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

Deployment Guide

4.5

March 2015

Contents

Introduction

The Cisco TelePresence MCU (referred to in this document as "MCU") supports several deployment types, from a single device standalone model to large scale deployments with Cisco TelePresence Video Communication Server (Cisco VCS) or Cisco Unified Communications Manager (Unified CM). This guide outlines the Cisco recommended deployment models.

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 Communications Manager, Cisco TelePresence Video Communication Server, Cisco TelePresence Management Suite, 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 instructions for deploying the MCU 4500 Series and MCU 5300 Series devices, and the chassis-based MSE 8510 in the following deployments that are available using Cisco infrastructure:

- MCU registered to Cisco TelePresence Video Communication Server (Cisco VCS).
- MCU behind Cisco TelePresence Conductor (TelePresence Conductor), which can be used with either Unified CM or Cisco VCS.
- MCU as a media resource in Cisco Unified Communications Manager (Unified CM).
- MCU trunked to Unified CM for rendezvous conferencing.

(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 Cisco 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 TelePresence Conductor Deployment Guide.

This guide has been tested against the following software revisions:

Table 1: Software Revisions

Device	Software Revision
Unified CM	10.0
VCS	X8.5
MCU	4.5
Conductor	XC 3.0
TMS	14.5

Background

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 also be used for non-scheduled conferences to guarantee port availability for scheduled calls. Therefore we recommend that MCUs used for scheduled conferences are never used for non-scheduled calls and separate MCUs are provided for non-scheduled 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 Cisco TMS, either using Cisco TMS directly or via an integration point such as Microsoft Exchange.

Non-scheduled conferences

There are various means of creating or joining a non-scheduled MCU conference. These methods are not supported on MCUs that Cisco 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 MCUs auto attendant number. It can be used to create a new conference or to join one that already exists. 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 used as a media resource with Unified CM or when using TelePresence Conductor.

Dynamic escalation conferences

When an MCU is registered to Cisco VCS the Multiway mechanism can be used, however it can only be initiated by endpoints that support Multiway. When an MCU is used as a media resource with Unified CM

dynamic escalation can only be initiated by endpoints that support the configuration of a conference button which is used to escalate the call.

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 Cisco VCS but not TelePresence 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 TelePresence 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.

These conferences can be configured in a similar way to an MCU registered to Cisco VCS or trunked to Unified CM, either by predefining the conference number and configuration or by allowing the MCU to dynamically create the 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 IP overhead, typically 20%). Therefore, MCUs should be placed at a network location that has enough bandwidth to host these calls.

We recommend that MCUs be placed on the internal network with firewall protection from outside access. For external calling, a Cisco VCS Expressway should be used in conjunction with a Cisco 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), we recommend that this port is also connected to an 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.

For a broader discussion of system components and architecture see Cisco Collaboration 9.x Solution Reference Network Design 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	Favor Motion
Transmitted video resolutions	Allow all resolutions
Default bandwidth from TelePresence MCU	4.00 Mbit/s
Default bandwidth to TelePresence MCU	<same as transmit>
Use full screen view for two participants	Enabled
Media port reservation	Disabled (Unless deploying as a media resource using Unified CM, in which case 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
Conferences > Templates > Top Level, Adaptive Gain Control on Join	Enabled

Securing the TelePresence MCU

The MCU has a default administrator password that is blank. Cisco recommends that a secure password is added before the product is used.

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.

We recommend 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).

SSL Certificates

The MCU has a self-signed local certificate and private key pre-installed and these are used by default when accessing the unit over HTTPS or for TLS encryption. However, we recommend 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.

Note: Cascading is only supported when using H.323 to call between MCUs and should be set up using the API (see the API Reference Guide for more information). This can be done using TelePresence Conductor which will dynamically cascade MCUs as and when needed which provides a much improved administrator and user experience compared to manually cascading.

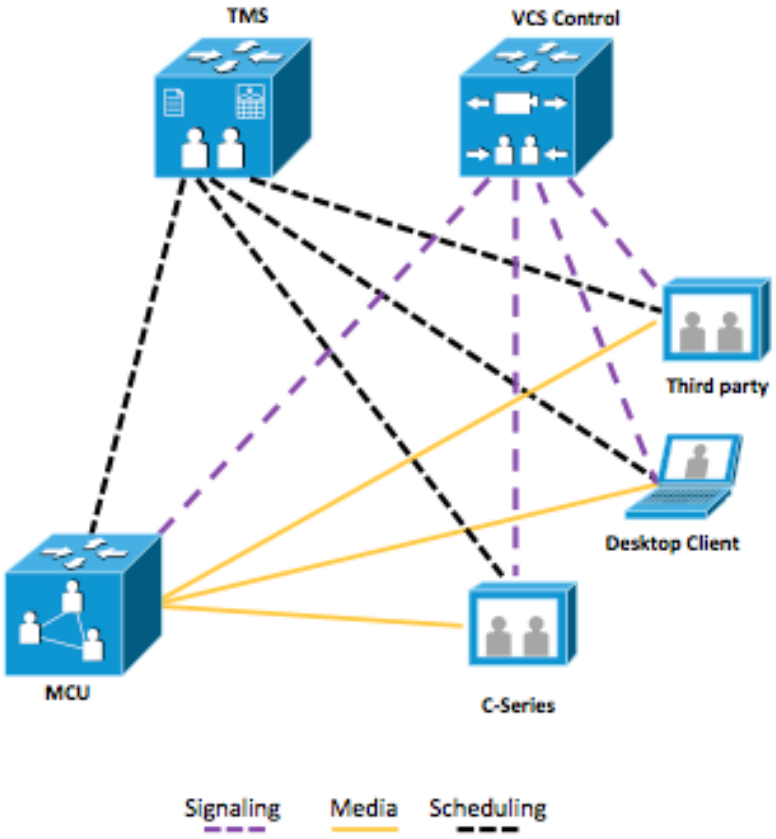
Which deployment?

Each deployment has unique benefits that are described below.

Deploying an MCU using Cisco TelePresence Video Communication Server

This deployment uses Cisco VCS as the call control device for the MCU (see the figure below). In deployments where Unified CM is used in conjunction with Cisco VCS, devices registered to Unified CM can use these conferencing devices via a SIP trunk between Unified CM and Cisco VCS.

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



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

Table 3: MCU with Cisco VCS deployment capability overview

Conference type	Options
Scheduled	■ Using Cisco TMS either directly or via an integration, for instance with Microsoft Exchange
Non-scheduled	■ Auto attendant ■ Rendezvous – either statically configured on an MCU or dynamically created by MCU on dialing a conference number. ■ Dynamic escalation – using Multiway Note: non-scheduled MCU not shown in the figure above.

Scalability and resiliency

Cisco VCS can support as many MCUs as the total number of Cisco 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 TelePresence MCUs to be used directly with Cisco VCS. Cisco VCS can provide load balancing and resiliency across MCUs registered via H.323 only. For more information see Cisco VCS MCU Connection Using H323 Deployment Guide.

For scheduled calls, Cisco 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 Cisco 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 of any one MCU is required.

Deploying an MCU with Cisco TelePresence Conductor

In this deployment MCUs are placed behind TelePresence Conductor and TelePresence Conductor can be used with either Cisco VCS or Unified CM. Conferences are controlled by TelePresence Conductor.

Figure 2: Cisco VCS deployment with TelePresence Conductor: media and signaling overview

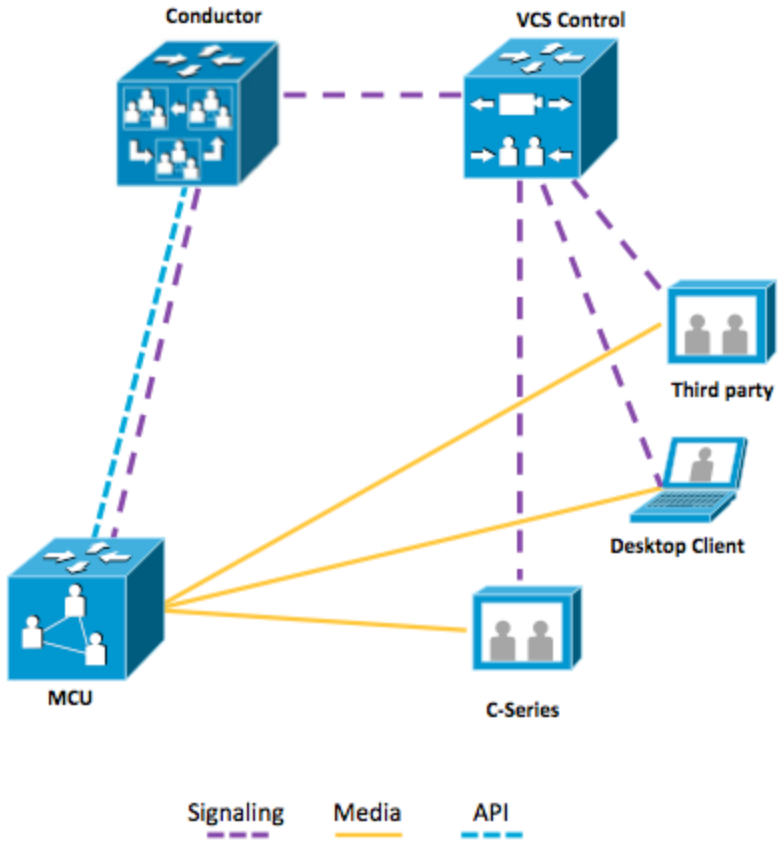
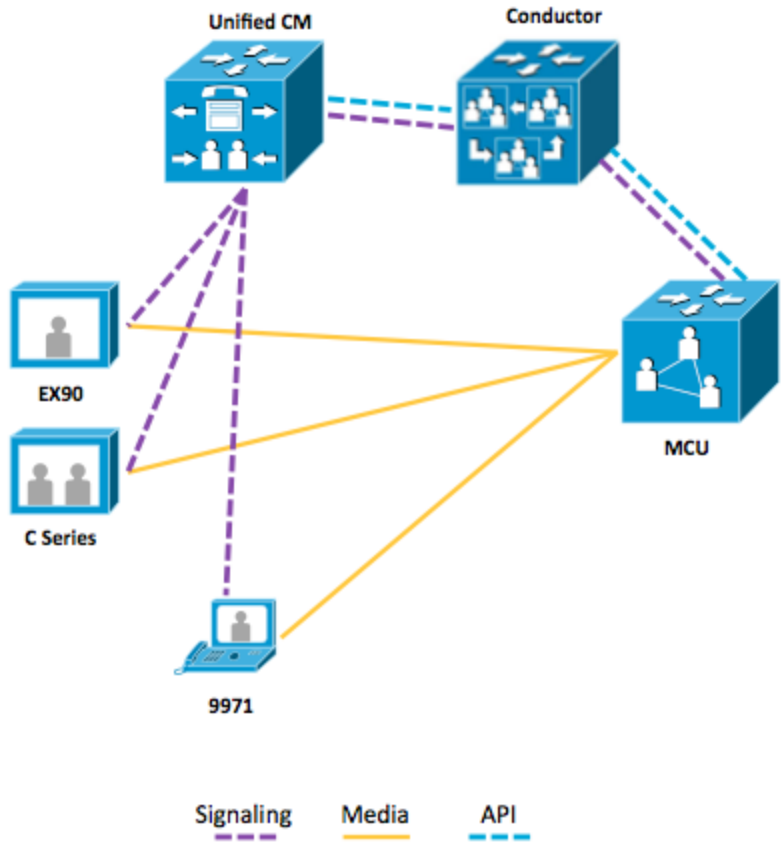


