Cisco TelePresence MCU 45X0, 53X0 and MCU MSE 8510

Cisco TelePresence Deployment Guide

May 2012

D14962

Contents

Tables

Figures

Introduction

There are many ways to deploy a Cisco TelePresence MCU (referred to in this document as “MCU”) and configure it to allow video calling: this guide provides a number of configuration options that allow the widest capability set and best scalability for the future.

Audience

This document is for Partners or Technical Sales who have a good understanding of all the relevant products and how they work together. As a minimum, you must understand how to install and configure Cisco Unified CM, Cisco VCS, Cisco TMS and Cisco TelePresence MCU as individual products. It is expected that all the components of the solution are already installed and on the network, ready for configuration. Therefore, this document is not a complete installation manual for an end-customer.

Scope

This guide provides step-by-step instructions for deploying the 4500 series MCU and 5300 series MCU devices, and the chassis-based MSE 8510 in the following deployments that are available using Cisco infrastructure**:**

- MCU registered to Cisco TelePresence Video Conferencing Server (Cisco VCS).
- MCU registered to VCS in a deployment using Cisco TelePresence Conductor (Conductor).
- MCU as a media resource in Cisco Unified Collaboration Manager (Unified CM).

(A standalone MCU deployment is not considered, because this is not a preferred deployment type.)

Each deployment is covered in a separate section. For example, the “registered to VCS” scenario explains:

- Cisco VCS configuration required for MCU registration and conference call routing.
- Setting up and configuring the MCU.
- Configuring Cisco TelePresence Management Suite (Cisco TMS) for conference booking and management, if used.
- Verification and troubleshooting instructions.
- Known limitations.

For all deployments, administration guides are referenced for setup that is outside of the scope of MCU deployment, and existing deployment guides are referenced where applicable; for example, the Conductor Deployment Guide.

This guide has been tested against the following software revisions:

Table 1: Software Revisions

Device	Software Revision
Unified CM	8.6.1
VCS	X7.0.1
MCU	4.3
Conductor	XC1.1

Background

MCU overview

An MCU is predominantly used to connect SIP or H.323 based single-screen endpoints into virtual meeting rooms.

The number of ports on the MCU limits the total number of concurrent participants. The number of ports is dependent on the model of MCU/number of blades in the Cisco MSE 8000, the licenses they have applied to them and the mode in which they are running.

See the Cisco website for more detail on the MCU models.

Conference initiation

Conferences can be initiated on an MCU in a number of ways detailed below; however, not all of them are available in every deployment.

Note: A resource used for scheduled conferences should not be also used for ad hoc conferences in order to guarantee port availability for scheduled calls. Therefore Cisco recommends that MCUs used for scheduled conferences are never used for ad hoc calls and separate MCUs are provided for ad hoc conferencing.

Scheduled conferences

Scheduled conferences are pre-booked conferences with a start and end time and a pre-defined set of participants. MCU scheduled conferences are booked via TMS, either using TMS directly or via an integration point such as Microsoft Exchange.

Non-scheduled conferences

There are various means of creating or joining an ad hoc MCU conference. These methods are not supported on MCUs that TMS uses for scheduled calls, and some methods are only supported when the MCU is deployed in a certain way, as detailed below.

The MCU auto attendant

The MCU auto attendant is an interactive menu that is displayed when users dial the MCU's auto attendant number. It can be used to create a new conference or to join one of the existing ones. More than one auto attendant can be configured, each with a unique dial-in number.

Note: The auto attendant is not supported when the MCU is deployed on Unified CM or when using Conductor.

Dynamic escalation conferences

There are two mechanisms that support the ability to escalate from a point-to-point call to a multipoint call hosted on an MCU. Multiway is the VCS based mechanism that can only be initiated by endpoints that support Multiway. Unified CM also supports a mechanism that requires the endpoint to support the conference button in order to escalate the call.

Multiway escalation is only supported when using an ad hoc MCU registered to VCS. Conductor does not fully support all Multiway features. Similarly, escalation using the Unified CM method must be to an MCU configured as a media resource on Unified CM.

Rendezvous conferences

Rendezvous conferences on an MCU are those that a participant can join at any time. These conferences can be configured for individual use, or for communal first-come, first-served conferences.

Rendezvous conferences can be statically configured on an MCU by defining a conference room on the device. It is also possible to dynamically create a conference room so that no pre-configuration is required. Statically configured conferences allow unique settings to be set per conference, whilst dynamic conferences must follow a single template.

When using the MCU with VCS but not Conductor, static conferences must be defined on individual MCUs and therefore are vulnerable to a single point of failure.

When using Conductor, Rendezvous conferences are configured on the Conductor; therefore the conference is never statically defined on a single MCU. This increases conference resilience while maintaining the ability to have unique conference settings.

When an MCU is registered to Unified CM, it is also possible to make Rendezvous conferences. The administrator defines a range of numbers that can be used for Rendezvous conferences, and when users require a conference they press a “Meet Me” button and choose a conference number to start a conference.

Network topology

An MCU causes a concentration of video traffic at its location because each port can have a video call connected to it at up to 4Mbit/s (plus 20% overhead). Therefore, MCUs should be placed at a network location that has enough bandwidth to host these calls.

Cisco recommends that MCUs be placed on the internal network with firewall protection from outside access. For external calling, a Cisco TelePresence VCS Expressway should be used in conjunction with a VCS Control in order to allow video calls to traverse the firewall.

If the second Ethernet port is activated (on the MCU 4500 and 5300 series this requires the Video Firewall Option key), Cisco recommends that this port is also on the internal network and used for purposes such as separating MCU management traffic from MCU video traffic.

For a broader discussion of centralized and distributed architectures see the Cisco TelePresence Multipoint Conferencing Design Guidance document.

Baseline configuration

Some MCU settings are independent of the MCU deployment but can affect the quality experienced. The table below lists the most important of these and the value assumed for the deployments in this guide:

Table 2: Recommended Baseline MCU settings

MCU Setting	Recommended
Maximum video size	Receive Max, transmit Max
Motion / sharpness tradeoff	Balanced (unless 60fps is required, in which case Motion)
Transmitted video resolutions	Allow all resolutions
Default bandwidth from MCU	4.00 Mbit/s
Default bandwidth to MCU	<same as transmit>
Use full screen view for two participants	Enabled
Media port reservation	Disabled (Unless deploying using Unified CM, in which case

MCU Setting	Recommended
	Enabled is required)
ClearVision	Enabled
Video format	NTSC – 30 fps
Video receive bit rate optimization	Enabled
Flow control on video errors	Enabled
Don't see yourself in small panes	Enabled
Don't duplicate in small panes	Enabled
Loudest speaker pane placement behavior	Never duplicate placed participants
Settings > SIP Use local certificate for outgoing connections and registrations (under SIP settings)	Enabled

Securing the MCU

The MCU has a default administrator password that is blank but Cisco recommends that this is changed.

