Cisco Meeting Server

Cisco Meeting Server 3.9

Deployments with Cisco Unified Communications Manager

March 05, 2024

Contents

Change History

Date	Change Summary
March 05, 2024	Updated for version 3.9.
September 07, 2023	Updated for version 3.8. Updated information on CMS certificate verification in IMPS/CUCM
March 16, 2023	Updated for version 3.7. Added steps to create AXL users and presence users.
November 04, 2022	Minor correction.
April 08, 2021	Updated for version 3.2. Load limits for Cisco Meeting Server platforms updated.
December 02, 2020	Corrected note at start of section 4.2
October 20, 2020	Minor update.
September 11, 2020	Updated for version 3.0.
April 08, 2020	Updated for version 2.9. Replaced information on using API Methods with accessing the API through the Web Admin interface.
September 26, 2019	Minor correction.
May 31, 2019	Minor correction.
February 27, 2019	Note added before step 4 in section 2.1.2
January 02, 2019	No changes for version 2.5
October 02, 2018	Minor change to documentation map for version 2.4.
May 10, 2018	Cross reference added re: changing minimum TLS version.
February 01, 2018	Updated for version 2.3. Added note on TLS 1.2 as default at start of chapter 4.
January 23, 2018	General minor edits and improvements.
November 08, 2017	Added Appendix A: Adhoc escalation with multiple clusters, and other minor corrections.
July 14, 2017	Additional information added to chapter 3.
May 09, 2017	Updated for version 2.2. Added section on load balancing outgoing calls.
December 20, 2016	Updated for version 2.1. Added chapter on load balancing calls of incoming calls.
August 03, 2016	Rebranded for Cisco Meeting Server 2.0

1 Introduction

The Cisco Meeting Server software can be hosted on specific servers based on Cisco Unified Computing Server (UCS) technology or on a specification-based VM server. Cisco Meeting Server is referred to as the Meeting Server throughout this document.

Note: Cisco Meeting Server software version 3.0 onwards does not support X-Series servers.

Note: The term Meeting Server in this document means either a Cisco Meeting Server 2000, Cisco Meeting Server 1000 or the software running on a virtual host.

This guide provides examples of how to configure the Meeting Server to work with Cisco Unified Communications Manager. The examples may need to be adapted according to your specific deployment. For details on using the Avaya and Polycom call control devices, see the Deployments with Third Party Call Control Guide. If you are using Cisco Expressway, see the Expressway documentation for more information.

These instructions apply equally to all Meeting Server deployment topologies (single server and scaled/resilient deployments).

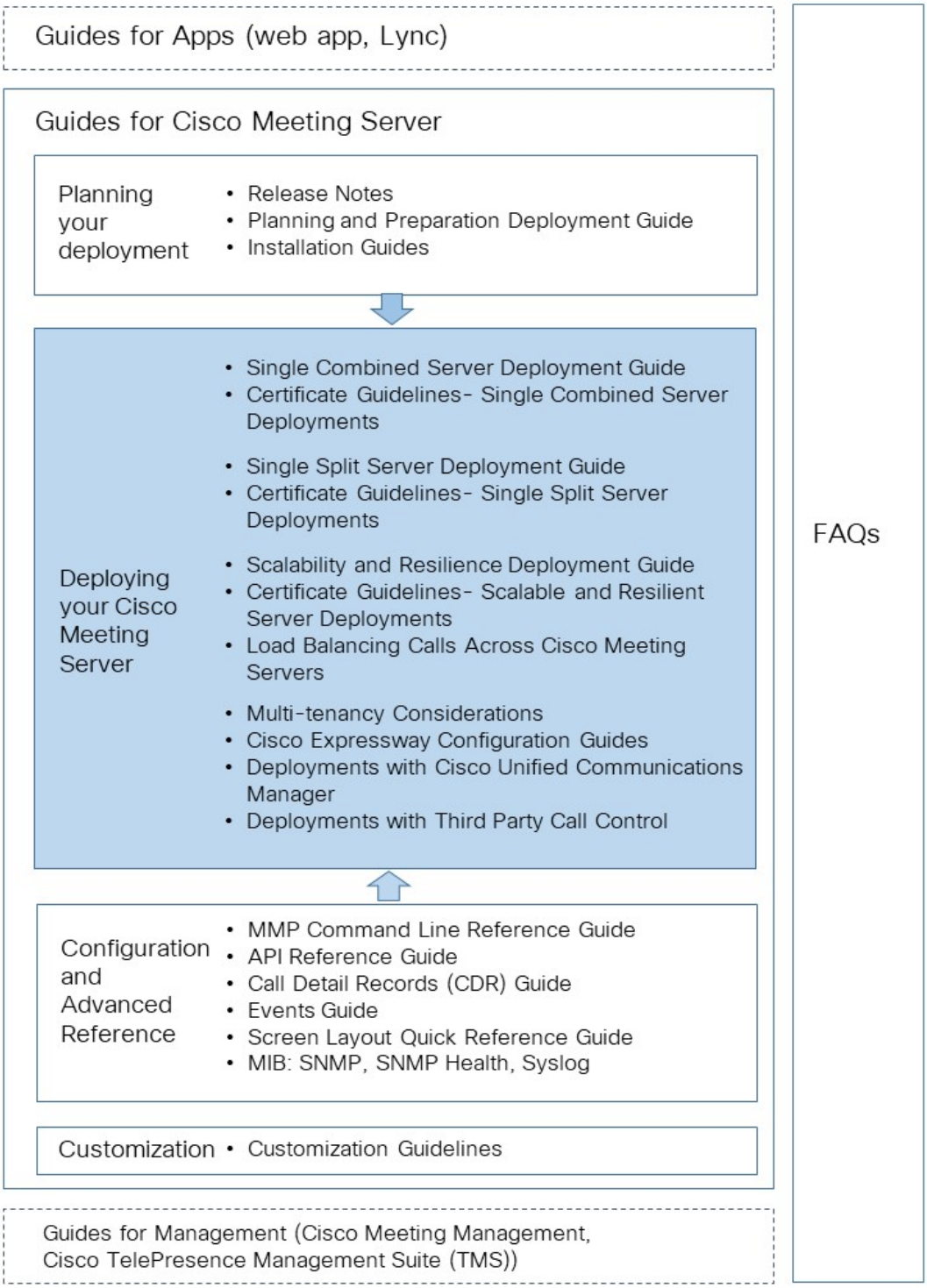
Note: The Meeting Server can only forward DTMF inband tones (RFC 2833). For example: if an endpoint sends DTMF out of band to Cisco Unified Communications Manager which forwards it to the Meeting Server, the Meeting Server will not forward the DTMF to another endpoint.

1.1 How to Use this Guide

This guide is part of the documentation set (shown in Figure 1) for the Meeting Server.

These documents can be found on cisco.com.

Figure 1: Cisco Meeting Server documentation set



1.1.1 Commands

In this document, commands are shown in **`black`** and must be entered as given - replacing any parameters in <> brackets with your appropriate values. Examples are shown in **`blue`** and must be adapted to your deployment.

1.1.2 Terminology

Throughout this document the conferencing types mentioned are those as defined in Table 1.