Figure 3: Cisco Unified CM deployment with TelePresence Conductor: media and signaling overview



The supported methods are described in the table below.

Table 4: MCU with TelePresence Conductor deployment capability overview

Conference type	Options
Non-scheduled	Cisco VCS: ■ Rendezvous – configured on Conductor and dynamically placed on an TelePresence MCU at conference start. ■ Dynamic escalation – using Multiway. Unified CM: ■ Rendezvous – configured on Conductor and dynamically placed on an TelePresence MCU at conference start. ■ Dynamic escalation – using Conference Button.
Scheduled	■ Using Cisco TMS either directly or via an integration, for instance with Microsoft Exchange.

Scalability and resiliency

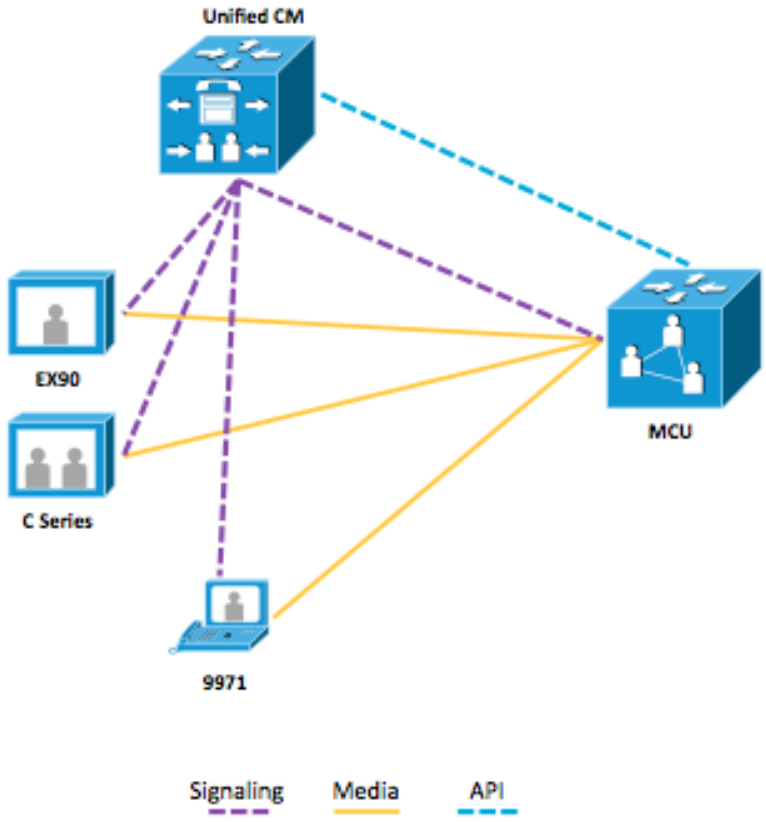
A single TelePresence Conductor or TelePresence Conductor cluster supports 30 MCUs. TelePresence Conductor also allows seamless growth of conferences beyond the limits of a single MCU's port count by dynamically cascading MCUs to form conferences that span multiple devices.

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

Deploying an MCU as a media resource 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.

Figure 4: Unified CM media resource deployment: media and signaling overview



The supported methods are described in the table below.

Table 5: Unified CM media resource deployment capability overview

Conference type	Options
Non-scheduled	■ Rendezvous – **Meet Me** using the Unified CM Meet Me mechanism. ■ Dynamic escalation – using conference button
Scheduled	■ Using Cisco TMS either directly or via an integration, for instance with Microsoft Exchange.

Scalability and resiliency

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

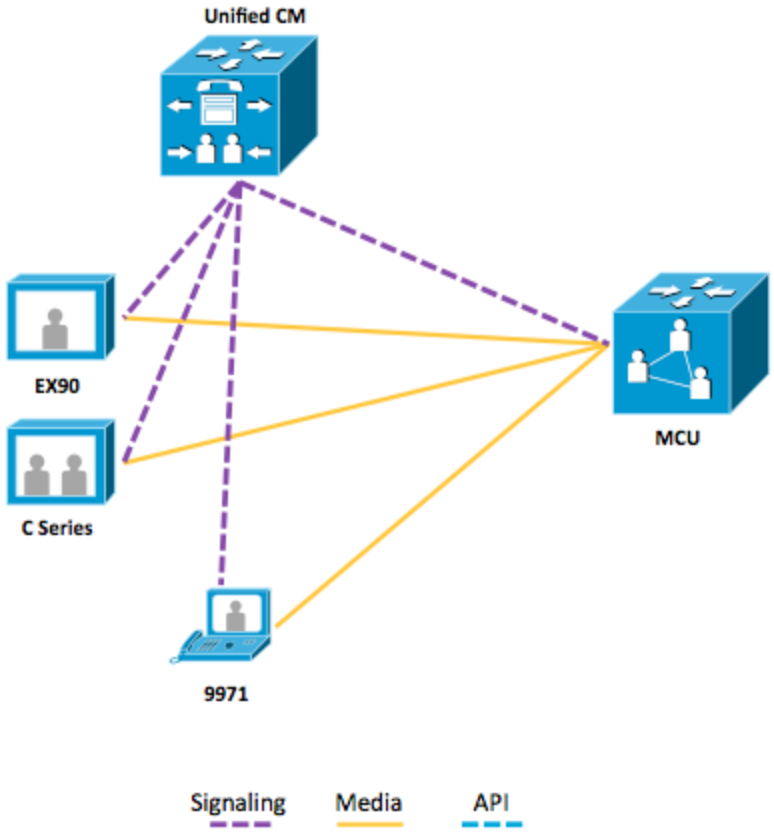
Known limitations

- Cascading is not supported.
- Configuring the MCU as a Unified CM media resource and the MCU as a trunk for Rendezvous conferencing at the same time without the use of another device such as TelePresence Conductor is not supported.

Deploying an MCU as a trunk for Rendezvous conferencing using Unified CM

In this deployment a trunk is created between Unified CM and the MCU (see figure below). Unified CM can be trunked to Cisco VCS to allow calling from devices registered to either call control platform.

Figure 5: Unified CM Rendezvous deployment: media and signaling overview



The supported methods are described in the table below.

Table 6: Unified CM Rendezvous deployment capability overview

Conference type	Options
Non-scheduled	■ Rendezvous – using static meeting numbers
Scheduled	■ Using Cisco TMS either directly or via an integration, for instance with Microsoft Exchange.

Scalability and resiliency

Unified CM provides excellent resiliency if using a prefix method where conferences are not configured on a specific MCU. Setting static meeting numbers up on MCUs limits resiliency. Many MCUs can be added to Unified CM in order to provide a large pool of available ports.

Known limitations

- Cascading is not supported
- Configuring the MCU as a Unified CM media resource and the MCU as a trunk for Rendezvous conferencing at the same time without the use of another device such as TelePresence Conductor is not supported.

Summary of deployment types

Table 7: Choosing a deployment type

	MCU deployed on Cisco VCS	MCU deployed on Cisco VCS with TelePresence Conductor	MCU deployed as a media resource on Unified CM	MCU deployed with TelePresence Conductor on Unified CM	MCU trunked to Unified CM
Assumed Equipment & Versions	MCU 4.5 Unified CM 10.0 Cisco VCS X8.5 Cisco TMS 14.5	MCU 4.5 TelePresence Conductor XC2.*x* Cisco VCS 8.5 Cisco TMS 14.5	MCU 4.5 Unified CM 10.0 Cisco TMS 14.5	MCU 4.5 Unified CM 10.0 TelePresence Conductor XC3.0 Cisco TMS 14.5	MCU 4.5 Unified CM 10.0 Cisco TMS 14.5
Non-scheduled call methods supported	Auto Attendant Rendezvous Multiway	Rendezvous Multiway	**Conference** button Unified CM Rendezvous	Rendezvous, Multiway*, **Conference** button, Unified CM Rendezvous	Auto Attendant, Rendezvous
Scheduled calls	Supported via TMS	Supported via TMS	Supported via TMS	Supported via TMS	Supported via TMS
Scalability	Basic scalability	High scalability	High scalability	High Scalability	High Scalability
Resiliency	Basic resiliency	High resiliency	High resiliency	High resiliency	High resiliency

Limitations	In order to have very large conferences, manual cascading of MCUs is required.