It is only possible to use https when accessing the MCU if the Encryption key is installed. This key is free; however, it is only available in territories that allow encrypted communications.

The Encryption key also enables video calls to be encrypted. This allows AES encryption of H.323 media, SRTP encryption of SIP media and TLS encryption of SIP signaling.

Cisco recommends that the **Advanced account security mode** is enabled in **Settings > Security**. This setting enforces stricter account security (read the MCU online help page before activating this setting to ensure that you understand the consequences). If this setting is not desirable due to the constraints it brings, Cisco recommends that it be activated and then deactivated once in order to hash all MCU passwords (bear in mind that this expires the passwords of all current accounts).

Note: Currently, the MCU is unable to transmit BFCP to a SIP endpoint when the call is encrypted. In this circumstance the MCU composites the content into the main video channel so that the participant can see the content. In order to send BFCP, SIP calls must be unencrypted.

SSL Certificates

The MCU has a local certificate and private key pre-installed and these are used by default when accessing the unit over HTTPS or for TLS encryption. However, Cisco recommends that a new certificate and private key be uploaded (**Network > SSL Certificates**) to ensure security because all MCUs shipped from manufacturing have identical default certificates and keys.

Cascading

If an extremely large conference is required, sometimes the number of MCU ports available on a single MCU is too few. In these cases it is possible to connect one MCU to another in order to create larger conferences. This technique is called cascading and involves dialing from one MCU conference to another MCU conference. Each MCU is seen as an additional participant on the local MCU conference. This technique limits the experience available to participants because they can only see a large proportion of the participants on one or another MCU.

The best user experience is always achieved by using one MCU with all participants connected to that MCU; however, where this is not possible cascading can expand the maximum conference size.

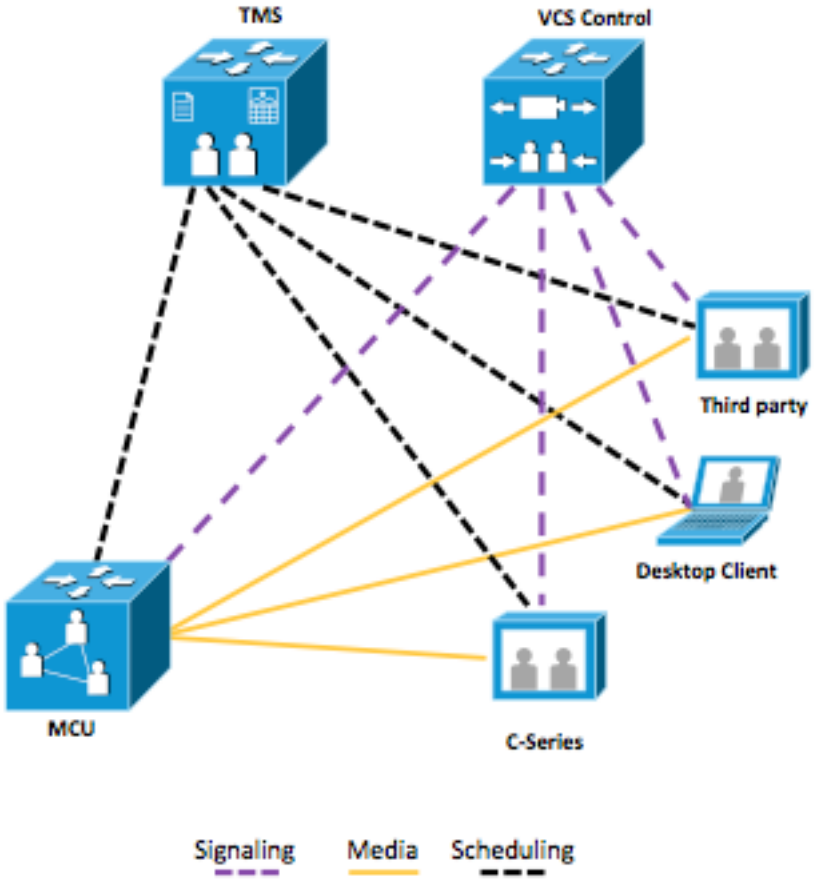
Which deployment?

Each deployment has unique benefits that are described below.

Deploying an MCU using Cisco TelePresence VCS

This deployment uses VCS as the call control device for the MCU (see the figure below). (However in deployments where Unified CM is installed it can be trunked to VCS and devices registered to either call control platform can call the MCU. See the combined MCU section below for more detail.)

Figure 1: VCS deployment: media, signaling and scheduling overview



This deployment allows scheduled conferences and those initiated by the ad hoc methods described in the following table.

Table 3: MCU with VCS deployment capability overview

Conference type	Options
Scheduled	• Using TMS either directly or via an integration, for instance with Microsoft Exchange
Ad hoc	• Auto attendant • Rendezvous – either statically configured on an MCU or dynamically created by MCU on dialing a conference number. • Dynamic escalation – using Multiway

Scalability and resiliency

VCS can support as many MCUs as the total number of VCS registrations and call licenses allow. The MCU can be configured to register individual conferences but higher scale can be achieved by using an H.323 service prefix and a SIP trunk so that all calls can be routed to the MCU without each conference being registered individually. This enables very large deployments of MCUs to be used directly with VCS. VCS can provide load balancing and resiliency across MCUs registered via H.323 only. For more information see the Cisco VCS MCU Connection Using H323 Deployment Guide.

For scheduled calls, TMS can reschedule conferences onto a different MCU if an MCU becomes unavailable before or during a scheduled conference.