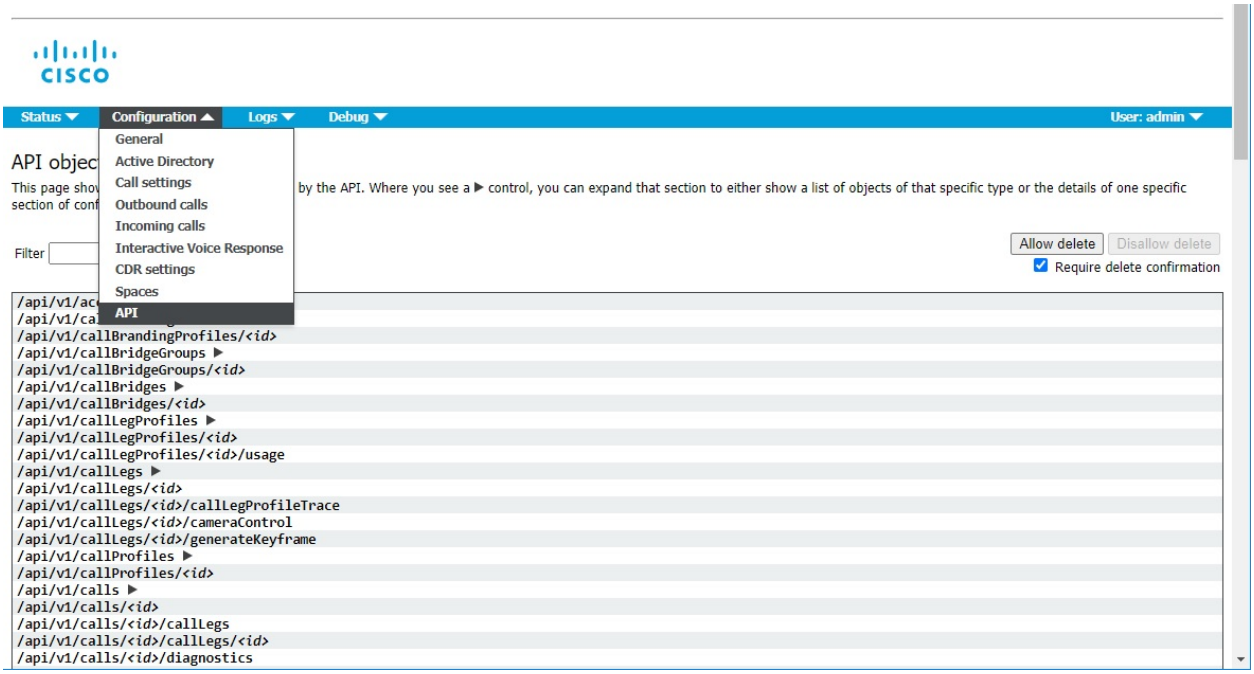
Table 1: Conferencing Types

Conference type	Description
Rendezvous (also known as personal CMR or VMR)	Pre-defined, permanently available addresses that allow conferencing without previous scheduling. The host shares the address with other users, who can call in to that address at any time.
Ad hoc	Instant or escalated conferencing, for example manually escalated from a point-to-point call to a multiparty call with three or more participants.
Scheduled	Pre-booked conferences with a start and end time.

1.2 Simplifying How To Use the Meeting Server API

From version 2.9, the API can be accessed using the Meeting Server Web Admin Interface rather than using API Methods and third-party applications. After logging in to the Web Admin interface, navigate to the **Configuration** tab and select **API** from the pull-down list. See Figure 2.

Figure 2: Accessing the API via the Meeting Server web admin interface



Note: To access the API via the web interface you still need to do the initial Meeting Server configuration settings and authentication using the MMP as you would if you were using a third party application.

2 Configuring a SIP Trunk to Cisco Unified Communications Manager

This chapter explains how to set up a SIP trunk between Cisco Unified Communications Manager and a Meeting Server. The Meeting Server can be configured as:

- a single combined server, or
- a Core server in a split server deployment or a scalable and resilient deployment.

Note: For scalable and resilient deployments, SIP trunks should be set up between each Cisco Unified Communications Manager and each Meeting Server. A single trunk for multiple Call Bridges is not advisable. For ad hoc calls it is a requirement to have a separate trunk set up to each Call Bridge node.

Cisco recommends setting up secure SIP trunks, however if your company policy is for traffic within your organization to be non secure, then non-secure SIP trunks can be configured. However, the escalation of a 2-way call on Cisco Unified Communications Manager to a conference on the Meeting Server, requires the Cisco Unified Communications Manager to communicate with the API of the Cisco Meeting Server. The API requires HTTPS communication, so certificates need to be created and uploaded to both the Cisco Meeting Server and Cisco Unified Communications Manager, and Cisco Unified Communications Manager needs to trust the Meeting Server's certificate, in order for escalated ad hoc calls to work.

If you are just allowing scheduled or rendezvous calls between the Meeting Server and Cisco Unified Communications Manager, and you set the SIP trunks as non-secure, then certificates are not required. Definitions of call types are given in Section 1.1.2.

Note: If you are not your organization's Cisco Unified Communications Manager server administrator, then Cisco strongly advises you to seek the advice of your local administrator on the best way to implement the equivalent on your server's configuration.

If you want to configure a secure SIP trunk, see Section 2.1. If you want to configure a non-secure SIP trunk, go straight to Section 2.2.

2.1 Configuring a secure SIP trunk

Follow the steps in Section 2.1.1 and Section 2.1.2 to set up the secure SIP trunk, then Chapter 4 to enable escalation of a 2-way call on Cisco Unified Communications Manager to a conference on the Meeting Server.

Note: For ad hoc calls, Cisco Unified Communications Manager needs to access the API of the Meeting Server through an HTTPS connection. If you have different certificates for the Call Bridge and Web Admin, you need to upload any Root and Intermediate CA certificates that signed the Meeting Server Web Admin certificate to the trust store on Cisco Unified Communications Manager.

Step 2 in Section 2.1.2 explains how to upload certificates to the trust store on Cisco Unified Communications Manager through **CallManager-trust**.

2.1.1 Configuration required on the Meeting Server

Follow the Cisco Meeting Server deployment guides to configure your Meeting Server, once configured, follow these steps for each Call Bridge:

1. SSH into the MMP of the Meeting Server.
2. If you have not already done so, specify a listening interface using the MMP command **`callbridge listen`**
3. Generate a private key and Certificate Signing Request (.csr) file for the Call Bridge. For details on how to create a private key and Certificate Signing Request (.csr) file, refer to the appropriate Certificate Guidelines for the Meeting Server deployment.

   Note: The Call Bridge certificate must have a CN that matches the FQDN of the network interface that the Call Bridge is listening on.

   Cisco Unified Communications Manager has some requirements on what TLS certificates it will accept. You should ensure that the Call Bridge certificate has the SSL client and SSL server purposes enabled. This is done during the certificate signing stage.
4. Submit the Call Bridge certificate to the CA (public CA or internal CA) for signing. An internal CA signed certificate is acceptable. However, a self-signed certificate is not supported.
5. Once signed, check that the certificate is OK using openSSL or the **`pki inspect`** command:

   - Enter **`pki inspect <certificatename>`** and check under **`X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication`**.
   or
   - Enter: **`openssl x509 -in <certificatename> -noout -text -purpose`**
   for example
   `openssl x509 -in callBridge1.crt -noout -text -purpose`

   The important lines in the output are **`SSL client`** and **`SSL server`** which must have a **`Yes`** against them, for example:

   ```
   Certificate purposes:
   SSL client : Yes
   ```

```
SSL client CA : No
SSL server : Yes
```

6. Upload the signed certificate, and intermediate CA bundle (if any) using SFTP to the Call Bridge.
7. Assign the certificate and private key to the Call Bridge:
   a. SSH into the MMP
   b. Enter the command:

      `callbridge certs <keyfile> <certificatefile>[<cert-bundle>]`

      where **`keyfile`** and **`certificatefile`** are the filenames of the matching private key and certificate. If your CA provides a certificate bundle then also include the bundle as a separate file to the certificate.

      For example:

      `callbridge certs callBridge1.key callBridge1.crt callBridge1-bundle.crt`

   c. Restart the Call Bridge interface to apply the changes.

      `callbridge restart`

      If the certificate installs successfully on the Call Bridge, then the following is displayed:

      ```
      SUCCESS: listen interface configured
      SUCCESS: Key and certificate pair match
      ```

      If the certificate fails to install, the following error message is displayed:

      ```
      FAILURE: Key and certificate problem: certificate and key do not match
      ```

Note: Your Cisco Unified Communications Manager will need to trust the CA and any Intermediate CAs that signed the certificate of the Call Bridge. This is achieved by uploading the Call Bridge certificates created in step 4 above to the trust store on Cisco Unified Communications Manager through **CallManager-trust**, see step 2 in Section 2.1.2

Note: For more information on creating and uploading certificates to the Meeting Server, see the appropriate Cisco Meeting Server Certificate Guidelines.

2.1.2 Configuration required on the Cisco Unified Communications Manager

Our testing has been done on trunks without Media Termination Point (MTP) configured. Therefore:

- Disable MTP if this will not negatively affect your deployment. Turning off MTP might have a negative impact on your deployment if you are using SCCP phones and need to send DTMF

to the Meeting Server.

- If the above is not a valid implementation, you may need to increase the MTP capacity on the Cisco Unified Communications Manager depending on the number of simultaneous calls.

