Contents

About Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway

Notes:

- Use Cisco Unified MeetingPlace H.323/SIP IP Gateway software Release 6.0 with IP PBX systems that are running standard H.323 or SIP call control-such as Avaya, Nortel, Alcatel, and Pingtel systems.

- For information about configuring third-party call-control applications: If you are using an IP PBX that runs standard H.323 or SIP call control, see the About Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway page for required system settings and see your IP PBX documentation for information about how to configure those settings.

- For more information about installing Multi Access (MA) blades or configuring the Cisco Unified MeetingPlace Audio Server system for IP, see the Additional References for Working with Cisco Unified MeetingPlace H.323/SIP IP Gateway Software page.

Configure Cisco Unified MeetingPlace H.323/SIP IP Gateway for use with one of the following servers:

- Cisco Unified Communications Manager
- Cisco SIP Proxy Server
- (Optional) H.323 gatekeeper

Note: If you are using an IP PBX that runs standard H.323 or SIP call control, see the How to Configure Cisco Unified MeetingPlace H.323/SIP IP Gateway page for the required system settings and see your IP PBX documentation for information about how to configure those settings.

The following tables describe the Cisco Unified MeetingPlace H.323/SIP IP Gateway Management Console fields and list the default settings:

- Table: General Settings
- Table: H.323 Settings
- Table: SIP Settings

Note: Starting with Cisco Unified MeetingPlace Release 6.0 Maintenance Release 3 (MR3), the Cisco Unified MeetingPlace H.323/SIP IP Gateway no longer uses the Management Console. Instead, to configure the gateway, use the Cisco Unified MeetingPlace Gateway Configuration utility. Access the utility by double-clicking the orange door icon in the system tray.

Table: General Settings

Setting	Description	Default
Max Number of Callers	Maximum number of callers Cisco Unified MeetingPlace H.323/SIP IP Gateway will accept. This maximum number can be a combination of H.323 and SIP callers.	960
Outdial Protocol	Controls whether outdials from the IP-gateway server are placed by using H.323 or SIP. **Note:** In mixed H.323-SIP, call-control environments, you must select one protocol for outdials; otherwise, the default protocol will be used.	H.323
Verbose Logging	Sets the level of logging information.	Normal

Table: H.323 Settings

Setting	Description	Default
Enabled	Enables or disables the H.323 protocol.	Yes
Max Number of Callers	Maximum number of H.323 callers Cisco Unified MeetingPlace H.323/SIP IP Gateway accepts.	960
E.164 Address	A dialable number for the IP-gateway server.	-
H323 ID	Caller ID name that is used by Cisco Unified MeetingPlace H.323/SIP IP Gateway.	MeetingPlace
Gateway Address and Gateway Port	IP address and port number of the server responsible for routing H.323 calls. Outdials using H.323 are directed to this IP address and port if an H.323 gatekeeper is not used. **Note:** You must enter this gateway information if you are using H.323 without a gatekeeper.	Address: - Port: 1720
Use Gatekeeper	Enables the IP-gateway server to register with an H.323 gatekeeper.	No
Gatekeeper Address and Gatekeeper Port	IP address and port number of the H.323 gatekeeper. If an H.323 gatekeeper is used, Cisco Unified MeetingPlace H.323/SIP IP Gateway registers with the server and directs H.323 outdials to the server. **Note:** If using an H.323 gatekeeper, ensure that your system allows traffic to pass through ports 1024-65535 because MeetingPlace H.323/SIP IPGW uses these ports for dynamic TCP and UDP traffic.	Address: - Port: 1719
QOS DSCP	**Note:** This field is only used for Cisco Unified MeetingPlace Release 6.0 MR3 and later. Differentiated Services Code Point value for the Quality of Service configuration setting.	26

Table: SIP Settings

Setting	Description	Default
Enabled	Enables or disables the SIP protocol.	Yes
Max Number of Callers	Maximum number of SIP callers Cisco Unified MeetingPlace H.323/SIP IP Gateway accepts.	960
Display Name	Display name of the IP-gateway server that is used for SIP messages.	MeetingPlace
User Name	A dialable number for the IP-gateway server.	(blank)
Session Name	Session name used in Session Description Protocol (SDP) body.	MeetingPlace IP Call
RSNA Prefix	**Note:** This field is only used for Cisco Unified MeetingPlace Release 6.0 MR3 and later. The prefix used for RSNA transfers used to identify the referring system to the voice gateway.	(blank)
Proxy Server Address and Proxy Server Port	IP address and port number of the Cisco SIP Proxy Server. Cisco Unified MeetingPlace system outdials placed by using SIP are directed to this IP address and port.	Address: - Port: 5060