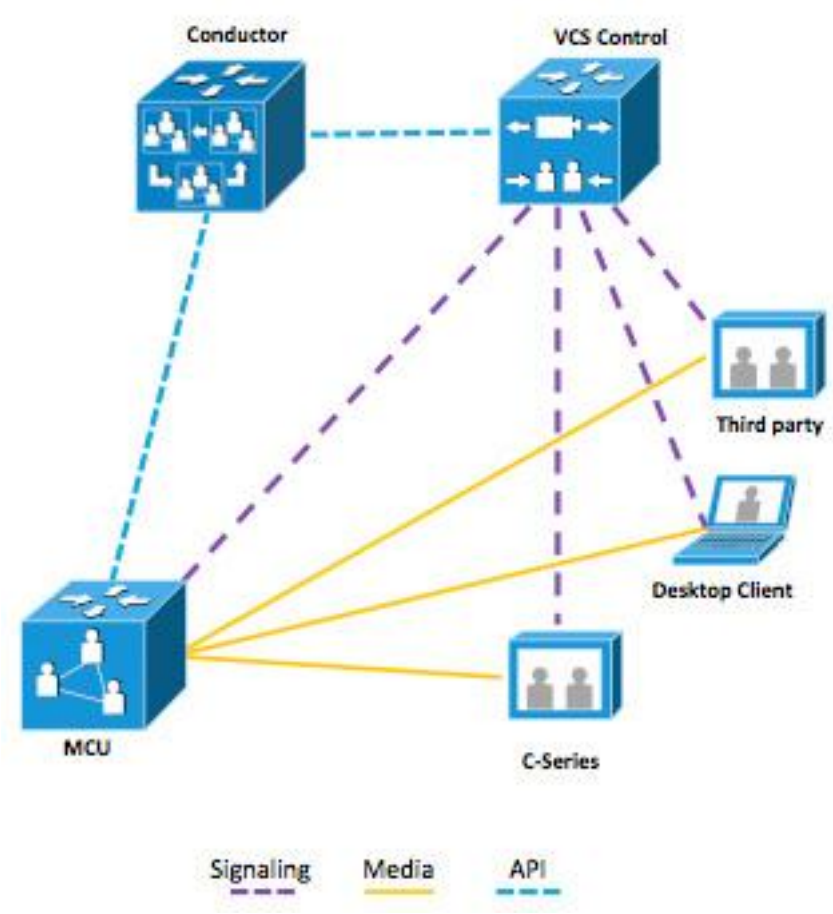
Known limitations

- MCU load balancing and resiliency (through VCS) is limited to H.323 conferences only and is basic in nature.
- MCU cascading is a manual process that requires pre-configuration. It is only necessary to cascade MCUs when a conference with more participants than the maximum on one MCU is required.

Deploying an MCU with Cisco TelePresence Conductor

In this deployment, MCUs are registered to VCS but conferences are controlled by Conductor and are ad hoc only: see the figure and table below for details.

Figure 2: VCS deployment with Conductor: media, signaling and scheduling overview



The supported ad hoc methods are described in the table below.

Table 4: MCU with Conductor deployment capability overview

Conference type	Options
Ad hoc	• Rendezvous – configured on Conductor and dynamically placed on an MCU at conference start. • Dynamic escalation – using Multiway (partially supported)

Scalability and resiliency

A single Conductor or Conductor cluster supports 30 MCUs, and multiple Conductor clusters can be deployed to the same VCS, if required. Conductor also allows seamless growth of conferences beyond the limits of a single MCU's port count by dynamically cascading MCUs to form conferences that span multiple devices.

Conductor provides excellent resiliency by removing the need to configure conferences directly on individual MCUs. In addition, Conductors can be clustered to provide resiliency at the Conductor level.

Known limitations

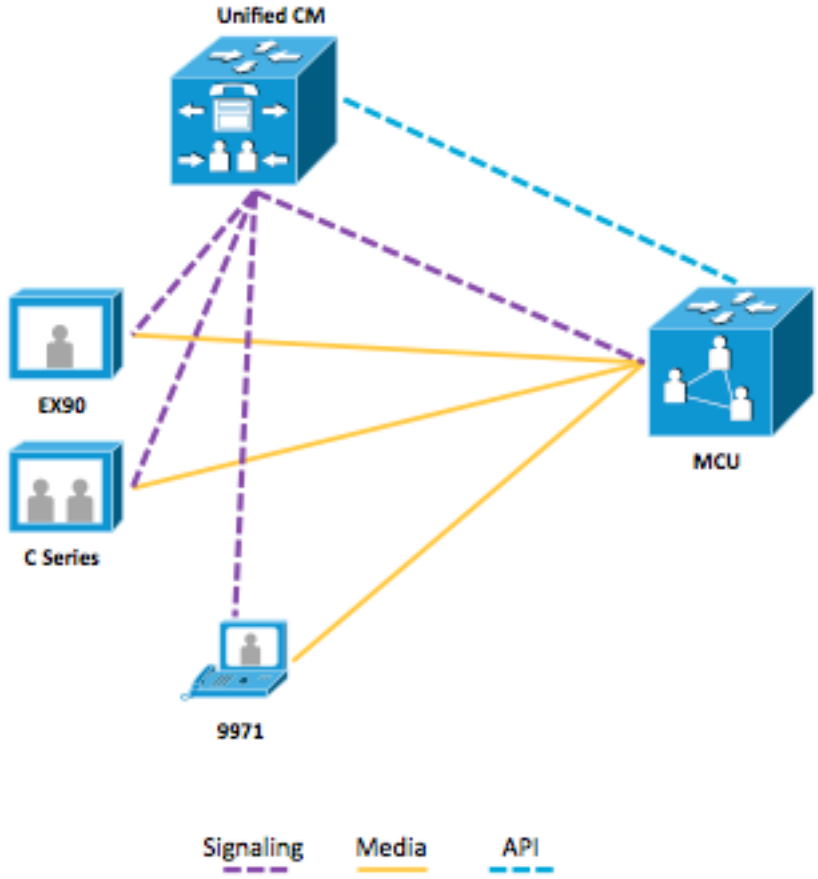
- Limited Multiway support: certain corner cases such as using Multiway during a cascaded call are unsupported.
- Conductor controlled MCUs cannot be used for scheduled conferences.
- If an MCU becomes unavailable while a conference is in progress participants must redial in order to join a new MCU.

Deploying an MCU using Unified CM

In this deployment the MCU is used as a media resource in Unified CM (see the figure below), which also manages the MCU. Unified CM can be trunked to VCS to allow calling from devices registered to either call control platform.

There is no scheduling in this scenario, but devices registered to Unified CM that support the conference softkey can join multiple calls together on an MCU, and Rendezvous conferences can be configured for users to join.

Figure 3: Unified CM deployment: media, signaling and scheduling overview



The supported ad hoc methods are described in the table below.

Table 5: MCU with Unified CM deployment capability overview

Conference type	Options
Ad hoc	• Rendezvous – using “Meet Me” button • Dynamic escalation – using conference button

Scalability and resiliency

CUCM provides excellent resiliency by removing the need to configure conferences directly on individual MCUs. Many MCUs can be added to CUCM in order to provide a large pool of available ports.