1. If not done so already, install a CA signed certificate for the CallManager service on each Cisco Unified Communications Manager which has the CallManager service activated.
   Note: This is a recommendation and not a requirement as Meeting Server does not validate received certificates by default, it accepts all valid certificates and will accept Call Manager's self-signed certificate.
   a. Log into the Cisco Unified Communications Manager **OS Administration** page, choose **Security > Certificate Management**.
   b. In the **Certificate List** window, click **Generate CSR**.
   c. From the **Certificate Name** drop-down list, choose **CallManager**.
   d. Click **Generate CSR** to generate a Certificate Signing Request.
   e. Once the CSR is successfully generated, click **Download CSR**. From the Download Signing Request dialog box choose **CallManager** and click **Download CSR**.
   f. Get this CSR signed by a Certificate Authority. An internal CA signed certificate is acceptable.
   g. Once a certificate is returned from the CA, go to the **Upload Certificate/Certificate chain** window. From the **Certificate Purpose** drop-down list select **CallManager-trust**. Browse and upload first the root certificate, followed by the intermediate certificates. From the **Certificate Purpose** drop-down list select **CallManager**. Browse and upload the certificate for the CallManager Service.
   h. For the new certificate to take effect you need to restart the CallManager service in **Cisco Unified Serviceability**, do this during a maintenance period.
2. Upload the root and intermediate certificates of the certificate you generated in step 4 of Section 2.1.1 to the Cisco Unified Communications Manager trust store.
   a. From the Cisco Unified Communications Manager **OS Administration** page, choose **Security > Certificate Management**.
   b. Click **Upload Certificate/Certificate Chain**. The Upload Certificate/Certificate Chain popup window appears.
   c. From the **Certificate Purpose** drop-down list choose **CallManager-trust**.
   d. Browse and upload first the root certificate, followed by the intermediate certificates to **CallManager-trust**.
3. Create a SIP trunk security profile.

Cisco Unified Communications Manager applies a default security profile called **Non Secure SIP Trunk** when you create the SIP Trunk, this is for TCP. To use TLS, or something other than the standard security profile, follow these steps:

a. Log into Cisco Unified Communications Manager Administration.

b. Go to **System > Security > SIP Trunk Security Profile**.

c. Click **Add New**.

d. Complete the fields as follows:

- **Name** = type in a name, e.g. " CMS_SecureTrunk"
- **Device Security Mode** =select **Encrypted**
- **Incoming Transport Type** = select **TLS**
- **Outgoing Transport Type** = select **TLS**
- **X.509 Subject Name** = enter the CN of the Call Bridge certificate.
- **Incoming Port** = enter the port which will receive TLS requests. The default for TLS is **5061**
- **Accept Replaces Header** = check this box if you intend to use Call Bridge Grouping (see Section 6).

e. Click **Save**

Note: For an Ad Hoc conference with at least two conference participants capable of video, Cisco Unified Communications Manager will allocate an encrypted audio conference bridge when the **Device Security Mode** is set to **Encrypted** and if the Service Parameter **Choose Encrypted Audio Conference Instead of Video Conference** is set to **true** (the default). If the parameter has been set to **false** then Cisco Unified Communications Manager will allocate an unencrypted video conference bridge, because encrypted video conference bridges are not currently supported by Cisco Unified Communications Manager. To reset Service Parameter **Choose Encrypted Audio Conference Instead of Video Conference** go to **System > Service Parameters > Clusterwide Parameters (Feature – Conference)**.

---

4. Check that your SIP Profile is configured correctly. If using the default **Standard SIP Profile For TelePresence Conferencing** on Cisco Unified Communications Manager version 10.5.2 or later, this should be sufficient. (If using an older version of Cisco Unified Communications Manager, see Section 5.5.) The key values to ensure are checked are: **Allow iX Application Media**, **Use Fully Qualified Domain Name in SIP Requests**, and **Allow Presentation Sharing use BFCP**.
5. Create the SIP trunk

a. In Cisco Unified Communications Manager, go to **Device >Trunk**.
b. Click **Add New**.
c. Configure these fields:
   - **Trunk Type** = **SIP trunk**
   - **DeviceProtocol** =**SIP**
   - **Trunk Service Type** = **None** (default)
d. Click **Next**
e. Configure the destination information for the SIP trunk, see Table 2 below.

Table 2: Destination information for the SIP Trunk

Field	Description
Device name	Type in a name e.g. CiscoMeetingServer (no spaces allowed)
Device pool	The pool you want your device to belong to (as configured in **System >Device Pool** in Cisco Unified Communications Manager
SRTP Allowed	Select **SRTP Allowed** to allow media encryption
Inbound Calls > Calling Search Space	Select default, not required if only allowing escalated 2-way adhoc calls from Cisco Unified Communications Manager to a meeting on the Meeting Server.
Outbound Calls > Calling Party Transformation CSS	Select as appropriate.
SIP Information > Destination address	Enter the FQDN of a single Meeting Server, it must match the CN of the Meeting Server certificate. Note: For clusters, enter the FQDN of a single Meeting Server
SIP Information > Destination Port	Enter **5061** for TLS
SIP Trunk Security Profile	Select the security profile that you created in step 3.
Rerouting Calling Search Space	When doing call bridge grouping, set this to a calling search space that contains the partitions of the calling parties.
SIP Profile	Select the **Standard SIP Profile For TelePresence Conferencing**
Normalization Script	Assign **cisco-telepresence-conductor-interop** to this SIP trunk. Note: ideally download the latest normalization script from the Cisco website. Even if you do not have a Conductor, the Meeting Server has the same interop issues that Conductor would have, and therefore this script is suitable for a trunk to the core Meeting Server.

Field	Description
Run On All Active Unified CM Nodes	Check this checkbox if you wish calls to egress other CUCM nodes as well.

6. Click **Save** and apply the configuration.
   Use the Trunk List to confirm that the trunk goes into service after a few minutes.

2.2 Configuring a non-secure SIP trunk

Follow the steps in Section 2.2.1 and Section 2.2.2 to set up a non-secure SIP trunk, then follow Chapter 3 to enable rendezvous and scheduled calls between Cisco Unified Communications Manager and Meeting Server.

2.2.1 Configuration required on the Meeting Server

Follow the Cisco Meeting Server deployment guides to configure your Meeting Server, once configured:

1. SSH into the MMP of the Meeting Server
2. If you have not already done so, specify a listening interface using the MMP command **`callbridge listen`**

2.2.2 Configuration required on the Cisco Unified Communications Manager

Our testing has been done on trunks without Media Termination Point (MTP) configured. Therefore:

- Disable MTP if this will not negatively affect your deployment. Turning off MTP might have a negative impact on your deployment if you are using SCCP phones and need to send DTMF to the Meeting Server.
- If the above is not a valid implementation, you may need to increase the MTP capacity on the Cisco Unified Communications Manager depending on the number of simultaneous calls.

1. Create a SIP trunk security profile

   Cisco Unified Communications Manager applies a default security profile called **Non Secure SIP Trunk** when you create the SIP Trunk, this is for TCP. You can use this default security profile, or you can create a new profile by just giving it a name and leaving the other options at their defaults. To verify the default profile settings or create a new one, follow these steps:

   a. Log into Cisco Unified Communications Manager Administration.
   b. Go to **System > Security > SIP Trunk Security Profile**.
   c. Click **Add New**.

d. Complete the Name field as follows:

- **Name** = type in a name, e.g. " CMS_SecureTrunk"

and then verify that the default fields are as follows:

- **Device Security Mode** =select **Non Secure**
- **Incoming Transport Type** = select **TCP+UDP**
- **Outgoing Transport Type** = select **TCP**
- **Incoming Port**. The default for TCP is **5060**
- **Accept Replaces Header** = check this box if you intend to use Call Bridge Grouping (see Section 6).

e. Click **Save**

2. Create the SIP trunk

a. In Cisco Unified Communications Manager, go to **Device >Trunk**.

b. Click **Add New**.

c. Configure these fields:

- **Trunk Type** = **SIP trunk**
- **DeviceProtocol** =**SIP**
- **Trunk Service Type** = **None** (default)

d. Click **Next**

e. Configure the destination information for the SIP trunk, see Table 3 below.

Table 3: Destination information for the SIP Trunk

Field	Description
Device name	Type in a name e.g. CiscoMeetingServer (no spaces allowed)
Device pool	The pool you want your device to belong to (as configured in **System >Device Pool** in Cisco Unified Communications Manager
SRTP Allowed	Do not allow SRTP
Inbound Calls > Calling Search Space	Select default.
Outbound Calls > Calling Party Transformation CSS	Select as appropriate.
SIP Information > Destination address	We recommend entering the Meeting Server FQDN (or rely on the DNS lookups).

Field	Description
SIP Information > Destination Port	Enter **5060** for TCP
Rerouting Calling Search Space	When doing call bridge grouping, set this to a calling search space that contains the partitions of the calling parties.
SIP Trunk Security Profile	Select the security profile created in step 1.
SIP Profile	Select the **Standard SIP Profile For TelePresence Conferencing**
Normalization Script	Not required for a non-secure SIP trunk.

f. Click **Save**.

3 Setting up scheduled and rendezvous calls

After setting up a secure SIP trunk (Section 1.1) or non-secure SIP trunk (see Section 1.2), follow the steps in Section 3.1 and Section 3.2 to enable rendezvous and scheduled calls to be made from the Meeting Server to Cisco Unified Communications Manager.

