Cisco Meeting Server

Cisco Meeting Server Release 2.0.6

Release Notes

October 12, 2016

Cisco Systems, Inc.   www.cisco.com

Contents

1 Introduction ... 4

2 New Features/Changes in 2.0 ... 5

2.1 Introducing the Cisco Meeting Server 1000 and Cisco Meeting Server software ... 6

2.1.1 Cisco Meeting Server 1000 Release 2.0 ... 6

2.1.2 Supported Hardware ... 7

2.2 Cisco Licensing ... 7

2.2.1 Cisco Meeting Server Licensing and Activation Keys ... 7

2.2.1.1 Call Bridge Activation keys ... 8

2.2.1.2 Branding ... 8

2.2.1.3 Recording ... 9

2.2.1.4 XMPP licenses ... 9

2.2.2 Cisco User Licensing ... 9

2.2.2.1 Personal Multiparty plus Licensing ... 10

2.2.2.2 Shared Multiparty plus Licensing ... 10

2.2.2.3 Cisco Meeting Server Capacity Units ... 10

2.2.3 Obtaining Cisco User Licenses ... 10

2.2.4 Assigning Personal Multiparty Licenses to Users ... 11

2.2.5 How Cisco Multiparty Licenses are assigned ... 12

2.2.6 Determining Cisco Multiparty Licensing Usage ... 12

2.3 Ad hoc call escalation between Cisco Unified Communications Manager and Cisco Meeting Server ... 12

2.3.1 Configuring a secure SIP trunk ... 13

2.3.2 Setting up escalated ad hoc calls ... 16

2.4 “OnePlusN”screen layout for SIP endpoints ... 17

2.5 Maximum call duration ... 18

2.6 Controlling the bandwidth for sharing content on Microsoft Lync and Skype for Business calls ... 18

2.7 Message board chat disabled by default ... 19

2.8 Changes to configuring the TURN server ... 19

2.9 Summary of API Additions & Changes ... 21

2.9.1 API Additions for Cisco Multiparty Licensing ... 21

2.9.2 API additions to /coSpaces object ... 22

2.9.3 API additions to /callLegProfiles object ... 22

2.9.4 API additions to /forwardingDialPlanRules object ... 22

2.9.5 Additional screen layout for SIP endpoints ... 22

2.9.6 API additions to /userProfiles 23
2.9.7 API addition to /system/status 23
2.9.8 New API objects to bulk create/update/delete a set of spaces 23

3 Notes on Installing and Upgrading to Cisco Meeting Server 2.0 28
3.1 Cisco Meeting Server 2.0 Deployments 28
3.1.1 Deployments using a single host server 28
3.1.2 Deployments using a single split server hosted on a Core server and an Edge server 28
3.1.3 Deployments for scalability and resilience 29
3.2 Upgrading to Release 2.0 29
3.3 Downgrading 31

4 Resolved Issues 32
Resolved in Meeting Server 2.0.6 32
Resolved in Meeting Server 2.0.5 32
Resolved in Meeting Server 2.0.4 33
Resolved in Meeting Server 2.0.3 34
Meeting Server 2.0.2 not released 35
Resolved in Meeting Server 2.0.1 35
Resolved in Meeting Server 2.0.0 (formerly released as RC3) 36
Resolved in Meeting Server 2.0 (prior to release) 36

5 Known Limitations 38

Cisco Legal Information 39

1 Introduction

This release note describes the new features, improvements and changes in release 2.0 of the Cisco Meeting Server software.

Note: From 2.0.4, there is a change to the ports used by the TURN server, this is described in the New Features section.

The Cisco Meeting Server was formerly called the Acano Server. The Cisco Meeting Server can be hosted on:

- the Cisco Meeting Server 1000 released at the same time as Cisco Meeting Server 2.0.
- Acano X-Series hardware,
- or on a specification based VM server.

For more information, see Section 2.1. The Cisco Meeting Server software is referred to as the Meeting Server throughout the remainder of this guide.

CAUTION: the message board chat is disabled by default from version 2.0 if not used in previous versions. If this is a new deployment or your existing version does not use Cisco Meeting Apps or Acano clients, and you decide to deploy the Cisco Meeting Apps and want to allow users to use chat, then you will need to enable chat via the API. This can be done prior to upgrading to version 2.0, see Section 2.7. The setting will then be retained when you upgrade.

For existing version 1.9 deployments that use message board chat, chat will remain enabled when you upgrade to 2.0.

If you are upgrading from 2.0.x, you are advised to take a configuration backup using the **`backup snapshot <filename>`** command, and save the backup safely on a different device. See the MMP Command Reference document for full details.

Note about beta features: The SIP and Lync Call Traversal feature and the XMPP resiliency feature first introduced in Acano Server release 1.8 are still beta features in Cisco Meeting Server 2.0.6 The beta features are provided for beta testing only and not intended for a production environment.

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

2 New Features/Changes in 2.0

Release 2.0 of the Meeting Server software comprises:

- support for the Cisco Meeting Server 1000.
- support for Cisco Multiparty Licensing (personal and shared).
- rebranding of the Meeting Server to reflect it is now a Cisco product, this includes a new product name, a new Cisco Lobby screen, rebranded Web Admin Interface, new voice prompts, and new default background images, and Join pane for the Web Bridge.
- ability to escalate a 2-way call on Cisco Unified Communications Manager (CUCM) to a conference on the Meeting Server via ad hoc call escalation.
- ability to control the bandwidth for sharing content on Lync and Skype for Business calls.
- support for TMS to schedule calls on the Meeting Server, see the TMS release notes for further information.
- addition of a "onePlusN" layout which automatically changes the screen layout on SIP endpoints as more participants join the meeting.
- ability to set the maximum duration for a call.
- ability to restrict audio, video, and presentation sharing for users of the Cisco Meeting App. For example, people just using the Cisco Meeting App for pairing, to share a presentation or to control a meeting, do not need media. These restrictions do not apply to dialing directly into the call via SIP, or slaving to a SIP endpoint.
- ability to control non-member access to a space, for example allow or prevent joining via a SIP endpoint, and controlling guest access.
- an increase in supported cores from 64, to accommodate the Cisco Meeting Server 1000. To take advantage of this increase in cores, you will also need to upgrade to ESXi 6 and VM hardware version 11.
- ability to monitor the number of active database connections. A new syslog message will be generated every minute on each (database-enabled) server reporting the number of connections in use on the database master, and its configured maximum number of connections (from release 2.0.1).
- from 2.0.4, the default configuration of the TURN server has changed. By default, the TURN server now listens on port 3478 for TCP communication from the Call Bridge, instead of port 443 as in previous releases.

  If you are using the TURN server in your deployment, then refer to Section 2.8 for further details.

- additional API objects and parameters to:
  - support Cisco User Licensing, see Section 2.9.1
  - control non-member access to a space (known as coSpace in the API), see Section 2.9.2
  - disconnect a call after a set time, see Section 2.9.3
  - control whether additional parameters that are present in the destination URI of an incoming call, are forwarded to the destination URI of the outbound call, see Section 2.9.4
  - select onePlusN screen layout for SIP endpoints, see Section 2.9.5
  - restrict audio, video, and presentation sharing for users of the Cisco Meeting App, see Section 2.9.6.
  - determine whether a Call Bridge is currently operating with clustering enabled, see Section 2.9.7.
  - support bulk creation of spaces, for Cisco TelePresence Management Suite and other management tools, see Section 2.9.8.

In addition, there is a change to deploying chat for users of Cisco Meeting Apps. From version 2.0, message board chat is no longer enabled by default for new deployments or deployments that have not previously used chat. For details on how to enable chat, see Section 2.7.

Note: The term spaces is used throughout the documentation apart from the API guide which still uses the old terminology of coSpaces.