Known limitations

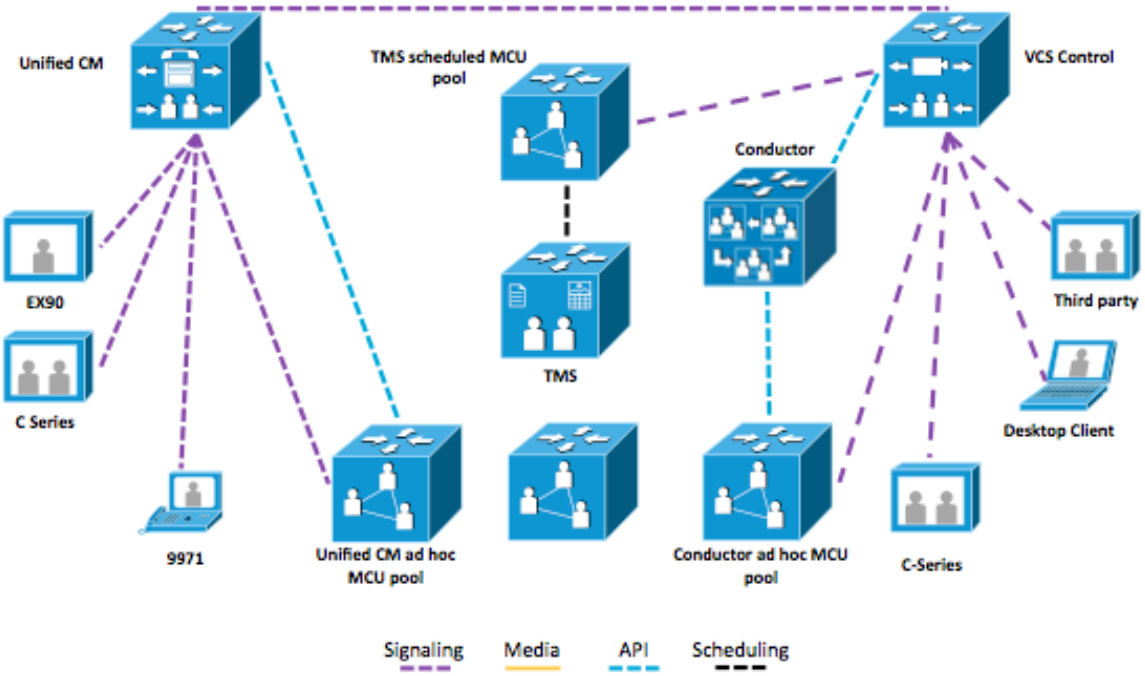
Currently using Unified CM 8.6.1:

- Scheduled conferencing is not supported.
- Cascading is not supported.
- TLS is not supported.
- BFCP not supported.

Combined solution

Although each type of MCU deployment is discussed separately, it is possible to use the three types simultaneously, as shown below.

Figure 4: MCU pools in a combined solution



This solution is viable so long as each type of MCU pool has separate MCU resources to use.

Although endpoints registered to Unified CM do not support escalating a call to Multiway, they can be escalated by an endpoint that supports the mechanism on VCS.

Similarly, although endpoints registered to VCS do not support the “Meet Me” button for rendezvous conferencing, or the conference button for dynamic escalation, they can attend calls on the Unified CM conferencing resource. These VCS-registered endpoints can either call the dial in number or be escalated by an endpoint that supports the mechanism on Unified CM.

Summary of deployment types

Table 6: Choosing your deployment summary

	MCU deployed on VCS	MCU on VCS with Conductor	MCU deployed as a media resource on Unified CM
Minimum Equipment & Versions	MCU 4.2 VCS X7	MCU 4.2 Conductor XC1.1 VCS X7	Unified CM 8.6.1 MCU 4.2
Ad hoc call methods supported	Auto Attendant Rendezvous Multiway	Rendezvous Multiway (partially supported)	“Conference” button Unified CM Rendezvous
Scheduled calls	Supported via TMS	Unsupported	Unsupported
Scalability	Basic scalability	High scalability	High scalability
Resiliency	Basic resiliency	High resiliency	High resiliency
Limitations	In order to have very large	Multiway is partially	TLS is not supported.

	MCU deployed on VCS	MCU on VCS with Conductor	MCU deployed as a media resource on Unified CM
	conferences, manual cascading of MCUs is required.	supported. For example when cascading MCUs a Multiway escalation may fail. Ad hoc only conference creation.	BFCP is not supported. Ad hoc only conference creation.

Deploying an MCU registered to Cisco TelePresence VCS

Deployment overview

This deployment uses VCS as the registration mechanism for the MCU and conferences are scheduled using TMS: separate MCUs are used for scheduling and ad hoc conferencing. Endpoints registered to VCS (or a Unified CM trunked to the VCS) can join MCU calls. All MCUs are provided with a unique prefix in order to route calls correctly and avoid the possibility of identical conference numbers for scheduled or ad hoc conferences. This deployment covers:

Table 7: Overview of covered functionality

Functionality	Description
Management	MCU is manageable from TMS. The management access to the MCU is restricted to the administrator**.**
Ad hoc conferencing	A conference can be: • Created on the fly by dialing a service prefix and a conference numeric identifier. • Statically configured on an MCU • Created and joined via the auto attendant • Created and joined using the Multiway mechanism
Pre-defined permanent conferences	The administrator can create permanent conferences.
Secure conferencing	• Encrypted media and signaling using AES, SRTP and TLS encrypted calls. • Restricted access to call into conference; the caller has to enter a PIN to connect to the conference.

Prerequisites

Before carrying out the configuration of Cisco VCS, Cisco MCU and Cisco TMS ensure that the following prerequisites are met:

- At least one Cisco TelePresence VCS running X7.0 software.
- At least one MCU using 4.2 software for scheduled conferences.
- Additional MCU for ad hoc conferences.
- Cisco TMS running 13.1.2 software.
- Cisco VCS and TMS are installed and configured for base operation using the relevant deployment guide (listed below).
- MCUs used start with the base settings covered in Table 2 above.
- Cisco TMS has enough system licenses to add the relevant number of MCUs.

Document List

VCS Deployment Guide

Deploying VCS with Unified CM

Deploying MCUs with Resilience and Resiliency using H.323

Configuring Multiway

Summary of procedure

The process consists of:

1. Designing the dial plan
2. Configuring zones and a domain in the Cisco VCS for the MCU.
3. Installing and configuring the MCU.
4. Configuring Cisco TMS for management and scheduling of the MCU.

Configuration Steps

Step 1: Dial plan

The dial plan of a video deployment should be considered early on to ensure that a scalable easy-to-use solution is deployed. This dial plan is a conceptual one that is not defined in any one place but on a variety of systems: therefore it is important to follow the same guidelines throughout a deployment. Recommendations that fulfill these core requirements are provided; however some deployments may have specific requirements that require a different implementation.

