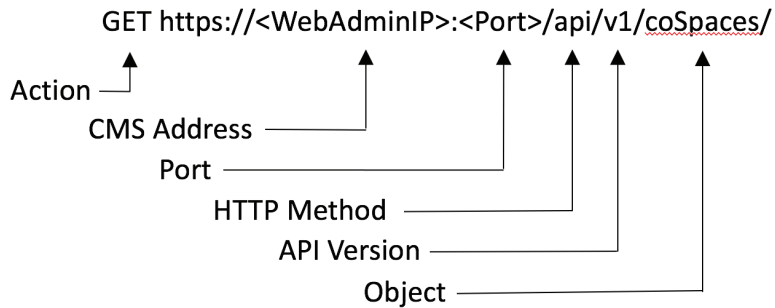
```
[acano>
[acano> user add api api
[Please enter new password:
[Please enter new password again:
Success
[acano>
[acano> user list
  USERNAME      ROLE          PASSWORD EXPIRY   LOGGED IN
  admin         admin         2017-Aug-02      yes
  apiadmin      api           2017-Aug-06      no
  adhocadmin    api           2017-Sep-13      no
  api           api           2017-Oct-24      no
[acano> _
```

A new user has been created. This CVD uses the Postman tool which is available as an extension for the Google Chrome browser.

The APIs Actions used to configure CMS are:

- GET - Retrieves existing information
- POST - Creates new instance
- PUT - Modifies existing instance
- DELETE - Deletes existing instance

API commands are entered as an URL in the following format:



Following steps would verify the newly created API user works on CMS.

- Step 5.** Open Google Chrome, and go to: <https://chrome.google.com/webstore/category/apps>.
- Step 6.** In the search bar, search for **Postman**.

Postman
 offered by www.getpostman.com
 ★★★★★ (7963) | [Developer Tools](#) | 3,490,099 users

OVERVIEW | REVIEWS | SUPPORT | RELATED G+1 2.6k

Collaborate with Cloud

Runs Offline
 Compatible with your device

Supercharge your API workflow with Postman! Build, test, and document your APIs faster. More than a million developers already do...

Supercharge your API workflow with Postman!

Build, test, and document your APIs faster. More than a million developers already do.

The idea for Postman arose while the founders were working together, and were

[Website](#)
[Report Abuse](#)

Additional Information
 Version: 4.10.5
 Updated: March 29, 2017
 Size: 5.7MiB
 Language: English

USERS OF THIS APP HAVE ALSO USED

Step 7. Install the Postman app and **restart** Chrome.

Step 8. Enter `chrome://apps/` and **Enter**.

Step 9. Click the Postman app installed above to open the application.

Step 10. Enter the following values to check if **GET** messages are working for CMS:

- Select **GET** from the dropdown list
- Enter `https://10.106.170.214:443/api/v1/system/status` in the **parameter** section,
- Select **Authorization** tab, select **Type** as **Basic Auth** and enter the **username** `api` and the **password**



https://10.106.170.214 × +

No Environment

GET https://10.106.170.214:443/api/v1/system/status Params Send Save

Authorization Headers (1) Body Pre-request Script Tests Code

Type Basic Auth Clear Update Request

Username api

Password ...

Save helper data to request

Show Password

The authorization header will be generated and added as a custom header

Step 11. Click **Send**.

Step 12. If you get the following error, then log in via the Chrome browser to the CMS Webadmin interface and accept the certificates.

Could not get any response

There was an error connecting to <https://10.106.170.214:443/api/v1/system/status>.

Why this might have happened:

- **The server couldn't send a response:** Ensure that the backend is working properly
- **SSL connections are being blocked:** Fix this by [importing SSL certificates in Chrome](#)
- **Cookies not being sent:** Use the Postman Interceptor extension
- **Request timeout:** Change request timeout in *Settings > General*

Step 13. After you can successfully log in to CMS server, sending the above GET message should give a similar output.

```

1 <?xml version="1.0"?>
2 <status>
3   <softwareVersion>2.2(Beta1)</softwareVersion>
4   <uptimeSeconds>1470906</uptimeSeconds>
5   <cdrTime>2017-04-24T02:43:35Z</cdrTime>
6   <activated>true</activated>
7   <clusterEnabled>false</clusterEnabled>
8   <cdrCorrelatorIndex>15</cdrCorrelatorIndex>
9   <callLegsActive>0</callLegsActive>
10  <callLegsMaxActive>4</callLegsMaxActive>
11  <callLegsCompleted>4</callLegsCompleted>
12  <audioBitRateOutgoing>0</audioBitRateOutgoing>
13  <audioBitRateIncoming>0</audioBitRateIncoming>
14  <videoBitRateOutgoing>0</videoBitRateOutgoing>
15  <videoBitRateIncoming>0</videoBitRateIncoming>
16 </status>

```

The created API user works fine.

Procedure 2

Enabling WebAdmin, CallBridge, Recorder, XMPP and WebBridge modules

WebAdmin is the module that enables https access to the CMS server for GUI configurations. WebAdmin is accessible only through https. Security certificates have to be created and installed on the CMS server for logging in.

- Step 1.** Log in to the MMP of CMS for conferencing using the admin account and enter the following command to create webadmin1.key and webadmin.csr files:
- Step 2.** Download the CSR file using a SFTP from the CMS server.
- Step 3.** Get the CSR file signed by a Certificate Authority(CA), get a signed certificate and upload the signed certificate file to the CMS server using SFTP.
- Step 4.** Enter the following commands to enable the WebAdmin module on CMS:

```

webadmin certs webadmin1.key webadmin1.crt
webadmin listen a 445
webadmin restart
webadmin enable

```

```
[acano> webadmin
Enabled                : true
TLS listening interface : a
TLS listening port     : 445
Key file               : webadmin1.key
Certificate file       : webadmin1.crt
HTTP redirect         : Enabled
STATUS                : webadmin running
[acano>
```

Now CMS can be accessed using <https://10.106.170.214:445/>.

CallBridge is the module that enables audio and video conferencing in CMS. Following steps enable the CallBridge module on CMS.

- Step 5.** Log in to the MMP of CMS for conferencing using the admin account and enter the following command to create callbridge.key and callbridge.csr files:

```
pki csr callbridge
```

- Step 6.** Download the CSR file using a SFTP from the CMS server.

- Step 7.** Get the CSR file signed by a Certificate Authority (CA), get a signed certificate and upload the signed certificate file to the CMS server using SFTP.

- Step 8.** Enter the following commands to enable the CallBridge module on CMS:

```
callbridge certs callbridge.key callbridge.crt
callbridge listen a
callbridge restart
```

```
[acano> callbridge
Listening interfaces  : a
Preferred interface  : none
Key file             : callbridge.key
Certificate file     : callbridge.crt
Address              : none
[acano>
```

CallBridge is now enabled.

Recorder is the module that enables the recording of conference spaces on the CMS server. Following steps enable recorder.

- Step 9.** Log in to the MMP of CMS for recording using the admin account and enter the following command to create cms2recorder.key and cms2recorder.csr files:

```
pki csr cms2recorder
```

- Step 10.** Download the CSR file using a SFTP from the CMS server.



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

Step 11. Get the CSR file signed by a Certificate Authority(CA), get a signed certificate and upload the signed certificate file to the CMS server using SFTP.

Step 12. Upload the callbridge signed certificate file to the CMS server using SFTP.

Step 13. Enter the following commands to enable the recorder module on CMS:

```
recorder certs cms2recorder.key cms2recorder.crt
recorder trust callbridge.crt
recorder listen a:8443
recorder nfs 10.106.170.84:/
recorder enable
```

```
[acano> recorder
Enabled                : true
Interface whitelist    : a:8443
Key file               : cms2recorder.key
Certificate file       : cms2recorder.crt
Trust bundle          : callbridge.crt
NFS domain name       : 10.106.170.84
NFS directory          : /
[acano>
```

Step 14. Issue the following API command on CMS for conferencing:

- Method - **POST**
- URL - **<https://10.106.170.214:445/api/v1/recorders>**

POST ▾	https://10.106.170.214:445/api/v1/recorders	Params	Send ▾
--------	---	--------	--------

Step 15. Check the created recorders instance on CMS for conferencing by issuing the following command:

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/recorders>**

GET ▾	https://10.106.170.214:445/api/v1/recorders	Params	Send ▾
-------	---	--------	--------

Contents | Technology Use Case | Design Overview | Deployment Details | Product List

```

1 <?xml version="1.0"?>
2 <recorders total="1">
3   <recorder id="f3dbe066-fa97-4f8c-8771-a3612895cf06">
4     <url></url>
5   </recorder>
6 </recorders>

```

Step 16. Add the recording URL on the CMS for conferencing by issuing the following API command:

- Method: PUT
- URL: <https://10.106.170.214:445/api/v1/recorders/f3dbe066-fa97-4f8c-8771-a3612895cf06>
- Key: url, Value: <https://10.106.170.215:8443>

The screenshot shows an API client interface with the following details:

- Method: PUT
- URL: <https://10.106.170.214:445/api/v1/recorders/f3dbe066-fa97-4f8c-8771-a3612895cf06>
- Params: (empty)
- Authorization: (empty)
- Headers: (3)
- Body: Selected, with format set to x-www-form-urlencoded
- Pre-request Script: (empty)
- Tests: (empty)
- Form-data: (unselected)
- raw: (unselected)
- binary: (unselected)
- Key-Value Table:

Key	Value
<input checked="" type="checkbox"/> url	https://10.106.170.215:8443

Step 17. Verify the configuration by using the following command:

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/recorders/f3dbe066-fa97-4f8c-8771-a3612895cf06>

The screenshot shows an API client interface with the following details:

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/recorders/f3dbe066-fa97-4f8c-8771-a3612895cf06>
- Params: (empty)
- Body: Selected, with format set to XML
- Cookies: (empty)
- Headers: (10)
- Tests: (empty)
- Status: 200 OK
- Response Body (XML):


```

1 <?xml version="1.0"?>
2 <recorder id="f3dbe066-fa97-4f8c-8771-a3612895cf06">
3   <url>https://10.106.170.215:8443</url>
4   <callBridge>ad112008-0f39-4d6d-b8b6-2b30530a0284</callBridge>
5 </recorder>

```

Step 18. Create a new callProfile to enable recording using the following command:

- Method: POST
- URL: <https://10.106.170.214:445/api/v1/callProfiles/>

The screenshot shows an API client interface with the following details:

- Method: POST
- URL: <https://10.106.170.214:445/api/v1/callProfiles/>
- Params: (empty)

Contents | Technology Use Case | Design Overview | Deployment Details | Product List

Step 19. Verify the configuration using the following command:

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/callProfiles/>**

GET ▼ | <https://10.106.170.214:445/api/v1/callProfiles> | Params | **Send** ▼

Body | Cookies | Headers (10) | Tests | Status: 200 OK

Pretty | Raw | Preview | XML ▼ |

```

1 <?xml version="1.0"?>
2 <callProfiles total="1">
3   <callProfile id="602eb7e1-4152-4737-8aec-81a4008d7985"></callProfile>
4 </callProfiles>

```

Step 20. Enable recording in the above created callProfile using the following command:

- Method: **PUT**
- URL: **<https://10.106.170.214:445/api/v1/callProfiles/602eb7e1-4152-4737-8aec-81a4008d7985>**
- Key: **recordingMode**, value: **manual**

PUT ▼ | <https://10.106.170.214:445/api/v1/callProfiles/602eb7e1-4152-4737-8aec-81a4008d7985> | Params | **Send** ▼

Authorization | Headers (3) | **Body** | Pre-request Script | Tests

form-data x-www-form-urlencoded raw binary

Key	Value
<input checked="" type="checkbox"/> recordingMode	manual

Step 21. Create a callLegProfile to enable recording control for every user by using the following commands:

- Method: **POST**
- URL: **<https://10.106.170.214:445/api/v1/callLegProfiles/>**

POST ▼ | <https://10.106.170.214:445/api/v1/callLegProfiles> | Params | **Send** ▼