2.1 Introducing the Cisco Meeting Server 1000 and Cisco Meeting Server software

2.1.1 Cisco Meeting Server 1000 Release 2.0

The Cisco Meeting Server 1000 is a pre-configured UCS C-Series server, pre-installed with VMware and the Meeting Server software. Each Cisco Meeting Server 1000 supports up to 96 HD ports, see Table 1.

Table 1: Call capacities

Type of calls	Cisco Meeting Server 1000	Cisco Multiparty Media 410v	Cisco Multiparty Media 400v
HD calls	96	64	36
SD calls	192	128	72
Audio calls	3000	2000	1000

Note: Lync calls into a Call Bridge consume the same resources as a SIP call.

2.1.2 Supported Hardware

In addition to the Cisco Meeting Server 1000, Acano X-Series Servers and specification-based VM platforms, the Cisco Meeting Server software can also be run on the following Cisco platforms:

- Cisco Multiparty Media 400v, 410v and 410vb.

Existing Cisco TelePresence Server customers that bought the Cisco Multiparty media 400v/410v/410vb are able to migrate to Cisco Meeting Server by uploading the Meeting Server software and licenses.

2.2 Cisco Licensing

You will need activation keys and licenses for the Cisco Meeting Server and Cisco user licenses. For information on purchasing and assigning Cisco licenses, see Section 2.2.3 and Section 2.2.4.

2.2.1 Cisco Meeting Server Licensing and Activation Keys

The following activation keys or licenses are required to use the Meeting Server:

- Call Bridge
- Branding
- Recording
- XMPP license activation key, this is now included in the software

For customers new to the Meeting Server the four areas are explained in the sections below.

For Acano Server customers there are four changes to note:

- the XMPP license is now included in the software.
- you need to have the Call Bridge activated to create any calls, if you require demo licenses to evaluate the product then contact your Cisco partner.
- if you are deploying a cluster of Call Bridges then you require a license file for each Call Bridge in the cluster. If you already have a single activation key covering the multiple MAC addresses of the Call Bridges in the cluster, then you can continue to use the key. However, it is no longer possible to purchase a single key covering multiple MAC addresses.
- you will need to change the name of each newly purchased Cisco license file to **cms.lic**

2.2.1.1 Call Bridge Activation keys

The activation key allows the Call Bridge to be used for media calls. Activation keys need to be installed on:

- the Cisco Meeting Server 1000,
- VM servers with Cisco Meeting Server software installed and configured as a combined server deployment (all components are on the same server),
- VM servers with Cisco Meeting Server software installed and configured as a Core server in a split server deployment.

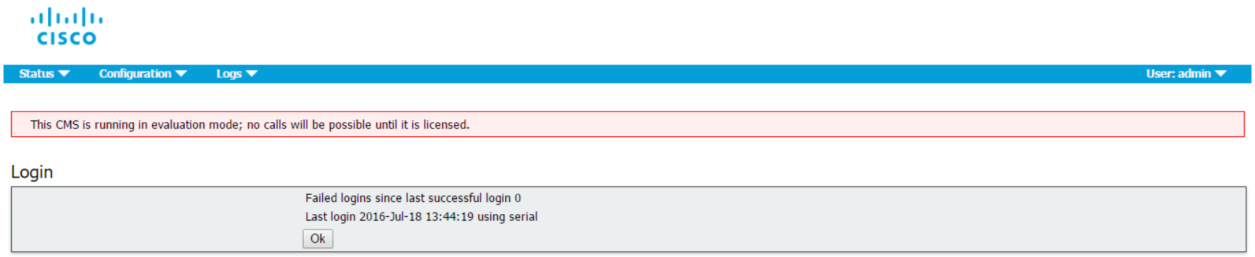
You need to have the Call Bridge activated to create any calls, if you require demo licenses to evaluate the product then contact your Cisco sales representative or Cisco partner.

Acano X-Series Servers do not require an activation key. VMs configured as Edge servers do not require an activation key for the Call Bridge.

Note: If you are deploying a cluster of Call Bridges you require a license file for each Call Bridge in the cluster. When you purchase license files you will be asked for the MAC address of each server hosting a Call Bridge which requires activation. This is the MAC address of interface A of your VM, not the MAC address of the server platform that the VM is installed on. The name of the license file will have the MAC address within it, so that you can identify the appropriate license file to load on a server. Before uploading the license file rename it as **cms.lic**

To apply the license after uploading the license file, you need to restart the Call Bridge. However, you must configure the Call Bridge certificates and a port on which the Call Bridge listens before you can do this. These steps are part of the Meeting Server configuration and described in the Cisco Meeting Server deployment guides.

The banner “This CMS is running in evaluation mode; no calls will be possible until it is licensed.” is displayed in the Web Admin interface until a valid cms.lic file is uploaded. After you upload the license file, the banner is removed.



This CMS is running in evaluation mode; no calls will be possible until it is licensed.

Failed logins since last successful login 0
Last login 2016-Jul-18 13:44:19 using serial

2.2.1.2 Branding

Customization is controlled by license keys with different keys providing different levels of customization.

The levels of customization supported are:

- No key: control of the background image and logo on the WebRTC landing page of a single Web Bridge via the Web Admin Interface; no API configuration is allowed.
- Single brand via API: only a single set of resources can be specified (1 WebRTC page, 1 set of voice prompts etc). These resources are used for all spaces, IVRs and Web Bridges.
- Multiple brand via API: different resources can be used for different spaces, IVRs and Web Bridges. These resources can be assigned at the system, tenant or space/IVR level.

To purchase branding license keys, you will need the following information:

- level of branding required (single/multiple),
- MAC address of interface A on servers hosting the Call Bridge.

2.2.1.3 Recording

Recording is controlled by license keys, where one license allows one simultaneous recording. The license is applied to the server hosting the Call Bridge (core server) which connects to the Recorder, not the server hosting the Recorder.

Note: The recommended deployment for production usage of the Recorder is to run it on a dedicated VM with a minimum of 4 physical cores and 4GB . In such a deployment, the Recorder should support 2 simultaneous recordings per physical core, so a maximum of 8 simultaneous recordings.

To purchase recording license keys, you will need the following information:

- number of simultaneous recordings,
- MAC address of interface A on the servers hosting the Call Bridges.

2.2.1.4 XMPP licenses

Customers who are using Cisco Meeting Apps require an XMPP license installed on the server(s) running the XMPP server application. The XMPP license is included in the Cisco Meeting Server software. You will also need a Call Bridge activated on the same Meeting Server as the XMPP server.

2.2.2 Cisco User Licensing

Call Multiparty licensing is the primary licensing model used for Cisco Meeting Server; Acano Capacity Units (ACUs) can still be purchased, but cannot be used on the same Call Bridge as Multiparty licenses. Contact your Cisco sales representative if you need to migrate ACUs to Multiparty licenses.

Multiparty licensing is available in two variations: Personal Multiparty plus (PMP plus) licensing, which offers a named host license, and Shared Multiparty plus (SMP plus) licensing, which offers a shared host license. Both Personal Multiparty plus and Shared Multiparty plus licenses can be used on the same server.

2.2.2.1 Personal Multiparty plus Licensing

Personal Multiparty plus (PMP plus) provides a named host license assigned to each specific user who frequently hosts video meetings. This can be purchased through Cisco UWL Meeting (which includes PMP plus). Personal Multiparty plus is an all-in-one licensing offer for video conferencing. It allows users to host conferences of any size (within the limits of the Cisco Meeting Server hardware deployed). Anyone can join a meeting from any endpoint, and the license supports up to full HD 1080p60 quality video, audio, and content sharing.