*Multiway (VCS registered endpoint required)

Deploying an MCU registered to Cisco VCS

Deployment overview

This deployment uses Cisco VCS as the registration mechanism for the MCU and conferences are scheduled using Cisco TMS: separate MCUs are used; one for scheduled conferences and one for non-scheduled conferences. Endpoints registered to Cisco VCS (or a Unified CM trunked to the Cisco VCS) can join MCU calls.

In order to route calls correctly and avoid the possibility of identical conference numbers for scheduled or ad hoc conferences, all MCUs are provided with a unique prefix, unless the Cisco VCS is being used to provide load balancing and resiliency across MCUs registered via H.323 only. For more information on this option see Cisco VCS MCU Connection Using H323 Deployment Guide.

This deployment covers:

Table 8: Overview of covered functionality

Functionality	Description
Management	MCU is manageable from Cisco TMS. The management access to the MCU is restricted to the administrator.
Non scheduled 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
Scheduled conferencing	A conference created by Cisco TMS and connected to by either dialing the scheduled number, using One Button to Push or being auto-dialled out from the MCU.
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 VCS running X8.5 software.
- At least one MCU using 4.5 software for scheduled conferences.
- Additional MCU for non-scheduled conferences.
- Cisco TMS running 14.5 software.
- Cisco VCS and Cisco 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.
- Cisco TMS has enough system licenses to add the relevant number of MCUs.

Document List

For the latest VCS Deployment Guides, see:

http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

See also:

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 Tasks

Task 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 non-scheduled 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 9: 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: 001@mcu1.cisco.com
	011 - 909	non-scheduled/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 (Cisco TMS will make the MCU dial out by default): H.323: 82812 SIP 812@mcu2.cisco.com or 82812@cisco.com

Task 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 Cisco VCS deployment guide (both found at http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/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 on the Cisco VCS as follows:

1. Go to **Configuration > Domains**.
2. Click **New**

3. Enter the domain name into the Name field:

Table 10: 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 Cisco VCS as follows:

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

Table 11: Settings for creating a SIP zone on a Cisco VCS

Cisco 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 do not use encryption, set this to 5060.
SIP Transport	TLS	If you do not 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 Cisco 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 Cisco VCS as follows:

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

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

Cisco 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
Protocol	Any	
Source	Any	
Request must be authenticated	Configure the authentication settings according to your authentication policy	Refer to Authentication Policy configuration options in the Cisco VCS online help for full details.
Mode	Alias pattern match	
Pattern type	Regex	
Pattern string	Example pattern: 81(\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 **Create search rule**.

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: 811111@cisco.com

This matches the search rule for MCU1 which has prefix 81, 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 Cisco VCS as follows:

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

Table 13: Settings for creating a search rule on a Cisco VCS

Cisco 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
Protocol	Any	
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 **Create search rule**.

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 Cisco VCS as follows:

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

Table 14: Settings for enabling Multiway

Cisco 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 Cisco VCS as follows:

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

Table 15: Settings for creating a Multiway search rule on a Cisco VCS

Cisco 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
Protocol	Any	

Source	Any	
Request must be authenticated	Configure the authentication settings according to your authentication policy	Refer to Authentication Policy configuration options in the Cisco VCS online help for full details.
Mode	Alias pattern match	
Pattern type	Exact	
Pattern string	Conference Factory Alias as configured under Applications > Conference Factory	Example: multiway@cisco.com
Pattern behavior	Leave	
On successful match	Stop	
Target zone	LocalZone	
State	Enabled	

4. Click **Create search rule**.

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 resources.

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

Task 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 **Settings > Upgrade**.
2. Ensure that the following keys are present:

Table 16: 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. If the keys are not present, install them one at a time by entering the string into the **Add key** box and clicking **Add key**.

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 17: 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 18: 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 19: Services settings for the MCU

MCU Setting	Value	Comment
HTTPS	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 20: SNMP settings for the MCU

MCU Setting	Value	Comment
Name	MCU name	Example:MCU1
Enable traps	Enabled	
Trap receiver address 1	IP address of Cisco TMS	
RO community	Community name of Cisco TMS	Default: public
RW community	Community name of Cisco TMS	Default: private
Trap community	Community name of Cisco 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 21: 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 only be encrypted when the signaling is TLS encrypted. Cisco VCS will only allow media encryption when the signalling is TLS. SRTP encryption using any other transport is not possible in this deployment.

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 22: 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	When used with Multiway it is important that the MCU does not ask for a PIN on conference creation as other participants will not know what the PIN is as they are joined to the MCU.

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 23: H.323 settings on the MCU

MCU Setting	Value	Comment
H.323 gatekeeper usage	Required	
H.323 gatekeeper address	FQDN of the Cisco VCS or Cisco VCS cluster	DNS A record must resolve to the Cisco VCS IP address

Gatekeeper registration type	MCU (standard)	For the Cisco 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 Cisco 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 Cisco VCS this setting is required to inform the Cisco VCS when not to route calls to the device.

3. Click **Apply changes**.

Configuring SIP settings

Configure SIP on the MCU:

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

Table 24: SIP settings on the MCU

MCU Setting	Value	Comment
Outbound call configuration	Use registrar	
Outbound address	FQDN of Cisco VCS or Cisco VCS cluster	DNS A record must resolve to the Cisco VCS IP address
Outbound domain	MCU FQDN	Example: mcu1.cisco.com
Username	String	Example: mcu1 Note: Should match the H.323 URI before the @
Password	None	Only required if the Cisco VCS requires authentication for registration
Outbound transport	TLS	Encryption Key required, otherwise use TCP.
Allow numeric ID registration for conferences and auto addendants	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 25: Settings for a pre-configured 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 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 non-scheduled 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 conferences' 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 26: 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 auto-attendant.
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 auto-attendant.
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 Cisco 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 27: 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 SIP Trust store SSL certificates as follows:

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

Table 28: Settings for SIP Trust Store SSL certificates

MCU setting	Value	Comment
SIP 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.

Configure an MCU with HTTPS Trust store SSL certificates as follows:

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

Table 29: Settings for HTTPS Trust Store SSL certificates

MCU setting	Value	Comment
HTTPS 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.

Task 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 Cisco TMS

Add the MCU to Cisco TMS in the normal manner.

Choosing the function of your MCU

Still logged in to Cisco TMS as a global administrator,

1. Go to **System > Navigator**.
2. Click on the newly added MCU.
3. Go to **Settings > Edit Settings**.

For scheduled MCUs

Only complete this section if your MCU will be used for scheduled calls.

To allow bookings for scheduled MCUs:

1. Configure the field on Cisco TMS as follows:

Table 30: Allow bookings for scheduled MCUs on Cisco TMS

Cisco TMS Setting	Value	Comment
Allow bookings	Enabled	

2. Click **Save**.

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

1. Go to **Settings > Extended Settings**.
2. Configure the fields on Cisco TMS as follows:

Table 31: Extended settings for scheduled MCUs on Cisco TMS

Cisco TMS Setting	Value	Comment
Numeric ID Base	100	In order to make sure the ID length matches the dial plan, 100 is the lowest figure that Cisco TMS accepts.
Numeric ID Step	1	

3. Click **Save**.

For non-scheduled MCUs

Disallow bookings for non scheduled MCUs as follows:

1. Configure the field on Cisco TMS as follows:

Table 32: Disallow bookings for non-scheduled MCUs on Cisco TMS

Cisco TMS Setting	Value	Comment

Allow bookings	Disabled

2. Click **Save**.

Setting preferred type MCU usage

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

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

Table 33: Settings for preferred MCU type usage

Cisco TMS Setting	Value	Comment
Preferred MCU Type in Routing	Cisco TelePresence 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 34: 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).
Non scheduled conferencing	Verify Non scheduled conferences are working	Dial into the MCU with a number within the non scheduled 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 is supported with either Unified CM or Cisco VCS as the call control platform.

TelePresence Conductor adds unique benefits such as conference virtualization, rather than defining conferences directly on TelePresence MCUs they are defined on TelePresence Conductor. TelePresence Conductor also offers better resiliency and scalability than directly registering an MCU to Cisco VCS.

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

Document List

TelePresence 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 Unified CM System Guide

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

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

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

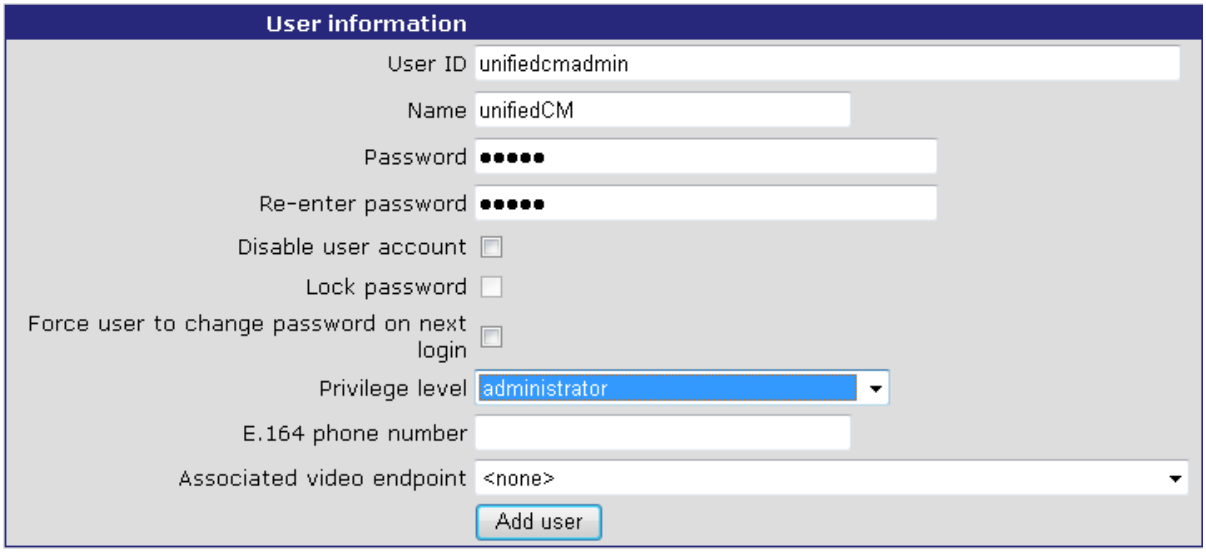
Configuring the TelePresence MCU

Task 1: Create a user

For the Unified CM to communicate with the TelePresence MCU it must use credentials for a user that has administrator rights. Cisco recommends that you create a dedicated administrator level user for this task.