3.1 Configuring the Meeting Server

1. Configure an outbound dial plan rule for calls that will be sent to Cisco Unified Communications Manager from the Meeting Server.
2. Using the Web Admin interface of the Meeting Server, select **Configuration**>**API**:
   a. From the list of API objects, tap the ► after **/outboundDialPlanRules**
   b. Click **Create new**
   c. Enter the parameters in Table 4 below

Table 4: Setting up the outbound dial plan rule

Parameter	Description
Domain	Enter the domain that will be matched for calls that need to be sent to Cisco Unified Communications Manager
SIP proxy to use	Either: leave this field blank and the server will perform a DNS SRV lookup for the domain entered in step b using **`_sips.tcp.<yourcucmdomain>`**. If this fails to resolve, the server will try a DNS A lookup of **`<yourcucmdomain>`**. If this fails it will try an SRV lookup of **`_sip.tcp.<yourcucmdomain>`**and it that fails then a look up of **`_sips.udp.<yourcucmdomain>`**. or, enter the SIP proxy for the server to use, for example the FQDN of your Cisco Unified Communications Manager. This domain will be resolved as described in the bullet point above. or, enter the IP address of your Cisco Unified Communications Manager.
Local contact domain	Leave this field blank, it is only required when setting up a SIP trunk to Lync or Skype for Business.
Local from domain	Enter the domain that you want the call to be seen as coming from (the Caller ID). **Note:** If you leave **Local from domain** blank, the domain used for the Caller ID defaults to that entered in the **Local contact domain**, in this case blank.
Trunk type	Select Standard SIP.
Priority	Set as required.

Parameter	Description
Encryption	Select the mode that is appropriate to your deployment. For instance, if traffic is not encrypted on the SIP trunk then select “Unencrypted”.

d. Click **Create**

3.2 Configuring Cisco Unified Communications Manager

Cisco Unified Communications Manager uses route patterns, route groups and route lists to direct calls to the correct location.

A route group allows you to designate the order in which trunks are selected. For example, if you use two long-distance carriers, you could add a route group, so long-distance calls to the less expensive carrier are given priority; calls route to the more expensive carrier only if the first trunk is unavailable.

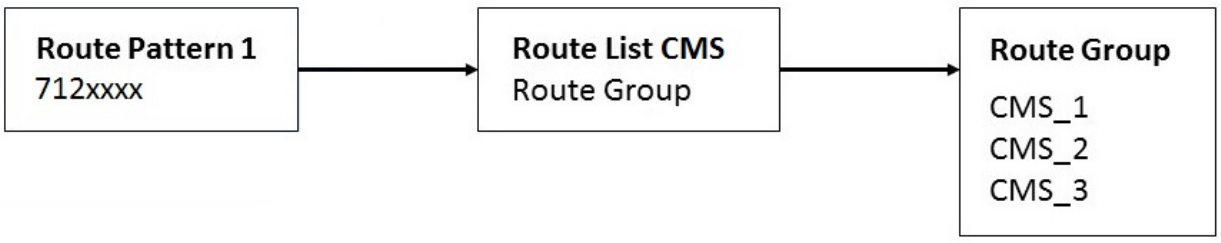
A route list associates a set of route groups in a specified priority order. A route list then associates with one or more route patterns and determines the order in which those route groups are accessed. The order controls the progress of the search for available devices for outgoing calls. A route list can contain only route groups. Each route list should have at least one route group. You can add a route group to any number of route lists.

A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns work in conjunction with route filters and route lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

Media resource groups define logical groupings of media servers. You can associate a media resource group with a geographical location or a site, as desired. You can also form media resource groups to control the usage of servers or the type of service (unicast or multicast) that is required.

For more information on route groups, route lists and resource groups, see the Cisco Unified Communications Manager System Guide for your Cisco Unified Communications Manager version.

Figure 3: Directing calls to the correct location



Note: If you are not configuring a scalable and resilient Meeting Server deployment then you do not need to set up route groups or route lists on Cisco Unified Communications Manager. When configuring the dial plan for outbound calls from the Cisco Unified Communications Manager simply create a route pattern, for domain based routing point the **SIP Trunk/Route List** to the SIP trunk you configured previously, for numeric dialing point **the Gateway/Route List** to the SIP trunk you configured previously, and then select the **Route Option** as **Route this pattern**.

3.2.1 Configure Route Groups

1. Log into the Cisco Unified Communications Manager Administration interface:
2. Go to **Call Routing** > **Route/Hunt** > **Route Group**. A list of existing Route Groups is displayed.
3. If none are appropriate, click **Add New**.
4. Complete the following:
   - Route Group Name = type a name that reflects the purpose of the Route Group, for instance: CMS_1
   - Select the distribution algorithm from the drop-down, for example **Top Down**
   - Select the appropriate SIP trunk from the **Available Devices** list and click on the **Add to Route Group** button
   - The other fields appropriate to this Route Group
5. Click **Save**.
6. Check that the new Route Group has been created by checking the list of Route Groups.

3.2.2 Configure Route Lists

1. Go to **Call Routing** > **Route/Hunt** > **Route List**. A list of existing Route Lists is displayed.
2. If none are appropriate, click **Add New**.
3. Complete the following:
   - Name = type a name that reflects the purpose of the Route List, for instance: Route List US
   - From the **Cisco Unified Communications Manager Group** drop-down select **Default**
   - Click **Save**.
   - From the **Route List Member Information** section, select **Add Route Group** and select the Route Group to add to the list of **Selected Groups**.
   - The other fields appropriate to this Route List
4. Click **Save**.
5. Check that the new Route List has been created by checking the list of Route Lists.

3.2.3 Configure route patterns (dial plans for outbound calls)

You can configure domain based routing e.g. @mydomain.example.com or number based routing e.g. 7XXX, to the Meeting Server through the Cisco Unified Communications Manager interface. For example:

Domain based routing example

To route all domain based calls from Cisco Unified Communications Manager to the Meeting Server:

1. Go to **Call Routing** > **Sip Route Pattern**.
2. If none are appropriate, click **Add New**.
3. Complete the following:
   - Pattern Usage = Domain Routing
   - IPv4 pattern something like **mydomain.example.com**
   - Description = anything you want
   - Route Partition = the route partition you want this rule to belong to

   Note: : Various dial plan rules are attached to a route partition and a Calling Search Space (CSS) comprises a list of route partitions. You can have a different CSS for different people, each phone, or trunk. When a call is made, Cisco Unified Communications Manager goes through each route partition in the CSS until it finds one that has a matching rule.
4. Click **Save**.

Numeric dialing example

This basic example routes everything starting with a 7 to the Meeting Server.

1. Go to **Call Routing** > **Route/Hunt** > **Route Pattern**. A list of existing Route Patterns is displayed.
2. If none are appropriate, click **Add New**.
3. Complete the following:
   - Route pattern = 703777XXX (Further down the page you can set various transforms e.g. in the Discard Digits field you can select PreDot to strip off the leading 7 in our example.)
   - Route partition = the route partition you want this rule to belong to

     Note: : Various dial plan rules are attached to a route partition and a Calling Search Space (CSS) comprises a list of route partitions. You can have a different CSS for different people, each phone, or trunk. When a call is made, Cisco Unified Communications Manager goes through each route partition in the CSS until it finds one that has a matching rule.
   - Description = any appropriate text
   - From the **Gateway/Route List** drop-down, select the Route List to add to the Route Pattern
4. Click **Save**.
5. Make some test calls. You will need an endpoint registered to Cisco Unified Communications Manager, and on the Meeting Server you need to create a space and an inbound dial plan rule to accept the call from Cisco Unified Communications Manager. See the appropriate Cisco Meeting Server Deployment Guide for information on how to do this.

3.3 Updating Cisco Jabber presence

Meeting Server can be configured to update the presence status of Cisco Jabber (Jabber) users, while they are in a Cisco Meeting Server web app meeting.

For presence to be updated on Jabber:

- Meeting Server login ID should be email and it should map to $mail$ attribute of AD.
- In Cisco Unified Communications Manager, the same user should have $mail$ attribute mapped to Directory URI field.
- Jabber login can happen either through Directory URI or User ID field from Cisco Unified Communications Manager.

Note: Cisco does not guarantee that a beta feature will become a fully supported feature in the future. Beta features are subject to change based on feedback, and functionality may change or be removed in the future.

When a Jabber user signs into web app and joins a meeting, Meeting Server updates the Jabber status to 'On a call' and reverts to their previous status after the user ends the meeting.