2.2.2.2 Shared Multiparty plus Licensing

Shared Multiparty plus (SMP plus) provides a concurrent license that is shared by multiple users who host video meetings infrequently. It can be purchased at a reduced price with a UCM TP Room Registration license included when purchasing room endpoints, or it can be purchased separately. Shared Multiparty plus enables all employees who do not have Cisco UWL Meeting licenses to access video conferencing. It is ideal for customers that have room systems deployed that are shared among many employees. All employees, with or without a Cisco UWL Meeting license have the same great experience, they can host a meeting with their space, initiate an ad-hoc meeting or schedule a future one. Each shared host license supports one concurrent video meeting of any size (within the limits of the hardware deployed). Each Shared Multiparty plus license includes one Rich Media Session (RMS) license for the Cisco Expressway, which can be used to enable business-to–business (B2B) video conferencing.

2.2.2.3 Cisco Meeting Server Capacity Units

Acano Capacity Units (ACUs) have been renamed Cisco Meeting Server Capacity Units. Each Capacity Unit (CU) supports the following quantity of concurrent media streams to the Meeting Server software (for the CU software license terms and conditions refer here).

Table 2: Capacity Unit Licensing

Media Stream	Number of licenses per Capacity Unit	Number of licenses required per call leg
1080p30	0.5	2
720p30	1	1
480p30	2	0.5

Each CU also entitles the Licensee to content sharing in each meeting containing at least one video participant. For more information refer to the terms and conditions of the CU license.

2.2.3 Obtaining Cisco User Licenses

If you are an existing Acano customer and have purchased a license, continue to email the MAC address of your Meeting Server to support@acano.com for a license file. If you require a demo license, contact Cisco sales. Once you have moved to a Cisco contract follow the steps below.

For customers with a Cisco contract:

1. Purchase your activation keys and licenses through Cisco's ecommerce tool.

   You will receive an email with a “PAK” code, and the url of a web site where you need to register the PAK code with the MAC address of your Meeting Server.

2. Obtain the MAC address of your Meeting Server by logging in to the MMP of your server, and enter the following command: **`iface a`** .

   Note: This is the MAC address of your VM, not the MAC address of the server platform that the VM is installed on.

3. Register the PAK code and the MAC address of your Meeting Server.
4. You will be sent a single license file via email. Rename the license file to cms.lic either before or during transfer.
5. Transfer the license file to the MMP of your Meeting Server using SFTP.
   a. Find the IP address of the MMP using the MMP command **`iface a`**
   b. Connect your SFTP client to the IP address of the MMP and log in using the credentials of an MMP admin user.
6. Restart the Call Bridge.

2.2.4 Assigning Personal Multiparty Licenses to Users

Follow these steps to apply Multiparty licensing to the Meeting Server.

Note: This procedure requires that users imported from a single LDAP source are either all licensed or all not licensed.

1. Create a userProfile (POST /userProfiles) or update an existing one (PUT to /userProfiles/<user profile id>) with the hasLicence field set to “true” to indicate users associated with this userProfile have a Cisco user license.

   Or create a userProfile or update an existing one with the hasLicence field set to “false” to indicate users associated with this userProfile do not have a Multiparty license. Alternatively, leaving the hasLicense field unset will select the default setting of false.

2. Create an ldapSource (POST /ldapSources) or update an existing one (PUT to /ldapSources/<ldap source id>) with the userProfile id parameter. This associates the userProfile created in step 1 with the appropriate LDAP source.
3. POST /ldapSyncs with ldapSource id parameter to sync the LDAP source. All imported users will be associated with the given userProfile

To determine whether a specific user has as a license, use GET /users/<user id> to retrieve the userProfile associated with this user.

Note: If the userProfile is deleted, then the userProfile is unset for the ldapSource and the imported users.

2.2.5 How Cisco Multiparty Licenses are assigned

When a meeting starts in a space, a Cisco license is assigned to the space. Which license is assigned by the Meeting Server is determined by the following rules:

- if one or more members with a Cisco PMP plus license has joined a space, then one of their licenses will be used, if not, then
- if the person that created the space (the owner) has a Cisco PMP plus license, then the license of that owner is assigned, if not, then
- if present a Cisco SMP plus license is assigned.

2.2.6 Determining Cisco Multiparty Licensing Usage

New API objects, and additional fields to existing objects, have been added in release 2.0 to enable administrators to determine the consumption of Multiparty licenses. See Section 2.9.1.

2.3 Ad hoc call escalation between Cisco Unified Communications Manager and Cisco Meeting Server

Release 2.0 supports the escalation of a 2-way call on Cisco Unified Communications Manager to a conference on the Meeting Server via ad hoc call escalation. This section provides an overview on how to configure Cisco Unified Communications Manager and the Meeting Server. Cisco Unified Communications Manager needs to be running Release 10.5(2) or later.

Cisco recommends setting up a secure SIP trunk, however if your company policy is for traffic within your organization to be non-secure, then a non-secure SIP trunk 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.

The following instructions describe setting up a secure SIP trunk between Cisco Unified Communications Manager and the Meeting Server. If you decide to set up the SIP trunk as non-secure, you will still need to use certificates. Refer to the “Cisco Meeting Server Deployment with Call Control” guide for the steps on setting up a non-secure SIP trunk, and for information on setting up rendezvous and scheduled calls between Cisco Unified Communications Manager and Cisco Meeting Server.

2.3.1 Configuring a secure SIP trunk

Follow the steps below to set up the secure SIP trunk, then Section 2.3.2 to enable escalation of a 2-way call on Cisco Unified Communications Manager to a conference on the Meeting Server.

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`
3. Generate a private key and Certificate Signing Request (.csr) file for the Call Bridge, call it “cucm-trust.csr”

   Cisco Unified Communications Manager has some requirements on what TLS certificates it will accept. You should ensure that “cucm.csr” has the SSL client and SSL server purposes enabled. This is done during the certificate signing stage.
4. Submit “cucm-trust.csr“ to the CA (public CA or internal CA) for signing. An internal CA signed certificate is acceptable.
5. Once signed, use openSSL to check that the certificate is OK:

   ```
   openssl x509 -in <certificatename> -noout -text –purpose
   ```

   for example

   ```
   openssl x509 -in cucm-trust.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, private key, and intermediate CA bundle (if any) to the Call Bridge
   a. SSH into the MMP
   b. Assign the certificate and private key to the Call Bridge using 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 cucm-trust.key cucm-trust.crt cucm-trust-
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: You will need to add the Call Bridge certificate and certificate bundle to the Cisco Unified Communications Manager's trust store, see step 8 below.

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

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.

7. Generate a certificate for Cisco Unified Communications Manager
   a. Log into the Cisco Unified Communications Manager OS Administration page
   b. Select **Security>Certificate Management**. The Certificate List window displays.
   c. Click the **Generate CSR** button and generate a Certificate Signing Request(CSR) for Cisco Unified Communications Manager.
   d. Sign the CSR with a Certificate Authority. An internal CA signed certificate is acceptable.
   e. Upload the signed certificate, and intermediate CA bundle (if any) to Cisco Unified Communications Manager
8. Upload to the Cisco Unified Communications Manager's trust store, the signed certificate created in step 4 for the Meeting Server's Call Bridge, and the root certificate or chain of certificates from the Certificate Authority.

   a. Log into the Cisco Unified Communications Manager OS Administration page
   b. Select **Security>Certificate Management**.
   c. Select **Upload Certificate/Certificate Chain**.
   d. Click **Choose File** to find your certificate. This can be the root certificate or the Call Bridge's certificate and certificate bundle.
   e. Click **Upload File**.

9. 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**
   e. Click **Save**

10. 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	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 the Meeting Server, it must match the CN of the Meeting Server certificate
SIP Information>Destination Port	Enter **5061** for TLS
SIP Trunk Security Profile	Select the security profile that you created in step 3.
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.

f. Click **Save**.

2.3.2 Setting up escalated ad hoc calls

After setting up the secure SIP trunk (see Section 2.3.1), follow the steps below 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, so that the Cisco Unified Communications Manager can 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.

Configuring the Meeting Server:

1. Set up an incoming dial plan on the Meeting Server see the Cisco Meeting Server Deployment Guide. For ad hoc calls the rule should match against spaces.
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.

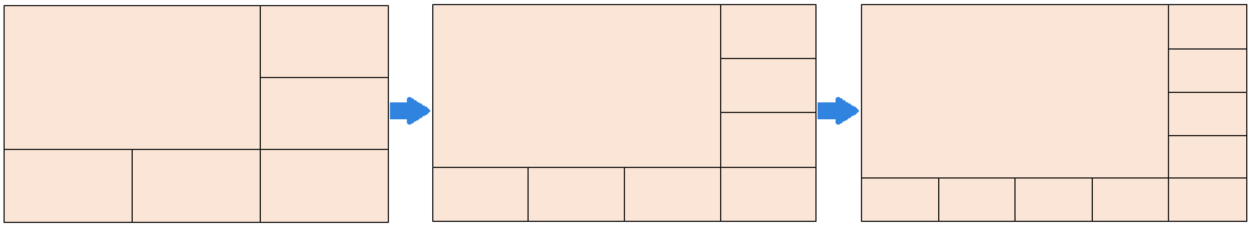
Configuring Cisco Unified Communications Manager:

3. 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 TelePresence Conductor** from the **Conference Bridge Type** drop-down list.
    d. Enter a name and description for the Meeting Server in the **Device Information** pane.
    e. Select a SIP trunk from the **SIP Trunk** drop-down list.
    f. Enter the HTTP interface information and check the HTTPS check box to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco Meeting Server. See 2.3 below.
4. If not already done so, upload the Call Bridge's certificate and key pair to the Cisco Unified Communications Manager's trust store.

2.4 “OnePlusN”screen layout for SIP endpoints

Release 2.0 supports a new “onePlusN” layout family which automatically changes the screen layout on SIP endpoints as more participants join a meeting. For example from onePlus5 to onePlus7 to onePlus9.

Figure 1: onePlus5 > onePlus7 > onePlus 9



Applying the onePlusN layout results in the the screen layout changing as participants join and leave a meeting. The onePlusN layout can be applied to the defaultLayout, chosenLayout, activeLayout and layout parameters of the following API objects: /coSpaces, /calls, /callLegs, /callLegProfiles. See the API Reference Guide for more details.

If the layout cycle triggered by DTMF tones has been configured through the API, the layouts scroll through in order: 'allEqual', 'stacked', 'telepresence','speaker only', 'onePlusN', defaultLayout.

- If defaultLayout='allEqualNinths' then the order is 'allEqual', 'stacked', 'telepresence', 'speaker only', 'onePlusN', 'allEqualNinths'.
- If the defaultLayout is set to one of the other layouts then only 5 layouts will be in the cycle. For example: if defaultLayout='allEqual' then the order is 'allEqual', 'stacked ', 'telepresence', ' speakerOnly', 'onePlusN'.

Figure 2: Using DTMF to scroll through allEqual, stacked, telepresence (speaker large), speaker only, onePlus5 and defaultLayout

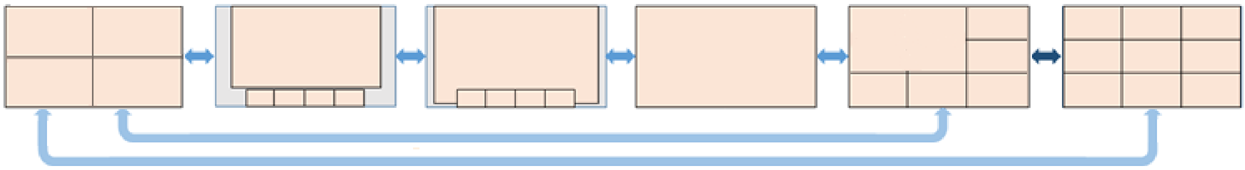
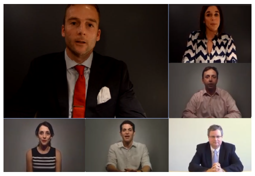


Figure 3: Example of onePlus5 screen layout



Note: For clustered deployments a maximum of 4 remote video streams per remote Call Bridge will be shown, even if there are more than four remote participant dial-ins to the call on that Call Bridge.

2.5 Maximum call duration

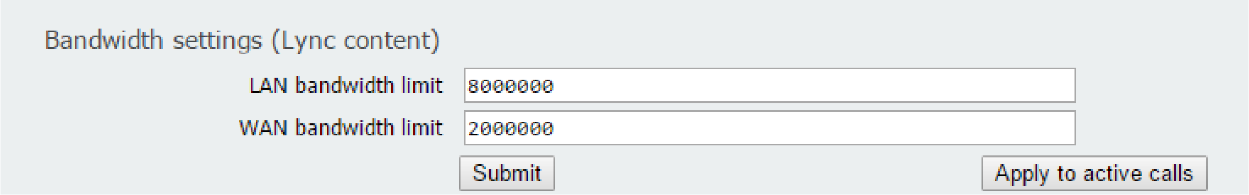
You can set the maximum duration for a call. Use the maxCallDurationTime parameter on the /callLegProfiles object to set a maximum time in seconds for the call to last, after which the call will be disconnected. You can apply the callLegProfile to the following API objects: /coSpaces, /coSpaceUsers, /accessMethods, and at /system and /tenant levels.

2.6 Controlling the bandwidth for sharing content on Microsoft Lync and Skype for Business calls

The Call Bridge imposes a limit on the amount of bandwidth used for outgoing Lync presentation media. For calls where the connection is directly to the host computer, the LAN bandwidth limit will be applied; for all other cases, for example when the connection involves traversal across the DMZ, as for remote Lync clients, the WAN bandwidth limit will be applied. The default limits are: 8 Mbytes for the LAN bandwidth and 2 Mbytes for the WAN bandwidth.

You can change the bandwidth used to share content with Lync calls through the Web Admin Interface. Navigate to **Configuration>Call settings** and set the LAN and WAN bandwidth limits for Lync content. Click on the **Submit** button and click on **Apply to active calls** button if appropriate.

Figure 4: Setting bandwidth for Lync content sharing



Bandwidth settings (Lync content)

LAN bandwidth limit: 8000000

WAN bandwidth limit: 2000000

2.7 Message board chat disabled by default

From version 2.0, message board chat is no longer enabled by default on new deployments or for deployments which did not previously use chat. If you plan to allow your users to use the message board chat feature in the Cisco Meeting Apps, then you will need to enable chat via the API.

To enable chat in message boards, use the API to create a callProfile with parameter **messageBoardEnabled** set to **true**. Set this callProfile as the default Global Profile to be used for all calls by copying the callProfile id from the Location field and PUTing it to /api/v1/system/profiles.

2.8 Changes to configuring the TURN server

From version 2.0.4, the default configuration of the TURN server has changed. By default, the TURN server now listens on port 3478 for TCP communication from the Call Bridge, instead of port 443 as in previous releases.

If you are using the TURN server in your deployment then:

- **For combined deployments:** after upgrading to 2.0.4, the TURN server must be configured to listen on the loopback interface. Ensure that the whitelist of interfaces to listen on contains at least one interface, and specify the loopback interface. Use the MMP command:

  ```
  turn listen <interface whitelist>
  ```

  For example: `turn listen c lo`

  Note: The loopback interface must not be the first interface in the whitelist.

- **For split deployments:** before upgrading to 2.0.4, you must open TCP port 3478 in the firewall separating the core and edge servers; UDP port 3478 should already be open. TCP port 3478 and UDP port 3478 are used in the event that ports 32768-65535 are blocked by the internal firewall.

Figure 5: Ports to open if using the TURN server in a Combined server deployment

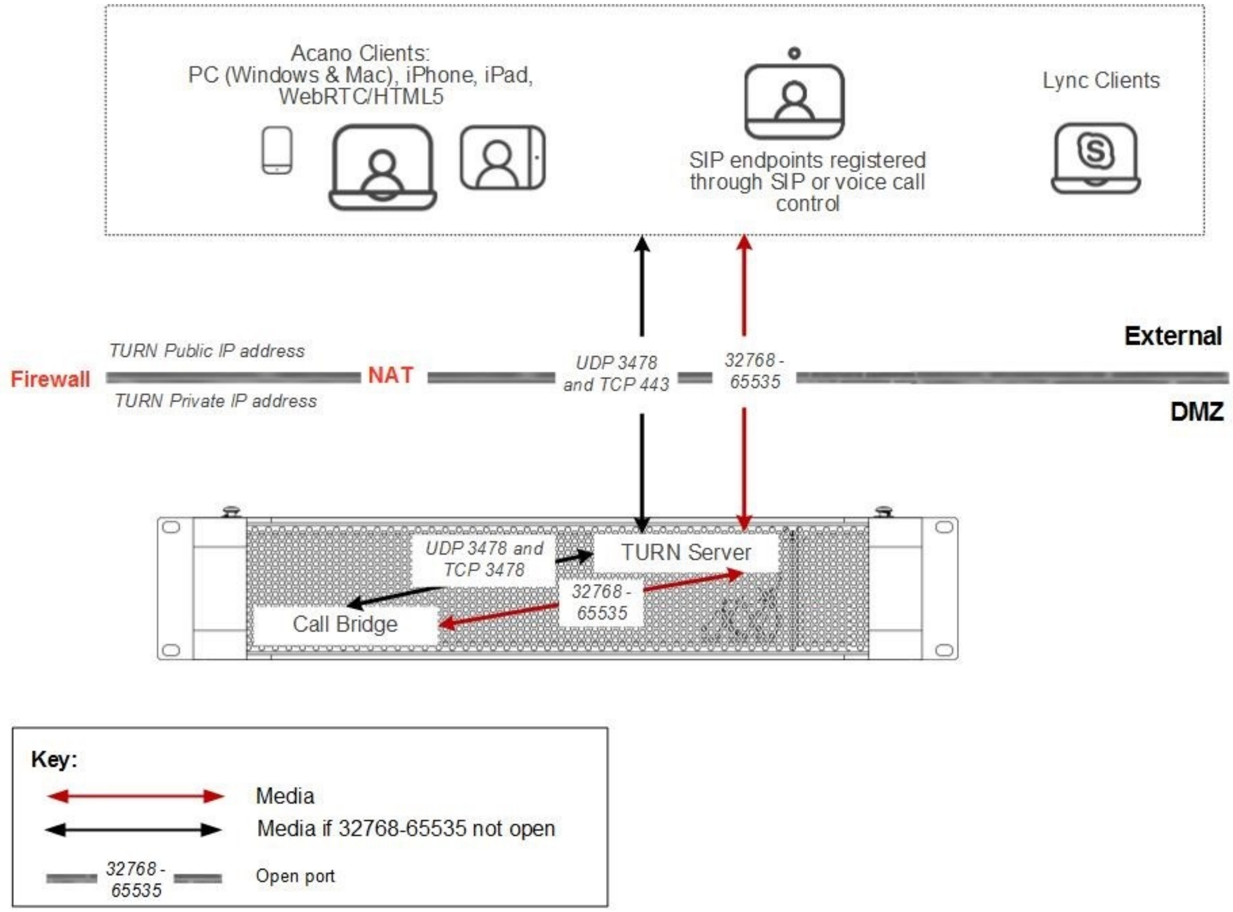
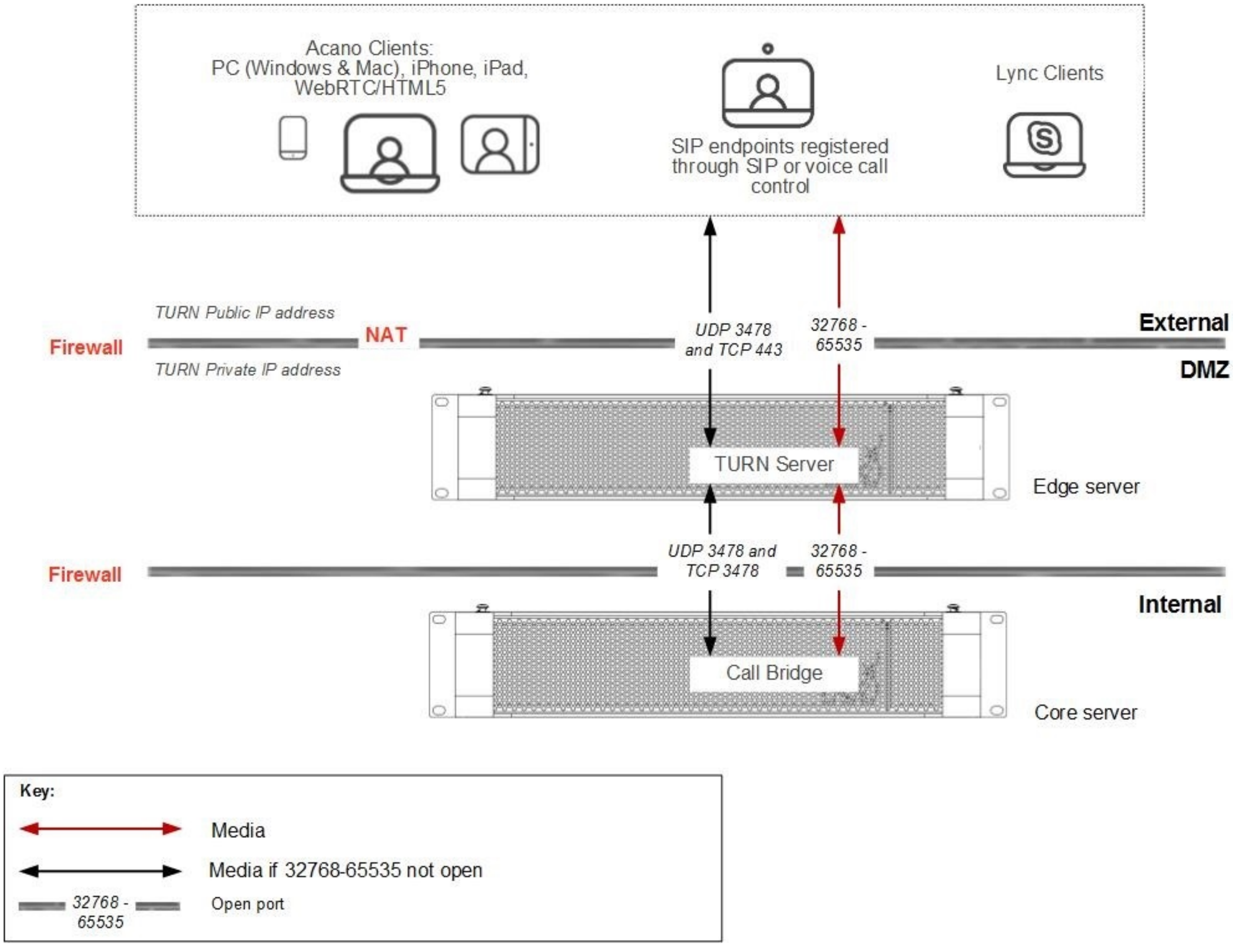


Figure 6: Ports to open if using the TURN server in a Split server deployment



2.9 Summary of API Additions & Changes

2.9.1 API Additions for Cisco Multiparty Licensing

The following objects and fields have been added to the API to enable Admins to determine the consumption of Multiparty licenses:

- a new /system/licensing object, enabling an Admin to determine whether components of the Meeting Server have a license and are activated,
- a new /system/multipartyLicensing object that returns the number of licenses available and in use, and
- a new /system/multipartyLicensing/activePersonalLicenses object that indicates the number of active calls that are using a Personal Multiparty plus user license,

- new userProfile field as part of LDAP Sync
- new hasLicense field to the userProfile, this indicates if a user has a license
- new ownerId and ownerJid fields per /coSpace object. If present, the ownerId field holds the GUID of the user that owns this coSpace, and ownerJid holds the JID of the user.

Note: The owner is set using the field ownerJid when POSTing or PUTing a /coSpace object. When GETing the /coSpace both the ownerJid and ownerId are returned for the user.

For more information on these additional object and fields to support Cisco Multiparty licensing, refer to the Cisco Meeting Server API Reference Guide 2.0.

2.9.2 API additions to /coSpaces object

The following has been added to the /coSpaces object:

- addition of nonMemberAccess parameter. If set to true then non-members of a coSpace are able to have access to the coSpace. This is the default if the parameter is not set. If set to false, non-members cannot access the coSpace.
- new ownerJid parameter per /coSpace object, if provided the space will be owned by the user with the given JID. A GET operation on the coSpace will return both the ownerJid and the ownerId.

2.9.3 API additions to /callLegProfiles object

The following parameters have been added to the /callLegProfiles object:

- name = name of the /callLegProfile
- maxCallDurationTime = maximim number of seconds that the call leg will exist, after this set time the call will be disconnected

2.9.4 API additions to /forwardingDialPlanRules object

The following parameters have been added to the /forwardingDialPlanRules object:

- uriParameters = when forwarding an incoming call to a new destination address, this parameter determines whether to discard any additional parameters that are present in the destination URI of the incoming call, or whether to forward them on to the destination URI of the outbound call. If this parameter is not supplied in a create (POST) operation, it defaults to “discard”.

2.9.5 Additional screen layout for SIP endpoints

A new “onePlusN” family of layouts automatically change the screen layout on SIP endpoints as more participants join a meeting. The onePlusN layout can be applied to the defaultLayout, chosenLayout, activeLayout and layout parameters of the following API objects: /coSpaces. /calls, /callLegs, /callLegProfiles. See the API Reference Guide for more details.

2.9.6 API additions to /userProfiles

The following parameters have been added to the /userProfiles object to provide the ability to restrict audio, video, and presentation sharing for users of the Cisco Meeting App.

- audioParticipationAllowed - determines whether or not a user associated with this user profile will be allowed to send or receive live audio when in a call.
- videoParticipationAllowed - determines whether or not a user associated with this user profile will be allowed to send or receive live video when in a call.
- presentationParticipationAllowed - determines whether or not a user associated with this user profile will be allowed to send or receive presentation media when in a call.

2.9.7 API addition to /system/status

The following parameter has been added to the /system/status:

- clusterEnabled = if set to true then the Call Bridge is currently running with clustering enabled

2.9.8 New API objects to bulk create/update/delete a set of spaces

The following objects have been added to support the bulk creation of spaces:

- /cospaceBulkParameterSets
- /cospaceBulkParameterSets/<bulk parameter sets guid>
- /cospaceBulkSyncs
- /cospaceBulkSyncs/<bulk sync guid>

/cospaceBulkParameterSets

POST: creates a new parameter set, see Table 4. Returns location of new parameter set/cospaceBulkParameterSets/<bulk parameter set guid>

GET: returns enumeration of parameter sets. (guid, start index and end index returned at this level)

PUT: not supported

DELETE: not supported

/cospaceBulkParameterSets/<bulk parameter sets guid>

POST: not supported

GET: reads the parameters within the parameter set (all parameters at this level).

PUT: updates the parameters within this parameter set, but needs to be synchronized for it to take effect.

DELETE: is only possible if it is not referenced anywhere. Trying to do so when it still refers to spaces will cause an error. It is expected that a Sync operation is run to delete all spaces created using the parameter set before it is deleted.

Table 4: /cospaceBulkParameterSets

Parameter	Required	Default	Notes
startIndex	Y	N/A	(this index is inclusive)
endIndex	Y	N/A	(this index is inclusive)

coSpaceUriMapping	N	Not set	If not set, coSpace will not have a dialable URI.
			Syntax:
			uri-mapping = [uri-component] [“$index$”] [uri-component]
			Where:
			uri-component = *(uri-character / escaped-character)
			uri-character = *(unescaped-character EXCLUDING ‘@’)
			unescaped-character = any character EXCLUDING ‘$’ and ‘\’
			escaped-character = “\\” / “\$” ; producing ‘\’ and ‘$’ respectively.
			These need to be unique so if index is not used there will be clashes, unless the field is just left completely blank .

coSpaceNameMapping	N	Not set	Syntax:
			name-mapping = [name-component] [“$index$”] [name-component]
			Where:
			name-component = *(unescaped-character / escaped-character)
			unescaped-character = any character EXCLUDING ‘$’ and ‘\’
			escaped-character = “\\” / “\$” ; producing ‘\’ and ‘$’ respectively.
			These are not required to be unique.

coSpaceCallIdMapping	N	Not set	If not set then the coSpace will not have a CallID Syntax: id-mapping = [id-component] [“$index$”] [id-component] Where: id-component = *(unescaped-character / escaped-character) unescaped-character = any character EXCLUDING ‘$’ and ‘\’ escaped-character = “\\” / “\$” ; producing ‘\’ and ‘$’ respectively These need to be unique so if index is not used there will be clashes, unless the field is just left completely blank. Secrets will be autogenerated if CallIDMapping is set.