1. Go to the web interface of the TelePresence MCU you want to configure and log in as an administrator.
2. Go to **Users** and click **Add new user**.
3. Enter the following in the relevant fields:

User ID	Enter a username for the Unified CM to use.
Name	Enter a name for this user.
Password	Enter a password for the Unified CM to use.
Force user to change password on next login	Uncheck.
Privilege level	Select *administrator*.

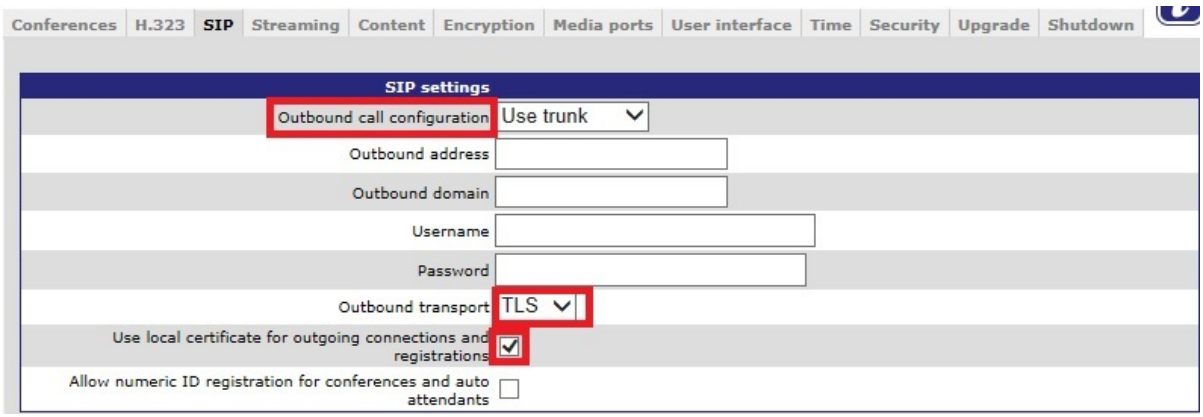


4. Click **Add user**.
5. Repeat the steps for any other TelePresence MCUs.

Task 2: Configure SIP

1. Go to **Settings > SIP**.
2. Enter the following into the relevant fields, leave other fields as their default values:

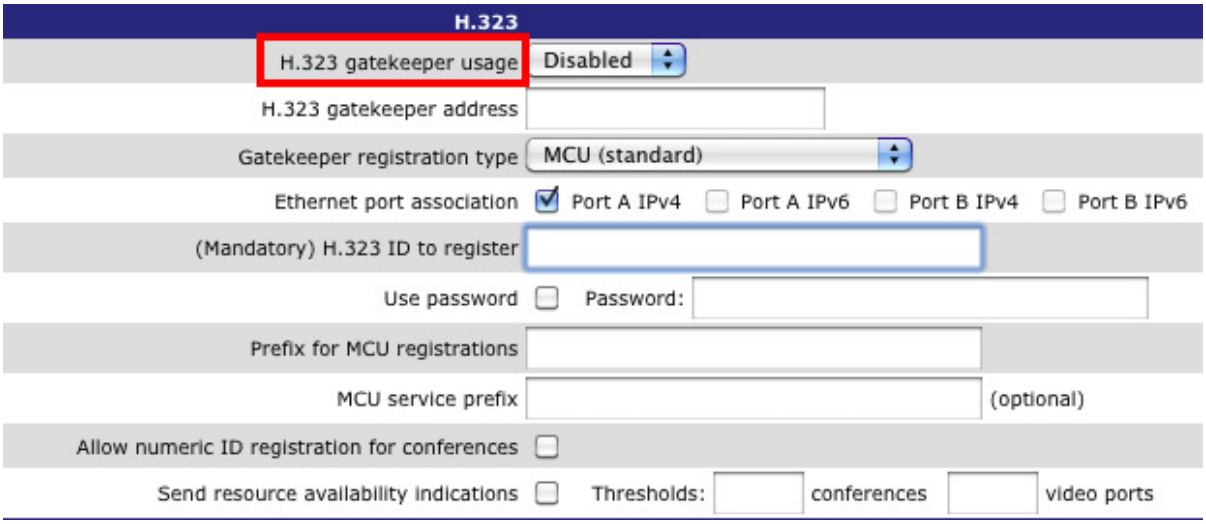
Outbound call configuration	Select *Use trunk*.
Outbound address	This is the IP address of the Unified CM.
Outbound transport	Select *TLS* if using encryption otherwise select *TCP*.
Use local certificate for outgoing connections and registrations	Check the box.



3. Click **Apply changes**.

Task 3: Disable H.323 Registration

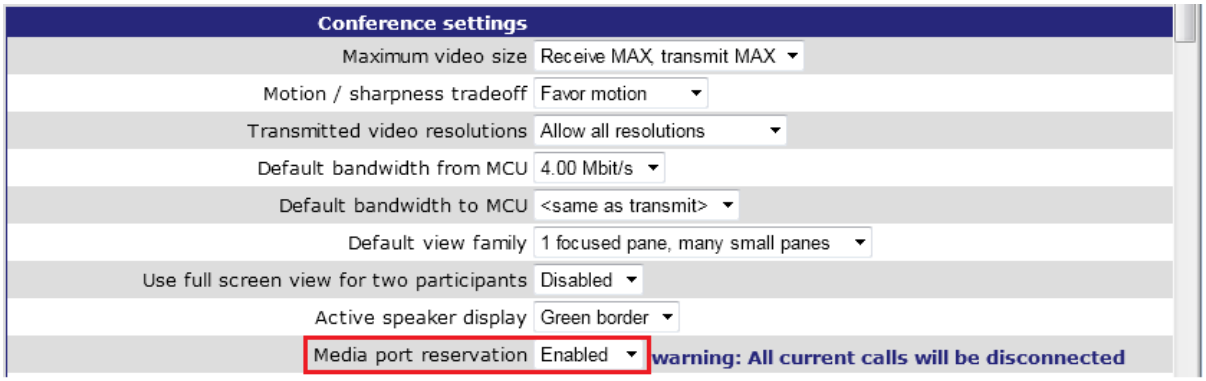
1. Go to **Settings > H.323**.
2. Set **H.323 gatekeeper usage** to *Disabled*.



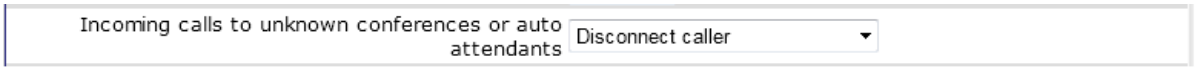
3. Click **Apply changes**.

Task 4: Change miscellaneous settings

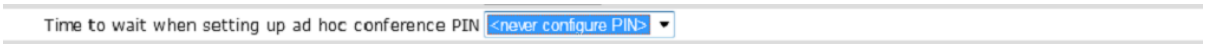
1. Go to **Settings > Conferences**.
2. Under **Conference Settings** ensure **Media port reservation** is set to *Enabled*. This should only be done when using the device as a media resource, when using as a Rendezvous device on a trunk it should be set to *Disabled*.



Ensure **Incoming calls to unknown conferences or auto attendants** is set to *Disconnect caller*.

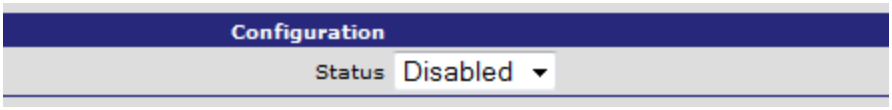


3. Ensure **Time to wait when setting up ad hoc conference PIN**is set to *<never configure PIN>* .



4. Click **Apply changes**.
5. Go to **Gatekeeper > Built in Gatekeeper**.
6. Under **Configuration** ensure **Status** is set to *Disabled*.

Note: The MCU 5300 series does not have a built-in Gatekeeper.



7. Click **Apply changes**.

Configuring the Unified CM for Ad hoc conferencing

This deployment assumes you are using a non-secure deployment. If you are using a secure deployment you will need to generate a certificate and private key. Refer to Appendix 1: Additional information [p.50] for more information.

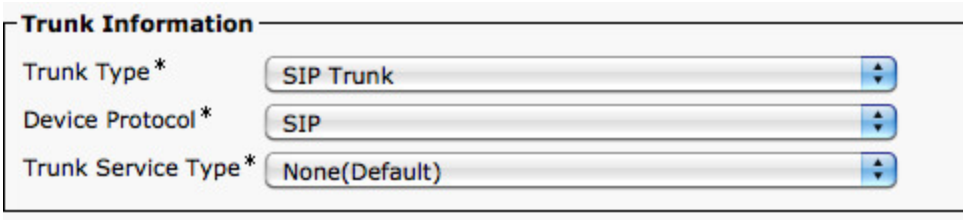
Task 1: Adding a SIP trunk connecting to the MCU for Ad hoc conferences

From Unified CM version 10.x onwards a SIP trunk between Unified CM and the MCU must be explicitly configured for ad hoc conferences. The task is not required when running an earlier version of Unified CM.

