



## CHAPTER 2

# Setting Up Cisco Unified MeetingPlace Audio Server

---

Cisco Unified MeetingPlace offers several ways to organize, maintain, secure, and customize information about the system and the people who use the application.

See the following sections:

- [System Administrator Responsibilities, page 2-1](#)
- [About Profiles, page 2-4](#)
- [About User Groups, page 2-13](#)
- [About User Profiles, page 2-14](#)
- [About Teams, page 2-22](#)
- [About Searching for Users, Groups, and Teams, page 2-23](#)
- [About Establishing Security, page 2-24](#)
- [About Customizing Cisco Unified MeetingPlace Audio Server, page 2-29](#)
- [About Flex Fields, page 2-30](#)
- [About Flex Menus, page 2-32](#)
- [About Customizing Voice Prompts, page 2-38](#)
- [About Multiserver Meetings, page 2-41](#)
- [About Reservationless Meetings, page 2-56](#)
- [About RSNA, page 2-66](#)
- [About Cisco Unified MeetingPlace Language System Option, page 2-77](#)

## System Administrator Responsibilities

Cisco Unified MeetingPlace requires a minimal level of management. As system administrator, you perform the following tasks:

- Maintain the database of Cisco Unified MeetingPlace profiles
- Set up an internal support strategy
- Track resource usage
- Perform traditional maintenance functions

- Handle system alarms
- Ensure system security

## Maintaining Profiles

Each person in your user community needs a Cisco Unified MeetingPlace user profile defined in the Cisco Unified MeetingPlace database. User profiles contain information such as:

- User ID and passwords
- Class-of-service privileges
- Meeting preferences
- Notification information (e-mail address)
- Attend information (phone number and pager number)

As the system administrator, you are responsible for maintaining a directory of users and their associated privileges (as is the case with many in-house communications systems, such as e-mail, groupware, and voice mail systems).

The amount of ongoing work for profile maintenance often depends on the level of up-front planning and coordination you perform. If you have Cisco Unified MeetingPlace Directory Services or can obtain database access to user lists from another source, such as an e-mail system directory or a human resources database, you can easily automate the process of synchronizing Cisco Unified MeetingPlace with that other source.

If you do not have a means of synchronizing Cisco Unified MeetingPlace with another source of users, you must set up a fulfillment process for new users who request Cisco Unified MeetingPlace profiles.

## Planning Internal Support

As system administrator, you are responsible for planning and implementing the various levels of support in your organization. Some support considerations include:

- **Decentralized, departmental support.** For the bulk of simple requests, such as help with scheduling or forgotten passwords, Cisco Unified MeetingPlace can empower departmental support personnel or administrative assistants to provide help. In Cisco Unified MeetingPlace, special department contacts have privileges to support a subset of the overall user community.
- **Company-wide support.** Either a company receptionist or help desk personnel can provide attendant-level support. Cisco Unified MeetingPlace attendants have privileges to support all users.
- **Help desk support.** You may consider providing help desk employees with additional capabilities to resolve problems when you are not available. The range of system management capabilities available to help desk attendants include creating/deleting user profiles and the ability to run reports.

When Cisco Unified MeetingPlace encounters more serious problems, such as T1 failure or a system failure, you can set up the system to notify you. A critical part of your internal support strategy is a set of procedures to follow for handling alarm conditions.

## Tracking Resource Usage

Tracking resource usage on the system is important for several reasons:

- Ensures that users are effectively distributed across conference servers
- Ensures you have enough capacity for current usage
- Enables you to perform internal bill backs
- Helps audit potential abuse

To help track resource usage, Cisco Unified MeetingPlace offers a series of standard reports and capacity management tools. The system also enables you to export database tables in a raw format for analysis or reporting in other applications.

For more information on capacity management, see [Chapter 5, “Managing and Maintaining Cisco Unified MeetingPlace.”](#) For more information on reporting, see [Chapter 4, “Running Reports.”](#)

## Maintaining the Cisco Unified MeetingPlace System

Cisco Unified MeetingPlace requires very little system maintenance. However, like any other system, you need to perform backups on a regular basis. You may also need to shut down and restart the system on occasion, such as when moving your offices to another location.

For information on system maintenance, see [Chapter 5, “Managing and Maintaining Cisco Unified MeetingPlace.”](#)

## System Administrator Schedule

Some of your tasks should be performed routinely on a weekly or monthly basis. Others require your response as needed. [Table 2-1](#) summarizes typical system administrator tasks.



### Note

To establish default values for the parameters that control basic Cisco Unified MeetingPlace operations, see the “Usage Parameters” worksheet in the applicable *Installation Planning Guide for Cisco Unified MeetingPlace*, at [http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html).

**Table 2-1** System Administrator Schedule

Frequency/Reason	Tasks
Weekly	<ul style="list-style-type: none"> <li>• Add profiles and teams to the Cisco Unified MeetingPlace system, distribute documentation, and provide MeetingTime access to support staff</li> <li>• Review alarm table activity for the past week</li> <li>• Print or save the list of meetings for the next week</li> <li>• Run a system backup</li> </ul>

Table 2-1 System Administrator Schedule (continued)

Frequency/Reason	Tasks
Monthly	<ul style="list-style-type: none"> <li>Run and review a system usage report</li> <li>Run the monthly trending capacity management tools to review system usage, conferencing growth, and service levels</li> <li>Update and save the historical data file for the monthly trending tools</li> <li>Perform internal bill backs</li> </ul>
Planning and strategy	<ul style="list-style-type: none"> <li>Coordinate profile import strategy</li> <li>Train other employees who have user support responsibilities</li> <li>Define processes for handling Cisco Unified MeetingPlace alarms</li> <li>Review system usage and capacity requirements</li> </ul>
As needed	<ul style="list-style-type: none"> <li>Respond to alarm conditions</li> <li>Coordinate planned outages (such as relocations and software upgrades)</li> <li>Act as contact to Cisco TAC</li> </ul>

## About Profiles

Profiles offer different levels of service to different users, track use for billing purposes, maintain better security on your system, and provide effective ways for your users to conduct secure meetings.