Each conference has a numeric identifier. When a conference is booked using Cisco TMS, Cisco TMS uses a pre-configured number range to create the conference. This registers numeric identifiers on the Cisco VCS, so that participants can dial into the conference. For a scheduled conference, Cisco TMS can configure the MCU to initiate calls to the participants (through the Cisco VCS); this is most commonly done as a dial out call from the MCU to the endpoint.

All the conferences running on a specific MCU can be addressed using a number with a prefix assigned from the address plan, for example: 81xxx, where 8 is the reserved prefix for data centre resources and 1 is the prefix for a specific MCU. The same conference can also be reached using a Unified Resource Identifier (URI), for example, xxx@mcu1.cisco.com, both on SIP and H.323 (interworked) signaling protocols. (It is also possible to register multiple MCUs using the same prefix in order to provide load balancing for ad hoc MCU conferences.)

Using a prefix allows a simplified dial plan where users need only dial <prefix><conference number>@domain, whether using SIP or H.323.

The table below shows an example of an address plan for conferencing services. The range allocated to ad hoc and permanent conferences can be divided as required. In both cases, a conference address can be used across multiple sessions; for example, 81555 can be used for a specific team's shared meetings. Pre-registering a conference allows persistent tailoring of layouts/settings across sessions.

Table 8: Overview of an address plan using five digits

Prefix/suffix	Range	Purpose	Dialing examples
8 – Central resources **1 – Cisco MCU/MCU pool number**	000 - 010	Auto attendant calls	H.323: 81001 SIP: 001@mcu1.cisco.com or 81001@cisco.com Interworked from H.323 -> SIP: 81001@mcu1.cisco.com
	011 - 909	Ad hoc/preconfigured conferences	H.323: 81123 SIP: 123@mcu1.cisco.com or 81123@cisco.com Interworked from H.323 -> SIP: 123@mcu1.cisco.com
	910 - 999	Reserved for Multiway	Never dialed directly
8 – Central resources **2 – Cisco MCU number**	100-999	Scheduled conferences	Only for dial-in (TMS will make the MCU dial out by default):

Prefix/suffix	Range	Purpose	Dialing examples
			H.323: 82812 SIP 812@mcu2.cisco.com or 82812@cisco.com

Step 2: Configuring the Cisco VCS

The Cisco VCS Control should be deployed according to the recommendations of the *Cisco VCS Base configuration* or the *Unified CM with VCS deployment guide* (both found at *http://www.cisco.com/en/US/partner/products/ps11337/products_installation_and_configuration_guides_list.html*). Configuring the Cisco VCS ready for the MCU installation requires the following steps:

1. Configuring the MCU SIP sub domain.
2. Creating an MCU SIP zone.
3. Configuring search rules.
4. Optional: Configuring Multiway.

Note: This section is here in order to configure SIP calls to reach the MCU. H.323 calling is handled via H.323 prefixes (configured in a subsequent section within the MCU). The configuration for these steps is described in the tables below.

Configuring the MCU SIP domain

The MCU registers to the Cisco VCS using a sub-domain, e.g. mcu1.cisco.com. Therefore, the Cisco VCS has to be configured with a SIP domain name that matches the MCU sub-domain; otherwise the Cisco VCS rejects the SIP registration request from the MCU.

Configure a SIP domain:

1. Go to **VCS configuration > Protocols > SIP > Domains**.
2. Click **New**.
3. Enter the domain name into the Name field:

Table 9: Settings for SIP domain

VCS Setting	Value	Comment
Name	MCU fully qualified domain name (FQDN)	Example: mcu1.cisco.com or mcu1.cisco.net

4. Click **Create domain**.

Creating the MCU SIP zone

To provide the same call behavior for SIP as for H.323, configure the Cisco VCS with a SIP neighbor zone pointing to the MCU. (When using H.323, the MCU registers a service prefix; the same does not exist for SIP.) Configure the neighbor zone with a pattern match equal to the H.323 service prefix. To allow ad hoc calls to the MCU using a URI (for example, <conference ID>@mcu1.cisco.com), configure the SIP zone with a suffix match with the pattern string @mcu1.cisco.com.

This guide assumes that all video infrastructure devices that can be dialed use the 8 prefix according to the address plan. The first MCU in a video network should then be assigned the service prefix 1, thus giving the MCU prefix 81.

Create a SIP zone on the VCS as follows:

1. Go to **VCS configuration > Zones**.
2. Click **New**.
3. Configure the fields on the VCS as follows:

Table 10: Settings for creating a SIP zone on a Cisco VCS

VCS Setting	Value	Comment

VCS Setting	Value	Comment
Name	Zone name	Example: ToMCU1
Type	Neighbor	
Hop count	15	
H.323 Mode	Off	
SIP Mode	On	
SIP Port	5061	If you don't use encryption, set this to 5060.
SIP Transport	TLS	If you don't use encryption, set this to TCP.
SIP TLS verify mode	Configure the TLS verification settings according to your security policy	
Authentication policy	Configure the authentication settings according to your authentication policy	Refer to Authentication Policy configuration options in the VCS online help for full details.
Peer 1 address	IP address or FQDN of MCU	Example: mcu1.cisco.com
Zone profile	Infrastructure device	

4. Click **Create zone**.

Configuring search rules

Search rules decide which calls will be routed to the MCU SIP zone.

Create a search rule on the VCS as follows:

1. Go to **VCS configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields on the VCS as follows:

Table 11: Settings for creating a search rule on a Cisco VCS

VCS Setting	Value	Comment
Rule name	Descriptive name for the search rule	Example name: MCU1 zone – no domain
Description	Description of the rule	Example name: Search MCU1 zone for SIP conferences
Priority	50	The match priority must be the same as the local zone full URI
Source	Any	
Request must be authenticated	Configure the authentication settings according to your authentication policy	Refer to Authentication Policy configuration options in the VCS online help for full details.
Mode	Alias pattern match	
Pattern type	Regex	
Pattern string	<mcu service prefix>(\d+)@.*	It is expected that Business to Business calls will require a full E.164 to dial, e.g. +1753810001@companyb.com
Pattern behavior	Replace	
Replace string	\1@<mcu-fqdn>	Example: \1@mcu1.cisco.com **Note**: Using the FQDN is critical
On successful match	Stop	

Target	<Name of zone configured above>	Example: mcu1
State	Enabled	

4. Click **Save**.

This search rule will match SIP calls made using the full number with prefix and manipulate the URI to what the MCU expects.

Example:

SIP call: 801111@cisco.com

This matches the search rule for MCU1 which has prefix 80, but the MCU expects to receive a call to conference 1111@mcu1.cisco.com; therefore, the search rule makes this alteration before passing the call to the MCU zone.