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/callLegProfiles/>**

Contents | Technology Use Case | Design Overview | Deployment Details | Product List

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

```

1 <?xml version="1.0"?>
2 <callLegProfiles total="1">
3   <callLegProfile id="6735d228-7cde-4298-ad6a-452068b8337e"></callLegProfile>
4 </callLegProfiles>

```

- Method: PUT
- URL: <https://10.106.170.214:445/api/v1/callLegProfiles/6735d228-7cde-4298-ad6a-452068b8337e>
- Key: **recordingControlAllowed**, Value: **true**

PUT Params

Authorization Headers (3) Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

Key	Value
<input checked="" type="checkbox"/> recordingControlAllowed	true

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/callLegProfiles/6735d228-7cde-4298-ad6a-452068b8337e>

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

```

1 <?xml version="1.0"?>
2 <callLegProfile id="6735d228-7cde-4298-ad6a-452068b8337e">
3   <recordingControlAllowed>true</recordingControlAllowed>
4 </callLegProfile>

```

Step 22. Create the **dtmfProfile** to map the DTMF tones to start and stop the recording by using the following commands:

- Method: POST
- URL: <https://10.106.170.214:445/api/v1/dtmfProfiles>

POST Params



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/dtmfProfiles>

GET ▼ <https://10.106.170.214:445/api/v1/dtmfProfiles> Params Send ▼

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML ▼ ↻

```

1 <?xml version="1.0"?>
2 <dtmfProfiles total="1">
3   <dtmfProfile id="0e613fff-3f31-4996-aff5-aef12449da08"></dtmfProfile>
4 </dtmfProfiles>

```

- Method: PUT
- URL: <https://10.106.170.214:445/api/v1/dtmfProfiles/0e613fff-3f31-4996-aff5-aef12449da08>
- Key: **startRecording**, Value: *7
- Key: **stopRecording**, Value: *8

PUT ▼ <https://10.106.170.214:445/api/v1/dtmfProfiles/0e613fff-3f31-4996-aff5-aef12449da08> Params Send ▼

Authorization Headers (3) Body ● Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

Key	Value
<input checked="" type="checkbox"/> startRecording	*7
<input checked="" type="checkbox"/> stopRecording	*8

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/dtmfProfiles/0e613fff-3f31-4996-aff5-aef12449da08>

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

```

1 <?xml version="1.0"?>
2 <dtmfProfile id="0e613fff-3f31-4996-aff5-ae12449da08">
3   <muteSelfAudio></muteSelfAudio>
4   <unmuteSelfAudio></unmuteSelfAudio>
5   <toggleMuteSelfAudio></toggleMuteSelfAudio>
6   <lockCall></lockCall>
7   <unlockCall></unlockCall>
8   <muteAllExceptSelfAudio></muteAllExceptSelfAudio>
9   <unmuteAllExceptSelfAudio></unmuteAllExceptSelfAudio>
10  <endCall></endCall>
11  <nextLayout>2</nextLayout>
12  <previousLayout></previousLayout>
13  <startRecording>*7</startRecording>
14  <stopRecording>*8</stopRecording>
15  <startStreaming></startStreaming>
16  <stopStreaming></stopStreaming>
17  <allowAllMuteSelf></allowAllMuteSelf>
18  <cancelAllowAllMuteSelf></cancelAllowAllMuteSelf>
19  <allowAllPresentationContribution></allowAllPresentationContribution>
20  <cancelAllowAllPresentationContribution></cancelAllowAllPresentationContribution>
21  <muteAllNewAudio></muteAllNewAudio>
22  <unmuteAllNewAudio></unmuteAllNewAudio>
23  <defaultMuteAllNewAudio></defaultMuteAllNewAudio>
24  <muteAllNewAndAllExceptSelfAudio></muteAllNewAndAllExceptSelfAudio>
25  <unmuteAllNewAndAllExceptSelfAudio></unmuteAllNewAndAllExceptSelfAudio>
26 </dtmfProfile>

```

Step 23. Apply the above created `callProfile`, `callLegProfile` and `dtmfProfile` to the system default profile by following the commands:

- Method: PUT
- URL: <https://10.106.170.214:445/api/v1/system/profiles>
- Key: `callLegProfile`, Value - `6735d228-7cde-4298-ad6a-452068b8337e`
- Key: `callProfile`, Value - `602eb7e1-4152-4737-8aec-81a4008d7985`
- Key: `dtmfProfile`, Value - `0e613fff-3f31-4996-aff5-ae12449da08`

PUT Params

Authorization Headers (3) Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

Key	Value
<input checked="" type="checkbox"/> callLegProfile	6735d228-7cde-4298-ad6a-452068b8337e
<input checked="" type="checkbox"/> callProfile	602eb7e1-4152-4737-8aec-81a4008d7985
<input checked="" type="checkbox"/> dtmfProfile	0e613fff-3f31-4996-aff5-ae12449da08

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/system/profiles>



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

```

1 <?xml version="1.0"?>
2 <profiles>
3   <callLegProfile>6735d228-7cde-4298-ad6a-452068b8337e</callLegProfile>
4   <callProfile>602eb7e1-4152-4737-8aec-81a4008d7985</callProfile>
5   <dtmfProfile>0e613fff-3f31-4996-aff5-aef12449da08</dtmfProfile>
6 </profiles>

```

The Recorder is configured but would need the XMPP module to be enabled too.

XMPP server is needed for recording and for participants joining spaces through CMA or webRTC based browsers. Following steps enables XMPP server on CMS for conferencing.

- Step 24.** Create DNS A record for `cms1.mmcvd.ciscolabs.com` as this server will be used to host the XMPP Server and set it to the IP address `10.106.170.214` which is the interface that the XMPP server is listening on.
- Step 25.** Create DNS SRV record for `_xmpp-server` for tcp port `5269` resolving to the DNS A record `cms1.mmcvd.ciscolabs.com`.
- Step 26.** Create DNS SRV record for `_xmpp-client` for tcp port `5222` resolving to the DNS A record `cms1.mmcvd.ciscolabs.com`.
- Step 27.** SSH into the CMS for conferencing and enter the following commands to enable the XMPP module:

```

xmpp listen a:8443
xmpp certs callbridge.key callbridge.crt
xmpp domain mmcvd.ciscolabs.com
xmpp enable

```

```

[acano> xmpp
Enabled           : true
Clustered        : false
Domain           : mmcvd.ciscolabs.com
Listening interfaces : a
Key file         : callbridge.key
Certificate file  : callbridge.crt
Max sessions per user : unlimited
STATUS          : XMPP server running
[acano>

```

XMPP server is enabled.



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

WebBridge is being used by the WebRTC app. The users or guests who want to join a conference can use a WebRTC-supported web browser to join the conference. The following steps enable WebRTC on the CMS for conferencing.

Step 28. SSH into the CMS for conferencing, create a key and csr file using the following command:

```
pkc csr webbridg1
```

Step 29. Get the csr signed by a CA server, then upload the crt file back on the server:

Step 30. SSH in to the CMS for conferencing server, and enter the following commands:

```
webbridge listen a:443
webbridge certs webbridg1.key webbridg1.crt
webbridge trust callbridge.crt
webbridge enable
```

```
[acano> webbridge
Enabled                : true
Interface whitelist    : a:443
Key file               : webbridg1.key
Certificate file       : webbridg1.crt
Trust bundle          : callbridge.crt
HTTP redirect         : Disabled
Clickonce URL         : none
MSI download URL      : none
DMG download URL      : none
iOS download URL      : none
[acano>
```

Step 31. Create a DNS A record for the WebBridge and set it to resolve to the IP address:
10.106.170.214.

The WebBridge is now enabled.

Procedure 3

Setting up CMS to be an ad-hoc resource in CUCM

Step 1. Log in to the GUI of CMS for conferencing, navigate to **Configuration > Incoming Calls**, under Call Matching section enter the following and hit Add New:

- Domain name: **10.106.170.214**
- Priority: **1**
- Targets Spaces: **Yes**
- Targets users: **Yes**
- Targets IVRs: **Yes**
- Targets Lync: **No**



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

- Targets Lync Siplejoin: **No**

10.106.170.214	1	yes	yes	yes	no	no	Add New	Reset
----------------	---	-----	-----	-----	----	----	---------	-------

Step 2. Log in to the GUI of CMS for conferencing, navigate to **Configuration > Incoming Calls**, under Call Matching section enter the following and hit Add New:

- Domain name: **mmcvd.ciscolabs.com**
- Priority: **1**
- Targets Spaces: **Yes**
- Targets users: **Yes**
- Targets IVRs: **Yes**
- Targets Lync : **No**
- Targets Lync Siplejoin: **No**

mmcvd.ciscolabs.com	2	yes	yes	yes	no	no	Add New	Reset
---------------------	---	-----	-----	-----	----	----	---------	-------

Procedure 4

Setting up CMS for Personal Spaces

For Personal Spaces for users in the Active Directory will be automatically created when we import the users in Cisco Meeting Server. This section configures the LDAP related settings and imports users from the AD.

In this CVD a separate Organizational Unit called `cmaUsers` have been created with users who can log in to the CMA application or via webRTC supported browsers.

Step 1. Create a **ldapServer** by issuing the following API command on CMS for conferencing through Postman:

- Method: **POST**
- URL: **https://10.106.170.214:445/api/v1/ldapServers**
- Key: **address**, Value - **10.106.170.130**
- Key: **PortNumber**, Value: **389**
- Key: **username**, Value: **cn=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com**
- Key: **password**, Value: **Password**
- Key: **secure**, Value: **false**



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

POST	https://10.106.170.214:445/api/v1/ldapServers	Params	Send
<input checked="" type="checkbox"/>	address	10.106.170.130	
<input checked="" type="checkbox"/>	username	cn=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com	
<input checked="" type="checkbox"/>	portNumber	389	
<input checked="" type="checkbox"/>	password	*****	
<input checked="" type="checkbox"/>	secure	false	
	New key	value	

Step 2. Check the created instance of ldapServer by issuing the following command:

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/ldapServers>

GET	https://10.106.170.214:445/api/v1/ldapServers	Params	Send
<p>Body Cookies Headers (10) Tests Status: 200 OK</p> <p>Pretty Raw Preview XML</p> <pre> 1 <?xml version="1.0"?> 2 <ldapServers total="1"> 3 <ldapServer id="dc639ccb-c9bd-4183-848a-7fc893e0d8e4"> 4 <address>10.106.170.130</address> 5 <username>cn=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com</username> 6 <portNumber>389</portNumber> 7 <secure>>false</secure> 8 </ldapServer> 9 </ldapServers></pre>			

Step 3. Create a ldapMappings by issuing the following API command on CMS for conferencing through Postman:

- Method: POST
- URL: <https://10.106.170.214:445/api/v1/ldapMappings>
- Key: **jidMapping**, Value: **\$mail\$@mmcvd.ciscolabs.com**
- Key: **nameMapping**, Value: **\$cn\$**
- Key: **coSpaceNameMapping**, Value: **\$cn\$'s Space**
- Key: **coSpaceUriMapping**, Value: **\$mail\$.space**
- Key: **coSpaceSecondaryUriMapping**, Value: **\$telephoneNumber\$**
- Key: **coSpaceCallIdMapping**, Value: **\$telephoneNumber\$**

Method	URL	Params	Send
POST	https://10.106.170.214:445/api/v1/ldapMappings/		Send
<input checked="" type="checkbox"/>	jidMapping	\$cn\$@mmcvd.ciscolabs.com	
<input checked="" type="checkbox"/>	nameMapping	\$cn\$	
<input checked="" type="checkbox"/>	coSpaceNameMapping	\$cn\$'s Space	
<input checked="" type="checkbox"/>	coSpaceUriMapping	\$cn\$.space	
<input checked="" type="checkbox"/>	coSpaceSecondaryUriMapping	\$telephoneNumber\$	
<input checked="" type="checkbox"/>	coSpaceCallIdMapping	\$telephoneNumber\$	

Step 4. Check the created instance of **ldapMapping** by issuing the following command:

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/ldapMappings>

Method	URL	Params	Send
GET	https://10.106.170.214:445/api/v1/ldapMappings/		Send
<p>Body Cookies Headers (10) Tests Status: 200 OK</p> <p>Pretty Raw Preview XML</p> <pre> 1 <?xml version="1.0"?> 2 <ldapMappings total="1"> 3 <ldapMapping id="4d91054d-11d7-493e-bcd0-a9fb2fdf0e30"> 4 <jidMapping>\$mail\$@mmcvd.ciscolabs.com</jidMapping> 5 <nameMapping>\$cn\$</nameMapping> 6 </ldapMapping> 7 </ldapMappings> </pre>			

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/ldapMappings/4d91054d-11d7-493e-bcd0-a9fb2fdf0e30>

Method	URL	Params	Send
GET	https://10.106.170.214:445/api/v1/ldapMappings/4d91054d-11d7-493e-bcd0-a9fb2fdf0e30		Send
<p>Body Cookies Headers (10) Tests Status: 200 OK</p> <p>Pretty Raw Preview XML</p> <pre> 1 <?xml version="1.0"?> 2 <ldapMapping id="4d91054d-11d7-493e-bcd0-a9fb2fdf0e30"> 3 <jidMapping>\$mail\$@mmcvd.ciscolabs.com</jidMapping> 4 <nameMapping>\$cn\$</nameMapping> 5 <cdrTagMapping></cdrTagMapping> 6 <coSpaceNameMapping>\$cn\$'s Space</coSpaceNameMapping> 7 <coSpaceUriMapping>\$mail\$.space</coSpaceUriMapping> 8 <coSpaceSecondaryUriMapping>\$telephoneNumber\$</coSpaceSecondaryUriMapping> 9 <coSpaceCallIdMapping>\$telephoneNumber\$</coSpaceCallIdMapping> 10 <authenticationIdMapping></authenticationIdMapping> 11 </ldapMapping> </pre>			

Step 5. Create a **ldapSource** by issuing the following API command on CMS for conferencing through Postman:

- Method: POST

- URL: <https://10.106.170.214:445/api/v1/ldapSources>
- Key: **server**, Value: **dc639ccb-c9bd-4183-848a-7fc893e0d8e4**
- Key: **mapping**, Value: **4d91054d-11d7-493e-bcd0-a9fb2fdf0e30**
- Key: **baseDn**, Value: **ou=cmaUsers,dc=mmcvd,dc=ciscolabs,dc=com**
- Key: **filter**, Value: **(&(objectClass=user)(sAMAccountName=*))**

POST	https://10.106.170.214:445/api/v1/ldapSources	Params	Send
<input checked="" type="checkbox"/>	server	dc639ccb-c9bd-4183-848a-7fc893e0d8e4	
<input checked="" type="checkbox"/>	mapping	4d91054d-11d7-493e-bcd0-a9fb2fdf0e30	
<input checked="" type="checkbox"/>	baseDn	ou=cmaUsers,dc=mmcvd,dc=ciscolabs,dc=com	
<input checked="" type="checkbox"/>	filter	(&(objectClass=user)(sAMAccountName=*))	

Step 6. Check the created instance of `LdapSource` by issuing the following command:

- Method: **GET**
- URL: <https://10.106.170.214:445/api/v1/ldapSources>

GET	https://10.106.170.214:445/api/v1/ldapSources	Params	Send
<p>Body Cookies Headers (10) Tests Status: 200 OK</p> <p>Pretty Raw Preview XML</p> <pre> 1 <?xml version="1.0"?> 2 <ldapSources total="1"> 3 <ldapSource id="0271689d-6148-4c3a-9b6a-142c9286cc30"> 4 <server>dc639ccb-c9bd-4183-848a-7fc893e0d8e4</server> 5 <mapping>4d91054d-11d7-493e-bcd0-a9fb2fdf0e30</mapping> 6 <baseDn>ou=cmaUsers,dc=mmcvd,dc=ciscolabs,dc=com</baseDn> 7 <filter>&(objectClass=user)(sAMAccountName=*)</filter> 8 </ldapSource> 9 </ldapSources></pre>			

Step 7. Start a `LdapSync` with the above created `LdapSource` by issuing the following API command on CMS for conferencing through Postman:

- Method: **POST**
- URL: <https://10.106.170.214:445/api/v1/ldapSyncs>
- Key: **removeWhenFinished**, Value: **false**
- Key: **LdapSource**, Value: **0271689d-6148-4c3a-9b6a-142c9286cc30**

POST	https://10.106.170.214:445/api/v1/ldapSyncs	Params	Send
<input checked="" type="checkbox"/>	removeWhenFinished	false	
<input checked="" type="checkbox"/>	LdapSource	0271689d-6148-4c3a-9b6a-142c9286cc30	

Step 8. Check the status of `LdapSync` by issuing the following command:

- Method: **GET**

- URL: <https://10.106.170.214:445/api/v1/ldapSyncs>

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

```

1 <?xml version="1.0"?>
2 <ldapSyncs total="1">
3   <ldapSync id="20d9b9d6-7184-49e0-a476-4822a001926e">
4     <state>complete</state>
5     <numUsersImported>2</numUsersImported>
6     <numLdapSourcesComplete>1</numLdapSourcesComplete>
7   </ldapSync>
8 </ldapSyncs>
  
```

- Step 9.** Check the users imported by log in to the GUI of CMS for conferencing and navigating to Status > Users.

Users

Filter

Name	Email	XMPP ID	Tenant
Abhijit Dey	abhijitdey	abhijitdey@mmcvd.ciscolabs.com	None
Bilal Nasiri	bilalnasiri	bilalnasiri@mmcvd.ciscolabs.com	None

- Step 10.** Check the Spaces created by navigating to Configuration > Spaces.

Space configuration

Filter

<input type="checkbox"/>	Name	URI user part	Secondary URI user part	Additional access methods	Call ID	Passcode	Default layout	
<input type="checkbox"/>	Abhijit Dey's Space	abhijitdey.space	8511001		8511001		not set	[edit]
<input type="checkbox"/>	Bilal Nasiri's Space	bilalnasiri.space	8511002		8511002		not set	[edit]

Personal Spaces are created.

Procedure 5

Setting up Personal Multiparty Plus Licenses

To enable a set of users to be PMP+ users, a user profile has to be configured with `hasLicense` parameter as true. This represents the users with this user profile will use Personal Multiparty Plus License.

Before that CMS has to be configured with `ldapServer`, `ldapMapping` and `ldapSource` configuration, which is similar to the configuration in **Configuration > Active Directory** on CMS for conferencing.

- Step 11.** Create a **userProfile** by issuing the following API command on CMS for conferencing through Postman:

- Method: POST
- URL: <https://10.106.170.214:445/api/v1/userProfiles>

Step 12. Check the created instance of userProfile by issuing the following command:

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/userProfiles>

GET ▼ <https://10.106.170.214:445/api/v1/userProfiles/> Params Send ▼

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML ≡

```

1 <?xml version="1.0"?>
2 <userProfiles total="1">
3   <userProfile id="ed9af2dd-6f34-49ff-ba87-b5ce8e5baf20"></userProfile>
4 </userProfiles>

```

Step 13. Enable the personal multiparty parameter by issuing the following command:

- Method: PUT
- URL: <https://10.106.170.214:445/api/v1/userProfiles/ed9af2dd-6f34-49ff-ba87-b5ce8e5baf20>
- Key: **hasLicense**, Value: **true**

PUT ▼ <https://10.106.170.214:445/api/v1/userProfiles/ed9af2dd-6f34-49ff-ba87-b5ce8e5baf20> Params Send ▼

Authorization Headers (3) **Body** Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

Key	Value
<input checked="" type="checkbox"/> hasLicense	true

Step 14. Update the existing ldapSource, created in the previous procedure, by issuing the following API command on CMS for conferencing through Postman:

- Method: PUT
- URL: <https://10.106.170.214:445/api/v1/ldapSources/0271689d-6148-4c3a-9b6a-142c9286cc30>
- Key: **userProfile**, Value: **ed9af2dd-6f34-49ff-ba87-b5ce8e5baf20**

PUT ▼ <https://10.106.170.214:445/api/v1/ldapSources/0271689d-6148-4c3a-9b6a-142c9286cc30> Params Send ▼

<input checked="" type="checkbox"/> userProfile	ed9af2dd-6f34-49ff-ba87-b5ce8e5baf20
---	--------------------------------------

Step 15. Check the created instance of ldapSource by issuing the following command:

- Method: GET
- URL: <https://10.106.170.214:445/api/v1/ldapSources>

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

```

1 <?xml version="1.0"?>
2 <ldapSources total="1">
3   <ldapSource id="0271689d-6148-4c3a-9b6a-142c9286cc30">
4     <server>dc639ccb-c9bd-4183-848a-7fc893e0d8e4</server>
5     <mapping>4d91054d-11d7-493e-bcd0-a9fb2fdf0e30</mapping>
6     <baseDn>ou=cmaUsers,dc=mmcvd,dc=ciscolabs,dc=com</baseDn>
7     <filter>(&!(objectClass=user)(sAMAccountName=*))</filter>
8     <userProfile>ed9af2dd-6f34-49ff-ba87-b5ce8e5baf20</userProfile>
9   </ldapSource>
10 </ldapSources>

```

Step 16. Start a **ldapSync** with the above created **ldapSource** by issuing the following API command on CMS for conferencing through Postman:

- Method: **POST**
- URL: **<https://10.106.170.214:445/api/v1/ldapSyncs>**
- Key: **ldapSource**, Value: **0271689d-6148-4c3a-9b6a-142c9286cc30**

POST Params

<input checked="" type="checkbox"/> removeWhenFinished	false
<input checked="" type="checkbox"/> ldapSource	0271689d-6148-4c3a-9b6a-142c9286cc30

Step 17. Verify the **ldapSync** by issuing the following API command on CMS for conferencing through Postman:

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/ldapSyncs>**

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

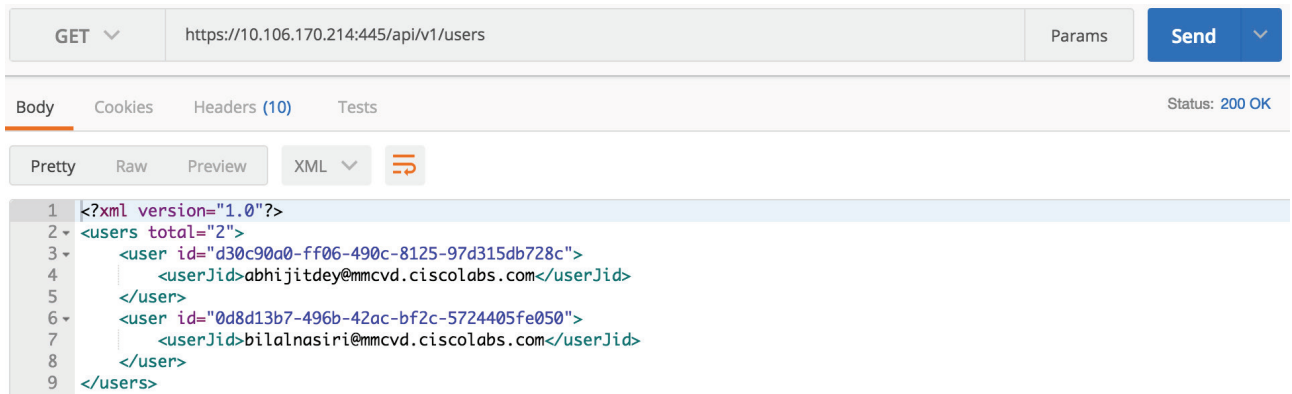
```

1 <?xml version="1.0"?>
2 <ldapSyncs total="2">
3   <ldapSync id="20d9b9d6-7184-49e0-a476-4822a001926e">
4     <state>complete</state>
5     <numUsersImported>2</numUsersImported>
6     <numLdapSourcesComplete>1</numLdapSourcesComplete>
7   </ldapSync>
8   <ldapSync id="5b8c12f1-5ed4-4ffb-ae91-c12e432ed6b2">
9     <state>complete</state>
10    <numUsersImported>2</numUsersImported>
11    <numLdapSourcesComplete>1</numLdapSourcesComplete>
12  </ldapSync>
13 </ldapSyncs>