You can define two types of profiles:

- User groups, which include information about groups of Cisco Unified MeetingPlace users that have common profiles. (To define user groups, see the [“About User Groups” section on page 2-13.](#))
- User profiles, which include information about individual Cisco Unified MeetingPlace users. (To define user profiles, see the [“About User Profiles” section on page 2-14.](#))

Define the user groups first, and then define the user profiles. User profiles within a group inherit many of the same group settings, which minimizes the work of duplicating those settings for each user in the group.

We recommend that you create a profile for every user in the system. Create a profile for each user who sets up meetings and attends meetings regularly.

## Benefits of Assigning Profiles

Users who have profiles established for them can use the following important features:

- Schedule meetings
- Query the system for a list of their meetings
- Attend meetings secured by profile
- Be invited as a speaker to lecture-style meetings
- Be paged or dialed at the time of their meetings
- Have the system reach them by dialing up to three different phone numbers at the time of their meeting

- Access meeting-related documents or voice comments that are secured by profile
- Be notified of meetings and changes to meetings (if the Notification option is installed)
- Gain access to Cisco Unified MeetingPlace over the LAN or WAN through MeetingTime or Cisco Unified MeetingPlace Web Conferencing

## Planning and Maintaining Profiles

You can define profiles for the following:

- Targeted meeting schedulers (see the [“Providing Profiles for Targeted Meeting Schedulers”](#) section on page 2-5).
- Only those who ask for profiles (see the [“Providing Profiles on Request”](#) section on page 2-5).
- Your entire user community

We recommend defining profiles for your entire user community.

## Providing Profiles for Targeted Meeting Schedulers

To minimize the number of profiles you maintain on your system, define profiles only for people who schedule conferences and create reservationless meetings. For example, these people might be departmental administrators, company operators, or specific “power users” within your organization. Everyone else is a guest. (For more information about guest users, see the [“Profile Properties”](#) section on page 2-5.)

Using this strategy, anyone can attend the conference as a guest user if the meeting scheduler allows guest participation. Providing guest access to meetings allows vendors, customers, and other partners to participate in conferences. However, you can have users who do not need to schedule conferences attend all meetings as guests.

Although this approach requires the least planning, it limits the features that users without profiles can use.

## Providing Profiles on Request

You can provide profiles only for users who request them. This strategy may be similar to the process you already have in place for requesting other types of information systems or telecommunications resources.

If you provide profiles on request, define the process for creating them. For example, assign this task to the help desk staff so that you, the system administrator, have time for other responsibilities.

## Profile Properties

A profile contains all the information about known users in the system. [Table 2-2](#) shows the types of information that profiles contain.

**Table 2-2** *User Profile Information*

Profile Information	Section
Class of user	<a href="#">User Class, page 2-6</a>
User ID and passwords	<a href="#">User ID and Password, page 2-7</a>
Address information, including phone and e-mail	<a href="#">User Contact Information, page 2-7</a>
Billing information	<a href="#">Billing Information, page 2-8</a>
Class of Service privileges	<a href="#">Class of Service Privileges, page 2-8</a>
Outdialing privileges	<a href="#">Outdialing Privileges, page 2-8</a>
Whether to allow guests to join meetings from the Web	<a href="#">Letting Guests Join Meetings from the Web, page 2-15</a> and <a href="#">Creating Guest Profiles, page 2-15</a>
Departmental support contacts	<a href="#">Departmental Support Contacts, page 2-12</a>
Time zone	<a href="#">Time Zone, page 2-12</a>
Meeting preferences	<a href="#">Meeting Preferences, page 2-13</a>
Video Terminal Parameters	<a href="#">Video Terminal Fields, page 2-13</a>

To define user groups, see the “[About User Groups](#)” section on page 2-13. To define user profiles, see the “[About User Profiles](#)” section on page 2-14.

## User Class

You can control the level of access that each user has to Cisco Unified MeetingPlace by assigning each user to a class. [Table 2-3](#) describes the four classes of users.

**Table 2-3** *User Classes*

User Class	Description
End user	End users can schedule meetings, attend meetings they have been invited to, and change certain settings in their profile.
Delegate (also Contact)	Delegates schedule and manage meetings for a group of end users. Delegates can schedule and reschedule meetings on behalf of these users and manage these users’ profiles. Delegates also have access to the In-session tab in MeetingTime, to monitor meetings that have been scheduled by them or their end users. Delegates are often administrative assistants in a company.
Attendant	Attendants support all end users and delegates. They can view all meetings that have been scheduled on Cisco Unified MeetingPlace and can use the In Session tab to monitor end meetings that are currently taking place.  Attendants may also create and delete profiles, lock and unlock profiles, run reports, monitor capacity management, and view alarms if a system administrator has given them these privileges. Attendants are typically the “zero out” position that users connect to when they need help during a meeting, and are often Cisco Unified MeetingPlace help desk staff in the company.
System manager	System administrators set up and maintain the system. As such, they need access to all information in the Cisco Unified MeetingPlace Audio Server database, including system configuration information and information about the user community.