tenant	N	Not set	
callProfile	N	Not set	

Parameter	Required	Default	Notes
callLegProfile	N	Not set	
callBrandingProfile	N	Not set	
nonMemberAccess	N	Not set	If not set then defaults to “true” and non members can access the coSpace.

/cospaceBulkSyncs

POST: queue bulk sync operation for execution as soon as possible; parameters as below; returns location /cospaceBulkSync/<bulk sync guid>

GET: returns enumeration of bulk sync operations that are queued, in progress, or complete (prior to their deletion)

PUT: not supported

DELETE: not supported

/cospaceBulkSyncs/<bulk sync guid>

GET: return status of bulk sync operation

DELETE: remove a queued operation from the queue; clear a completed operation; not supported for an operation in progress (i.e. cannot cancel an active bulk sync)

POST: not supported

PUT: not supported

Table 5: /coSpaceBulkSyncs

Parameter	Required	Default	Notes
cospaceBulkParameterSet	Y	N/A	Parameter set GUID that is going to be synchronised
removeAll	N	false	Whether the sync will remove all entries that were created using the parameter set. Used only if you need to remove all spaces that were created previously. If set to true then no spaces will be created. If set to false, or omitted, then all spaces previously created using this parameter set will be removed and new spaces based on the new mappings will be created.

Note: Bulk Sync will iterate between startIndex and endIndex (inclusive at both end) and expand and insert the mapping parts .

Examples:

1. Create a cospaceBulkParameterSet with parameters:

   - startIndex=1000&endIndex=1999&coSpaceUriMapping=space$index$&coSpaceNameMapping=Space $index$&coSpaceCallIdMapping=811$index$

2. Create a cospaceBulkSync with parameters:

   - cospaceBulkParameterSet=<GUID from above>

This will create 1000 spaces starting with **`"Space 1000" space.1000@domain.com,callID=8111000`** and ending in **`"Space 1999" space.1999@domain.com,callID=8111999`**

To update the range:

1. PUT new range to cospaceBulkParameterSets/<GUID from above>
2. Create a cospaceBulkSync with parameters:

   - cospaceBulkParameterSet=<GUID from above>

This deletes all the previous spaces and creates a new set. This whole operation will succeed or fail. In failure the transaction will be rolled back and the spaces that previously existed will still be there.

To delete a range:

1. Create a cospaceBulkSync with parameters:

   - cospaceBulkParameterSet=<GUID from above>&removeAll=true

This removes all spaces that were created using this parameter set. They will get removed even if they have been renamed, or edited in any other way.

3 Notes on Installing and Upgrading to Cisco Meeting Server 2.0

If you have purchased a Cisco Meeting Server 1000, the software is already installed, go to Section 3.1. If you are configuring a VM for the first time then follow the instructions in the Cisco Meeting Server Installation Guide for Virtualized Deployments, then go to Section 3.1.

This section assumes that you are upgrading an Acano server or VM from 1.9.x. If you are upgrading from R1.8.x, then Cisco recommends that you upgrade to 1.9.x first following the instructions in the 1.9 release notes, before following any instructions in these Cisco Meeting Server 2.0 Release Notes.

Note: It is possible to upgrade from release 1.8.x to CMS 2.0 without upgrading to 1.9, however this has not been tested by Cisco.

3.1 Cisco Meeting Server 2.0 Deployments

To simplify explaining how to deploy the Meeting Server, deployments are described in term of three models: the single combined Meeting Server, the single split Meeting Server and the deployment for scalability and resilience. All three different models may well be used in different parts of a production network.

3.1.1 Deployments using a single host server

If you are installing the Meeting Server for the first time on a single host server (a “combined” deployment), we recommend that you read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server (installation guide for Cisco Meeting Server 1000 and virtualized deployments or the installation guide for Acano X-Series Server).
2. The Single Combined Meeting Server Deployment Guide enabling all the solution components on the single host. This guide refers to the Certificate Guidelines for Single Combined Server Deployments for details on obtaining and installing certificates for this deployment.

3.1.2 Deployments using a single split server hosted on a Core server and an Edge server

If you are installing the Meeting Server for the first time in a split server model, we recommend that you deploy the XMPP server on the Core server, and deploy the Load Balancer on the Edge server.

Read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server
2. The Single Split Meeting Server Deployment Guide. This guide refers to the Certificate Guidelines for Single Split Server Deployments for details on obtaining and installing certificates for this deployment.

3.1.3 Deployments for scalability and resilience

If you are installing the Meeting Server for scalability and resilience using multiple host servers, we recommend that you deploy the XMPP server on Core servers, and deploy Load Balancers on the Edge server.

Read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server
2. The Scalability and Resilience Deployment Guide. This guide refers to the Certificate Guidelines for Scalable and Resilient Server Deployments for details on obtaining and installing certificates for this deployment.

3.2 Upgrading to Release 2.0

The instructions in this section apply to both Meeting Server and virtualized deployments with a previous Acano server release already installed and not clustered. Refer to the Scalability and Resilience Deployment Guide before upgrading clustered servers.

CAUTION: Before upgrading to release 2.0 you must take a configuration backup using the **`backup snapshot <filename>`** command and save the backup safely on a different device. See the MMP Command Reference document for full details. Do NOT use the automatic backup file that is created during the upgrade process.

Upgrading the firmware is a two-stage process: first, upload the upgraded firmware image; then issue the upgrade command. This restarts the server: the restart process interrupts all active calls running on the server; therefore, this stage should be done at a suitable time so as not to impact users – or users should be warned in advance.

To install the latest firmware on the server follow these steps:

1. Obtain the appropriate upgrade file from the support section of the Cisco website. There will be four files:

   Cisco_Meeting_Server_2_0_6_vm-upgrade.zip

   This file requires unzipping to a single upgrade.img file. Use this file to upgrade vm deployments, follow the instructions below.

Cisco_Meeting_Server_2_0_6.vhd

Use this file to upgrade Microsoft Hyper-V deployments

Cisco_Meeting_Server_2_0_6_x-series.zip

This file requires unzipping to a single upgrade.img file. Use this file to upgrade Acano X-series servers, follow the instructions below.

Cisco_Meeting_Server_2_0_6.ova

Use this file for new vm deployments, follow the steps in the Installation Guide for Virtualized Deployments.