```

Step 18. Check the users if the **userProfile** has been associated or not by issuing the following commands:

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/users/>**



GET ▼ <https://10.106.170.214:445/api/v1/users/> Params Send ▼

Body Cookies Headers (10) Tests Status: 200 OK

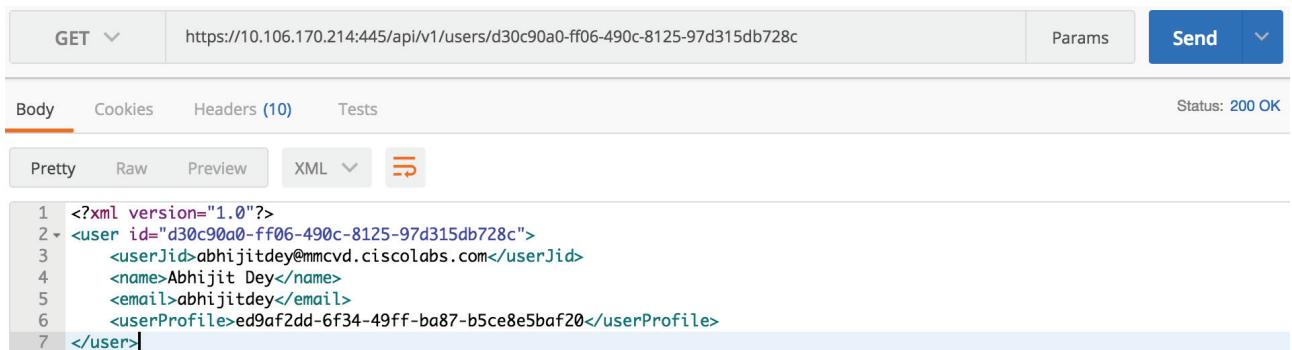
Pretty Raw Preview XML ↔

```

1 <?xml version="1.0"?>
2 <users total="2">
3   <user id="d30c90a0-ff06-490c-8125-97d315db728c">
4     <userJid>abhijitdey@mmcvd.ciscolabs.com</userJid>
5   </user>
6   <user id="0d8d13b7-496b-42ac-bf2c-5724405fe050">
7     <userJid>bilalnasiri@mmcvd.ciscolabs.com</userJid>
8   </user>
9 </users>

```

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/users/d30c90a0-ff06-490c-8125-97d315db728c>**



GET ▼ <https://10.106.170.214:445/api/v1/users/d30c90a0-ff06-490c-8125-97d315db728c> Params Send ▼

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML ↔

```

1 <?xml version="1.0"?>
2 <user id="d30c90a0-ff06-490c-8125-97d315db728c">
3   <userJid>abhijitdey@mmcvd.ciscolabs.com</userJid>
4   <name>Abhijit Dey</name>
5   <email>abhijitdey</email>
6   <userProfile>ed9af2dd-6f34-49ff-ba87-b5ce8e5baf20</userProfile>
7 </user>

```

Personal Multiparty Plus Licenses are applied to the imported users on CMS for conferencing.

Procedure 6

Setting up CMS for WebRTC

WebRTC capability enables the users to join into spaces without any Video endpoint. A user can log in to CMA through a webRTC supported browser.

XMPP and WebBridge modules must be enabled for the WebRTC to be working. It has been enabled in the [Enabling WebAdmin, CallBridge, Recorder, XMPP and WebBridge modules](#).

Following are the further steps to do the rest of the configurations.

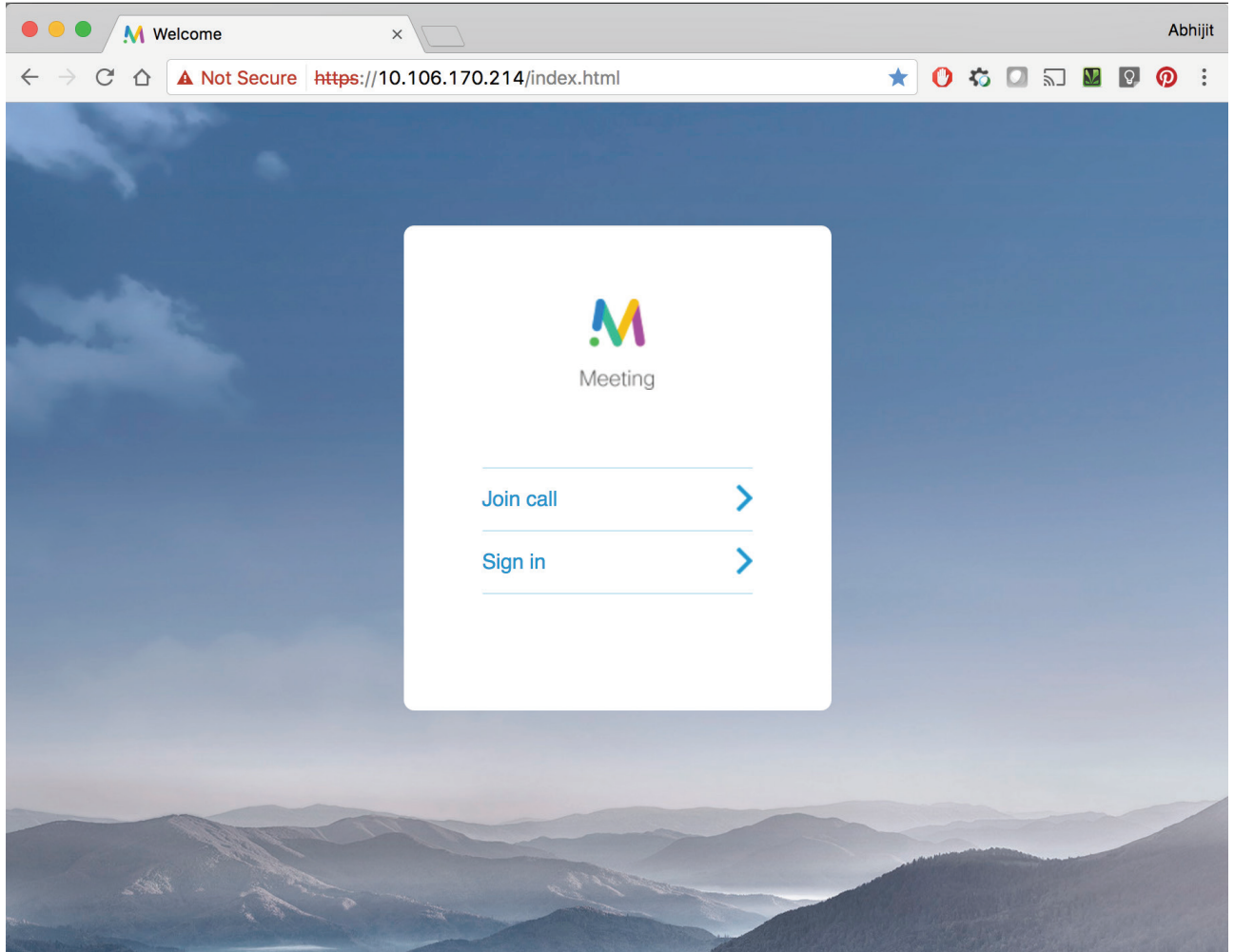
Step 1. Go to **Configuration > General** and configure the following in the WebBridge settings:



- Guest account client URI: **<https://10.106.170.214>**
- Guest account JID domain: **mmcvd.ciscolabs.com**
- Guest access via ID and passcode: **secure: require passcode to be supplied with ID**
- Guest access via hyperlinks: **allowed**
- User sign in: **allowed**

Web bridge settings	
Guest account client URI	<input type="text" value="https://10.106.170.214"/>
Guest account JID domain	<input type="text" value="mmcvd.ciscolabs.com"/>
Custom background image URI	<input type="text"/>
Custom login logo URI	<input type="text"/>
Guest access via ID and passcode	<input type="text" value="secure: require passcode to be supplied with ID"/>
Guest access via hyperlinks	<input type="text" value="allowed"/>
User sign in	<input type="text" value="allowed"/>
Joining scheduled Lync conferences by ID	<input type="text" value="not allowed"/>

- WebRTC capability is enabled on CMS for conferencing, users can browse the URL **<https://10.106.170.214>** and use this feature.

**Procedure 7**

Setting up CMS for Recording

Recording module must be enabled and has been enabled in the [Enabling WebAdmin, CallBridge, Recorder, XMPP and WebBridge modules](#).

Step 1. Create a recorder instance on the CMS for conferencing and give the IP address of the CMS for recording server by issuing the following API command:

- Method: **POST**
- URL: **<https://10.106.170.214:445/api/v1/recorders>**
- Key: **url**, Value: **<https://10.106.170.215:8443>**



POST	https://10.106.170.214:445/api/v1/recorders	Params	Send
<input checked="" type="checkbox"/>	url	https://10.106.170.215:8443	
	New key	value	

Step 2. Verify the created instance of recorder by issuing the following command:

- Method: **GET**
- URL: **https://10.106.170.214:445/api/v1/recorders**

GET	https://10.106.170.214:445/api/v1/recorders	Params	Send
<p>Body Cookies Headers (10) Tests Status: 200 OK</p> <p>Pretty Raw Preview XML</p> <pre> 1 <?xml version="1.0"?> 2 <recorders total="1"> 3 <recorder id="f3dbe066-fa97-4f8c-8771-a3612895cf06"> 4 <url>https://10.106.170.215:8443</url> 5 </recorder> 6 </recorders></pre>			

Step 3. Create a callProfile instance on the CMS for conferencing and set the recording mode as manual which means user has to enter a set of DTMF keys to start or stop recording, by issuing the following command:

- Method: **POST**
- URL: **https://10.106.170.214:445/api/v1/callProfiles**
- Key: **recordingMode**, Value: **manual**

POST	https://10.106.170.214:445/api/v1/callProfiles	Params	Send
<input checked="" type="checkbox"/>	recordingMode	manual	
	New key	value	

Step 4. Verify the created instance of callProfile by issuing the following command:

- Method: **GET**
- URL: **https://10.106.170.214:445/api/v1/callProfiles**

GET	https://10.106.170.214:445/api/v1/callProfiles	Params	Send
<p>Body Cookies Headers (10) Tests Status: 200 OK</p> <p>Pretty Raw Preview XML</p> <pre> 1 <?xml version="1.0"?> 2 <callProfiles total="1"> 3 <callProfile id="602eb7e1-4152-4737-8aec-81a4008d7985"></callProfile> 4 </callProfiles></pre>			

Step 5. Create a **callLegProfile** instance on the CMS for conferencing and set which users have the permission to start and stop recording by issuing the following command:

- Method: **POST**
- URL: **<https://10.106.170.214:445/api/v1/callLegProfiles>**
- Key: **recordingControlAllowed**, Value: **true**

POST	https://10.106.170.214:445/api/v1/callLegProfiles	Params	Send
<input checked="" type="checkbox"/>	recordingControlAllowed	true	
	New key	value	

Step 6. Verify the created instance of **callLegProfile** by issuing the following command:

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/callLegProfiles>**

GET	https://10.106.170.214:445/api/v1/callLegProfiles	Params	Send
Body			Status: 200 OK
<pre> 1 <?xml version="1.0"?> 2 <callLegProfiles total="1"> 3 <callLegProfile id="6735d228-7cde-4298-ad6a-452068b8337e"></callLegProfile> 4 </callLegProfiles> </pre>			

Step 7. Create a **dtmfProfile** instance on the CMS for conferencing to setup the keys used to start and stop the recording by issuing the following command:

- Method: **POST**
- URL: **<https://10.106.170.214:445/api/v1/dtmfProfiles>**
- Key: **startRecording**, Value: ***7**
- Key: **stopRecording**, Value: ***8**