## User ID and Password

Cisco Unified MeetingPlace identifies users based on their user ID. The user ID is a unique alphanumeric string of 3 to 17 characters. MeetingTime identifies users by their user IDs in all its screens and reports.

Users also need their user ID and a corresponding alphanumeric password to use MeetingTime and Cisco Unified MeetingPlace Web Conferencing over a Local Area Network (LAN) or Wide Area Network (WAN). Assign users Cisco Unified MeetingPlace user IDs that are the same as either their network or e-mail user names.

In addition to the user ID, Cisco Unified MeetingPlace profiles have a unique profile number. The profile number—3 to 17 digits—identifies users over the phone. Typically, the profile number is the same as a user phone number, extension, or voice-mail box. Profile numbers have corresponding numeric passwords that are independent of the alphanumeric passwords associated with the user ID for LAN or WAN access.

Remember the following important information:

- Do not set the user ID and profile numbers to the same value. Using numeric-only user IDs makes reports difficult to read. Also, because MeetingTime consistently refers to conference participants by user ID, managing conferences from within MeetingTime becomes difficult when you assign numeric-only user IDs.
- When the Reservationless Meetings feature is turned on, profile numbers cannot match existing meeting IDs (because reservationless meetings use profile numbers as reservationless meeting IDs). If you try to create a profile number that matches an existing meeting ID, you receive an error message about the conflict. To resolve the conflict, either change the existing meeting ID or select another profile number for the user. (For more information, see the [“About Reservationless Meetings”](#) section on page 2-56.)

## User Contact Information

Cisco Unified MeetingPlace maintains directory information for use with advanced features, such as automated outdialing (automatically dialing a participant at the time of the meeting) and paging.

For each user, the system tracks the following:

- Phone number to use for system outdials
- Pager type and phone number for start-of-meeting notification
- E-mail address to use for notifications
- Internet e-mail address used by Cisco Unified MeetingPlace Web Conferencing

For phone and pager numbers, the system uses its internal translation tables to map phone numbers stored in Cisco Unified MeetingPlace profiles to actual dialing strings. Do not put in extra digits required for dialing strings (such as 9 to dial out from your PBX) in the profile entries.

To make the best use of Cisco Unified MeetingPlace capabilities, enter all the address information that applies to your system. This information might be available if you import profiles from a company directory or other source.

For e-mail addresses, enter the e-mail addresses used by your e-mail system. [Table 2-4](#) shows the e-mail addresses to use.

**Table 2-4 E-Mail Address Formats by E-Mail System**

E-Mail System	E-Mail Address	Example
cc:Mail	User Name at Post Office	Chris Lee at MyCompany
Microsoft Mail	User Name	Chris Lee
IBM Lotus Notes	User Name/Server	Chris Lee/MyCompany
Microsoft Exchange	User Name	Chris Lee
Netscape Messenger	Internet address	ChrisLee@MyCompany.com
Qualcomm Eudora	Internet address	ChrisLee@MyCompany.com
Other	Internet address	ChrisLee@MyCompany.com

Remember the following information:

- When an Internet mail system is not the primary mail system communicating with your e-mail system, do not enter Internet e-mail addresses in the E-mail address field.
- Customers cannot configure the Cisco Unified MeetingPlace translation tables.

## Billing Information

You can assign billing codes to profiles and meetings, which allows companies to choose billing schemes based on scheduling or meeting participation.

You assign a billing code to user profiles. Meeting schedulers can override their default billing code for each meeting. Typically, user profiles inherit their billing codes from their user group.

## Class of Service Privileges

You can limit the resource usage of a user based on what user group they are placed in and how that user group is configured. These permissions and rights extend to ability of the user or group to schedule, outdial from, and record meetings.

Typically, user profiles inherit their class of service privileges from their user group. For more information on using class of service privileges to control resource use, see the [“About Managing Ports” section on page 5-1](#). For more information on securing the system through class of service privileges, see the [“About Establishing Security” section on page 2-24](#).

## Outdialing Privileges

Outdialing allows users to quickly and easily join meetings and add other users to meetings they are attending. By using the Outdial feature, users can:

- Add a user, team, missing invitees, or another Cisco Unified MeetingPlace server to a meeting in progress
- Join a meeting over the Web by clicking the Join Voice Conference button and having the system outdial to their phone
- Have the system call invited participants at the start of a meeting



For Cisco Unified MeetingPlace to perform these functions, a user must have outdial privileges. To provide outdial privileges to users, set the Can Call Out from Mtgs attribute to *Yes* in their user profile.


**Caution**

Toll fraud can occur if unauthorized users gain access to Cisco Unified MeetingPlace. For information on protecting your system from toll fraud, see the [“Preventing Toll Fraud” section on page 2-28](#).

## Using the “Find Me” Feature

You can configure Cisco Unified MeetingPlace Audio Server to outdial to up to three numbers to reach a user (or user group members) to join meetings. This section describes the “Find Me” feature and shows examples of various configurations.

If a Find Me outdial is initiated and there is a First Search Method field value, the system uses that number as the initial outdial destination. If there is no such value, the Phone Number value (from the user profile) is used. (This is also the Main value that you can choose to configure various fields.)

If the system has not located the user after the initial outdial attempt, it proceeds based on the # of Retry Attempts field value (in the system Usage Parameters), according to the following rules:

- If the parameter is 0, outdials continue to the Second Search Method and Third Search Method field values (if they exist), and then stop.
- If the parameter is greater than 0, the system counts retries as a set of outdials: to Second Search Method if it exists, then Third Search Method if it exists, and then back to First Search Method. After First Search Method is outdialed again, one retry has occurred.