This rule allows the caller to dial the same number whether they use H.323 or SIP and also allows for the automatic appending of the endpoint domain (which an endpoint will do if the user does not specify a domain when they make a call).

Create another search rule on the VCS as follows:

1. Go to **VCS configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields on the VCS as follows:

Table 12: Settings for creating a search rule on a Cisco VCS

VCS Setting	Value	Comment
Rule name	Descriptive name for the search rule	Example name: MCU1 zone – SIP domain
Description	Description of the rule	Example name: Search MCU1 zone for SIP conferences
Priority	50	The match priority must be the same as the local zone full URI
Source	Any	
Request must be authenticated	Configure the authentication settings according to your authentication policy	Refer to Authentication Policy configuration options in the VCS online help for full details.
Mode	Alias pattern match	
Pattern type	Suffix	
Pattern string	@<mcu-fqdn>	Example: @mcu1.cisco.com
Pattern behavior	Leave	
On successful match	Continue	
Target zone	Name of zone configured above	Example: MCU1
State	Enabled	

4. Click **Save**.

This search rule matches SIP calls made using the domain of the MCU; this is the call string that TMS will use for scheduled conferences, for example.

Example:

SIP call: 1111@mcu1.cisco.com

This matches the search rule for MCU1 which has domain mcu1.cisco.com, but the MCU expects to receive a URI in this format and so no alteration is made before the call is sent to the MCU zone.

Optional: Configuring Multiway

Enable Multiway on the VCS as follows:

1. Go **Applications > Conference Factory**.
2. Configure the fields on the VCS as follows:

Table 13: Settings for enabling Multiway

VCS Setting	Value	Comment
Mode	On	
Alias	URI of this Conference Factory (this is the Multiway ID that is configured into endpoints, that they call to initiate a Multiway conference)	Example: multiway@cisco.com
Template	A template for a URI that will route calls to an MCU ad hoc conference.	Example: 819%%@cisco.com **Note**: These calls will get routed to MCU based on the search rules configured above.
Number range start and end	A range that matches your dial plan.	Example: 10-99

3. Click **Save**.

To ensure that the Multiway request is processed quickly, configure a search rule on the VCS as follows:

1. Go to **VCS configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields on the VCS as follows:

Table 14: Settings for creating a Multiway search rule on a Cisco VCS

VCS Setting	Value	Comment
Rule name	Descriptive name for the search rule	Example name: Multiway Zone
Description	Description of the rule	Example name: Search Multiway Zone
Priority	1	To ensure the lowest possible latency before the call is initiated
Source	Any	
Request must be authenticated	Configure the authentication settings according to your authentication policy	Refer to Authentication Policy configuration options in the VCS online help for full details.
Mode	Alias pattern match	
Pattern type	Exact	
Pattern string	Conference Factory Alias as configured under Applications > Conference Factor	Example: multiway@cisco.com
Pattern behavior	Leave	
On successful match	Stop	
Target zone	LocalZone	
State	Enabled	

4. Click **Save**.

There is a detailed Multiway Deployment Guide.

Multiway should only be used with MCUs that are configured for ad hoc usage. Using Multiway to bring participants into an MCU used for scheduled calls can cause some scheduled calls to fail due to lack of resource.

Endpoints must be configured with Multiway and the same conference factory Alias as configured above. See the endpoint Administrator guides for details.

Step 3: Installing and configuring the MCU

Installing and configuring the MCU requires the following steps:

1. Installing feature keys.
2. Configuring network settings.
3. Configuring encryption settings.
4. Configuring conference settings.
5. Configuring gatekeeper settings.
6. Configuring SIP settings.
7. Optional: Pre-configuring conferences.
8. Optional: Configuring auto attendant.
9. Optional: Configuring custom SSL certificates.

The configuration for these steps is described below.

Installing feature keys

Install MCU feature keys as follows:

1. Go to **Setting > Upgrade**.
2. Ensure that the following keys are present or install them:

Table 15: Required MCU keys

Key	Name	Usage
Activation	Activation key	Required to activate the MCU
Encryption	Encryption option key	This is only required if the deployment uses encryption.

3. Click **Update features.**

Note: The 8510 also requires port licenses to be applied using the Supervisor before it can function.

Configuring network settings

Configure IP settings on the MCU as follows:

1. Go to **Network > Port A**.
2. Configure the fields on the MCU as follows:

Table 16: IP settings for the MCU

MCU Setting	Value	Comment
IP configuration	Manual	
Manual configuration	IPv4 or IPv6 address, subnet mask, default gateway	

3. Click **Update IP configuration**.

Configure DNS settings on the MCU as follows:

1. Go to **Network > DNS**.

2. Configure the fields on the MCU as follows:

Table 17: DNS settings for the MCU

MCU Setting	Value	Comment
DNS configuration	Manual	
Host name	MCU hostname	Example: mcu1
Name server	IP of DNS server	
Domain name (DNS suffix)	Domain	Example: cisco.com

3. Click **Update DNS configuration**.

Configure network services on the MCU as follows:

1. Go to **Network > Services**.
2. Configure the fields on the MCU as follows:

Table 18: Services settings for the MCU

MCU Setting	Value	Comment
Secure web	Enabled port 443	Encryption Key Required
Encrypted SIP (TLS)	Enabled port 5061	Encryption Key Required
SNMP	Enabled port 161	

3. Click **Apply changes.**

Configure SNMP on the MCU as follows:

1. Go to **Network > SNMP**.
2. Configure the fields on the MCU as follows:

Table 19: SNMP settings for the MCU

MCU Setting	Value	Comment
Name	MCU name	Example:MCU1
Enable traps	Enabled	
Trap receiver address 1	IP address of TMS	
RO community	Community name of TMS	Default: public
RW community	Community name of TMS	Default: private
Trap community	Community name of TMS	Default: public

3. Click **Update SNMP settings**.

Configuring encryption

Configure encryption on the MCU as follows:

1. Go to **Settings > Encryption**.
2. Configure the fields on the MCU as follows:

Table 20: Encryption settings on the MCU

MCU Setting	Value	Comment
Encryption status	Enabled	
SRTP encryption	All transports	Encryption key required. This will encrypt SIP media wherever possible. You may choose to set this to “Secure transports (TLS) only”, in which case SIP media will

MCU Setting	Value	Comment
		only be encrypted when the signaling is TLS encrypted.