POST	https://10.106.170.214:445/api/v1/dtmfProfiles	Params	Send
<input checked="" type="checkbox"/>	startRecording	*7	
<input checked="" type="checkbox"/>	stopRecording	*8	
	New key	value	

Step 8. Verify the created instance of **dtmfProfile** by issuing the following command:

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/dtmfProfiles>**

Contents | Technology Use Case | Design Overview | Deployment Details | Product List

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

```

1 <?xml version="1.0"?>
2 <dtmfProfiles total="1">
3   <dtmfProfile id="0e613fff-3f31-4996-aff5-aef12449da08"></dtmfProfile>
4 </dtmfProfiles>

```

Step 9. Apply the above created `callLegProfile`, `callProfile` and `dtmfProfile` to the system profile by issuing the following command:

- Method: **PUT**
- URL: **<https://10.106.170.214:445/api/v1/system/Profiles>**
- Key: **callLegProfile**, Value: **6735d228-7cde-4298-ad6a-452068b8337e**
- Key: **callProfile**, Value: **602eb7e1-4152-4737-8aec-81a4008d7985**
- Key: **dtmfProfile**, Value: **0e613fff-3f31-4996-aff5-aef12449da08**

PUT Params

<input checked="" type="checkbox"/>	callLegProfile	6735d228-7cde-4298-ad6a-452068b8337e
<input checked="" type="checkbox"/>	callProfile	602eb7e1-4152-4737-8aec-81a4008d7985
<input checked="" type="checkbox"/>	dtmfProfile	0e613fff-3f31-4996-aff5-aef12449da08
	New key	value

Step 10. Verify the system Profile by issuing the following command:

- Method: **GET**
- URL: **<https://10.106.170.214:445/api/v1/system/Profiles>**

GET Params

Body Cookies Headers (10) Tests Status: 200 OK

Pretty Raw Preview XML

```

1 <?xml version="1.0"?>
2 <profiles>
3   <callLegProfile>6735d228-7cde-4298-ad6a-452068b8337e</callLegProfile>
4   <callProfile>602eb7e1-4152-4737-8aec-81a4008d7985</callProfile>
5   <dtmfProfile>0e613fff-3f31-4996-aff5-aef12449da08</dtmfProfile>
6 </profiles>

```



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

Configuring Cisco TelePresence Management Suite

Easy Access Configuration Sheet

Cisco TMS Configuration Requirements		
Element	CVD Configuration	Site-Specific Configuration
WebAdmin IP:Port	10.106.170.214:445	
WebAdmin Username/password	api / Password	
Domain	Mmcvd.ciscolabs.com	
Numeric Base ID for Scheduled conferences	8211001	
WebBridge URI	https://10.106.170.214/	

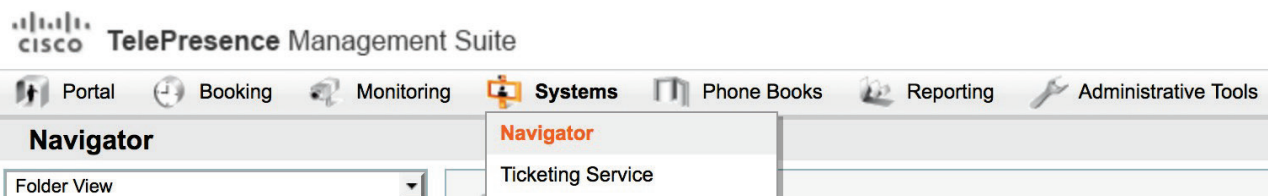
PROCESS

1. [Add Cisco Meeting Server on TMS](#)
2. [Configuring CMS in TMS for Scheduled Conferences](#)
3. [Configure Conference Settings on TMS](#)

Procedure 1

Add Cisco Meeting Server on TMS

Step 1. Log in to the TMS and navigate to **Systems > Navigator**.



Step 2. Click **Add Systems**.

Step 3. Under the Add by Address tab, enter the following:

- IP Address: **10.106.170.214:445**
- Username: **api**
- Password: **Password**

Add by Address | Add from Unified CM or TMS | Add Unmanaged Endpoint | Add Unmanaged Bridge | Pre-register Systems

Specify Systems by IP Addresses or DNS Names

Enter the IP address, DNS name or IP range of the systems to be added. Each entry must be separated by a comma. The following example will add two systems, and scan ten systems in a range: user.example.org, 10.0.0.1, 10.1.1.0 - 10.1.1.10 For Cisco Meeting Server, you can also add IP address and port number separated by a colon. For example, 10.0.0.1:445. For IPV6 systems, it is mandatory to have the IPV6 address within [] and port number separated by a colon. For example, [2001:10:10:10:10:10]:445

10.106.170.214:445

Location Settings

ISDN Zone: None | IP Zone: HQ

Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Advanced Settings

It is mandatory to enter valid Username and Password for all Cisco Meeting Servers.

Username: api

Password: ...

SNMP Community Names: public,Public

Persistent Template: No Template

Usage Type: Meeting Room

Step 4. Click **Next** and then click **Finish Adding Systems**.



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

Add Result

Systems Found					
<input type="checkbox"/>	Network Address	System Name	System Type	Description	Actions
<input type="checkbox"/>	10.106.170.214:445	No Name (10.106.170.214:445)	Cisco Meeting Server	✓ System added despite warnings	

Procedure 2 Configuring CMS in TMS for Scheduled Conferences

- Step 1.** Click the newly added CMS system from the Navigator section, and then select the **Settings** tab.
- Step 2.** Configure the following and click **Save**:
 - Name: **cms1**
 - Allow Incoming H.323 Dialing: **Unchecked**
 - Allow Outgoing H.323 Dialing: **Unchecked**



TelePresence Management Suite Search...

Portal | Booking | Monitoring | **Systems** | Phone Books | Reporting | Administrative Tools

Navigator You are here: Systems > Navigator

Folder View

- Company Name
 - CVD Endpoints
 - Discovered Systems
 - Infrastructure
 - ucmp
 - No Name (10.106.170.214:445)**

No Name (10.106.170.214:445)
 Cisco Meeting Server Status: Idle Address: 10.106.170.214:445 Connectivity: Reachable on LAN

Domain, Numeric ID Base and Numeric ID Quantity details are not set. - Domain, Numeric ID Base and Numeric ID Quantity are blank. Enter the details under Settings > Extended Settings and save. [More...](#)

Summary **Settings** Connection Permissions Logs

View Settings **Edit Settings** Extended Settings Ticket Filters

General

Name: Status:
 System Type: Your Access:
 System Connectivity: System Contact:
 Network Address: Alert System Contact when Booked:
 Manufacturer: Description:
 IP Zone:
 Time Zone:
 Web Bridge URI:

Configuration

Software Version:

Network Settings


SIP Mode:

TMS Scheduling Settings

Allow Booking:
 Allow Incoming H.323 Dialing:
 Allow Incoming SIP URI Dialing:
 Allow Outgoing H.323 Dialing:
 Allow Outgoing SIP URI Dialing:


Step 3. Click the **Extended Settings** sub-tab, enter the following and click **Save**:

- Domain: **mmcvd.ciscolabs.com**
- Numeric ID Base: **8211001**
- Numeric ID Quantity: **10**



cms1

Cisco Meeting Server Status: Idle
 Address: 10.106.170.214:445
 Connectivity: Reachable on LAN



Summary
Settings
Connection
Permissions
Logs

View Settings
Edit Settings
Extended Settings
Ticket Filters

Extended Settings

Domain:

Numeric ID Base:

Numeric ID Quantity:

Now 10 Spaces with the above shown ID will be created on CMS for the conferencing server. These spaces will be used as scheduled spaces when a user schedules a conference. These spaces will be enabled only during the time of a scheduled conference and are disabled other times.

Step 4. Verify the creation of spaces by logging in to the GUI of CMS for conferencing and navigating to **Configuration > Spaces**.

Space configuration

Filter

<input type="checkbox"/>	Name	URI user part	Secondary URI user part	Additional access methods	Call ID	Passcode	Default layout	
<input type="checkbox"/>	Abhijit Dey's Space	abhijitdey.space	8511001		8511001		not set	[edit]
<input type="checkbox"/>	Bilal Nasir's Space	bilalnasiri.space	8511002		8511002		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211001	8211001			8211001		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211002	8211002			8211002		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211003	8211003			8211003		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211004	8211004			8211004		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211005	8211005			8211005		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211006	8211006			8211006		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211007	8211007			8211007		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211008	8211008			8211008		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211009	8211009			8211009		not set	[edit]
<input type="checkbox"/>	TMS_Scheduled_Meeting_8211010	8211010			8211010		not set	[edit]

SIP Trunks must be configured for scheduled calls to work. (Covered in the Configuring CUCM section).

The following steps, enable users to join a conference instantly with a single click. This requires the WebBridge module to be enabled (already configured in the previous sections).

Step 5. Log in to TMS and navigate to **Systems > Navigator**.

Step 6. Select cms1, click the **Settings** tab and select **Edit Settings**.

Step 7. Configure the following and click **Save**:

- Web Bridge URI: <https://10.106.170.214/>

Portal Booking Monitoring **Systems** Phone Books Reporting Administrative Tools

Navigator You are here: Systems Navigator

Folder View

- Company Name
 - CVD Endpoints
 - Discovered Systems
 - Infrastructure
 - cms1**
 - cucmp

cms1
Cisco Meeting Server Status: Idle Address: 10.106.170.214:445 Connectivity: Reachable on LAN

Summary **Settings** Connection Permissions Logs

View Settings **Edit Settings** Extended Settings Ticket Filters

General

Name: cms1 Status: Idle
 System Type: Cisco Meeting Server Your Access: Book, Edit Settings, Manage Calls, Set Permissions, Read
 System Connectivity: Reachable on LAN System Contact:
 Network Address: 10.106.170.214:445 Alert System Contact when Booked: No
 Manufacturer: Cisco Description:
 IP Zone: HQ
 Time Zone: (UTC+05:30) Chennai, Kolkata, Mun
 Web Bridge URI: https://10.106.170.214/

Procedure 3

Configure Conference Settings on TMS

Step 8. Navigate to **Administrative Tools > Configuration > Conference Settings**.

Step 9. Enter **Preferred MCU Type in Routing** as **Cisco Meeting Server**. And click **Save**.

Advanced	
External MCU Usage in Routing:	Only if needed
Preferred MCU Type in Routing:	Cisco Meeting Server

The conference settings are configured.



Configuring Cisco Unified Communications Manager

Easy Access Configuration Sheet

Cisco Unified CM Configuration Requirements		
Element	CVD Configuration	Site-Specific Configuration
Video bandwidth for video region	32256	
Route pattern for personal conferences	821XXXX	
Route pattern for scheduled conferences	851XXXX	
URI pattern for personal CMR conferences	user.space@mmcvd.ciscolabs.com	

PROCESS

1. [Configure Region for Video](#)
2. [Configure Device Pool for Video and Add the Video Region](#)
3. [Configure SIP Trunk to Cisco Meeting Server for Conferences](#)
4. [Configure Directory Number Route Pattern for Personal and Scheduled Conferences](#)
5. [Configure Unified CM SIP Route Pattern for Personal CMR Conferences](#)
6. [Configure Cisco Meeting Server as Conference Bridge for Ad-Hoc Conferences](#)
7. [Add this MRGL to the Device Profile for Video](#)

Procedure 1

Configure Region for Video

- Step 1.** Navigate to **System > Region Information > Region**, and click **Add New** in order to create a new Region.
- Step 2.** In **Name**, enter **Video_Reg**, and then click **Save**.

- Step 3.** Under **Regions**, select **Default**.
- Step 4.** Under **Maximum Session Bit Rate for Video Calls**, enter **32256** kbps and click **Save**.

Regions	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
Default REG_HQ1 REG_Site01 Video_Reg	Keep Current Setting	Keep Current Setting kbps	<input type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input checked="" type="radio"/> 32256 kbps

This CVD is using **32256** as the configured video bandwidth for this region.

The region is configured.