The following restrictions apply to the Find Me settings:

- All values except None can be set in any order.
- None can occur only after a non-None value.
- No values other than None can follow None.
- No values other than None can be repeated.

[Table 2-5](#) shows the allowable values in each search field.

**Table 2-5 Allowable Values in Search Field**

First Search Method	Second Search Method	Third Search Method
None	None	None
Primary	None	None
Primary	Alternate	None
Primary	Pager	None
Primary	Alternate	Pager
Primary	Pager	Alternate
Alternate	None	None
Alternate	Primary	None
Alternate	Pager	None
Alternate	Primary	Pager
Alternate	Pager	Primary

**Table 2-5 Allowable Values in Search Field (continued)**

First Search Method	Second Search Method	Third Search Method
Pager	None	None
Pager	Primary	None
Pager	Alternate	None
Pager	Primary	Alternate
Pager	Alternate	Primary

Table 2-6 shows some invalid settings.

**Table 2-6 Invalid Values in Search Field**

First Search Method	Second Search Method	3rd Search Method
None	Primary	None
None	None	Pager
None	Alternate	Primary
Primary	Primary	Alternate

There must be a corresponding number for each value that is set. For example, if Pager is specified as a Find Me setting, there must be a pager number and type specified for the user in the profile.

## Examples of Find Me Settings

The following examples show the sequence followed for a Find Me outdial with various combinations of settings, including None. The format is:

[FindMe settings: 1st, 2nd, 3rd], “# of retry attempts” Outdial Destination

The examples apply to the following actions in MeetingTime and voice user interface (VUI), as noted:

- Team outdial (MeetingTime: Search For Users option selected)
- Get missing invitees (MeetingTime: Search For Users option selected)
- Have system find user (MeetingTime: Meeting Attendance options)
- #32 (VUI Team Outdial)
- #33 (VUI Get Missing Invitees)

**Table 2-7 Find Me Settings Example**

Call Number, # of Retry Attempts	Outdial Destination
[None, None, None], 0	Main
[None, None, None], 1	Main Main
[None, None, None], 2	Main Main Main
[Main, None, None], 0	Main

**Table 2-7 Find Me Settings Example (continued)**

<b>Call Number, # of Retry Attempts</b>	<b>Outdial Destination</b>
[Main, None, None], 1	Main Main
[Main, None, None], 2	Main Main Main
[Alternate, None, None], 0	Alternate
[Alternate, None, None], 1	Alternate Alternate
[Alternate, None, None], 2	Alternate Alternate Alternate
[Main, Alternate, None], 0	Main Alternate
[Main, Alternate, None], 1	Main Alternate Main
[Main, Alternate, None], 2	Main Alternate Main Alternate Main
[Main, Alternate, None], 3	Main Alternate Main Alternate Main Alternate Main
[Alternate, Main, None], 0	Alternate Main
[Alternate, Main, None], 1	Alternate Main Alternate
[Alternate, Main, None], 2	Alternate Main Alternate Main Alternate
[Main, Alternate, Pager], 0	Main Alternate Pager

**Table 2-7 Find Me Settings Example (continued)**

Call Number, # of Retry Attempts	Outdial Destination
[Main, Alternate, Pager], 2	Main Alternate Pager Main Alternate Pager Main

## When Find Me Settings Are Not Used

The following example shows when Find Me settings are not used.

The examples apply to the following actions in MeetingTime:

- Team Outdial (MeetingTime: Search for users option cleared)
- Get Missing Invitees (MeetingTime: Search for users option cleared)
- Have System Call User (MeetingTime: Meeting Attendance options)

**Table 2-8 Example Without Find Me**

Call Number, # of Retry Attempts	Outdial Destination
[Alternate, None, None], 0	Main
[Alternate, None, None], 1	Main Main
[Alternate, Main, None], 0	Main

## Departmental Support Contacts

To each Cisco Unified MeetingPlace profile, you assign a delegate (also called a contact)—a departmental support person or administrator who can represent the profile user. With each user profile, you must specify the Cisco Unified MeetingPlace user ID of the contact. Typically, user profiles inherit their contacts from their user group.

You can configure the system to let users get assistance before they enter a meeting if they do not enter a number at the first voice prompt or if they try to access an inactive profile. For more information on getting assistance, see the [“About Assisting Users” section on page 6-19](#).

## Time Zone

Each profile has a time zone setting. Set the time zone for the geographical location in which the user does business. For all meetings the user schedules or is invited to, the system accepts and reports start times in the time zone of that user.

When participants in different time zones are invited to the same meeting, the times reported to each participant are converted to their time zones.

When you schedule a recurring meeting, all instances of that meeting are at the same time of day in the scheduler time zone. So, for example, if someone in Arizona schedules a weekly meeting, callers from New York must adjust their schedules during daylight savings time.

## Meeting Preferences

Each user profile has default meeting preferences. Whenever users schedule a new meeting, these default meeting preferences initially determine the behavior of the meeting, such as whether it will be recorded. Users can override their default meeting preferences for each meeting.

Because users set up different types of meetings, select default meeting preferences for a user group that make sense for their application.

## Video Terminal Fields

Each video terminal has a user profile that includes the following fields for scheduling, reporting, and other functions.

**Table 2-9** Video Terminals Fields

Field	Setting
Video Terminal ID	The unique identifier that the Cisco Unified MeetingPlace Video Administration has associated with the video terminal.
Video Terminal Name	The name that the Cisco Unified MeetingPlace Video Administration uses to identify the video terminal.
Video Terminal Classification	The list of classifications, if any, that are associated with the video terminal. Each classification must be individually defined as a Meeting Category.