3. Click **Apply changes**.

Configuring conference settings

Configure conference settings on the MCU as follows:

1. Go to **Settings > Conferences**.
2. Configure the fields on the MCU as follows:

Table 21: Conference settings on the MCU

MCU Setting	Value	Comment
Incoming calls to unknown conferences or auto attendants	Create new ad hoc conference	This setting can be set to "Disconnect caller" if the MCU is to be used for scheduled calls only.
Use conference name as the called ID	Enabled	
Require H.323 gatekeeper callers to enter PIN	Enabled	Used only if a PIN is to be configured on the conference
Time to wait when setting up ad hoc conference PIN	Never configure PIN	

3. Click **Apply changes**.

Configuring H.323 gatekeeper settings

Configure H.323 on the MCU:

1. Go to **Settings > H.323**.
2. Configure the fields on the MCU as follows:

Table 22: H.323 settings on the MCU

MCU Setting	Value	Comment
H.323 gatekeeper usage	Required	
H.323 gatekeeper address	FQDN of the VCS or VCS cluster	DNS A record must resolve to the VCS IP address
Gatekeeper registration type	MCU (standard)	For the VCS to be able to route ad hoc calls to the correct MCU when there is more than one MCU registered with the same prefix
H.323 ID to register	URI	Example: mcu1@mcu1.cisco.com **Note**: The domain must match the FQDN configured in the VCS under SIP domains
Prefix for MCU registrations	Prefix	The prefix for MCU registration and the MCU service prefix have to be the same, e.g. 81
MCU service prefix	Prefix	The prefix for MCU registration and the MCU service prefix have to be the same, e.g. 81
Allow numeric ID registration for conferences	Enabled	
Send resource availability indications	Optional: Enabled Video ports: number value	If using the H.323 load balancing capabilities of the VCS this setting is required to inform the VCS when not to route calls to the device.

3. Click **Apply changes**.

Configuring SIP registrar settings

Configure SIP on the MCU:

1. Go to **Settings > SIP**.
2. Configure the fields on the MCU as follows:

Table 23: SIP settings on the MCU

MCU Setting	Value	Comment
SIP registrar usage	Enabled	
SIP registrar domain	MCU FQDN	Example: mcu1.cisco.com
SIP registrar type	Standard SIP	This option is not available on the 5300 series.
Username	String	Example: mcu1 **Note**: Should match the H.323 URI before the @
Password	None	Only required if the VCS requires authentication for registration
Allow numeric ID registration for conferences	Enabled	
SIP proxy address	FQDN of VCS or VCS cluster	DNS A record must resolve to the VCS IP address
Outgoing transport	TLS	Encryption Key required, otherwise use TCP.
Use local certificate for outgoing connections and registrations	Enabled	When using TLS ensure this is enabled.

3. Click **Apply changes**.

Optional: Pre-configuring static rendezvous conferences

This step must be repeated for each pre-configured conference. A pre-configured conference is always available (as long as the MCU that it is configured on is available and has resource) and maintains a consistent configuration for conference users, e.g. conference PIN.

To pre-configure a conference:

1. Go to **Conferences > Conference list**.
2. Click **Add new conference**.
3. Configure the fields on the MCU as follows:

Table 24: Settings for a preconfigured conference

MCU setting	Value	Comment
Name	Name of conference	Name that identifies the conference.
Numeric ID	Unique three digit numeric identifier from address plan	Used for dialing into the conference. This ID should not include the MCU registration prefix and should be taken from the range in the address plan allocated to preconfigured conferences.
Numeric ID registration – H.323 gatekeeper	Optional	If the MCU is configured as above then the conference does not have to be registered in order for a call to reach the conference.
Numeric ID registration – SIP registrar	Optional	If the MCU is configured as above then the conference does not have

MCU setting	Value	Comment
		to be registered in order for a call to reach the conference.
Permanent	Enabled (optional)	If this is not enabled the conference will be available for as long as the duration configured.

4. Click **Add conference**.

Note: It is not necessary to configure each conference as above. It is also possible to use MCU prefixing to automatically generate generic ad hoc conferences on the MCU. For example, if an MCU is configured as above with a prefix of 81, when a user dials 81123, the MCU creates conference 123 automatically if the conference does not exist already. Using this method, no per conference setup is necessary; however every conference uses the default ad hoc template.

Optional: Configuring the auto attendant

This step can be repeated for up to twenty auto attendants as is required by the deployment. An auto attendant is always available (as long as the MCU it is configured on is available and has resource). Depending on the configuration of the auto attendant users can join or create conferences from the auto attendant page.

To configure an auto attendant:

1. Go to **Conferences > Auto attendants**.
2. Click **Add new auto attendant**.
3. Configure the fields on the MCU as follows:

Table 25: Settings for an auto attendant

MCU setting	Value	Comment
Name	Name of auto attendant	Name that identifies the auto attendant.
Numeric ID	Unique three digit numeric identifier from address plan	Used for dialing into the conference. This ID should not include the MCU registration prefix and should be taken from the range in the address plan allocated to auto attendants. e.g. 001
Numeric ID registration – H.323 gatekeeper	Optional	If the MCU is configured as above then the conference does not have to be registered in order for a call to reach the conference.
Numeric ID registration – SIP registrar	Optional	If the MCU is configured as above then the conference does not have to be registered in order for a call to reach the conference.
Creation of new conferences	Enabled (optional)	If this is not enabled users will only be able to use the auto attendant to join existing calls.
Access to ad hoc conferences	Enabled (optional)	If this is not enabled users will only see conferences that have been preconfigured on the MCU
All scheduled conferences	Enabled (optional)	If this is not selected it is possible to specify which conferences will appear in the auto attendant.

4. Click **Add auto attendant**.

Optional: Configuring SSL certificates

Cisco recommends adding a custom local certificate and private key to the MCU. The VCS must also have the relevant certificates installed in order to negotiate encrypted connections. See the VCS Certificate Creation and Use Deployment Guide for details:

Configure an MCU with custom local SSL certificates as follows:

1. Go to **Network > SSL certificates**.
2. Configure the fields on the MCU as follows:

Table 26: Settings for custom local SSL certificates

MCU setting	Value	Comment
Certificate	Choose your local server certificate file (PEM format)	
Private key	Choose your local private key file (PEM format)	
Private key encryption password	Add your Private Key password	If you did not use an encrypted private key then leave this blank.

3. Click **Upload certificate and key**.

Configure an MCU with Trust store SSL certificates as follows:

1. Go to **Network > SSL certificates**.
2. Configure the fields on the MCU as follows:

Table 27: Settings for Trust Store SSL certificates

MCU setting	Value	Comment
Trust store	Choose your trust store or CA file (PEM format)	If you want to add multiple trusted authorities you can add multiple certificates to the .PEM file by copying and pasting certificates together.
Certificate verification settings	Configure the certificate verification settings according to your security policy	

3. Click **Upload trust store.**
4. Click **Apply changes**.
5. Restart the MCU in order for these changes to take effect.