Procedure 2

Configure Device Pool for Video and Add the Video Region

- Step 1.** Navigate to **System > Device Pool**, and then click **Add New** in order to add a new device pool.
- Step 2.** Enter the following into the relevant fields, leaving the other fields at their default values and click **Save**.
- Device Pool Name: **Video_DP**
 - Cisco Unified Communications Manager Group: **Sub1_Pub1**
 - Date/Time Group: **CMLocal**
 - Region: **Video_Reg**

Device Pool Information	
Device Pool:	Video_DP (8 members**)
Device Pool Settings	
Device Pool Name*	Video_DP
Cisco Unified Communications Manager Group*	Sub1_Pub1
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >
Local Route Group Settings	
Standard Local Route Group	< None >
Roaming Sensitive Settings	
Date/Time Group*	CMLocal
Region*	Video_Reg
Media Resource Group List	MRGL-1-cond-1

The device pool is configured.

Procedure 3

Configure SIP Trunk to Cisco Meeting Server for Conferences

A *trunk* is a communications channel on Unified CM that enables it to connect to other servers. Using one or more trunks, Unified CM can receive or place voice, video, and encrypted calls, exchange real-time event information, and communicate in other ways with call control servers and other external servers.

Step 1. Navigate to **Device > Trunk**, and then click **Add New** in order to create a new SIP trunk.

Step 2. Enter the following into the relevant fields:

- Trunk Type: **SIP Trunk**
- Device Protocol: **SIP**
- Trunk Service Type: **None(Default)**

Trunk Information	
Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Step 3. Click **Next**.

Step 4. Enter the following into the relevant fields, leaving other fields at their default values:

- Device Name: **TR-2-CMS1**
- Device Pool: **Video_DP**
- Destination Address: **10.106.170.214**
- Destination Port: **5060**
- SIP Trunk Security Profile: **Non Secure SIP Trunk Profile**
- SIP Profile: **Standard SIP Profile for TelePresence Conferencing**
- Normalization Script: **cisco-telepresence-conductor-interop**

Device Information	
Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	TR-2-CMS1
Description	to CMS 10.106.170.214
Device Pool*	Video_DP

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.170.214		5060

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

DTMF Signaling Method*

Normalization Script

Normalization Script

Step 5. Click **Save**, and then click **Reset**.

Step 6. Now click **Reset** again in the pop-up window that appears and click **Close**.

The Unified CM trunk is now configured to the Cisco Meeting Server for conferences.

Procedure 4

Configure Directory Number Route Pattern for Personal and Scheduled Conferences

In this CVD, **851XXXX** is the range of Directory Numbers for Personal Conferences and **821XXXX** is the range of Directory Numbers for Scheduled Conferences.

Step 1. Navigate to **Call Routing > Route/Hunt > Route Pattern**, and then click **Add New** to create a new route pattern.

Step 2. To route calls to the personal conferences, enter the following in the relevant fields, leave other fields at their default values and click **Save**.

- Route Pattern: **851XXXX**
- Gateway/Route List: **TR-2-CMS1**

Pattern Definition	
Route Pattern*	851XXXX
Route Partition	< None >
Description	Calls to Personal Spaces on CMS1
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	TR-2-CMS1

Step 3. Navigate to **Call Routing > Route/Hunt > Route Pattern**, and then click **Add New** to create a new route pattern.

Step 4. To route calls to scheduled conferences, enter the following in the relevant fields, leave other fields at their default values and click **Save**.

- Route Pattern: **821XXXX**
- Gateway/Route List: **TR-2-CMS1**

Pattern Definition	
Route Pattern*	821XXXX
Route Partition	< None >
Description	Calls to TMS Scheduled Spaces on CMS1
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	TR-2-CMS1

The route patterns are now configured.

Procedure 5

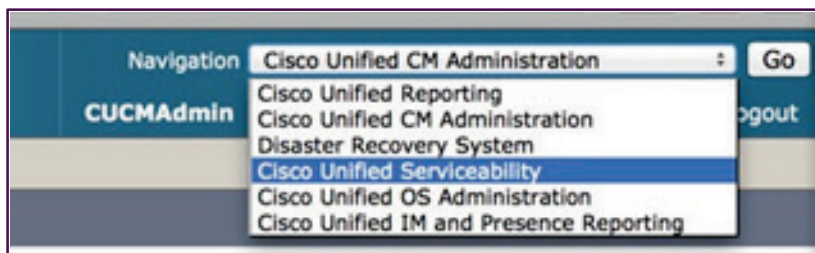
Configure Unified CM SIP Route Pattern for Personal CMR Conferences

The regular Unified CM SIP route pattern routing cannot be used for routing calls to the personal CMR conferences created in this document because Unified CM can only route URIs based on domains (e.g. mmcvd.ciscolabs.com) and not the URIs created for the personal conferences (e.g. space@mmcvd.ciscolabs.com).

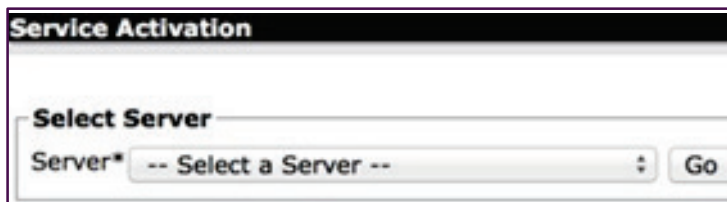
To route the calls to the personal CMR conference URIs, you must use the Intercluster Lookup Service (ILS) in the Unified CM and manually import the personal CMR conference URIs into Unified CM.

The following steps configure the Unified CM to enable ILS and import the personal CMR conference URLs.

- Step 1.** Click the **Navigation** tab on the top right corner of the **Unified CM Administration** page, select **Cisco Unified Serviceability** from the dropdown list and click **Go**.



- Step 2.** Navigate to **Tools > Service Activation**.

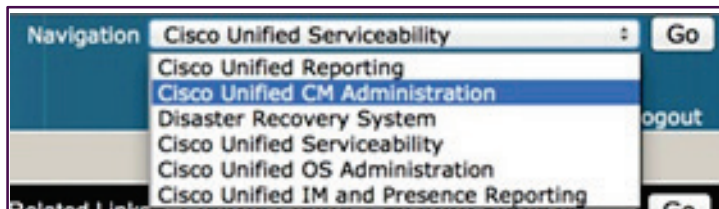


- Step 3.** Select **CUCM-Pub--CUCM Voice/Video** from the drop-down list under the **Server** field, and click **Go**.
- Step 4.** Select the **Cisco Bulk Provisioning Service** under the **Database and Admin Services** pane, and click **Save**.

Database and Admin Services	
	Service Name
<input checked="" type="checkbox"/>	Cisco Bulk Provisioning Service
<input checked="" type="checkbox"/>	Cisco AXL Web Service
<input checked="" type="checkbox"/>	Cisco UXL Web Service
<input checked="" type="checkbox"/>	Cisco TAPS Service

Step 5. Go back to the **Cisco Unified CM Administration** page by clicking on the **Navigation** tab at the top-right corner of the **Cisco Unified Serviceability** page.

Step 6. Select the **Cisco Unified CM Administration**, and then click **Go**.



ILS must be enabled and working for the following steps to work. ILS can work either in “Hub Cluster” or “Spoke Cluster” mode. In this CVD we follow a single cluster deployment, so we will configure this publisher in “Hub Cluster” mode.

Step 7. Navigate to **Advanced Features > ILS Configuration**, select **Hub Cluster** as the **Role** under the **Intercluster Lookup Service Configuration** tab, and then click **Save**.

Intercluster Lookup Service Configuration

Role

Step 8. Navigate to **Call Routing > Global Dial Plan Replication > Imported Global Dial Plan Catalogue**, and click **Add New**.

Step 9. Enter the following into the relevant fields:

- Name: **CMS_Personal_Space_Catalog**
- Route String: **space.mmcvd.ciscolabs.com**

Imported Global Dial Plan Catalog Information

Name*

Description

Route String*



Tech Tip

The Route String is just a name, it does not represent that the user will have to dial *cmr.mmcvd.ciscolabs.com.

Step 10. Click **Save**.

Step 11. Create a **cvd_space.csv** file in the following format for all the personal CMR conference URIs that must be imported into the ILS of the Unified CM.


	A	B	C
1	PatternType	PSTNFailover	Pattern
2	uri		abhijitdey.space@mmcvd.ciscolabs.com

Step 12. Navigate to **Bulk Administration > Upload/Download Files** and click **Add New**.

Step 13. Enter the following into the relevant fields:


- File: **cvd_space.csv**
- Select The Target: **Imported Directory URIs and Patterns**
- Select Transaction Type: **Insert Imported Directory URIs and Patterns**
- Overwrite File if it exists: **Selected**


Status

 Status: Ready

Upload the CSV file

File: * cvd_space.csv

Select The Target * 

Select Transaction Type * 

Overwrite File if it exists.**


Step 14. Click **Save**.

Step 15. Navigate to **Bulk Administration > Directory URIs and Patterns > Insert Imported Directory URI and Pattern Configuration**.

Step 16. Enter the following into the relevant fields:

- File Name: **cvd_space.csv**
- Imported Global Dial Plan Catalog: **CMS_Personal_Space_Catalog**
- Run Immediately: **Selected**

Status

 Status: Ready

Bulk Imported Directory URI and Pattern Information

File Name * [\(View File\)](#) [\(View Sample File\)](#)

Imported Global Dial Plan Catalog *

Job Information

Job Description

Run Immediately Run Later (To schedule and activate this job, use Job Scheduler page.)

Step 17. Click **Submit**.

Step 18. Navigate to **Call Routing > SIP Route Pattern**.

Step 19. Click **Add New**.

Step 20. Enter the following into the relevant fields, leave other fields at their default values, and click **Save**.

- IPv4 Pattern: **space.mmcvd.ciscolabs.com**
- SIP Trunk/Route List: **TR-2-CMS1**

Pattern Definition

Pattern Usage

IPv4 Pattern*

IPv6 Pattern

Description

Route Partition

SIP Trunk/Route List*

The SIP route pattern is now configured.

Procedure 6

Configure Cisco Meeting Server as Conference Bridge for Ad-Hoc Conferences

This procedure describes configuring Cisco Meeting Server as a conference bridge in Unified CM for Ad-Hoc conferences.

Ad-Hoc conferences on Cisco Meeting Server require the Cisco Unified CM to communicate with the API of the Cisco Meeting Server. The API requires HTTPS communication, so certificates must be created and



Contents | Technology Use Case | Design Overview | **Deployment Details** | Product List

uploaded to both the Cisco Meeting Server and Cisco Unified Communications Manager. For escalated ad hoc calls to work, each must trust the other's certificate, .

Certificates on Cisco Meeting Server are already uploaded in the previous procedures.

This process covers certificates on Unified CM.

- Step 1.** Log in to the CUCM OS Administration page and Navigate to **Security > Certificate Management**.
- Step 2.** Click the **Generate CSR** button and generate a Certificate Signing Request (CSR) for Cisco Unified Communications Manager.
- Step 3.** Get the CSR signed by a Certificate Authority and upload the signed certificate and private key to Unified CM.
- Step 4.** Select **Upload Certificate / Certificate Chain**.
- Step 5.** Click **Browse** to find your certificate. (This can be the root certificate or the call bridge's certificate and certificate bundle) and click **Upload**.
- Step 6.** Navigate to **Media Resources > Conference Bridge**, and then click **Add New** in order to create a new conference bridge.
- Step 7.** Enter the following into the relevant fields, and leave other fields at their default values:
 - Conference Bridge Type: **Cisco TelePresence Conductor**
 - Conference Bridge Name: **cms1**
 - SIP Trunk: **TR-2-CMS1**
 - Allow Conference Bridge Control of the Call Security Icon: **UnSelected**
 - Override SIP Trunk Destination as HTTP Address: **Selected**
 - Hostname/IP Address: **cms1.mmcvd.ciscolabs.com**
 - Username: **api**
 - Password: **password**
 - Use HTTPS: **Selected**
 - HTTP Port: **445**



Device Information

Conference Bridge Type* Cisco TelePresence Conductor

Device is trusted

Conference Bridge Name* cms1

Description CMS (.214) as ad-hoc bridge

Conference Bridge Prefix

SIP Trunk* TR-2-CMS1

Allow Conference Bridge Control of the Call Security Icon

HTTP Interface Info

Override SIP Trunk Destination as HTTP Address

Hostname/IP Address

1 cms1.mmcvd.ciscolabs.com

Username* api

Password*

Confirm Password*

Use HTTPS

HTTP Port* 445

Step 8. Click **Save**.