To configure a SIP trunk to the MCU:

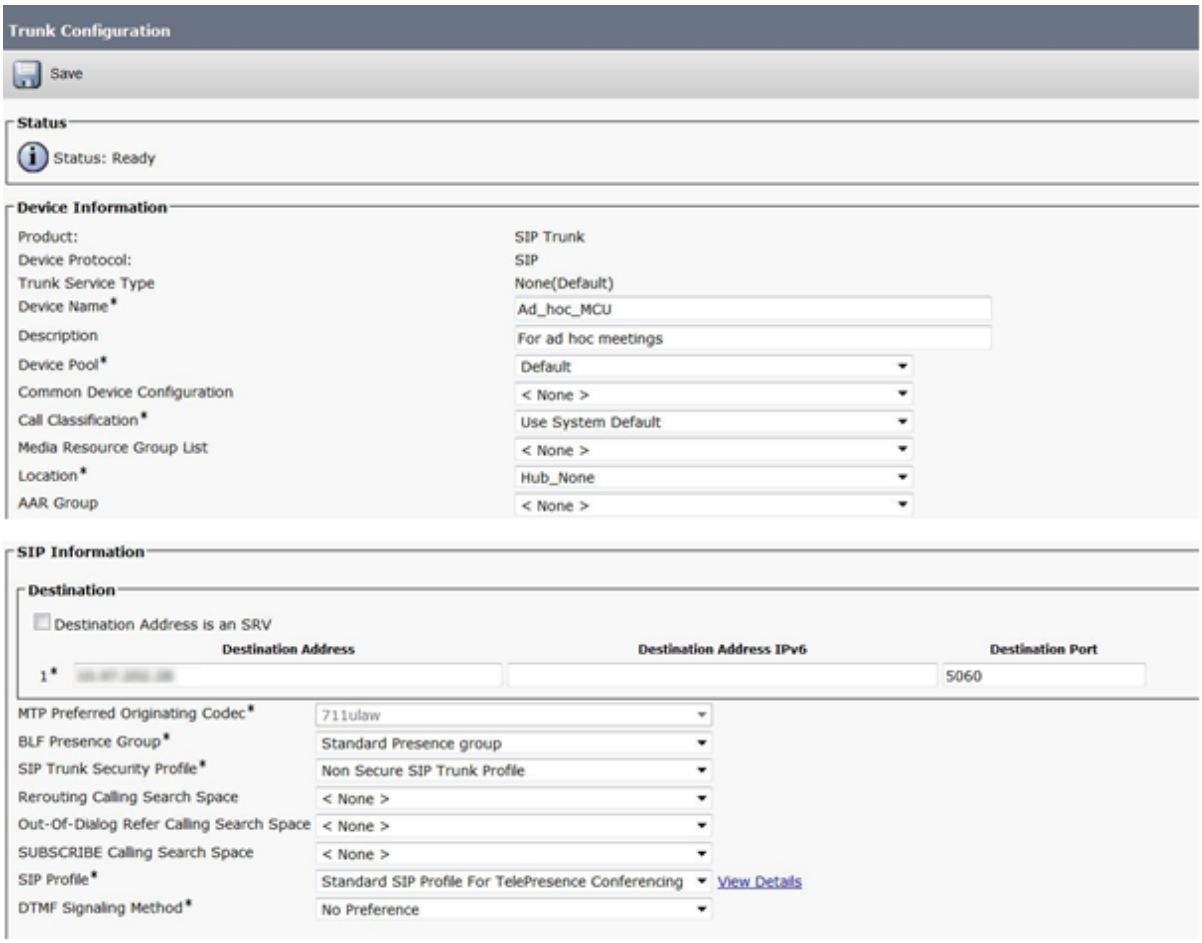
1. Go to **Device > Trunk**.
2. Click **Add New** to create a new SIP trunk.
3. Enter the following into the relevant fields:

Trunk Type	Select *SIP Trunk*.
Device Protocol	Leave as default: *SIP*.
Trunk Service Type	Leave as: *None(Default)*.



4. Click **Next**.
5. Enter the following into the relevant fields, leave other fields as their default values:

Device Name	Enter a trunk name.
Device Pool	Select the appropriate Device Pool.
Location	Set to the appropriate location.
TelePresence MCUs IP address	Enter the MCU's IP address.
SIP Trunk Security Profile	Select *Non-secure SIP Trunk Profile* from the drop-down list.
SIP Profile	Select *Standard SIP Profile for TelePresence Conferencing*



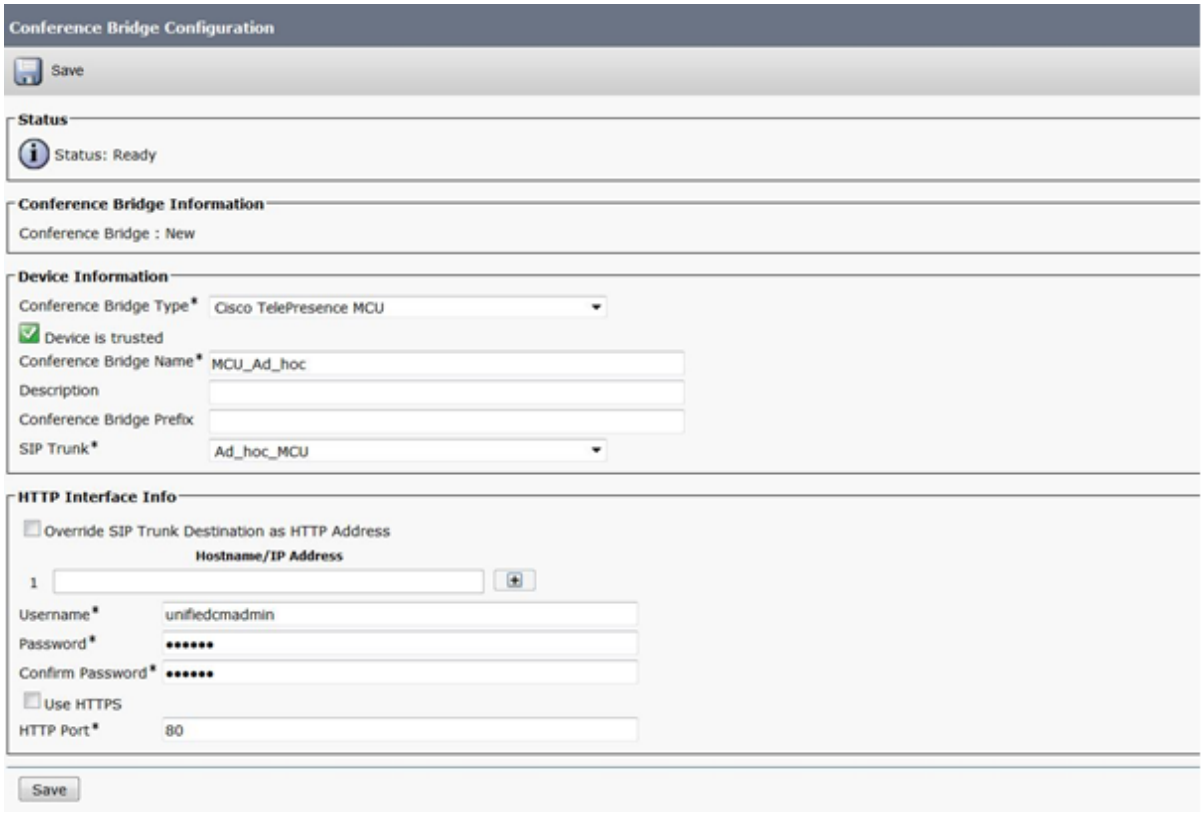
6. Click **Save**.
7. Click **Reset**.

Task 2: Add the MCU as a Conference bridge to Unified CM for Ad hoc conferences

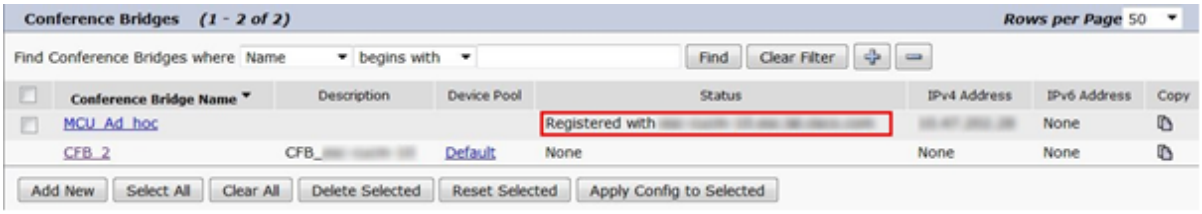
1. Go to **Media Resources > Conference Bridge**.
2. Click **Add New** to create a new conference bridge.
3. Enter the following into the relevant fields, leave other fields as their default values:

Conference Bridge Type	Select *Cisco TelePresence MCU*.
Conference Bridge Name	Enter the MCU's name.
SIP Trunk	Select from the drop-down list the SIP Trunk for ad hoc conferences created in Task 1: Adding a SIP trunk connecting to the MCU for Ad hoc conferences [p.39].
Username	Enter the username of the MCU administration user set up earlier. This appears on the MCU's **Administrator accounts** page (**Users > Administrator accounts**).

Password	Enter the password of the MCU administration user.
Use HTTPS	Disabled
HTTP Port	Enter '80'.