2. Validate the download; the checksums for the 2.0.6 release are shown in a pop up box that appears when you hover over the description for the download.

Note: If you are using WinSCP for the file transfer, ensure that the Transfer Settings option is ‘binary’ not ‘text’. Using the incorrect setting results in the transferred file being slightly smaller than the original – and this prevents successful upgrade.

---

2. Using an SFTP client, log into the MMP using its IP address. The login credentials will be the ones set for the MMP admin account. If you are using Windows, we recommend using the WinSCP tool.

   Note:
   a) You can find the IP address of the MMP’s interface with the **`iface a`** MMP command.
   b) The SFTP server runs on the standard port, 22.
   c) After copying the upgrade.img file, you will not be able to see it listed as being in the file system; this is normal.

   ---

3. Copy the software to the Server/ virtualized server.

4. To apply the upgrade, issue the upgrade command.

   a. Establish a SSH connection to the MMP and log in.

   b. Initiate the upgrade by executing the upgrade command.
   `upgrade`
   The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.

5. Verify that the Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:
   `version`
6. Check the **Configuration > Outbound Calls** rules updating the Local Contact Domain field and completing the new Local From Domain field if necessary.
7. Update the customization archive file when available.
8. If you are deploying a scaled or resilient deployment read the Scalability & Resilience Deployment Guide and plan the rest of your deployment order and configuration.
9. If you have deployed a database cluster, be sure to run the **`database cluster upgrade schema`** command after upgrading the database schema. For instructions on upgrading the database schema refer to the Scalability & Resilience Deployment Guide.
10. You have completed the upgrade.

3.3 Downgrading

To return to the previous version of the server software in a non-clustered environment, use the regular upgrade procedure to “upgrade” to the appropriate version. Then restore the configuration backup for the older version, using the **`backup rollback <name>`** command. See the MMP Command Reference document for full details. Do not rely on the backup generated automatically during upgrade.

Note: The **`backup rollback <name>`** command overwrites the existing configuration as well as the license.dat file and all certificates and private keys on the system, and reboots the Meeting Server. Therefore it should be used with caution. Make sure you copy your existing license.dat file and certificates beforehand because they will be overwritten during the backup rollback process. The .JSON file will not be overwritten and does not need to be re-uploaded.

4 Resolved Issues

Resolved in Meeting Server 2.0.6

Reference	Issue	Summary
11443	The WebRTC client had some French translations that could be improved.	Fixed in 2.0.6
11573	XMPP authentication bypass	This issue is reported as a security alert. See https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-msc and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6445. Fixed in 2.0.6

Resolved in Meeting Server 2.0.5

Reference	Issue	Summary
10957	The Meeting Server could crash if it was serving a branding resource and simultaneously disconnecting a call.	Fixed in 2.0.5
11400	If a TURN server was deployed behind a NAT, it could return its private IP address instead of the public one as a media relay destination. This would cause media to fail for devices using TURN.	Fixed in 2.0.5
11458	The Meeting Server could crash due to a race condition between TLS allocation at thread creation and dlopen.	Fixed in 2.0.5
11477	Meeting Server in a cluster could experience a media module crash.	Fixed in 2.0.5

Reference	Issue	Summary
11526	On client login, the Meeting Server sends the authentication message to AD. If the authentication message length exceeds 200 characters, the message was cropped, resulting in a failed login.	Fixed in 2.0.5. Now supports up to 1200; note that windows AD only supports a maximum of 255.

Resolved in Meeting Server 2.0.4

Reference	Issue	Summary
11186	A CTS 3000 or 3010 with a dedicate presentation codec could see pixelation and tearing in content video received from a CMS.	Fixed in 2.0.4
11204 and 11132	In previous releases, the TURN server could sometimes listen on all interfaces rather than those it was explicitly configured to use.	In some cases this led to some deployments working despite being incorrectly configured, and in other cases the TURN server not working at all. Fixed in 2.0.4. Configuration changes to your TURN configuration may be necessary, see Section 2.8 for details of ports to open in the firewall.
11351	If Cisco Jabber in desk phone mode joins a conference where content is already being shared, the Meeting Server will not send it any content video.	Fixed in 2.0.4.
11357	Simultaneous calls using a common codec may not connect	The number of simultaneous calls using the codecs AAC, G.728 or G.729 was limited in previous releases. If you have set up a SIP trunk between your Acano deployment and a Call Control deployment which restricts the codecs that may be selected to only one of these audio codecs, then you may experience audio calls failing once the limit has been reached. These limits have been removed in 2.0.4.
11374	After a downgrade from 2.0.0, 2.0.1 or 2.0.3 to any 1.9.x or older release, any attempt to create or update an LDAP source would fail, with a PGRES_FATAL_ ERROR in the event log.	Fixed in 2.0.4.

Reference	Issue	Summary
11421	A crash could occur if a Meeting Server received an instant message through a Lync conference from a Lync participant not in a call to that conference.	Fixed in 2.0.4.

Resolved in Meeting Server 2.0.3

Reference	Issue	Summary
9294	In some situations after an LDAP sync, a newly created user would be unable to log in using Cisco Meeting App.	Fixed in 2.0.3
9546	After restarting the H.323 Gateway, it would no longer accept any more calls.	The H.323 Gateway was failing to start correctly due to a port conflict. Fixed in 2.0.3
11092	CallLegUpdate and CallLegEnd CDR messages could stop being sent to a second CDR receiver.	If two CDR receivers are configured and one becomes inaccessible to the Cisco Meeting Server, CallLegUpdate and CallLegEnd CDR messages would cease being sent to the other. Fixed in 2.0.3
11140	When the API is in heavy use, responses to some queries could take over five seconds to complete.	GET queries for /users/ and /users/<guid> were taking longer than necessary to resolve. Any query queued behind large numbers of /users/ or /users/<guid> GET requests could wait for over five seconds to be processed. Fixed in 2.0.3
11218	No audio is heard in a two-participant, clustered AVMCU call	If two participants dial into an AVMCU conference through different CallBridges in a cluster, no audio will be heard until a third participant joins. Fixed in 2.0.3
11225	When you type **`help`** at the MMP prompt to show a list of commands, the short description for the **`callbridge`** command shows “Configure Acano Callbridge”.	Fixed in 2.0.3, the description now shows “ Configure CMS Callbridge”.