Step 9. Make sure that the Conference Bridge shows as registered to the Unified CM.

<input type="checkbox"/>	cms1	CMS (.214) as ad-hoc bridge	Registered with 10.106.170.178	10.106.170.214
--------------------------	----------------------	-----------------------------	--------------------------------	----------------

Step 10. Navigate to **Media Resources > Media Resource Group**, and then click **Add New**.

Step 11. In **Name**, enter **MRG-CMS1**

Step 12. In **Available Media Resources**, select **cms1 (CFB)**, click the down arrow to move it down to the **Selected Media Resources** and click **Save**.

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*

cms1 (CFB)

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

Step 13. Navigate to **Media Resources > Media Resource Group List**, and then click **Add New**.

Step 14. In **Name**, enter **MRGL-CMS1**

Step 15. In **Available Media Resources Groups**, select **MRG-CMS1** and click the down arrow to move it down to the **Selected Media Resources Groups** and click **Save**.

Media Resource Group List Information

Name*

Media Resource Groups for this List

Available Media Resource Groups

PCP_MRG_ANN
 PCP_MRG_CFB_Soft
 PCP_MRG_MOH
 PCP_MRG_MTP
 PCP_site one_MRG

▼ ▲

Selected Media Resource Groups

MRG-CMS1

▼ ▲

The Cisco Meeting Server is now configured as a media resource.

Procedure 7

Add this MRGL to the Device Profile for Video

- Step 1.** Navigate to **System > Device Pool**, and then click **Find** in order to list all configured Device Pools.
- Step 2.** Select **Video_DP**.
- Step 3.** In **Media Resource Group List**, select **MRGL-1-cond-1** and click **Save**.

Roaming Sensitive Settings

Date/Time Group* ▼

Region* ▼

Media Resource Group List ▼

The MRGL is added.

Configuring Endpoints

PROCESS

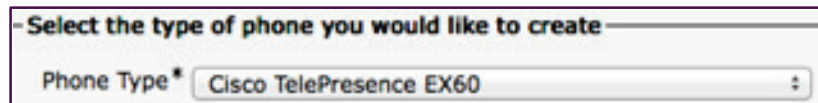
1. [Configure Unified CM for Endpoints](#).
2. [Configure SX20](#).

Procedure 1

Configure Unified CM for Endpoints

Step 1. Navigate to **Device > Phone**, and then click **Add New**.

Step 2. In **Phone Type**, select **Cisco TelePresence EX60**.



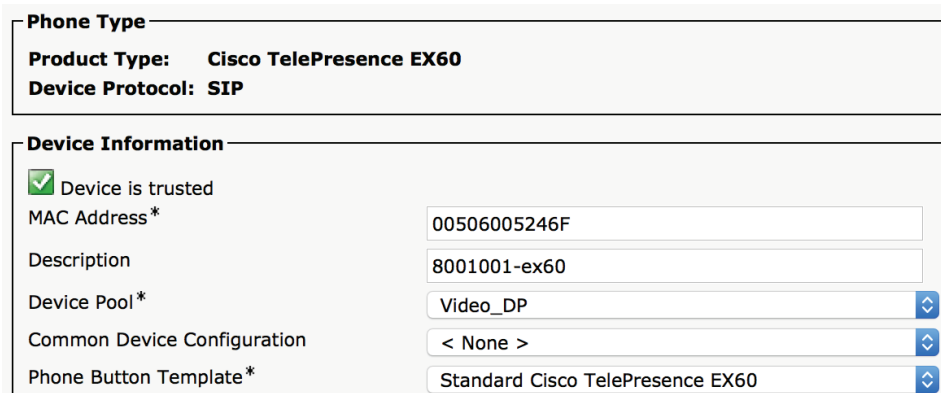
- Select the type of phone you would like to create -

Phone Type*

Step 3. Click **Next**.

Step 4. Enter the following into the relevant field, and leave the other fields at their default values:

- MAC Address: **00506005246F**
- Device Pool: **Video_DP**
- Phone Button Template: **Standard Cisco TelePresence EX60**
- Common Phone Profile: **Standard Common Phone Profile**
- Device Security Profile: **Cisco TelePresence EX60–Standard**
- SIP Profile: **Standard SIP Profile for TelePresence Endpoint**



Phone Type

Product Type: Cisco TelePresence EX60

Device Protocol: SIP

Device Information

Device is trusted

MAC Address*

Description

Device Pool*

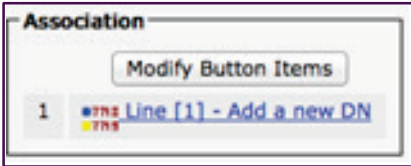
Common Device Configuration

Phone Button Template*

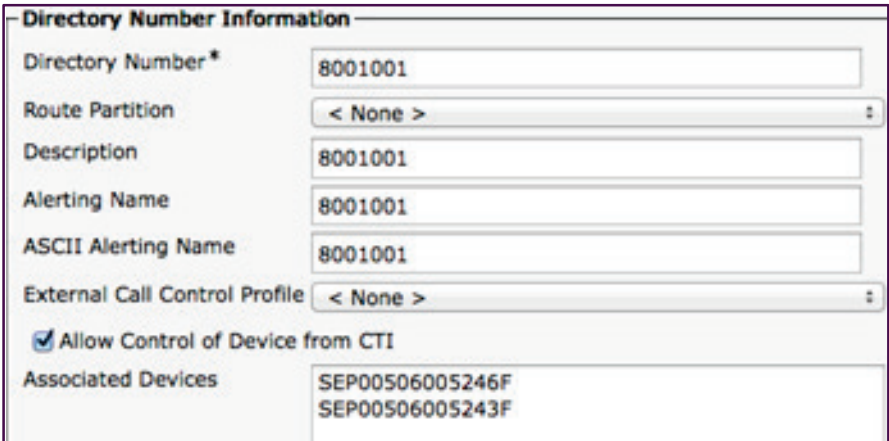
Step 5. Click **Save**.



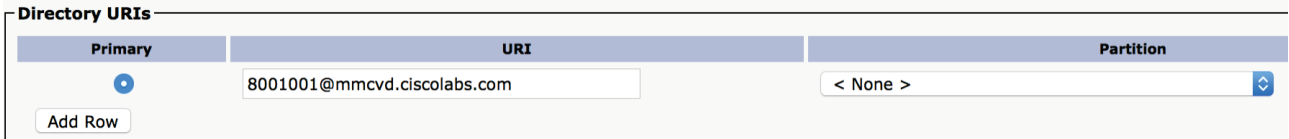
Step 6. Click Line [1] - Add a new DN.



Step 7. In Directory Number, enter **8001001**, and then click **Save**.



Step 8. Under Directory URIs, enter **8001001@mmcvd.ciscolabs.com** as the URI and click **Add Row**.



The endpoint is now added.

**Procedure 2**

Configure SX20

Step 1. Navigate to **Home > Settings > Administrator Settings > Advanced Configuration > Provisioning > External Manager > Address.**

Step 2. In **External Manager**, enter **10.106.170.135**, and then click **Save**.

The endpoint is added.

Initiating Conferences

PROCESS

1. [Initiate Ad-Hoc Conference](#)
2. [Initiate Personal Conference](#)
3. [Create Scheduled CMR Conference](#)

Procedure 1

Initiate Ad-Hoc Conference

Step 1. Call **8001002** from **8001001**.

Step 2. After the call is connected, press on the **Add+** button.

Step 3. Call **8001003** from **8001001**.

Step 4. Press the **Merge** button.

The Ad-Hoc conference should now be started.

Contents | Technology Use Case | Design Overview | Deployment Details | Product List

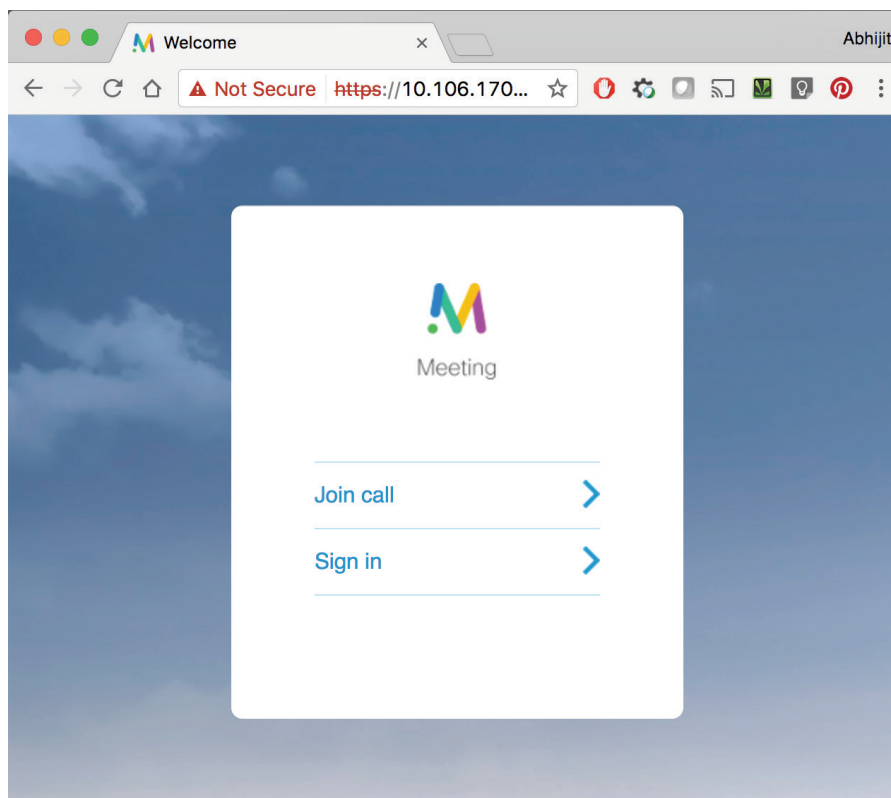
Procedure 2

Initiate Personal Conference

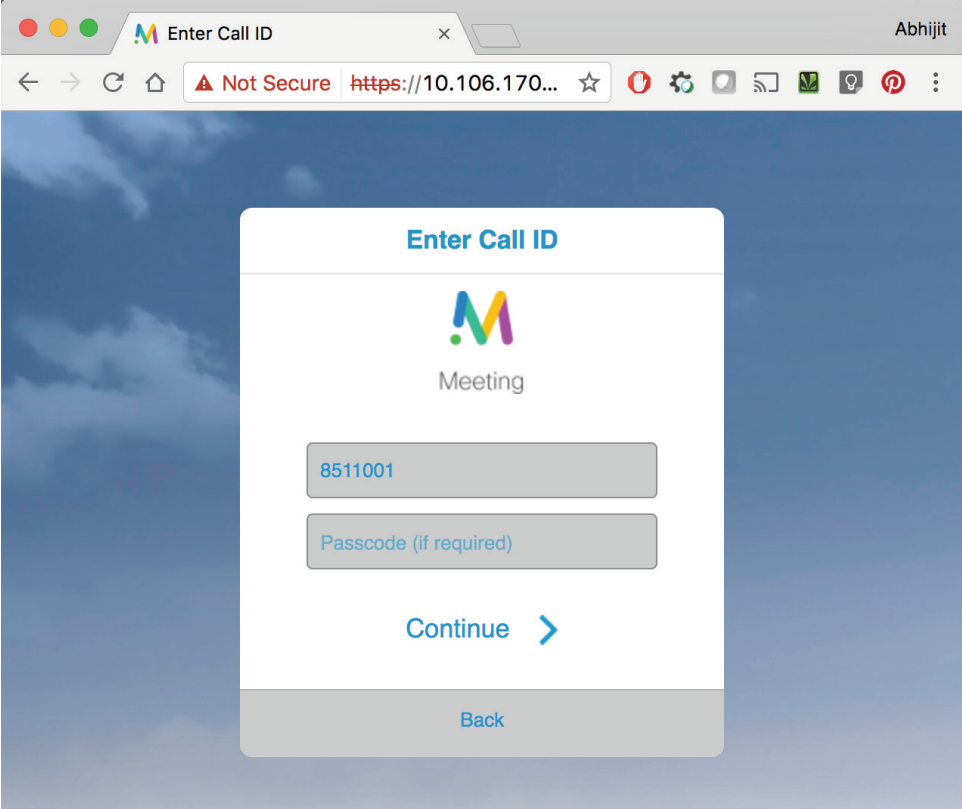
- Step 1.** Call abhijitdey.space@mmcvd.ciscolabs.com from 8001001.
- Step 2.** Call abhijitdey.space@mmcvd.ciscolabs.com from 8001003.
- Step 3.** Call abhijitdey.space@mmcvd.ciscolabs.com from 8001003.