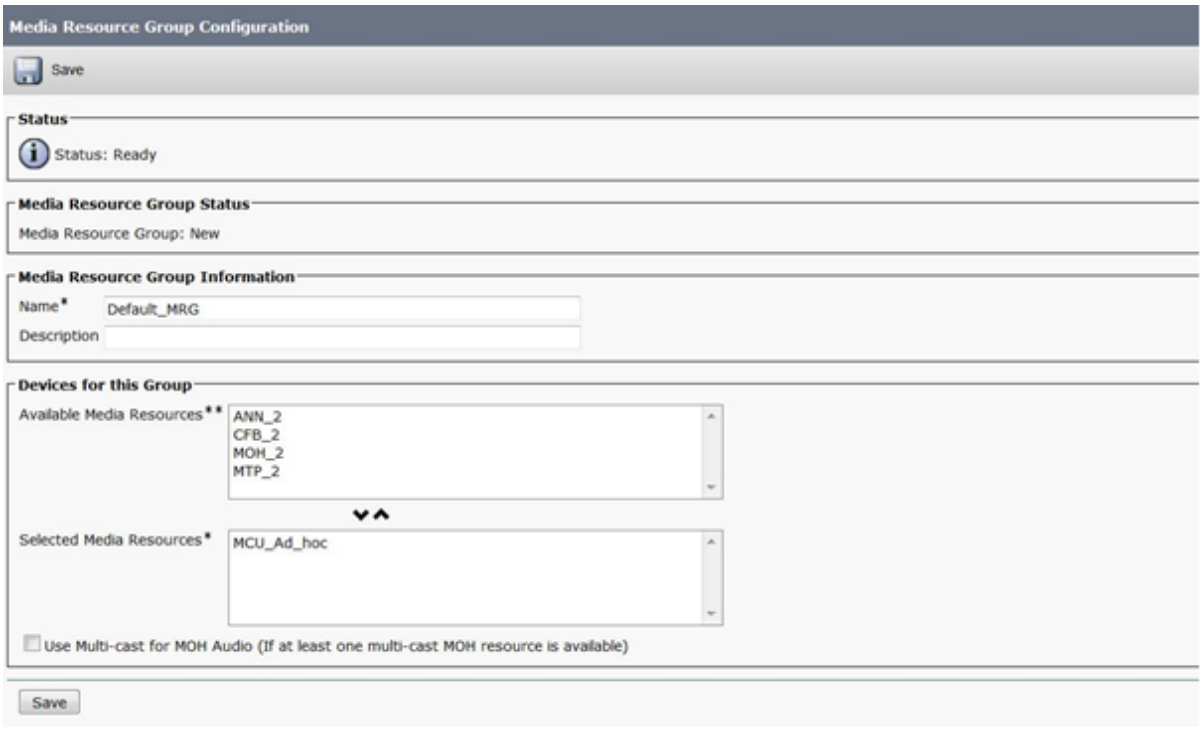
1. Find the **Related Links: Back to Find/List** and click **Go**.
2. Verify that the MCU is registered with Unified CM.



Task 3: Add the MCU to an MRG and MRGL

To configure the Unified CM with the MCU in a Media Resource Group (MRG):

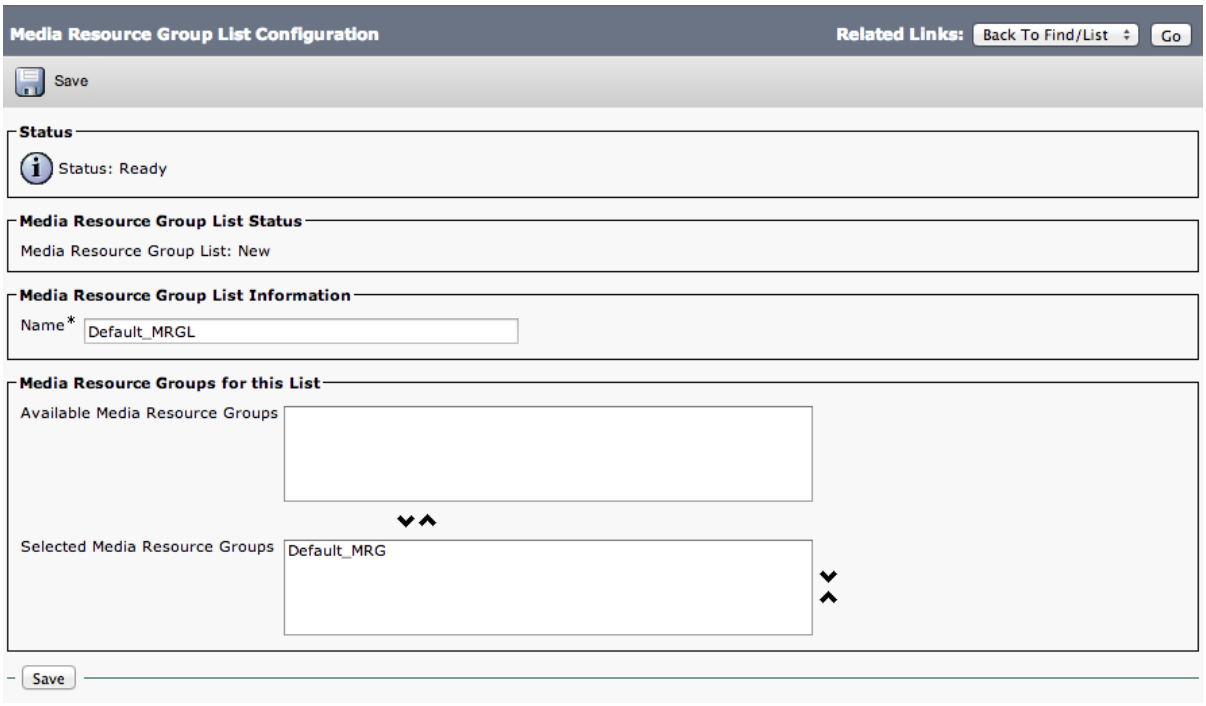
1. Go to **Media Resources> Media Resource Group**.
2. Click **Add New** to create a new media resource group.
3. Enter a name for the MRG.
4. Move the MCU media bridge (the conference bridge configured in Task 2: Add the MCU as a Conference bridge to Unified CM for Ad hoc conferences [p.40] down to the **Selected Media Resources** box.



5. Click **Save**.

To configure a Media Resource Group List (MRGL) in Unified CM:

6. Go to **Media Resources > Media Resource Group List**.
7. Click **Add New** to create a new media bridge group or find an existing MRGL and click on it to edit it.
8. Enter a name for the MRGL.
9. Move the TelePresence MCU media bridge group configured in sub-steps 2 – 5 above, down to the **Selected Media Resource Groups** box.



10. Click **Save**.

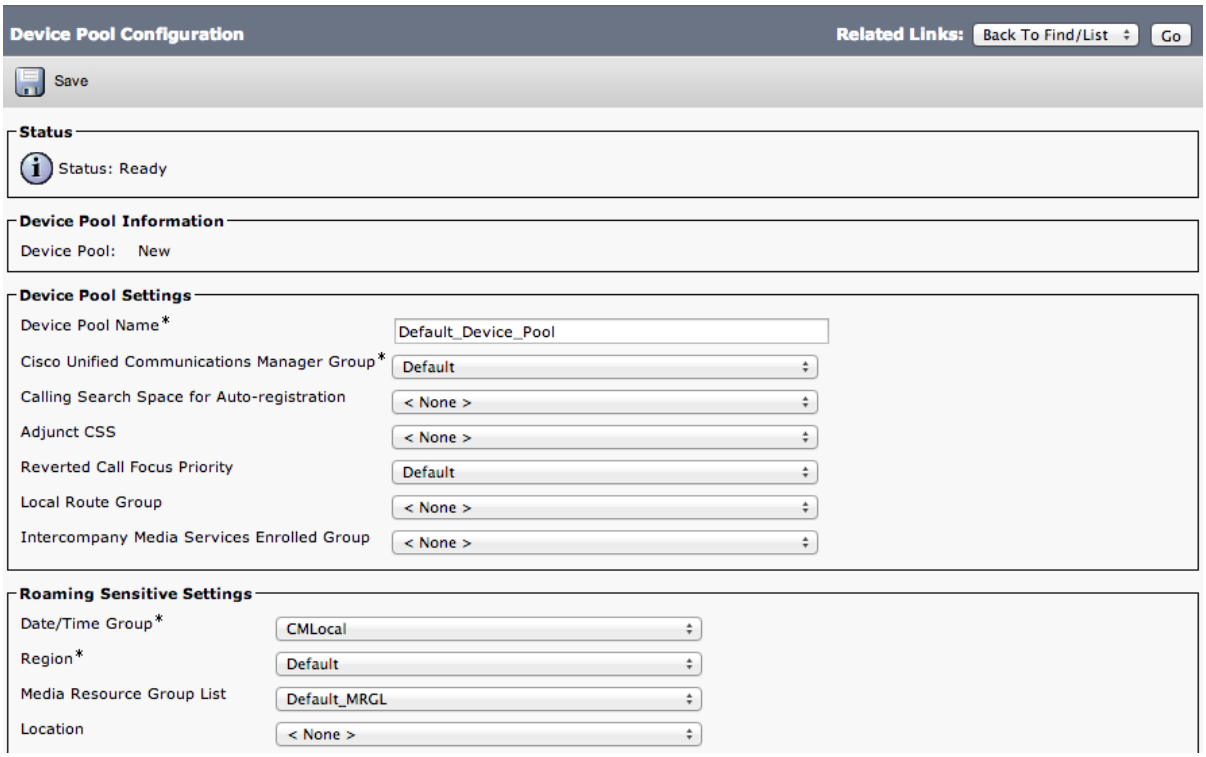
Task 4: Add an MRGL to a Device Pool or Device

Depending on the implementation, either a Device Pool can be configured and applied to all endpoints, or an individual device (i.e. an endpoint) can be assigned a specific MRGL. For further information on Device Pools or Devices reference the Unified CM documentation on Cisco.com under http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

To configure Media Bridge Group List (MRGL) to a Device Pool:

1. Go to **System > Device Pool**.
2. Click **Add New** to create a new Device pool or find a Device pool and click on it to edit an existing pool.
3. Enter the following into the relevant fields, leave other fields as their default (or previously configured) values:

Device Pool Name	Enter a Device pool name.
Cisco Unified Communications Manager Group	Select the appropriate group from the drop-down list.
Date/Time Group	Select the appropriate group from the drop-down list.
Region	Select the appropriate region from the drop-down list.
Media Bridge Group List	Select the MRGL created in Task 3: Add the MCU to an MRG and MRGL [p.41] (sub-steps 6 -10) from the drop-down list.



4. Click **Save** and **Reset** for the changes to take effect.

Note: If there are devices associated with the pool, they will reboot when **Reset** is clicked.