Meeting Server does not update the Jabber status in the following cases:

- If the Jabber user is in another meeting/call while joining the web app meeting Meeting Server does not update the Jabber status.
- If the Jabber user has set their status to **DND - Do not disturb** before joining the web app meeting, Meeting Server does not update the Jabber status.
- If the user updates the Jabber status manually anytime during the web app meeting, Meeting Server does not override the manually updated user status.

Note:

- This feature does not support web app participants joining as guest or participants joining through SIP endpoints, Lync, or Skype.
- Meeting Server will not update the presence for content share.

To update the user presence, configure the Meeting Server with a Cisco Unified Communications Manager node that provides AXL service. Meeting Server can be configured with multiple clusters, each with a maximum of 5 Cisco Unified Communications Manager clusters and 6 IMP nodes per Cisco Unified Communications Manager cluster. User presence will be updated regardless of the Cisco Unified Communications Manager/IMP node to which the users are assigned.

Note: The Meeting Server connects with the IMP server using TCP port 8083. If there is a firewall between IMP servers and Meeting Server call bridge, it is recommended to open this port to allow communication.

3.3.1 Configuring Cisco Unified Communications Manager

To update the presence on Jabber, the following users must be created on the Cisco Unified Communications Manager node:

- **AXL user - `<axl_user>`** - This user is an application user with the role **`Standard AXL API Access`**. Administrators must create a new user group with the role **`Standard AXL API Access`**, and assign it to the user.
- **Presence user** - **`<presence_user>`** - This user is an application user assigned to the predefined group **Admin-3rd Party Api**.

Note:

- All clusters must have ILS running in their deployments.
- Inter-cluster peering must be enabled on all IMPS nodes.

3.3.1.1 Creating user group and assigning roles

Follow the steps below to create a new group with the role **`Standard AXL API Access:`**

1. Log into the Cisco Unified Communications Manager Administration interface:
2. Go to **User Mnagement** > **User Settings** > **Access Control Group**.
3. Click **Add New**.
4. In the **Access Control Group Information** section, enter the following information:
   - **Name** = type the name of the axl group, for example: CUCM_AXL_Group
5. On the top right corner, go to **Related Links > Assign Role to Access Control Group**
6. Select **Standard AXL API Users** and click **Add selected**.
7. Click **Save**.

3.3.1.2 Creating users and assigning user groups

Follow the steps below to create AXL and presence users and assign appropriate groups to them:

1. Go to **User Management > Application User > Add New**
2. Complete all the information required in **Add New user** page.
3. In the section **Permissions Information**, select **Add to Access control group**.
4. From the list of available **Access Control Groups**:
   a. for AXL-user - select the group that was created by following the steps mentioned in Section 3.3.1.1.
   b. for presence_user - select the group **Admin-3rd Party API**
5. Click **Add Selected**.
6. Click **Save**.

3.3.2 Enabling secure communication between between Meeting Server and Cisco Unified Communications Manager/IMP Server

The callbridge certificate bundle must be uploaded to the CUPS trust store for IMP server and Tomcat trust store for Cisco Unified Communications Manager.

Similarly, the CUPS certificate for IMP Server and Tomcat certificate for Cisco Unified Communications Manager must be uploaded and verified in the Meeting Server. Refer to MMP user guide for details on certificate validation.

3.3.3 Configuring the Meeting Server

Configure Meeting Server with a Cisco Unified Communications Manager node that provides AXL service. Meeting Server can be configured with multiple clusters, each with a maximum of 5 CUCM clusters and 6 IMP nodes per CUCM cluster.

Provide the hostname/IP address of the Cisco Unified Communications Manager and the Application user credentials of AXL and IMP servers, using the MMP command **`callbridge ucm add <hostname/IP> <axl_user> <presence_user>`**. See Cisco Meeting Server MMP Command Line Reference Guide for the list of commands. The commands must be run individually for each CUCM cluster.

4 Setting up escalated ad hoc calls

After setting up the secure SIP trunk (see Section 1.1), follow the steps in Section 4.1 and Section 4.2 to enable the escalation of a 2-way call on Cisco Unified Communications Manager to a conference on the Meeting Server.

Note: If you decided to set up the SIP trunk as non-secure, you will still need to use certificates, as the escalation of a 2-way call on Cisco Unified Communications Manager to a conference on the Meeting Server, requires the Cisco Unified Communications Manager to communicate with the API of the Cisco Meeting Server. The API requires HTTPS communication, so certificates need to be created and uploaded to both the Cisco Meeting Server and Cisco Unified Communications Manager and each needs to trust the other's certificate, in order for escalated ad hoc calls to work.

Note: Cascades between a space and a S4B gateway call are supported. However, dialing into a space and adding an ad hoc call to escalate to the same Meeting Server (i.e. cascading between two spaces) is not supported. Cascading between two spaces on different Meeting Servers is possible but not recommended due to the possibility of poor user experience.

4.1 Configuring the Meeting Server

1. Set up an incoming dial plan on the Meeting Server. See the appropriate Cisco Meeting Server Deployment Guide. (Note: For adhoc calls the trunk address defined in Cisco Unified Communications Manager should be in your inbound call rules, i.e. your trunk address is what your incoming URIs from Cisco Unified Communications Manager will use.)
2. Set up an administrator user account with " api" permission for Cisco Unified Communications Manager to use. See the Cisco Meeting Server MMP Command Line Reference Guide.

4.2 Configuring Cisco Unified Communications Manager

For ad hoc calls between Cisco Unified Communications Manager and the Meeting Server, Cisco Unified Communications Manager needs to access the API of the Meeting Server through an HTTPS connection. If you have different certificates for the Call Bridge and Web Admin, you need to upload any Root and Intermediate CA certificates that signed the Meeting Server Web Admin certificate to the trust store on Cisco Unified Communications Manager. This must be done regardless of whether you configured a secure or non-secure SIP trunk. Check that this has been done before proceeding with the steps in this section.

Note: Step 2 in Section 4 explains how to upload certificates to the trust store on Cisco Unified Communications Manager through **CallManager-trust**.

The Meeting Server is treated as a conference bridge on Cisco Unified Communications Manager.

1. For each Meeting Server, create the Conference Bridge
    a. In Cisco Unified Communications Manager Administration, select **Media Resources > Conference Bridge**. The **Find and List Conference Bridges** window displays.
    b. Click **Add New**. The **Conference Bridge Configuration** window displays.
    c. Select **Cisco Meeting Server** from the **Conference Bridge Type** drop-down list. (If you are using an older version of Cisco Unified Communications Manager software that does not have **Cisco Meeting Server** as an option, select **Cisco TelePresence Conductor**.)
    d. Enter a name and description for the Meeting Server in the **Device Information** pane.
    e. Enter a **Conference Bridge Prefix** if deploying ad hoc conferencing for a centralized deployment where the Meeting Servers are not directly connected to this Cisco Unified Communications Manager cluster. This is explained in more detail in Appendix A.

        Note: Set a unique Conference Bridge Prefix for each pair of Meeting Server node and Cisco Unified Communications Manager cluster in the deployment.

    f. Select a SIP trunk from the **SIP Trunk** drop-down list.
    g. Enter the **HTTP interface information** to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco Meeting Server. Note:
        i. This must match your Web Admin Interface and port.
        ii. Check the **Override SIP Trunk Destination as HTTP Address** checkbox if your Web Admin is listening on a different address to your SIP trunk.
        iii. The address field must match your certificate loaded on Web Admin.
    h. Click **Save** and then click **Reset**.
    i. Verify the Meeting Server is registered with Cisco Unified Communications Manager.
2. Add the Meeting Servers to Media Resource Groups (MRGs):

    The number of MRGs will depend on the topology of your deployment.
    a. Go to **Media Resources** > **Media Resource Group**.
    b. Click **Add New** to create a new media resource group and enter a name.

c. Move one or more of the conference bridges created in step 1 from the **Available Media Resources** box to the **Selected Media Resources** box.

d. Click **Save**.

3. Add the Media Resource Groups (MRGs) to the Media Resource Group Lists (MRGLs). The number of MRGLs will depend on the topology of your deployment.

   For each MRGL:

   a. Go to **Media Resources** > **Media Resource Group List**.

   b. Click **Add New** to create a new media resource group list and enter a name, or select an existing MRGL and click on it to edit it.

   c. Move one or more of the Media Resource Groups created in step 2 from the **Available Media Resource Groups** box to the **Selected Media Resource Groups** box.

   d. Click **Save**.