	Note: If using Cisco SIP Proxy Server, ensure that your system allows traffic to pass through ports 1024-65535 because Cisco Unified MeetingPlace H.323/SIP IP Gateway uses these ports for dynamic TCP and UDP traffic.	
Stack Log Directory	**Note:** This field is only used for Cisco Unified MeetingPlace Release 6.0 MR3 and later. The SIP stack logging folder.	(blank)
Stack Log Level	**Note:** This field is only used for Cisco Unified MeetingPlace Release 6.0 MR3 and later. The SIP stack logging verbosity level.	3

How to Configure Cisco Unified MeetingPlace H.323/SIP IP Gateway

You must configure Cisco Unified MeetingPlace H.323/SIP IP Gateway to dial out by using one of the following servers:

- Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway for Use With Cisco Unified Communications Manager
- Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway for Use With Cisco SIP Proxy Server
- (Optional) Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway for Use With an H.323 Gatekeeper
- (Optional) Verifying MeetingPlace H.323/SIP IP Gateway Configuration

Note: Cisco Unified MeetingPlace H.323/SIP IP Gateway supports concurrent incoming H.323 and SIP calls; however, you must configure the Cisco Unified MeetingPlace H.323/SIP IP Gateway to use one protocol, either H.323 or SIP, to dial out.

Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway for Use With Cisco Unified Communications Manager

Note: If you are configuring the Cisco Unified MeetingPlace H.323/SIP IP Gateway for use with Cisco Unified Communications Manager on a system that also hosts the Cisco Unified MeetingPlace Web Server, you need to configure a separate gateway in Cisco Unified Communications Manager for each of the two IP addresses that the Cisco Unified MeetingPlace Web Server uses.

1. Access the server(s) Cisco Unified MeetingPlace H.323/SIP IP Gateway is installed on
2. **For Cisco Unified MeetingPlace Release 6.1**
    - ♦ Double-click the orange door icon in the system tray or go to Start > Programs > MeetingPlace Applications > MeetingPlace Gateway Configuration
3. Use the settings in Table: Configuration Settings for Use with Cisco Unified Communications Manager to configure Cisco Unified MeetingPlace H.323/SIP IP Gateway for use with Cisco Unified Communications Manager:

Table: Configuration Settings for Use with Cisco Unified Communications Manager

Setting Type	Field Name	Setting
General	Outdial Protocol	H.323
H.323	Enabled	Yes
H.323	E.164 Address	Dialable number for the MeetingPlace H.323/SIP IPGW
H.323	H.323 ID	MeetingPlace
H.323	Gateway Address	IP address of Cisco Unified Communications Manager
H.323	Gateway Port	1720
H.323	Use Gatekeeper	No

4. To accept the settings, click **Submit**.

5. Restart the IP-gateway server.

Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway for Use With Cisco SIP Proxy Server

Note: Cisco Unified MeetingPlace H.323/SIP IP Gateway does not support out-of-band digit detection with SIP.

1. Access the server(s) Cisco Unified MeetingPlace H.323/SIP IP Gateway is installed on
2. **For Cisco Unified MeetingPlace Release 6.1**
    - Double-click the orange door icon in the system tray or go to Start > Programs > MeetingPlace Applications > MeetingPlace Gateway Configuration
3. Use the settings in the following table to configure Cisco Unified MeetingPlace H.323/SIP IP Gateway for use with Cisco SIP Proxy Server: .

Table: Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 6.0 Configuration Settings for Use With Cisco SIP Proxy Server

Setting Type	Field Name	Setting
General	Outdial Protocol	SIP
SIP	Enabled	Yes
SIP	Display Name	MeetingPlace
SIP	User Name	Dialable number for the MeetingPlace H.323/SIP IPGW
SIP	Session Name	MeetingPlace IP Call
SIP	Proxy Server Address	IP address of the Cisco SIP Proxy Server
SIP	Proxy Server Port	5060

4. To accept the settings, click **Submit**.

5. Restart the IP-gateway server.

Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway for Use With an H.323 Gatekeeper

Note: Cisco Unified MeetingPlace H.323/SIP IP Gateway registers to the gatekeeper as a terminal device.