If a new Device pool has been created:

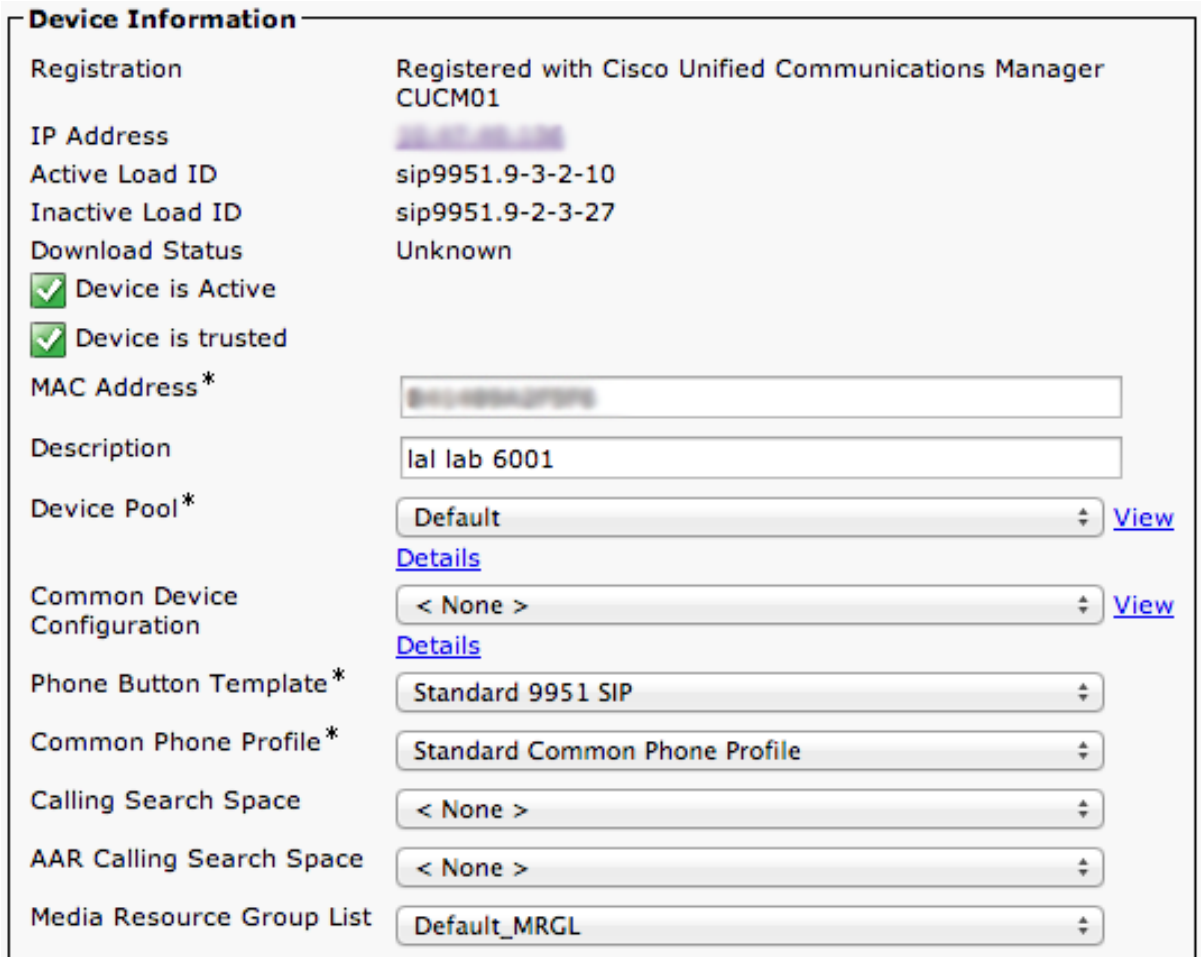
5. Go to **Device > Phones**.
6. Click **Find** and select the device to change the Device Pool settings on.
7. Select the Device Pool used above (in steps 1-4) from the drop-down list.

8. Click **Save**.
9. Click **Apply Config**.
10. Click **Reset** for the changes to take effect.
    Note: This will reboot the phones when applied.

To apply an MRGL directly to a device or endpoint as opposed to using a Device Pool do the following:

Note: The MRGL setting closest to the device will be the active setting. For example, if the endpoint has a Device Pool assigned to it, which had an MRGL defined within the Device Pool, and the endpoint has another MRGL selected at the device level, the device level setting will be used.

11. Go to **Device > Phones**.
12. Click **Find** and select the device to change the MRGL settings on.
13. Select the MRGL used in Task 3: Add the MCU to an MRG and MRGL [p.41] (steps 6 – 10) from the drop-down list.



14. Click **Save**.
15. Click **Apply Config**.
16. Click **Reset** for the changes to take effect.

Configuring the Unified CM for Rendezvous conferencing

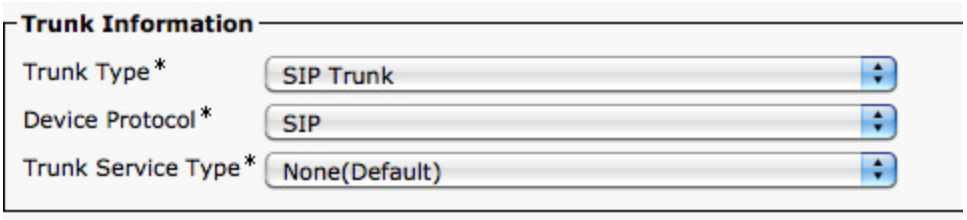
This deployment assumes you are using a non-secure deployment. If you are using a secure deployment you will need to generate a certificate and private key. Refer to Appendix 1: Additional information [p.50] for more information.

Task 1: Add a SIP trunk to MCU for Rendezvous conferences (and to receive TelePresence MCU out-dialed calls)

To configure a SIP trunk to the MCU:

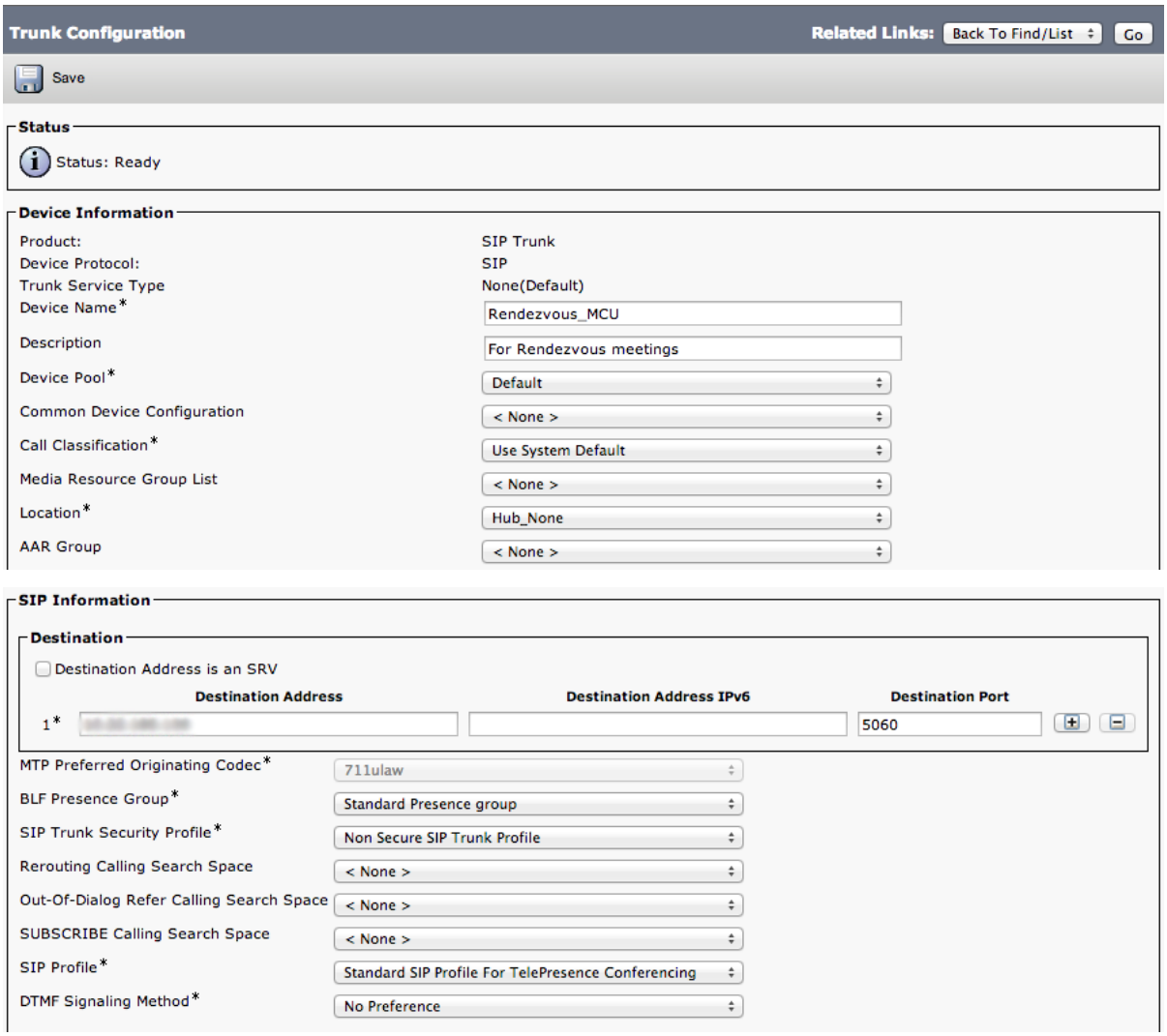
1. Go to **Device > Trunk**.
2. Click **Add New** to create a new SIP trunk.
3. Enter the following into the relevant fields:

Trunk Type	Select *SIP Trunk*.
Device Protocol	Leave as default: *SIP*.
Trunk Service Type	Leave as: *None(Default)*.