Step 4: Configuring Cisco TMS

After having installed and configured the MCU, the administrator must perform the following steps in Cisco TMS:

1. Adding the MCU to Cisco TMS.
2. Editing the extended MCU settings.
3. Setting external MCU usage.

Adding the MCU to TMS

Add the MCU to Cisco TMS in the normal manner, remembering to select “Discover Non-SNMP Systems” in Advanced Settings.

Editing the extended MCU settings

Still logged in to Cisco TMS as a global administrator,

1. Click on the newly added MCU,
2. Select the Settings tab, then select the Extended MCU Settings tab.
3. Complete the relevant section below based on the type of MCU that you are adding.

For scheduled MCUs

To allow bookings for scheduled MCUs:

1. Go to **System > Navigator > MCU > Settings**.
2. Configure the field on TMS: as follows

Table 28: Allow bookings for scheduled MCUs on TMS

TMS Setting	Value	Comment
Allow bookings	Enabled	

3. Click **Save.**

Set the scheduled conference number range for the MCU on TMS:

1. Go to **System > Navigator > MCU > Settings**.
2. Configure the fields on TMS as follows:

Table 29: Extended settings for scheduled MCUs on TMS

TMS Setting	Value	Comment
First meeting id	100	In order to make sure the ID length matches the dial plan, 100 is the lowest figure that TMS accepts.
Meeting id Step	1	

3. Click **Save.**

For ad hoc MCUs

Disallow bookings for non scheduled MCUs as follows:

1. Go to **System > Navigator > MCU > Settings > Edit Settings**.
2. Configure the field on TMS as follows:

Table 30: Disallow bookings for scheduled MCUs on TMS

TMS Setting	Value	Comment
Allow bookings	Disabled	

3. Click **Save.**

Setting preferred type MCU usage

To prefer the use of external MCUs rather than endpoint multisite when scheduling on TMS:

1. Go to **Administrative Tools > Configuration > Conference Settings**.
2. Configure the field on TMS: as follows

Table 31: Settings for preferred MCU type usage

TMS Setting	Value	Comment
Preferred MCU Type in Routing	TANDBERG Codian MCU	Default

3. Click **Save.**

Verifying the implementation

The table below summarizes the most important tests for verifying that the *MCU deployment has been* implemented correctly.

Table 32: Test table for verifying the implementation

Test group	Purpose	Tests
Management	Verify proper management control	Log in to Cisco TMS as an administrator and verify that: 1. Cisco TMS is in contact with the MCU when selecting the MCU from the Infrastructure folder (**Note**: verify if you can set Extended Settings). 2. The Conference Control Center shows access to the MCU (to see the MCU in the Conference Control Center, select Show MCU).
Ad hoc conferencing	Verify ad hoc conferences	Dial into the MCU with a number within the ad hoc range and verify that: 1. Dialing in using both H.323 and SIP reaches the same conference. 2. Calls to and from the MCU are encrypted if your deployment is configured for encryption.
Permanent/centrally booked conferencing	Verify configured conferences on the MCU	Use the web interface to set up a conference in the permanent/centrally booked conferencing range. Set a special layout, and verify that the correct conference layout is seen.
Scheduled conferences	Verify that scheduled conferences are working	Log in to Cisco TMS as an administrator and schedule a conference with at least two dial-out participants, one dial-in participant, and one external participant. Verify that: 1. All participants are automatically connected with encryption. 2. The conference verification email is sent out correctly to the user who made the booking. 3. The conference can be dialed using the H.323 number and the SIP URI found in the email (also seen in the confirmation message when booking).

Deploying an MCU with Cisco TelePresence Conductor

Deployment overview

This deployment requires that VCS be present and although the MCU is still registered to VCS, the configuration of VCS and the MCU are different. Conductor adds unique benefits such as conference virtualization, rather than defining conferences directly on MCUs they are defined on Conductor. Conductor also offers better resiliency and scalability than directly registering an MCU to VCS.

This deployment is detailed in the Cisco TelePresence Conductor Deployment Guide, listed below and therefore is not detailed in this document.

Document List

Conductor Deployment Guide.

Deploying an MCU as a Unified CM media resource

Deployment overview

This deployment uses the media resource management capabilities of Unified CM in order to provide ad hoc calling capabilities. Calls can either be dynamically escalated using the conference button or Rendezvous based using the “Meet Me” button.

Step-by-step configuration is available in the Unified CM Administrator and System guides, listed below. However an overview of the deployment process follows.

Document List

Overview: Conference bridges section of the Unified CM System Guide

Configuring the MCU: Conference Bridge Configuration section of the Unified CM Administrator Guide

Configuring a media resource group list: Media Resource Management section of the Unified CM System Guide

How to setup a “Meet Me”: Conference Bridge Configuration Checklist in the Unified CM System Guide

Configuration Steps

Step 1: On the MCU, configuring settings

1. Go to **Settings > Conferences**.
2. Configure the fields on the MCU as follows:

Table 33: MCU settings when registered to Unified CM

MCU Setting	Value	Comment
Media port reservation	Enabled	
Incoming calls to unknown conferences or auto attendants	Disconnect caller	

3. Click **Apply changes**.

Step 2: On Unified CM, configuring conference features

To configure conference features such as the maximum number of participants:

1. Go to **System > Service Parameters**.
2. Select the relevant Unified CM Server.
3. Select the **Cisco CallManager (Active)** as the service.
4. Select **Advanced** to show advanced options.
5. Configure the **Clusterwide Parameters (Feature - Conference)** section as required.

Step 3: On Unified CM, adding the MCU

Add the MCU to Unified CM as a manageable device as follows:

1. Go to **Media Resources > Conference Bridge**.
2. Click **Add New**.
3. Select **Conference Bridge Type** as **Cisco TelePresence MCU**.
4. Enter relevant fields and click **Save**.

Step 4: On Unified CM, configuring a media resource group list

1. Go **Media Resources > Media Resource Group**.
2. Click **Add New**.
3. Choose a name and move the MCU(s) into the **Selected Media Resources** area.
4. Click **Save**.
5. Go to **Media Resources > Media Resource Group List**.
6. Click **Add New**.
7. Choose a name and move the created Media Resource Groups into the **Selected Media Resource Groups** area.
8. Click **Save**.

Step 5: On Unified CM, assigning a Media Resource Group List to a device

1. Go to **Device > Phone**.
2. Select a device.
3. Choose the **Media Resource Group List** that you created earlier.
4. Click **Save**.

Optional: On Unified CM, setting up a “Meet Me” service

If a rendezvous service is required, this can be setup as per the documentation list above.