Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1

This chapter provides procedures for configuringRelease 5.2.1 and includes the following sections:

Information About Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1

After you install Release 5.2.1, you must configure it for use with one of the following servers:

- Cisco Unified CallManager
- 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 Software Release 5.2.1" section on page 3-3 for the required system settings and see your IP PBX documentation for information about how to configure those settings.

Table 3-1 describes the Release 5.2.1 Management Console fields and lists the default settings.

Table 3-1 Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 Management Console Fields and Default Settings

Setting	Description	Default
General Settings		
Max Number of Callers	Maximum number of callers Release 5.2.1 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
H.323 Settings		
Enabled	Enables or disables the H.323 protocol.	Yes
Max Number of Callers	Maximum number of H.323 callers Release 5.2.1 accepts.	960
E.164 Address	A dialable number for the IP-gateway server.	—
H323 ID	Caller ID name that is used by Release 5.2.1.	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, Release 5.2.1 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

Table 3-1 Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 Management Console Fields and Default Settings

Setting	Description	Default
SIP Settings		
Enabled	Enables or disables the SIP protocol.	Yes
Max Number of Callers	Maximum number of SIP callers Release 5.2.1 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
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. **Note** If using Cisco SIP Proxy Server, ensure that your system allows traffic to pass through ports 1024-65535 because Release 5.2.1 uses these ports for dynamic TCP and UDP traffic.	Address: — Port: 5060

How to Configure Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1

You must configure Release 5.2.1 to dial out by using one of the following servers:

- Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 for Use With Cisco Unified CallManager, page 3-4
- Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 for Use With Cisco SIP Proxy Server, page 3-4
- (Optional) Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 for Use With an H.323 Gatekeeper, page 3-5
- (Optional) Verifying MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 Configuration, page 3-6

Note Release 5.2.1 supports concurrent incoming H.323 and SIP calls; however, you must configure the Release 5.2.1 to use one protocol, either H.323 or SIP, to dial out.

Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 for Use With Cisco Unified CallManager

Step 1 From the IP-gateway server, choose **Start > Programs > MeetingPlace Applications > MeetingPlace Management**.

Step 2 Double-click the Cisco Unified MeetingPlace IP Gateway icon.

The Cisco Unified MeetingPlace IP Gateway Management Console opens.

Tip You can also access Release 5.2.1 configuration settings through the Registry Editor by navigating to \\HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\MeetingPlace IP Gateway.

Use the settings in Table 3-2 to configure Release 5.2.1 for use with Cisco Unified CallManager.

Table 3-2 Release 5.2.1 Configuration Settings for Use With Cisco Unified CallManager

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

Step 3 To accept the settings, click **Submit**.

Step 4 Restart the IP-gateway server.

Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 for Use With Cisco SIP Proxy Server

Note Release 5.2.1 does not support out-of-band digit detection with SIP.

Step 1 From the IP-gateway server, choose **Start > Programs > MeetingPlace Applications > MeetingPlace Management**.

Step 2 Double-click the Cisco Unified MeetingPlace IP Gateway icon.

The Cisco Unified MeetingPlace IP Gateway Management Console opens.

Tip You can also access Release 5.2.1 configuration settings through the Registry Editor by navigating to \\HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\MeetingPlace IP Gateway.

Step 3 Use the settings in Table 3-3 to configure Release 5.2.1 for use with Cisco SIP Proxy Server.

Table 3-3 Release 5.2.1 Configuration Settings for Use With Cisco SIP Proxy Server

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

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

Step 5 Restart the IP-gateway server.

Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 for Use With an H.323 Gatekeeper

Note Release 5.2.1 registers to the gatekeeper as a terminal device.

Step 1 From the IP-gateway server, choose **Start > Programs > MeetingPlace Applications > MeetingPlace Management**.

Step 2 Double-click the Cisco Unified MeetingPlace IP Gateway icon.

The Cisco Unified MeetingPlace IP Gateway Management Console opens.

Tip You can also access Release 5.2.1 configuration settings through the Registry Editor by navigating to \\HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\MeetingPlace IP Gateway.

Step 3 Use the settings in Table 3-4 to configure Release 5.2.1for use with an H.323 gatekeeper.

Table 3-4 Release 5.2.1 Configuration Settings for Use With an H.323 Gatekeeper

Field Name	Setting
General Settings	
Outdial Protocol	H.323

Table 3-4 Release 5.2.1 Configuration Settings for Use With an H.323 Gatekeeper

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

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

Step 5 Restart the IP-gateway server.

Verifying MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 Configuration

Step 1 To verify that Release 5.2.1 services are running, choose **Start > Settings > Control Panel** from the IP-gateway server; then, select **Services**.

Step 2 Make sure that the following services are running:

- Cisco Unified MeetingPlace Gateway SIM
- Cisco Unified MeetingPlace IP Gateway

Step 3 To verify that the IP-gateway server is logging in, telnet to the Cisco Unified MeetingPlace Audio Server system.

Step 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.

Step 5 Verify that you can access the Cisco Unified MeetingPlace Audio Server system by using a Cisco IP Phone.

Step 6 Verify that you can access Cisco Unified MeetingPlace Audio Server system by using a PSTN phone.

Information About Configuring Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 for Use With Cisco Unified MeetingPlace Web Conferencing

You can install Release 5.2.1 on either the same or separate server as Cisco Unified MeetingPlace Web Conferencing. Release 5.2.1 uses the primary address, and you must configure Cisco Unified MeetingPlace Web Conferencing to use the secondary address. If Release 5.2.1 is installed on a server with more than one IP address, you must define a gateway for each IP address either in Cisco Unified CallManager, Cisco SIP Proxy server, or H.323 Gatekeeper for outdials to work.

Note Before you install multiple Cisco Unified MeetingPlace system integration applications on the same server, ensure that your system meets the requirements for integration. For additional information, see *Important Information About Cisco Unified MeetingPlace Products and Cisco Media Convergence Servers* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/mpmcs.htm

Information About Configuring Multiple Cisco Unified MeetingPlace H.323/SIP IP Gateway Software Release 5.2.1 Servers for Load Balancing and Redundancy

If you have deployed multiple IP-gateway servers to route IP calls, you can configure Cisco Unified CallManager 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 a 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 to the Redundancy Chapter in the *Cisco Unified CallManager System Guide* for your software release at the following URL:

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

Information About Configuring a Dialing Group

Dialing groups customize the Cisco Unified MeetingPlace Audio Server system 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 system. 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 system.

How to Configure a Dialing Group

Step 1 Open the Cisco Unified MeetingPlace IP Gateway folder on your IP-gateway server.

Step 2 By using a text editor, open the dialgroups.txt file.

Step 3 Read the comment lines that start with the # symbol.

Step 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.

Step 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.

Step 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.

Step 7 Repeat Step 4 through Step 6 until the file contains one line for each dialing group that you want to configure.

Step 8 Save and close the dialgroups.txt file.

Step 9 Restart the IP-gateway server.

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 system.

```
2121 DIDMeeting 656565
.* Profile KEEP
```

Information 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 system 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 the *Administrator Guide* for Cisco Unified MeetingPlace Audio Server Release 5.3 at the following URL:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html

Note Gateways must support the Session Initiation Protocol (SIP) Refer Method, RFC 3515, to use the Reservationless Single Number Access feature.

Information About Reverse Connection to the MeetingPlace Audio Server System Configuration

The Cisco Unified MeetingPlace Audio Server system can initiate a reverse connection, eliminating the need for incoming port 5003 to be open on the Cisco Unified MeetingPlace Audio Server system. To initiate the reverse connection, you must open port 5003 on the IP-gateway server.