4. Add the 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 to a specific MRGL. If an MRGL is applied to both a Device Pool and an endpoint, the endpoint setting will be used. For further information on Device Pools or Devices see the Cisco Unified Communications Manager documentation.

   a. Go to **System** > **Device Pool**.

   b. Click **Add New** to create a new Device Pool and enter a name, or select an existing Device pool and click on it to edit it.

   c. In the **Device Pool Settings** section, select the appropriate Cisco Unified Communications Manager Group from the drop-down list.

   d. In the **Roaming Sensitive Settings** section, use the drop-down lists to select the **Date/Time Group**, **Region**, and the **Media Resource Group List** created in step 2f above. Leave other fields as their default (or previously configured) values.

   e. Click **Save** and **Reset** for the changes to take effect. If there are devices associated with the pool, they will reboot when Reset is clicked.

      If a new Device Pool has been created:

   f. Go to **Device** > **Phones**.

   g. Click **Find** and select the device to change the Device Pool settings on.

   h. Select the Device Pool created in step 3b above from the drop-down list.

   i. Click **Save**.

j. Click **Apply Config**.

k. Click **Reset** for the changes to take effect. This will reboot the endpoints when applied

5. If deploying with Cisco Unified Communications Manager Session Management Edition, then either:

   a. set up dial plan rules for calls that have the conference bridge prefix set (step 1e) which point to the appropriate Meeting Server node.

   b. configure the trunks from leaf nodes with an LUA script that strips out the call information header, and configure the dial plan rules to point to all Meeting Server nodes.

Note: See Appendix A for the steps in setting up ad hoc call escalation between a Meeting Server node and Cisco Unified Communications Manager. The appendix also provides an example LUA script that strips out the call information header.

4.3 Escalated ad hoc calls and licenses

Escalated ad hoc calls use either PMP Plus or SMP Plus licenses. For a PMP Plus license to be used:

1. Cisco Unified Communications Manager must provide the objectGUID of the user escalating the call.
2. A user with that objectGUID must have been imported into Meeting Server.
3. The user must have a PMP Plus license associated with them.

Note: Cisco Unified Communications Manager currently only provides the objectGUID for users imported from Active Directory. If using another LDAP source, Cisco Unified Communications Manager does not pass the necessary information to Meeting Server.

---

5 Support for ActiveControl

The Meeting Server supports ActiveControl for hosted calls. For participants using a Cisco SX, MX or DX endpoint with CE 8.3+ software installed, ActiveControl allows the meeting participant to receive details of the meeting and perform a few administrative tasks during the meeting, using the endpoint interface.

5.1 ActiveControl on the Meeting Server

The Meeting Server supports sending the following meeting information to ActiveControl enabled endpoints:

- Participant list (also known as the roster list) so that you can see the names of the other people in the call and the total number of participants,
- indicator of audio activity for the currently speaking participant,
- indicator of which participant is currently presenting,
- Indicators telling whether the meeting is being recorded or streamed, and if there are any non-secure endpoints in the call,
- on screen message which will be displayed to all participants,

and supports these administrative tasks on ActiveControl enabled endpoints:

- select the layout to be used for the endpoint,
- disconnect other participants in the meeting.

5.2 Limitations

- If an ActiveControl enabled call traverses a Unified CM trunk with a Unified CM version lower than 9.1(2), the call may fail. ActiveControl should not be enabled on older Unified CM trunks (Unified CM 8.x or earlier).
- ActiveControl is a SIP only feature. H.323 interworking scenarios are not supported.

5.3 Overview on ActiveControl and the iX protocol

ActiveControl uses the iX protocol, which is advertised as an application line in the SIP Session Description Protocol (SDP). The Meeting Server automatically supports ActiveControl, but the feature can be disabled, see section Section 5.4 . In situations where the far end network is not known or is known to have devices that do not support the iX protocol, it may be safest to disable iX on SIP trunks between the Meeting Server and the other Call control or Video Conferencing devices. For instance:

- for connections to Unified CM 8.x or earlier systems the older Unified CM systems will reject calls from ActiveControl-enabled devices. To avoid these calls failing, leave iX disabled on any trunk towards the Unified CM 8.x device in the network. In cases where the 8.x device is reached via a SIP proxy, ensure that iX is disabled on the trunk towards that proxy.
- for connections to third-party networks. In these cases there is no way to know how the third-party network will handle calls from ActiveControl-enabled devices, the handling mechanism may reject them. To avoid such calls failing, leave iX disabled on all trunks to third-party networks.
- for Cisco VCS-centric deployments which connect to external networks or connect internally to older Unified CM versions. From Cisco VCS X8.1, you can turn on a zone filter to disable iX for INVITE requests sent to external networks or older Unified CM systems. (By default, the filter is off.)

5.4 Disabling UDT within SIP calls

ActiveControl uses the UDT transport protocol for certain features, for example sending roster lists to endpoints, allowing users to disconnect other participants while in a call, and inter-deployment participation lists. UDT is enabled by default. You can disable UDT for diagnostic purposes, for example if your call control does not use UDT, and you believe this is the reason the call control does not receive calls from the Meeting Server.

Using the Web Admin interface of the Meeting Server, select **Configuration**>**API**:

1. From the list of API objects, tap the ► after **/compatibilityProfiles**
2. Either click on the **object id** of an existing compatibility profile or create a new one
3. Set parameter **sipUDT** = **false**. Click **Modify**.
4. From the list of API objects, tap the ► after **/system/profiles**
5. Click the **View or edit** button
6. Click **Choose** to the right of parameter **compatiilityProfile**. Select the **object id** of the compatibilityProfile created in step 3 above
7. Click **Modify**.

5.5 Enabling iX support in Cisco Unified Communications Manager

Support for the iX protocol is disabled by default on the Cisco Unified Communications Manager for some SIP profiles. To enable iX support in Unified CM, you must first configure support in the SIP profile and then apply that SIP profile to the SIP trunk.

Configuring iX support in a SIP profile

1. Choose **Device > Device Settings > SIP Profile**. The Find and List SIP Profiles window displays.
2. Do one of the following:
   a. To add a new SIP profile, click **Add New**.
   b. To modify an existing SIP profile, enter the search criteria and click **Find**. Click the name of the SIP profile that you want to update.

   The SIP Profile Configuration window displays.
3. Check the check box for **Allow iX Application Media**
4. Make any additional configuration changes.
5. Click **Save**

Applying the SIP profile to a SIP trunk

1. Choose **Device > Trunk**.

   The Find and List Trunks window displays.
2. Do one of the following:
   a. To add a new trunk, click **Add New**.
   b. To modify a trunk, enter the search criteria and click **Find**. Click the name of the trunk that you want to update.

   The Trunk Configuration window displays.
3. From the SIP Profile drop-down list, choose the appropriate SIP profile.
4. Click **Save**.
5. To update an existing trunk, click **Apply Config** to apply the new settings.

5.6 Filtering iX in Cisco VCS

To configure the Cisco VCS to filter out the iX application line for a neighbor zone that does not support the protocol, the zone must be configured with a custom zone profile that has the SIP UDP/IX filter mode advanced configuration option set to On.

To update advanced zone profile option settings:

1. Create a new neighbor zone or select an existing zone (**Configuration > Zones > Zones**).
2. In the Advanced parameters section, for **Zone profile**, choose *Custom* if it is not already selected. The zone profile advanced configuration options display.

3. From the **SIP UDP/IX filter mode** drop-down list, choose **On**.
4. Click **Save**.

5.7 iX troubleshooting

Table 5: Call handling summary for calls that contain an iX header

Scenario	Outcome
Unified CM 8.x or earlier	Calls fail
Unified CM 9.x earlier than 9.1(2)	Calls handled normally but no ActiveControl
Unified CM 9.1(2)	Calls handled normally plus ActiveControl
Endpoint - no support for iX and no SDP implementation	Endpoint may reboot or calls may fail

6 Overview of load balancing calls

This chapter explains how to increase the scalability and resilience of the Meeting Servers within a Cisco Unified Communications Manager deployment.

Call Bridge grouping is used to load balance calls across clustered Call Bridges. The Cisco Unified Communications Manager's primary role is to move calls between Call Bridge groups as instructed by the Cisco Meeting Servers. Each trunk to a local Call Bridge must be configured to use a SIP Trunk Security Profile that has the "Accept Replaces Header" check box selected. For more information see the Security Guide for Cisco Unified Communications Manager.

Balancing incoming calls over local Call Bridges is achieved by configuring a route group per location on the Cisco Unified Communications Manager, the route group contains links to the local conference resources in that location. The route group should be set up with circular distribution to load balance calls across the Meeting Servers. See Section 6.1.

Balancing outgoing calls over local Call Bridges is achieved by enabling load balancing of outbound SIP calls from spaces, and setting up outbound dial plan rules for load balancing outbound SIP calls. See Section 6.2.