11276	The Cisco Meeting Server API does not allow passwords containing a colon character.	Although a password containing a colon is allowed by the Web Admin interface and the MMP, the API rejected the password returning a 401 Unauthorized Error. Fixed in 2.0.3

Reference	Issue	Summary
11290	Under certain circumstances, after upgrading an Acano server XMPP did not work	Unless an Acano X-series server had previously applied a recording or branding license, then the server did not have a license file and on upgrading the XMPP server stopped working. Fixed in 2.0.3.

Meeting Server 2.0.2 not released

Resolved in Meeting Server 2.0.1

Reference	Issue	Summary
10987	Audio from Single Screen SIP endpoints was being echoed back when on a call with a TIP 3-Screen System.	Fixed in 2.0.1
11012	The Web Bridge redirect was not consistently working correctly.	The initial 8 characters were being stripped from some URL redirects. Fixed in 2.0.1
11120	On a large cluster, it was possible to exceed the maximum number of database connections supported, which led to users being dropped for active calls or unable to join new calls.	The maximum number of database connects has been increased from 100 to 500. In addition a new feature has been added so that the number of active database connections can be monitored (see Section 2). Fixed in 2.0.1
11147	For Audio Only calls the "You are the only Participant" and "Waiting for your host to join" prompts were being played continuously.	These are now played periodically with periods of silence in between. Fixed in 2.0.1
11200	The Web Bridge occasionally restarted when it attempted to use a TCP connection which had already been closed by the remote end.	Fixed in 2.0.1

Resolved in Meeting Server 2.0.0 (formerly released as RC3)

Reference	Issue	Summary
6932	Not possible to restrict selected users from creating additional spaces	Release 2.0.0 added the userProfile parameter to the ldapSources object, this enables a userProfile to be associated with the users imported through an LDAP sync. Restrictions to the group of imported users can be applied with userProfile.
10835	The Web Bridge could crash if it had an invalid or no TURN server configuration	Fixed in 2.0.0
11000	In a distributed TIP deployment, a new active speaker from a TIP room was not always being shown full screen.	Some improvements have been made in release 2.0.0
11013	Log fills with info message “mf report overflow general status”	These info messages are harmless, they are sent to the host when the media framework tries to send a message. The size of the message has been reduced in release 2.0.0. A large number of these messages indicates that the vm has been operational for a long time. Restarting the vm will clear the log.
11114	The Web Bridge occasionally crashed during periods of network instability	XMPP requests were not always being correctly terminated in cases where network connectivity failed for a server. Fixed in 2.0.0

Resolved in Meeting Server 2.0 (prior to release)

Reference	Issue	Summary
10569	The Meeting Server was using high bandwidth to transmit content from SIP endpoint to Lync user.	New LAN and WAN bandwidth limit settings added to Web Admin interface of the Meeting Server.
10765	Polycom Trio endpoint in H.264UC mode, is not interoperable with the Meeting Server	In H.264UC mode, the Polycom Trio ignores the response from the Acano server that it does not support H.264 High Profile.
10786	Server failed to supply URI on reconnecting call	
10787	Expired accounts continue to access the Meeting Server API	Typically, when an account expires the user is prompted to enter a new password on next login. This was not applying to the API access where there was no mechanism to prompt for a password change. API access is now prevented for expired user accounts.

Reference	Issue	Summary
10826	The filter parameter for the /ivrs API object was not working properly.	
10900	Meeting Server restart on XMPP disconnect	Occasionally a Meeting Server could restart if an XMPP connection was torn down while a client node was being created.
10949	“Passcode set on access method” does not work when calls are placed through an IVR part of tenant group.	
11065	Filter on /api/v1/webbridges does not work	Trying to filter an enumeration of web bridges does not work.

5 Known Limitations

The following are known issues in this release. If you require more details on any of these please contact support@acano.com.

Reference	Issue	Summary
3965	Unable to stop pcap capture on serial/ssh	Occasionally users running pcap from the serial console for a few minutes are unable to stop the capture with a Ctr+C. If this happens try Ctr+\ or contact Acano support.
4132	Prevent logging in to the Web Admin Interface	By going to the Web Admin Interface login page, clicking OK to login and then holding down F5, all the sessions will be “used” without even logging in. This prevents anyone else from logging in until those sessions expire.
5228	No DNS failover for AD sync	Although the initial problem of the Call Bridge not falling back to a second AD server address after the LDAP connection to the first failed has been fixed in R1.2, there remains the issue that trying to connect to a non-existent/non-responding remote address can take a long time to time out.
7808	Wiggling panes in dock area	Participant panes in dock at bottom of screen may appear unsteady.
8356	Syscall errors in logs	If a WAN optimizer is deployed between clustered database nodes, it may prevent keep-alive checks from completing, causing SYSCALL errors to appear in logs. In cases where a WAN optimizer is being used between cluster nodes, it is important to ensure that all keep alive traffic is sent in a timely manner. Consult your WAN optimizer documentation on how to either disable this functionality between specific IP addresses, or for options that control which optimizations are applied.
8623	No conference control possible by Acano Client of Lync Clients, although controls appear	When adding a space into a Lync conference with multiple Lync users, an Acano app user can select a Lync users name and conference control options appear (mute audio/video, remove) but these options don't do anything.
9140	Endpoint presence incorrect when already in a Lync meeting	When an endpoint is dragged and dropped into a Lync meeting its presence is not correctly updated as busy.
11058	Three screen TIP does not work when dialing into Meeting Server	When dialing a 3 Screen TIP endpoint into Cisco Meeting Server 2.0, it can fail to negotiate and drop to a normal single screen call. This happens if the SIP trunk from the CUCM to the Cisco Meeting Server is configured to use Early Offer. Workaround: Set the SIP Trunk from the CUCM to the Cisco Meeting Server to use Delayed Offer.

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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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, 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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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