## About User Groups

After you choose your profile maintenance strategy, determine how to segment your user population into user groups. In Cisco Unified MeetingPlace, user groups are organized according to a shared set of attributes.

Before you begin, decide how to arrange users into groups, using the following information:

- Billing information (see the [“Billing Information”](#) section on page 2-8)
- Class-of-service privileges (see the [“Class of Service Privileges”](#) section on page 2-8)
- Organizational boundaries (see the [“Time Zone”](#) section on page 2-12)
- Departmental support contacts (see the [“Departmental Support Contacts”](#) section on page 2-12)

Each Cisco Unified MeetingPlace profile contains over 50 attributes that control user class of service privileges (also called permissions) and their meeting preferences. By arranging users into groups, you can easily maintain profiles for similar users. When something about that group changes (such as the departmental contact), you can update all the users in that group at one time.

Groups also determine the sort order of records in Cisco Unified MeetingPlace standard reports. Information from users in the same group appears together.

**To Define User Groups**

**Note** Before you begin, make sure you complete the “User Groups” worksheet in the applicable *Installation Planning Guide for Cisco Unified MeetingPlace*, at [http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html).

- 
- Step 1** By using MeetingTime, log in to Cisco Unified MeetingPlace.
- Step 2** In the MeetingTime reception room, click the Register Book.  
(Or choose **Administration** menu > **Configure**.)  
The Register window opens with the Configure tab displayed.
- Step 3** From the Views list, select **User Groups** and click **New**.
- Step 4** Enter a value for each parameter (attribute).  
Use the information from the “User Groups” worksheet in the *Installation Planning Guide for Cisco Unified MeetingPlace*.
- Step 5** Click **Save Changes**.
- 

## About User Profiles

After you define the user groups, create the user profiles. Before you create user profiles, be sure you have the following information about each user:

- User group (optional)
- Unique user ID and profile number (for the user ID, consider using the user phone extension, or network or e-mail user name)
- User-specific address information (phone, e-mail, pager)

**To Define User Profiles**

**Note** Before you begin, make sure you complete the “User Profiles” worksheet in the applicable *Installation Planning Guide for Cisco Unified MeetingPlace*, at [http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html).

- 
- Step 1** By using MeetingTime, log in to Cisco Unified MeetingPlace.
- Step 2** In the MeetingTime Configure tab, in the Views list, select **User Profiles** and click **New**.
- Step 3** Enter a value for each user profile parameter (attribute).  
Use the information from the “User Profiles” worksheet in the *Installation Planning Guide for Cisco Unified MeetingPlace*.
- Step 4** Choose the user group for the profile.
- Step 5** For all attributes that you want to assign the group default setting, choose **Group Dflt**.

**Step 6** Click **Save Changes**.

---

By default, attendants cannot create End User, Delegate (Contact), or Attendant user profiles. However, you can grant them such privileges. For more information, see the [“User Class” section on page 2-6](#).

## Creating Guest Profiles

Cisco Unified MeetingPlace includes a user ID, called guest, with a user profile for guest users. You can modify the guest profile, but you cannot delete it.

Examples of parameters you might want to change for guests are:

- Billing code
- Prompt level (standard or abbreviated)
- Default time zone to appear on notifications

While not recommended, you can also modify the class of service privileges for guest users. For example, you can allow guests to start meeting recordings or initiate outdials from within a meeting.

The guest profile is also used as a template for future profiles created in MeetingTime. To speed up the process of creating profiles, make sure all guest profile settings are set to Group Dflt.

## Letting Guests Join Meetings from the Web

By default, Cisco Unified MeetingPlace prevents outdialing to guests when they click the Join Voice Conference button from the Web. You can change this setting to allow users to schedule meetings that let guests be outdialed when they click the Join Voice Conference button. This is especially useful in meetings attended by guests outside your organization, such as customers, partners, and suppliers.

### To Allow Users to Schedule Meetings That Let Guests Attend Over the Web

---

**Step 1** Do the following in your user profiles:

- For the Can Call Out From Mtgs attribute, choose **Yes**.
- For the Can Schedule Guest Outdial Mtgs attribute, choose **Yes**.

**Step 2** For the Allow Outdials to Guests from Web attribute, determine the default setting.

For security reasons, we recommend that you set this attribute to No.

Users can change this attribute when they schedule individual meetings, to either allow or prevent guest attendance over the Web.

---

Remember the following information:

- This configuration lets profile users without outdial privileges have the system outdial to them by using the Join Voice Conference button from the Web.
- The total number of outdials and breakout sessions permitted at any time is N/6, where “N” is equal to the maximum number of access ports on your system.

## Importing User Profile and Group Information

If the information required for user profiles or user groups already exists in another database (such as an e-mail directory, a voice-mail directory, or a human resources database), you can import the profile information directly into the Cisco Unified MeetingPlace database. There are two ways of importing information:

- Use Cisco Unified MeetingPlace Directory Services (see the [“Importing with Cisco Unified MeetingPlace Directory Services”](#) section on page 2-16).
- Manual file import (see the [“Importing with Manual File Import”](#) section on page 2-17).

Although creating a process for importing the initial database and keeping it current requires planning, doing so saves you time overall. Rather than worrying about accepting impromptu requests, you can manage the process by anticipating any circumstances that may occur.