For background information and examples of load balancing calls across Meeting Servers, see the white paper.

Note: Load balancing of incoming calls involves outbound calls from Call Bridges to Cisco Unified Communications Manager. For these outbound calls to work, outbound dial plan rules must be configured, see Section 3.1.

6.1 Configuring Call Bridges for load balancing incoming calls

There are three aspects to setting up the load balancing of calls across a Meeting Server cluster:

- creating the Call Bridge Groups,
- enabling load balancing,
- and optionally, fine-tuning the load balancing on each Call Bridge. In most deployments this will not be necessary.

In addition, load balancing incoming calls involves outbound calls from Call Bridges to Cisco Unified Communications Manager or Cisco Expressway. For these outbound calls to work, outbound dial plan rules must be configured, see Load balancing outbound SIP calls .

Note: If load balancing incoming calls involves outbound calls from Call Bridges to Cisco VCS, instead of Cisco Expressway, then a traversal license is required on the VCS. There is no

---

requirement for a Rich Media Session license on Cisco Expressway for any load balanced Meeting Server deployments.

Note: If you are not using load balancing with Call Bridge Groups, then calls will not be rejected, but the quality of all calls will be reduced when the load limit is reached. If this happens often, we recommend that you buy additional hardware.

6.1.1 Creating Call Bridge Groups

1. For each Meeting Server cluster, decide how to group the Call Bridges, for instance by data center or by country or region.
2. Using the Web Admin interface of one of the servers in the cluster, select **Configuration**>**API**
3. Create a new Call Bridge Group
   a. From the list of API objects, tap the ► after **/api/v1/callBridgeGroups**
   b. Select the **Create new** button, enter the name of the new callBridgeGroup and set the parameters for the Call Bridge Group. Select **Create**.
   c. The new group will appear in the list of callBridgeGroups.
4. Identify the Call Bridges to be grouped
   a. From the list of API objects, tap the ► after **/api/v1/callBridges**
   b. Select each Call Bridge to be added to the group by clicking on the callBridge id
      i. Click on the **Choose** button beside the **callBridgeGroup** field, and select the callBridgeGroup created in step3b
      ii. Click **Modify**
   c. Repeat step 4b for each Call Bridge that needs to be added to the Call Bridge Group.
5. Repeat for all other Call Bridge Groups.

6.1.2 Specifying the load limit on a cluster and enabling load balancing

1. On each Call Bridge in a cluster, specify the load limit for that server
   a. From the list of API objects, tap the ► after **/system/configuration/cluster**
   b. Select the **View or edit** button, and enter a value for **loadLimit**. Click the **Modify** button. This sets a load limit for the maximum load on the server, see Table 6 for load limits.

Table 6: Load limits for server platforms

System	Load Limit
Meeting Server 2000 M5v2	875,000

System	Load Limit
Meeting Server 2000	700,000
Meeting Server 1000 M5v2	120,000
Meeting Server 1000	96,000
VM	1250 per vCPU

Note: Increased load limits for Meeting Server 1000 M5v2 and Meeting Server 2000 M5v2 require Meeting Server software version 3.2.

Setting a load limit on any Call Bridge means it will reject calls based on the current load. By default, the rejection of calls from new participants occurs at 80% of the load limit to allow for the distribution of calls. This value can be fine tuned, see below.

2. Enable load balancing on each server in the cluster.

   For Cisco Unified Communications Manager deployments:

   a. From the list of API objects, tap the ► after **/callBridgeGroups**
   b. Click on the **object id** of the Call Bridge Group trunked to Cisco Unified Communications Manager
   c. Set **loadBalancingEnabled**=**true**. Click **Modify**

   For Cisco Expressway deployments:

   a. From the list of API objects, tap the ► after **/callBridgeGroups**
   b. Click on the **object id** of the Call Bridge Group trunked to Cisco Expressway
   c. Set **loadBalancingEnabled**=**true** and set **loadBalanceIndirectCalls**=**true**. Click **Modify**

   For Cisco Unified Communications Manager deployments:

   a. From the list of API objects, tap the ► after **/callBridgeGroups/<call bridge group>**
   b. Select the **View or edit** button, and set **loadBalancingEnabled**=**true**. Click the **Modify** button

Tip: If you have only one Call Bridge, and you want to reject calls rather than reducing quality, then create a Call Bridge Group with a single Call Bridge and enable load balancing.

6.1.3 Fine-tuning the load balancing

It is possible to fine tune the load balancing parameters, but take care as it could impact the availability of the solution. Changing the default values may lead to overloading of servers and a degradation of video quality. This could occur due to either conferences becoming fragmented over multiple Call Bridges, or conferences using too many resources on a single Call Bridge.

Load balancing calls on a Call Bridge is controlled by 3 parameters:

- **loadLimit** – a numeric value for the maximum load on the Call Bridge, as set above.
- **newConferenceLoadLimitBasisPoints** – a numeric value for the basis points (1 in 10,000) of the load limit at which incoming calls to non-active conferences will be disfavored, ranges from 0 to 10000, defaults to 5000 (50% load). Value is scaled relative to **LoadLimit**.
- **existingConferenceLoadLimitBasisPoints** – a numeric value for the basis points of the load limit at which incoming calls to this Call Bridge will be rejected, ranges from 0 to 10000, defaults to 8000 (80% load). Value is scaled relative to **LoadLimit**.

To change the default threshold values for a Call Bridge:

1. From the list of API objects, tap the ► after **/system/configuration/cluster**
2. Select the **View or edit** button, and set values for **newConferenceLoadLimitBasisPoints** and **existingConferenceLoadLimitBasisPoints**. Click **Modify**.

Note: distribution calls are always accepted, and will consume additional resources. If modifying the load balancing parameters, ensure that any necessary overhead for these calls has been included in the calculations.

6.1.4 How load balancing uses the settings

Within each Call Bridge Group there is a particular preference order in which Call Bridges will be chosen for each space. Any call for a space landing anywhere in the Call Bridge Group will be preferentially redirected to Call Bridges based on this order. The redirection is based on two thresholds: the existing conference threshold and the new conference threshold.

The thresholds are defined as:

existing conference threshold = existingConferenceLoadLimitBasisPoints/10000×loadLimit

new conference threshold = newConferenceLoadLimitBasisPoints/10000×loadLimit

When a call lands on a Call Bridge the load limit is checked, if the load limit is above the existing conference threshold, then the call is rejected. Note calls can also be rejected for other reasons. Rejected calls should be redirected by the call control device.

If the load limit is below the existing conference threshold, then the call will be answered and any IVRs traversed. Once the conference is known then the Call Bridge preference order within the group can be determined. This order is used to decide between Call Bridges in cases where there are multiple Call Bridges that could be chosen.

If any Call Bridges within the group are already running the conference, then the load limits of these Call Bridges are checked. If any of these are below the existing conference threshold, then one of these will be used.

If no Call Bridge has yet been chosen, then one of the Call Bridges with a load limit less than the existing conference threshold is chosen.

6.2 Load balancing outbound SIP calls

Call Bridge Groups supports the load balancing of outbound SIP calls, in addition to inbound SIP calls.

To load balance outbound SIP calls, do the following:

- enable load balancing of outbound SIP calls from spaces,
- set up outbound dial plan rules for load balancing outbound SIP calls,
- supply the Call Bridge Group or a specific Call Bridge for the outbound SIP calls.

Once load balancing is enabled, outbound SIP calls follow the logic:

- Find the highest priority outbound dial plan rule that matches the domain,
  - if this applies to a local Call Bridge, then balance the call within the local Call Bridge Group.
  - if this only applies to remote Call Bridges, then load balance the call within the Call Bridge Group to which the Call Bridge is a member.

For examples on load balancing SIP calls across Call Bridge Groups, see the white paper: Load Balancing Calls Across Cisco Meeting Servers.

Note: Load balancing of calls from/to Lync clients, is not currently supported by Call Bridge Groups.

6.2.1 How to enable load balancing of outbound SIP calls

To configure the Call Bridges in a specific Call Bridge Group, to attempt to load balance outgoing SIP calls from spaces:

1. From the list of API objects, tap the ► after **/callBridgeGroups**
2. Click on the **object id** of the selected Call Bridge Group or **Click new** to create a new Call Bridge Group.
3. Set **loadBalanceOutgoingCalls** = **true**. Click **Modify**.

For load balancing of outbound calls, each Call Bridge in the group must have the same dial plan rules.