1. Access the server(s) Cisco Unified MeetingPlace H.323/SIP IP Gateway is installed on
2. **For Cisco Unified MeetingPlace Release 6.1**
   - Double-click the orange door icon in the system tray or go to Start > Programs > MeetingPlace Applications > MeetingPlace Gateway Configuration
3. Use the settings in Table: Cisco Unified MeetingPlace H.323/SIP IP Gateway software Release 6.0 Configuration Settings for Use With an H.323 Gatekeeper to configure Cisco Unified MeetingPlace H.323/SIP IP Gateway for use with an H.323 gatekeeper.

Table: Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release Release 6.0 Configuration Settings for Use With an H.323 Gatekeeper

Setting Type	Field Name	Setting
General	Outdial Protocol	H.323
H.323	Enabled	Yes
H.323	E.164 Address	Dialable number for the MeetingPlace H.323/SIP IPGW
H.323	H.323 ID	MeetingPlace
H.323	Gateway Port	1720
H.323	Gatekeeper Address	IP address of the H.323 Gatekeeper
H.323	Gatekeeper Port	1719
H.323	Use Gatekeeper	Yes

4. To accept the settings, click **Submit**.

5. Restart the IP-gateway server.

Verifying MeetingPlace H.323/SIP IP Gateway Configuration

1. To verify that Cisco Unified MeetingPlace H.323/SIP IP Gateway services are running, choose **Start > Settings > Control Panel** from the IP-gateway server; then, select **Services**.
2. Make sure that the following services are running:
   - Cisco Unified MeetingPlace Gateway SIM
   - Cisco Unified MeetingPlace IP Gateway
3. To verify that the IP-gateway server is logging in, telnet to the Cisco Unified MeetingPlace Audio Server.
4. To verify that the IP-gateway server status is OK, enter **gwstatus**.

   Note: It can take up to five minutes for **gwstatus** to update; therefore, any recent changes to the gateway may not be reflected.
5. Verify that you can access the Cisco Unified MeetingPlace Audio Server system by using a Cisco IP Phone.
6. Verify that you can access Cisco Unified MeetingPlace Audio Server system by using a PSTN phone.

About Configuring Multiple Cisco Unified MeetingPlace H.323/SIP IP Gateway Servers for Load Balancing and Redundancy

If you have deployed multiple IP-gateway servers to route IP calls, you can configure Cisco Unified Communications Manager or your IP PBX to load balance and to provide Cisco Unified MeetingPlace system redundancy by creating route groups that send calls to other IP-gateway servers if gateway failure occurs. A route group allows you to designate the order in which IP-gateway servers are selected and to prioritize a list of IP-gateways and ports for outgoing trunk selection.

All IP-gateway servers actively handle calls, and calls are routed round-robin among the IP-gateway servers. Therefore, in-session calls that are connected to an IP-gateway server that has failed are disconnected, and those callers must call again to be reconnected to the Cisco Unified MeetingPlace Audio Server system. New callers, however, are routed to another IP-gateway server.

For information about configuring route groups, see the Redundancy Chapter in the *Cisco Unified Communications Manager System Guide* for your software release at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

About Configuring a Dialing Group

Note: The prompt menu that is configured to be played in a dialing group entry is also referred to as an "application type". Any references to a configurable application type in this documentation is functionally equivalent to the prompt menu in the following section.

Dialing groups customize the Cisco Unified MeetingPlace Audio Server by presenting specific voice prompts to callers who dial in to a meeting by using a particular IP phone number. For example, you can configure a dialing group to immediately place callers who dial extension 2121 into meeting ID 656565.

You configure dialing groups by editing the dialgroups.txt file to include the dial pattern with which to associate a specific dialing group; the application, or prompt, to play for the dialing group callers; and the meeting number to present to the Cisco Unified MeetingPlace Audio Server. Entries in dialgroups.txt are processed in order from top to bottom. If a match is not found, the caller is placed at the CombinedAccess menu, and the dialed digits are presented to the Cisco Unified MeetingPlace Audio Server.