For best results when doing any imports into Cisco Unified MeetingPlace Audio Server, remember the following information:

- To ensure the import process does not fail because of missing information, define your user groups before you import profiles.
- Plan the import for when network activity and Cisco Unified MeetingPlace use are both at an absolute minimum. The import process needs exclusive Cisco Unified MeetingPlace Audio Server system rights to ensure that packet timing happens in a predictable manner.
- If the import process is unsuccessful, the Import Status dialog box shows the last record that was processed. In this case, restart MeetingTime, edit the import file to remove the meetings that successfully loaded, and continue importing the remaining meetings.

## Importing Profiles for All Users

Cisco Unified MeetingPlace provides automated tools for synchronizing its list of profile users with other user lists in your company, such as e-mail directories, voice-mail directories, and human resources databases.

Although creating a process for importing the initial database and keeping it current requires planning, this approach saves you time. Rather than worrying about accepting impromptu requests, you can manage the process by anticipating any circumstances before they occur.

Alternatively, you can use Cisco Unified MeetingPlace Directory Services to automatically synchronize information in your corporate directory server with information in your Cisco Unified MeetingPlace server. For more information, see the [“Importing with Cisco Unified MeetingPlace Directory Services”](#) section on page 2-16.

## Importing with Cisco Unified MeetingPlace Directory Services

Using a directory service, a company can store all its resources and personnel information in one place and allow other applications to access that information from a single source. Doing so decreases the cost of managing information, increases control and consistency of information, and unifies security across applications.

Cisco Unified MeetingPlace Directory Services (a Cisco Unified MeetingPlace software option) synchronizes information in your corporate directory server with information in your Cisco Unified MeetingPlace server. It interacts with common corporate directories such as Microsoft Active Directory and Netscape Directory Server through Lightweight Data Access Protocol (LDAP).



When new employees join the company, their information is entered into the corporate directory. Cisco Unified MeetingPlace Directory Services detects the addition and instantly creates a profile for each new employee.

As employees change departments and offices, their contact information changes. To ensure that the system has the most accurate information, changes to a user information on the corporate directory are recognized and replicated on Cisco Unified MeetingPlace Directory Services. Automatic profile updates ease system use and limit help desk calls.

For more information about Cisco Unified MeetingPlace Directory Services, see the description in the *Installation Planning Guide for Cisco Unified MeetingPlace*, at [http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html). For more information about using this product, see the *Administration Guide for Cisco Unified MeetingPlace Directory Services*, at [http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html).

## Importing with Manual File Import

If you do not have Cisco Unified MeetingPlace Directory Services installed, you must complete a manual file import. To simplify this process, you can choose to import only fields that contain profile or group-specific information, such as user IDs, profile numbers, group names, group numbers, and contact information (e-mail addresses, phone numbers, and so on). Any fields you do not include in the import file derive their value from either the guest profile or the user group to which the user has been assigned.

If you are not assigning users to groups, review the settings in the guest profile to make sure they are appropriate for the users you are adding to the system. For example, if you want users to outdial from meetings but the guest profile has the Can Call Out from Mtgs attribute set to *No*, you must change this setting in the guest profile before importing your profiles. After the profiles are imported, you must change the settings in the guest profile back to their original values.

If you are assigning users to groups, be sure to include the Group Name or Group Number field in the import file.

The import file *must* include unique values for the profile number and user ID. If used, the group name and group number values must also be unique.

You can use any value as the user ID and profile number as long as it is unique. For example, if you are importing the data from your voice-mail system, you can use the user phone number as his or her profile number. If you are getting the information from an e-mail system database, you can use the e-mail user ID as the Cisco Unified MeetingPlace user ID.

For more information about file import, see [Appendix B, “File Import Specifications.”](#)

## Import File Requirements

The import file must be a comma-delimited ASCII file (an unformatted or flat file). The first line of the file is a group of keywords that acts as a header and identifies the order in which data appears in all subsequent lines.

For example, if each line of information starts with the first name of the user and then lists the first name, last name, user ID, profile number, phone number, contact user ID, group name, and time zone code, it would look like this:

```
fnm, lnm, uid, prfnum, phnum, ctuid, grpnm, tzcode  
Alex, Bell, Bell, 206, 5551234, Patton, system, 87  
Lee, Smith, Smith, 202, 5556789, Patton, system, 87
```

Before you create an import file, remember the following information:

- Any spaces placed at the beginning or end of a value are deleted during the import process unless the value and the leading or ending spaces are enclosed in double quotation marks (“ ”). Spaces within a value, for example in Tech Support for a billing code, are imported without being deleted.
- Any commas used in a value must be enclosed in double quotation marks, such as using “Yuen,Chris” for a user ID.
- All text types are case insensitive.

## Importing Files in the Cisco Unified MeetingPlace Database



### Caution

Before you import user or group profiles, be sure to define user groups.

### To Import Files in the Cisco Unified MeetingPlace Database

- 
- Step 1** Create the import file, and make sure the following are true:
- The import file contains the first name, last name, user ID, profile number, group name or number, and specific address information (phone number, Internet e-mail address, e-mail address, and pager number) for each user.
  - For group profiles, the import file contains the group name and group number.
- Step 2** In the MeetingTime System tab, set the following attributes:
- For Actions, select **Import User Profiles** or **Import Group Profiles**.
  - For Action to Perform, choose either **Add Profiles to System** or **Add Groups to System**.
  - For Data File to Use, click in the Values area. In the dialog box that displays, enter the name of the import file (the file to import into), or click **Browse** to locate the file. Then click **OK**.
  - For Overwrite Duplicate Info, choose an option.
 

In general, performance is better when this attribute is set to No. Also, you avoid writing over any changes that users have made to their profiles. To reset the system back to a particular state, you can set this attribute to Yes.
  - For Log File Name, enter a destination for error information.
 