4. Click **Next**.
5. Enter the following into the relevant fields, leave other fields as their default values:

Device Name	Enter a trunk name.
Device Pool	Select the appropriate Device Pool.
Location	Set to the appropriate location.
TelePresence MCUs IP address	Enter the MCU's IP address.
SIP Trunk Security Profile	Select *Non-secure SIP Trunk Profile* from the drop-down list.
SIP Profile	Select *Standard SIP Profile for TelePresence Conferencing*



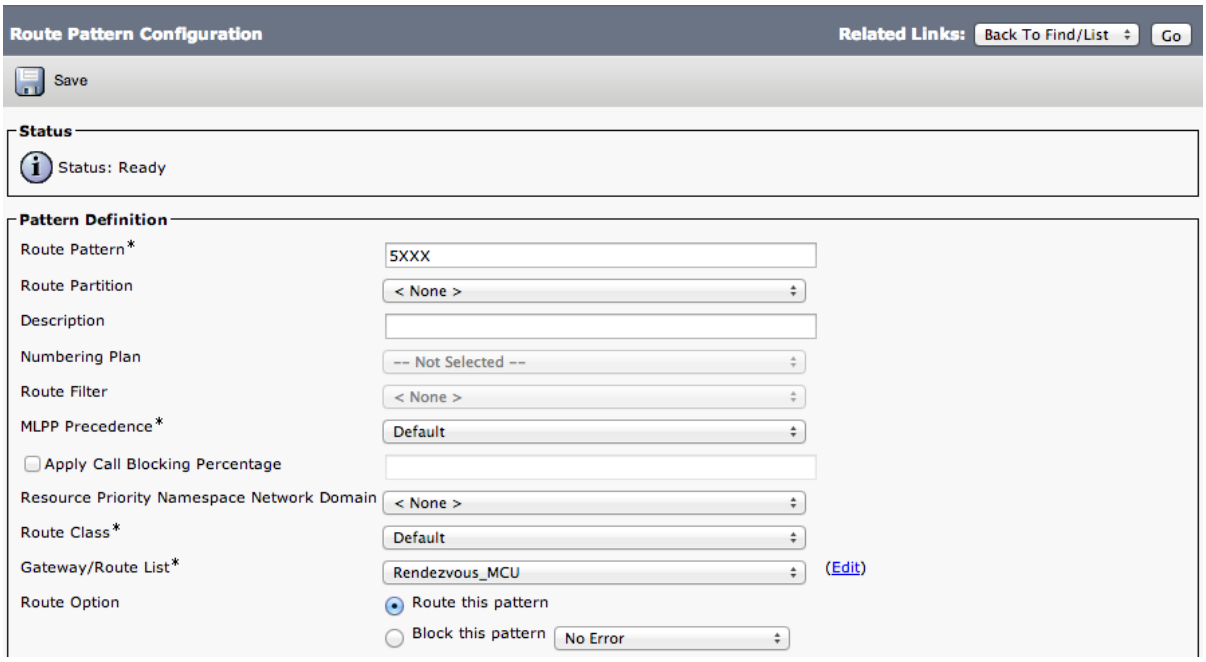
6. Click **Save**.
7. Click **Reset**.

Task 2: Add a route pattern to match the SIP trunk to TelePresence MCU for Rendezvous meetings

To configure a route pattern to match the SIP trunk to the TelePresence MCU for Rendezvous calls:

1. Go to **Call Routing > Route/Hunt > Route Pattern**.
2. Click **Add New** to create a new route pattern.
3. Enter the following into the relevant fields, leave other fields as their default values:

Route Pattern	Enter a route pattern to match against the destination string.
Gateway/Route List	Select the trunk created in the previous step.



4. Click **Save**.

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 on the MCU:

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

Table 35: Settings for a pre-configured conference

MCU setting	Value	Comment
Name	Name of conference	Name that identifies the conference.
Numeric ID	Unique three digit numeric identifier from address plan	Use a number that matches the route pattern configured earlier, e.g. 5001
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 non-scheduled 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 conferences' template.

If automatically generating non-scheduled conferences on the MCU the setting **Incoming calls to unknown conferences or auto attendants** must be set to *Create new ad hoc conference*.

Appendix 1: Additional information

This appendix contains additional information that is useful if you are using a secure deployment scenario.

Install an encryption key on the MCU

The MCU has the ability to use a secure connection for communications. These security features are enabled with the **Encryption** option key. You must install the option key for this deployment to work.

To verify that the key is installed or to install the key:

1. Go to **Settings > Upgrade**.
2. Go to the **Feature Management** section and verify that the **Encryption key** is installed. If the key is not installed, enter the **Activation code** and click **Add key**.

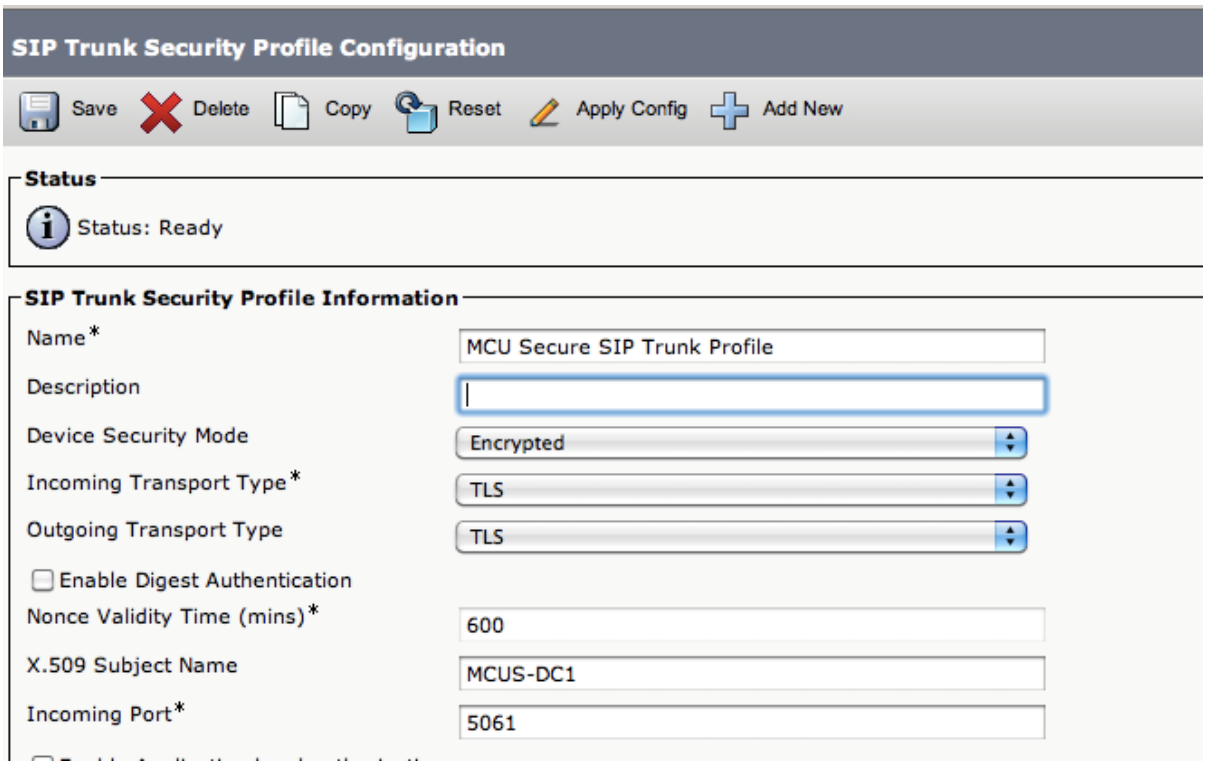
To enable the use of encryption on the MCU:

1. A valid local certificate and SIP trust store must be uploaded into the MCU and Unified CM must trust the certificate authority for TLS to be negotiated.
2. Go to **Settings > Encryption**.
3. Set **Encryption status** to *Enabled*.
4. Set **SRTP encryption** to *Secure transport (TLS) only*.
5. Click **Apply changes**.
6. Go to **Network > Services**.
7. Ensure that **HTTPS (port 443)** is checked.
8. Ensure that **Encrypted SIP (TLS)** is checked.
9. Ensure that **SIP (UDP)** is unchecked.
10. Click **Apply changes**.

Working with Unified CM

Setting up MCU with a secure trunk for Rendezvous

1. Unified CM must trust the MCU certificate, so the MCU certificate or the CA of the MCU certificate (if signed) must be added to the Call Manager trust store.
2. The SIP Trunk Security Profile on Unified CM for the trunk to the MCU must have the common name of the MCU certificate in the **X.509 Subject Name** on the **System > Security** page.



3. On the Unified CM trunk setting to the MCU check **SRTP Allowed**, use Destination port as 5061 to the MCU and choose the **vcs-interop** Normalization script.
4. If using TLS verify on the MCU, the Unified CM certificate must be trusted by the MCU, so the Unified CM certificate or the CA of the Unified CM certificate (if signed) must be added to the MCU trust store. Other MCU requirements are documented in the MCU help 'Configuring SSL certificates'.

Setting up a Secure Conference Bridge for Ad Hoc

1. Unified CM must trust the MCU certificate, so the MCU certificate or the CA of the MCU certificate (if signed) must be added to the Call Manager trust store.
2. The SIP Trunk Security Profile on Unified CM for the trunk to the MCU must have the common name of the MCU certificate in the **X.509 Subject Name** on the **System > Security** page.
3. On the Conference bridge configuration in Unified CM, use **MCU Conference Bridge SIP Port** as 5061, check **SRTP Allowed** and set the Normalization script to **vcs-interop**.
4. If using TLS verify on the MCU, the Unified CM certificate must be trusted by the MCU, so the Unified CM certificate or the CA of the Unified CM certificate (if signed) must be added to the MCU trust store. Other MCU requirements are documented in the MCU help 'Configuring SSL certificates'.

   If using HTTPS there are additional certificate requirements: MCU certificate must use its IP address as the common name or store the IP address as type IP in the **Subject alternate name**.

Document revision history

The following table summarizes the changes that have been applied to this document.

Revision	Date	Description
March 2015	March 2015	Updated for 4.5 release
D14962.01	September 2013	Updated for 4.4 release
D14962	May 2012	Initial release.