How to Configure a Dialing Group

1. Open the Cisco Unified MeetingPlace H.232/SIP IP Gateway folder on your IP-gateway server.
2. By using a text editor, open the dialgroups.txt file.
3. Read the comment lines that start with the # symbol.
4. Enter the dial pattern that you want to customize; then, enter a space. Valid selections are the following:

- [0-9] [A-D]-Presents the digits to the MeetingPlace audio server.
- [.]-Matches any valid digit.
- [*]-Matches 0 or more occurrences of the preceding digit.

5. Enter the type of prompt menu to play to the caller; then, enter a space. Valid selections are the following:
   - CombinedAccess-Selects the Main menu.
   - DIDMeeting-Prompts the caller for the meeting ID to join. This option can be used to place the caller directly into a meeting if the digits match an existing meeting ID on the Cisco Unified MeetingPlace Audio Server system.
   - Profile-Prompts the caller for a profile number, which is not passed along to the Cisco Unified MeetingPlace server for user authentication.
   - MeetingNotes-Prompts the caller to retrieve meeting notes.
6. Enter the digits to present to the Cisco Unified MeetingPlace Audio Server system. Valid selections are the following:
   - [0-9] [A-D]-Presents the entered digits to the Cisco Unified MeetingPlace Audio Server system.
   - KEEP-Preserves the dialed digits.
   - NONE-Presents no digits to the server.
7. Repeat Step 4 through Step 6 until the file contains one line for each dialing group that you want to configure.
8. Save and close the dialgroups.txt file.
9. Restart the IP-gateway server.

Caution: Do not enter any blank lines when editing the dialgroups.txt file. If there are any extra lines anywhere in the dialgroups.txt file (except for the normal blank line after the # symbols if dialgroups are not configured), the IP Gateway service will not start.

Configuring a Dialing Group Example

The following is a sample dialgroups.txt file that shows callers who dial extension 2121 are forwarded to meeting ID 656565. Callers who dial any other valid number are prompted to enter a profile number, and those digits are forwarded to the Cisco Unified MeetingPlace Audio Server.

```
2121 DIDMeeting 656565

.* Profile KEEP
```

About Reservationless Single Number Access Configuration

With Reservationless Single Number Access (RSNA), profiled users who host or attend a reservationless meeting as either profile users or guests can access their meetings by dialing the same phone number, regardless of which Cisco Unified MeetingPlace Audio Server is hosting the meeting. With RSNA, users always dial the number of their home server, which then transfers the call to the scheduler or host's home server.

For information about configuring Reservationless Single Number Access, see About RSNA.

Note: Gateways must support the Session Initiation Protocol (SIP) Refer Method, RFC 3515, to use RSNA.

Configuring Cisco Unified MeetingPlace 6.0 IP Gateway for SIP

You must configure Cisco Unified Communications Manager (CUCM) to operate with Cisco Unified MeetingPlace IP Gateway 6.x.

Configuring a SIP Trunk Profile

Configure your SIP trunk profile to select the correct communications protocol to work with IP gateway.

1. Go to **http**:*//ccm-server/*, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **System > Security Profile > SIP Trunk Security Profile**.
4. Create a new SIP trunk security profile with the following settings:
    - Device Security mode: **Non-secure**
    - Incoming Transport Type: **TCP + UDP**
    - Outgoing Transport Type: **UDP**
    - Incoming port: **5060**
    - Select **Accept Presence Subscription**
    - Select **Accept Out-of-Dialog REFER**
    - Select **Accept Unsolicited Notification**
    - Select **Accept Replaces Header**
5. Select **Save**.

Configuring a SIP Profile

Configure a SIP profile to set up your SIP device parameters.

1. Go to **http**:*//ccm-server/*, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **Device > Device Settings > SIP Profile**.
4. Create a new SIP profile with the following settings:
    - Default MTP Telephony Eevent Payload Type: **101**
    - Select **Conference Join Enabled**
    - Select **Semi Attended Transfer**
    - Leave all other settings as default
5. Select **Save**.

Configuring a SIP Trunk

Configuring a SIP trunk to establish a connection to the Cisco Unified MeetingPlace IP Gateway.