The personal conference should now be connected.

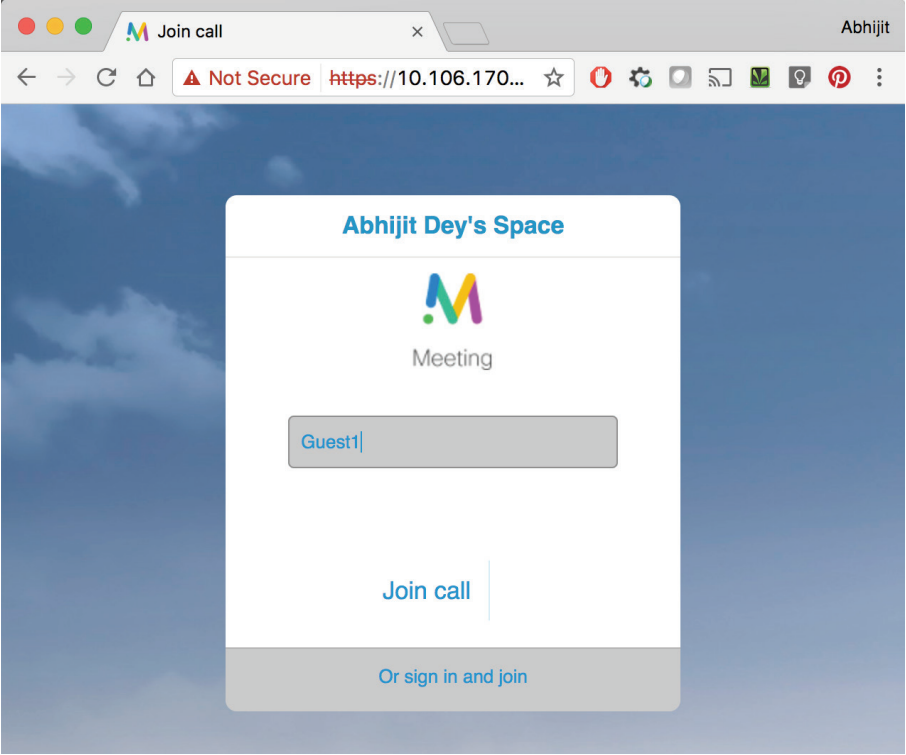
- Step 4.** Call 8511001 from endpoints that cannot dial a SIP URI to join the same conference.
- Step 5.** A guest or other users can join the same Personal Conference from a WebRTC based browser by entering <https://10.106.170.214/>.



- Step 6.** Click **Join call**, then enter 8511001 and click **Continue**.



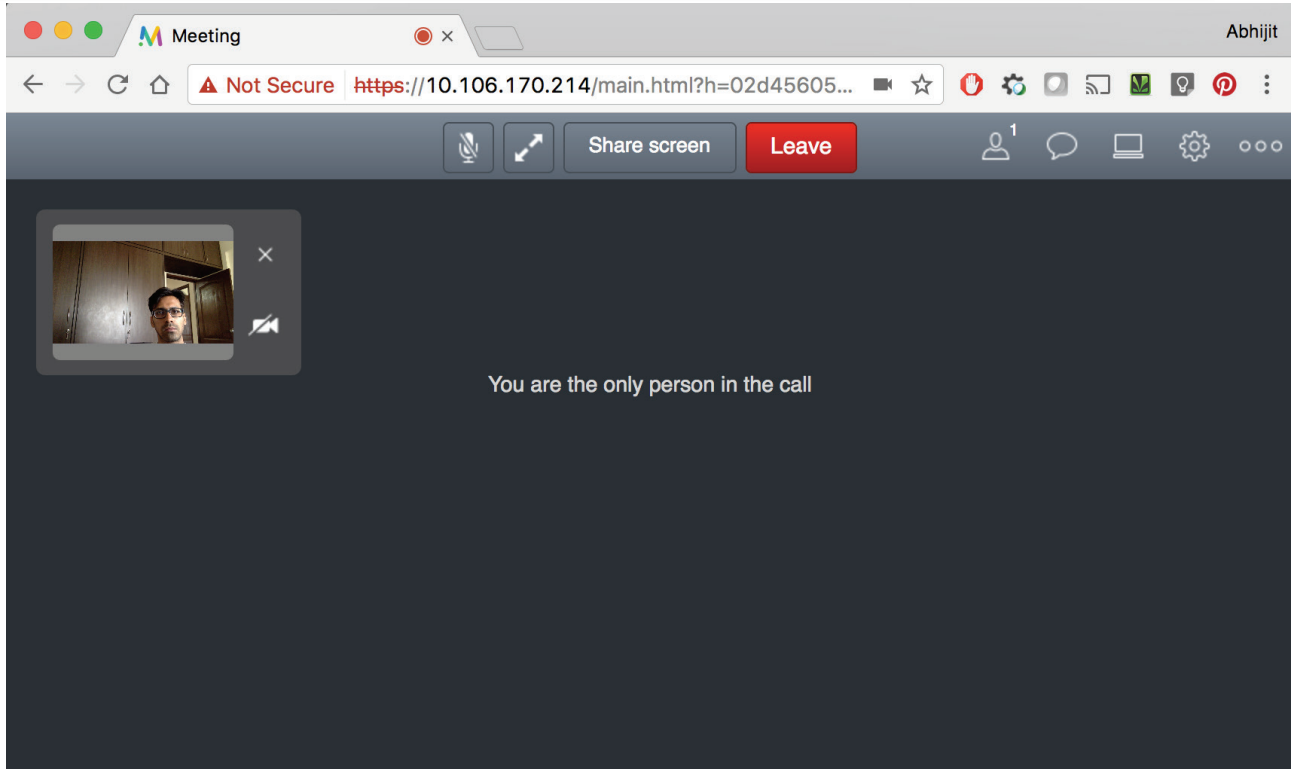
Step 7. Enter **Guest1** and click **Join call**.



Guest1 can join the above conference.



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

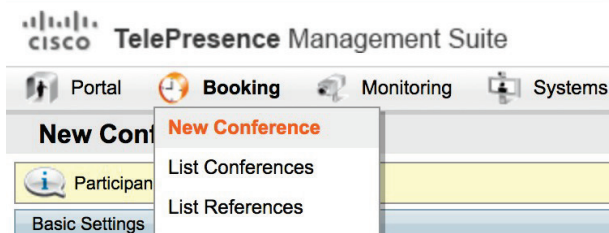


Procedure 3

Create Scheduled Conference

Step 1. Log in to TMS as a user by typing <http://10.106.170.203/tms/> in the browser.

Step 2. Click **Booking > New Conference**.



Step 3. Configure the settings based on the requirement and click **Add Participants** to add systems to the conference.

New Conference

Basic Settings

Title:	<input type="text" value="Test Meeting 1"/>	Start Time:	<input type="text" value="5/12/2017"/> <input type="text" value="8:46 PM"/>
Type:	<input type="text" value="One Button To Push"/>	End Time:	<input type="text" value="5/12/2017"/> <input type="text" value="8:56 PM"/>
Owner:	<input type="text" value="Dey, Abhijit"/> 	Duration:	<input type="text" value="0:10"/>
Language:	<input type="text" value="English (US)"/>	Time Zone:	(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Location:	<input type="text"/>	Recurrence:	<input type="button" value="Add Recurrence..."/>

Advanced Settings

Picture Mode:	<input type="text" value="Continuous Presence"/>	Billing Code:	<input type="text"/>
IP Bandwidth:	<input type="text" value="2560 kbps"/>	PIN:	<input type="text"/>
ISDN Bandwidth:	<input type="text" value="6b / 384 kbps"/>	Extend Mode:	<input type="text" value="Automatic Best Effort"/>
Secure:	<input type="text" value="If Possible"/>	<input type="checkbox"/> ISDN Restrict	

Participants

Conference Information

No participants added to the conference.

Step 4. After you add participants, click **Save**.

Participants

Connection Settings

Conference Information

<input type="checkbox"/> Name	Actions
<input type="checkbox"/>  Auto 8000007	Details
<input type="checkbox"/>  Auto 8000009	Details
<input type="checkbox"/>  Auto 8000017	Details
<input type="checkbox"/>  Auto 8000027	Details
<input type="checkbox"/>  Auto 8000028	Details
<input type="checkbox"/>  SIP Video Dial In	
<input type="checkbox"/>  SIP Video Dial In	
<input type="checkbox"/>  SIP Video Dial In	
<input type="checkbox"/>  SIP Video Dial In	
<input type="checkbox"/>  SIP Video Dial In	








Video Conference Master:

The Meeting is created and users can dial **8211003@mmcvd.ciscolabs.com** to join this conference.



Contents | Technology Use Case | Design Overview | Deployment Details | Product List

TelePresence Management Suite

 Portal  **Booking**  Monitoring  Systems  Phone Books  Reporting  Administrative Tools

New Conference

The conference has been saved.

Conference Title: Test Meeting 1
Conference ID: 60

Participant(s):
Auto 8000007
Auto 8000009
Auto 8000017
Auto 8000027
Auto 8000028
5 x SIP Video Dial In
cms1

The participants will connect using this route:
Auto 8000007 connects to cms1 (SIP: 8211003@mmcvd.ciscolabs.com)
Auto 8000027 connects to cms1 (SIP: 8211003@mmcvd.ciscolabs.com)
Auto 8000009 connects to cms1 (SIP: 8211003@mmcvd.ciscolabs.com)
Auto 8000017 connects to cms1 (SIP: 8211003@mmcvd.ciscolabs.com)
Auto 8000028 connects to cms1 (SIP: 8211003@mmcvd.ciscolabs.com)
5 x SIP Video Dial In connects to cms1 (SIP: 8211003@mmcvd.ciscolabs.com)

[Edit Conference](#) [New Conference](#) [List Conferences](#) [Meeting Details](#)

Recording Conferences

PROCESS

1. [Record Conferences](#)

Procedure 1

Record Conferences

- Step 1.** While in the conference, press *7 to start a recording.
- Step 2.** Press *8 to stop the recording.



Appendix A: Product List

Component	Product Description	Part Number	Software
Call Control	Cisco Unified CM Business Edition 6000 with up to 1000 users	BE6H-M4-K9= BE6H-M4-XU=	11.5(1)
Video Phones	Unified IP Phones 8800 series	CP-88xx-K9=	11.5
Video Endpoints	Cisco TelePresence DX70	CP-DX70-W-K9=	CE 8.3.1
	Cisco TelePresence DX80	CP-DX80-K9=	CE 8.3.1
	Cisco TelePresence SX10	CTS-SX10N-K9	CE 8.2
	Cisco TelePresence SX20	CTS-SX20N-PHD2.5X-K9	CE 8.2
Video Conference Bridge	Cisco Meeting Server	R-VTS-K9	2.2
Video Conference Scheduling	Cisco TelePresence Management Suite	CTI-TMS-SW-K9	15.5
Soft Client	Cisco Jabber for Windows	JAB9-DSK-K9	11.8



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)