If you are importing a large number of records, enter a filename to log the error to.
  - For Error Threshold, enter a value.
 

This value determines the number of errors that MeetingTime allows before aborting the import process. Do not set this number too high because a large number of errors indicates a problem with the import file.
- Step 3** Click **Execute**.
- A status dialog box reports any error conditions that occur during importing.
-

## Automating the Import Process

When importing is automated, you can publish the Cisco Unified MeetingPlace login schema through your intranet to greatly reduce your involvement in database management.

If Cisco Unified MeetingPlace Directory Services is not installed, you can simplify maintaining your Cisco Unified MeetingPlace database by writing a script that uses the Windows Batch Mode (see the [“Importing and Deleting Profiles in Windows Batch Mode”](#) section on page 2-19). Automating the import process deactivates employees who have left your company and adds new employees.

### To Write a Script to Automate Importing

---

- Step 1** Export your source database (for example, NT or Human Resources) to a LAN drive.
- Step 2** Compare the database to your last export.
- Step 3** Create two files (one for additions and one for deactivations).
- Step 4** Put the files into the proper import format.  
For more information, see the [“Import File Requirements”](#) section on page 2-17.
- Step 5** Run the two imports into Cisco Unified MeetingPlace (one to deactivate former users and one to add new users).
- 

## Importing and Deleting Profiles in Windows Batch Mode

Importing or deleting profiles in batch mode lets you perform the process overnight and avoid tying up your machine (importing takes about one second per profile). You can perform all the import operations in batch mode using command line options.

**Caution**

The batch import process overwrites duplicate profile information in the system.

---

### To Generate an Import in Batch Mode

---

- Step 1** Create the import file.  
Make sure the import file contains the first name, last name, user ID, profile number, group name or number, and specific address information (phone number, Internet e-mail address, e-mail address, and pager number) of the user.
- Step 2** Run MeetingTime by using a command line option described in [Table 2-10](#).  
Remember the following information:
- Enter all parameters, including import filename, as one line. Do not press Enter until after you enter the import filename.
  - Begin the command line string with this syntax (unless this information is stored in the MeetingTime settings):

```
C:\Program Files\Latitude\Mtgtime\mtgtime.exe  
[user ID] [user password] [hostname]
```

(For information on storing login settings, see the “Editing and Storing MeetingTime Settings” section on page A-2.)

- Step 3** To enter a command line from Windows 98 or Windows 2000, choose **Start** menu > **Run**, enter the command line, and click **OK**.

If you plan to run the batch import process frequently, you can create a shortcut for quick access to the file without having to remember the import string each time.

**Table 2-10** Command Line Options

Import Option	Sample Import String
Adding Profiles	ImportProfiles [Data file to use] [Add/Delete] For example: <code>importProfiles impfile.csv yes</code> <b>Note</b> If the batch file import string does not specify the action of adding (yes) or deleting (no), the system defaults to <i>yes</i> .
Adding Groups	ImportGroups [Data file to use] [Add/Delete] For example: <code>importGroups impfile.csv yes</code>
Adding Profiles with error file and threshold defined	ImportProfiles [Data file to use] [Add/Delete] For example: <code>importProfiles impfile.csv yes logfile.txt 50</code> <b>Note</b> If the batch file import string does not specify the log filename, the system creates a file named <i>loginfo.txt</i> .
Deleting Profiles	ImportProfiles [Data file to use] [Add/Delete] For example: <code>importProfiles impfile.csv no</code> <b>Note</b> If the batch file import string does not specify the error threshold number, the system defaults to 50.
Deleting Profiles with error file and threshold defined	ImportProfiles [Data file to use] [Add/Delete] [Log filename] [Error threshold] For example: <code>importProfiles impfile.csv no logfile.txt 50</code>

## Unlocking a Profile

Because more than one user may have tried unsuccessfully to log in, more than one user profile might be locked.

### To Review a List of Locked Profiles

- Step 1** In the MeetingTime System tab, for **Actions**, select **View Locked Profiles**.

In the Locked Profiles dialog box, you see the user ID, the active state of the profile, the group default value of the User Active? field, and the state that the profile will be set to.

**Step 2** Select the profile(s), and then unlock and reset them by clicking one of the following buttons.

To Update the User Active? Profile Field To	Click
Active (Yes), enabling the locked profile	<b>Set Active</b>
Inactive (No), disabling the locked profile	<b>Set Inactive</b>
The value specified in the group assigned to the user	<b>Set to Group</b>

**Step 3** Click **OK**.



**Note**

To remove a profile from the list without reactivating it, click the **Set Inactive** button in the Locked Profiles dialog box. For example, use this button when you need to research the security status of the user within your organization or to prevent a user from using the system until after training.

If the Lock/Unlock Profiles Help Desk privilege has been enabled, you can also view locked profiles by clicking the **View Locked Profiles** button in the Preference tab. Attendants and users with higher privileges can see this button when this Help Desk privilege has been enabled.

## Changing User Profile Records

You can also use the Import Profiles action to change a user ID or profile number.

### To Change a User Profile Record

- Step 1** Create an import file with a minimum of four fields: uid (user ID) and prfnum (profile number). These fields are used to find the existing user record.
- Step 2** Edit the import file by adding two new fields: newuid and newprfnum.
- Step 3** Under these fields, specify the new user IDs and profile numbers.
- Step 4** For users whose information does not change, copy the values from the original user ID and profile number fields.