1. Go to **http**:*//ccm-server/*, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **Device > Trunk**.
4. Enter the trunk name.
5. Configure the following settings:
    - ♦ Inbound Calls: **Significant Digits** (user configurable)
    - ♦ SIP Information
        - ◊ Destination Address: Enter the IP gateway IP address.
        - ◊ Destination Port: **5060** (matches with IPGW SIP configuration later).
        - ◊ SIP Trunk Security Profile: Use the security profile that you created in the procedure above.
        - ◊ SIP Profile: Use the profile that you created in the procedure above.
        - ◊ DTMF Signalling Method: **RFC 2833**
6. Select **Save**.

Configuring a SIP Route Pattern

Configure one SIP route pattern for each remote IP gateway to send the call to Cisco Unified MeetingPlace using a SIP trunk.

1. Go to **http**:*//ccm-server/*, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **Call Routing > SIP Route Pattern**.
4. Create a new SIP route pattern, and select an IPv4 address (MeetingPlace IP GWY).
5. Configure the SIP route pattern to use the SIP trunk that you created in the procedure above.
6. Select **Save**.

Configuring a Route Pattern

Configure a route pattern to send the call to Cisco Unified MeetingPlace using a SIP Trunk.

1. Go to **http**:*//ccm-server/*, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **Call Routing > Route/Hunt > Route Pattern**.

    Note: You can optionally select **Route Group > Route List** first.
4. Create a new route pattern, using the domain name that you plan to use to call Cisco Unified MeetingPlace. Configure the following settings:
    - ♦ Gateway/Route List: Select the SIP trunk that you created in the procedure above.
    - ♦ Route Option: **Route This Pattern**.
        - ◊ Call Classification: **OnNet**.
        - ◊ Deselect **Provide Outside Dial Tone**.
5. Select **Save**.

Configuring Cisco Unified MeetingPlace IP Gateway

1. Sign in to the MeetingPlace IP Gateway server (Windows log on as the server?s administrator).
2. Double-click the orange door in the System Tray.
    - Select **IP Gateway Common** and set Outdial Protocol to **maximum number of callers**. Select **IP Gateway SIP** and configure the following settings:
        - Enabled: **Yes**
        - User Name: Enter the domain name you configured for the Route Pattern in CUCM.
        - Enter a Session Name.
        - Proxy Settings and Proxy Server Address: Select **Add** and enter the CUCM IP address
3. Select **Save**.
4. Enter **5060** for the Proxy Server Port.
5. Select **Apply**.
6. Select **Save**.
7. Select **Control Panel > Services**.
8. Select **Cisco MeetingPlace IP Gateway** and then select **Restart** after all the call processing is correct (calling search space, partition, device pool, and device codec).

Allowing Reverse Connections to the MeetingPlace Audio Server

The Cisco Unified MeetingPlace Audio Server can initiate a reverse connection, eliminating the need for incoming port 5003 to be open on the Cisco Unified MeetingPlace Audio Server. To initiate the reverse connection, you must open port 5003 on the Cisco Unified MeetingPlace H.323/SIP IP Gateway.

Suppressing Music-On-Hold

You can configure Cisco Unified Communications Manager to play music for the held party when users put a call on hold. However, if a user places a meeting on hold, the music plays into the meeting until the user retrieves the held call. To prevent this, you can configure Cisco Unified Communications Manager not to play music on hold for calls routed through Cisco Unified MeetingPlace H.323/SIP IP Gateway.

Specifically, make sure you do not assign to the Cisco Unified MeetingPlace H.323/SIP IP Gateway a Media Resource Group List that includes any Media Resource Group that includes Music on Hold servers, as the MeetingPlace IP Gateway can join a multicast Music-On-Hold (MoH) group. Since MeetingPlace is a transmit/receive environment, being put on hold can mean meeting participants listen to MoH, as well meetings in progress to devices configured to participate in the multicast group, resulting unexpected and undesirable privacy breaches.

As an additional workaround/resolution, if the customer is using Cisco Unified Communications Manager (CUCM) Version 6.1 and later, verify the CUCM Service Parameter "Send Multicast MOH in H.245 OLC Message" is set to False.

For information on configuring Media Resource Groups and Media Resource Group Lists, and associating these lists with endpoints, see the documentation for your release of Cisco Unified Communications Manager.

Note: This solution does not suppress music on hold for remote endpoints which are registered to a different Cisco Unified Communications Manager cluster than Cisco Unified MeetingPlace. If the CUCM cluster connecting to MeetingPlace is v7.1.2 please also note of defect CSCtg45036.