6.2.2 How to set up an outbound dial plan rule for load balancing outbound SIP calls

There are 3 ways to set up outbound dial plan rules for load balancing outbound SIP calls:

1. Setting the **scope** parameter to **global** in all of the outbound dial plan rules. This ensures that all Call Bridges are able to use all of the outbound dial plan rules to reach a matching domain.
2. Creating identical outbound dial plan rules for each Call Bridge in the Call Bridge Group. Set the **scope** parameter to **callBridge**. Use the **callBridge** parameter to set the **ID** of the Call Bridge.
3. Creating outbound dial plan rules for the specific Call Bridge Group. Set the **scope** parameter to **callBridgeGroup**, and set the **callBridgeGroup** parameter to the **ID** of the Call Bridge Group.

Before using load balancing of outbound calls, review the existing outbound dial plan rules for each Call Bridge in the Call Bridge group:

1. From the list of API objects, tap the ► after **/outboundDialPlanRules**
2. Either create a new outbound dial plan rule or click on the **object id** of an existing outbound dial plan that you plan to use for load balancing outbound SIP calls
3. Select the settings for **scope**, **callBridge** and **callBridgeGroup** depending on how you plan to use the dial plan (see the 3 alternative ways above)

6.2.3 How to supply the Call Bridge Group or specific Call Bridge to use for outbound SIP calls to participants

To make a call from a specific Call Bridge Group,

1. From the list of API objects, tap the ► after **/calls**
2. Click on the **object id** of the individual call
3. Select **api/v1/calls/<call id>/participants** from the **Related objects** at the top of the page
4. Scroll down the parameters to **callBridgeGroup**, tick the box and click **Choose**. Select the **object id** of the Call Bridge Group to use for this call. Click **Create**.

6.2.4 Handling load balancing of active empty conferences

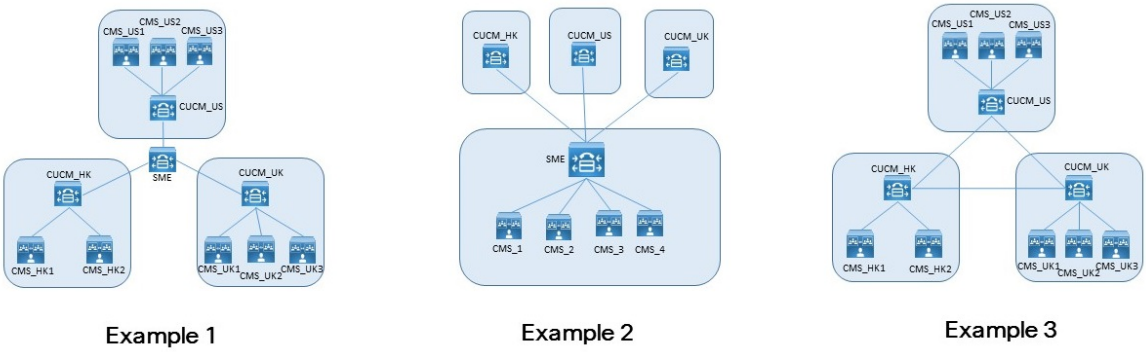
The load balancing algorithm preferentially places new calls onto a Call Bridge where the conference is already active. An empty conference can be started on a Call Bridge by selecting **/calls** from the API object list and then clicking on **Create new**. By default these empty conferences are treated as active. This means that the first call to the empty conference is preferentially load balanced to this Call Bridge. You can prevent the load balancing preferentially using the empty conferences, by setting the parameter **activeWhenEmpty** to **false** when creating the new call.

6.3 Example deployments of load balancing incoming calls using Cisco Unified Communications Manager

The white paper on Load balancing discusses three deployment examples to load balance calls using Cisco Unified Communications Manager as the call control device.

- Example 1 has the Meeting Servers trunked to their local Cisco Unified Communications Manager. The Cisco Unified Communications Managers connect to a Cisco Unified Communications Manager Session Management Edition (SME) as leaf nodes. The SME routes calls between the nodes.
- Example 2 has centralized Meeting Servers trunked to an SME and a global Cisco Unified Communications Manager deployment.
- Example 3 has the Meeting Servers trunked to their local Cisco Unified Communications Manager. The Cisco Unified Communications Managers are simply trunked together, there is no SME to centrally route the calls.

Figure 4: The three example deployments for load balancing incoming calls



Example 1 Example 2 Example 3

For any deployment, there are three options for how calls from different devices are mapped to specific resources:

- Multiple partitions with Calling Search Spaces used to select the correct partition.
- Single partition with Local Route Groups. Selection of routes is done via multiple device pools.
- Dial string manipulation within a single partition per cluster.

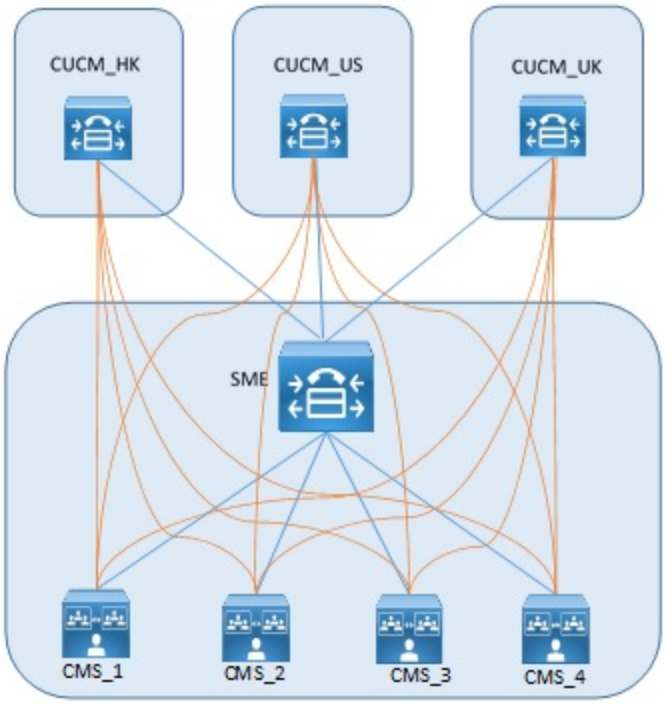
Each of these options can be used with any of the deployments.

The last option is easy to do for numeric dial plans, but for URI dialing, LUA scripts will be required. The other two options work equally well for numeric and URI dialing.

For further details on these examples of load balancing incoming calls across Meeting Servers, and examples of load balancing outbound calls, see the white paper.

Appendix A Adhoc escalation with multiple clusters.

In cases where adhoc resources are shared between multiple Cisco Unified Communications Manager clusters then additional considerations apply. The most common case where this occurs is when using a centralised deployment along with Cisco Unified Communications Manager Session Management Edition (SME).



For example in the figure above, the orange lines correspond to the https Meeting Server nodes, and the blue lines are the SIP trunks in use.

The two additional considerations are:

1. Use of unique Conference Bridge Prefixes
2. Ensuring calls hit the correct Call Bridge.

A.1 Use of unique Conference Bridge Prefixes

Since each Cisco Unified Communications Manager cluster acts independently, then two clusters could both try to use the same conference ID for a conference at the same time. This can be solved by assigning each conference bridge a unique conference bridge ID when setting it up in Cisco Unified Communications Manager (see step 1e in Section 4.2)

For example

Cisco Unified Communications Manager cluster	Meeting Server node	Conference bridge prefix
CUCM_HK	CMS_1	888101
CUCM_HK	CMS_2	888201
CUCM_HK	CMS_3	888301
CUCM_HK	CMS_4	888401
CUCM_US	CMS_1	888102
CUCM_US	CMS_2	888202
CUCM_US	CMS_3	888302
CUCM_US	CMS_4	888402
CUCM_UK	CMS_1	888103
CUCM_UK	CMS_2	888203
CUCM_UK	CMS_3	888303
CUCM_UK	CMS_4	888403

A.2 Ensuring calls hit the right Call Bridge

When using multiple Meeting Server nodes it is recommended to use either a dial plan or Call Bridge Groups to ensure that all calls for a single conference land on the same Call Bridge.

The use of unique prefixes for the calls means that calls can be directed to the correct resource, and by careful choice of prefix, the number of rules can be minimised. For example:

Prefix	Meeting Server node
88810	CMS_1
88820	CMS_2
88830	CMS_3
88840	CMS_4

When using Call Bridge Groups, an alternative is to use an LUA script on the SME to strip a Cisco Unified Communications Manager header. If this header is not stripped, then the attempt to load balance the call will fail.

```
M = {}
trace.enable()
trace.format("***Remove_Call_Info_header_with_conference_tag***")
function M.inbound_INVITE(msg)
trace.format("***Remove_Call_Info_header_with_conference_tag_Inside_
INVITE***")
msg:removeHeaderValue("Call-Info", "<urn:x-cisco-remotecc:conference>")
```

```
end
return M
```

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco Trademark