For example, importing the file displayed in the following example changes Pat Park's user ID to Bell\_newID and changes the profile number to 20611. It also changes Chris Lee's user ID to Lee\_Mgr but maintains the previous profile number. Alex Leeman's user ID and profile number remains the same.

```
fnm,lnm,uid,prfnum,newuid,newprfnum
Pat,Park,Park,206,Park_newID,20611
Chris,Lee,Lee,202,Lee_Mgr,202
Alex,Leeman,Leeman,204,Leeman,204
```

For information about removing profiles from the system, see the [“To Change User Profile Information Manually”](#) section on page 5-36.

## Viewing User Group and User Profile Records

You can quickly view a particular user group or user profile record. In the MeetingTime Configure tab, click the **Find Records** (magnifying glass) button.

To	Do This
See all defined user groups	In the Views list, click <b>User Groups</b> , then click the <b>Find Records</b> button. You see a list of all defined groups.
Search user profile records	In the Views list, click <b>User Profiles</b> , then click the <b>Find Records</b> button. In the dialog box that displays, choose an option for what to search on (the search criteria). Or, for <b>Begins With</b> , enter the characters that the search criteria begins with. Then click <b>OK</b> .

## About Teams

Authorized Cisco Unified MeetingPlace users can create and modify teams (lists of Cisco Unified MeetingPlace users), which all users can use when scheduling meetings or outdialing from a meeting. System administrators can limit the number of teams an authorized user can create.

### To Define Teams

- 
- Step 1** Open MeetingTime, click the Register Book, and select the **Teams** tab.
- Currently defined teams display in the Names list. Clicking a team in this list displays the properties of that team in the Team Information area.
- Step 2** Add, change or delete teams, as follows.

To	Do This
Add a team	Click the <b>New</b> button. Enter information about that team for Team Information, then click <b>Save</b> .  <b>Note</b> You can include up to 200 members in each team.
Change a team	Click the team to change. Change settings for Team Information, then click <b>Save</b> .
Include or change details about the team	With the team information displayed, click <b>Details</b> . You can add or change the team description, the ID of the person who last modified the team, or the date and time the team was modified.
Delete a team	Click the team to delete, and click the <b>Delete</b> button.
Search for teams in the database	Click the <b>Find Teams</b> button (the magnifying glass above the Names list), enter search information in the Directory window, then click <b>OK</b> .  The system searches for teams by name or number. If the Name or Number field is blank, all teams are found and displayed. Clicking the <b>Add</b> button also displays the Directory window.

For details about team attributes, see the [“Properties of Teams” section on page 2-23](#).

---

## Properties of Teams

Table 2-11 describes team properties.



**Caution**

All teams are public because users can see and use them for inviting or outdialing purposes.

**Table 2-11** Properties of Teams

Property	Description
Name	The name of the team. Each name must be unique. This is a required entry.
Number	A numeric identifier of the team, used to access teams from a touch-tone phone. Each number must be unique. This value is required.
Owner	The name of the team owner or creator. This is a read-only field.
Editable by Others?	Whether information about this team can be modified by others. By default, teams are non-editable.
Members	Displays a list of all team members.
Description (from the <b>Details</b> button)	A description of the team. You can enter up to 127 characters in this description field.
Last Modified (from the <b>Details</b> button)	For shared teams, this field displays the user ID of the person who last modified the team. For non-shared teams, this field always displays the team creator.
Last Modified (from the <b>Details</b> button)	For shared teams, this field displays the date and time of the last modification. For non-shared teams, this field always displays the date and time when the team was created.

## About Searching for Users, Groups, and Teams

You can search for and locate Cisco Unified MeetingPlace users in the users, groups, and teams databases. You search for information in the Directory window. This window displays when you:

- Invite profile users to a meeting
- Add members to teams
- Search profiles to do managed outdial

Use Table 2-12 for searching user and group profiles and teams.

**Table 2-12** Search Methods for Users, Groups, and Teams

To	In the Directory Window, Do This
Find a profile or team	For Search for Profiles, enter text or a number, then click the binoculars button. For details about each option, see the “ <a href="#">Search Options</a> ” section on page 2-24.
Add a profile or team	Double-click the profile or team name in Found. (Or click the profile or team name and click <b>Add</b> .) The profile or team name moves to Selection. Then click <b>OK</b> .
Remove a profile or team	Click the profile or team name and click <b>Remove</b> . Then click <b>OK</b> .
Change the database you want to search	Click <b>Options</b> , then click the binoculars button. The search results are displayed in Found. (Each new search results clears the previous result in this list.)

Remember the following information:

- You must enter the entire value that you are searching for. Partial search criteria can return unexpected results.
- Search criteria is case sensitive.
- To run reports that include this profile, deactivate this profile until all reports have been run for the time period that the profile was active. For information on deactivating profiles, see the [“About Maintaining Configuration Records”](#) section on page 5-36.

## Search Options

By default, profiles are searched according to the nature of the search string. So, for example, if the search string is a number, it searches for profiles where the criteria *profile number* matches the search number, as well as teams where the team number matches the search number. If the search string is text, it searches for profiles where the criteria *user ID* matches the text, as well as teams where *name* matches the search text.

### To Change Search Options

**Step 1** In the Directory window, click the **Options** button.

[Table 2-13](#) describes each search option.

**Table 2-13** Changing Search Options

Choose	To Search For
Using Smart Search	All profile entries (everything) according to the nature of the search string that is entered in Search For (this is the default option)
By User ID	Profiles that begin with the search text string that is entered in Search For
By Last Name	Profiles that begin with the search text string that is entered in Search For
By Profile Number	Profiles where the profile number matches the search string that is entered in Search For
By Group Name	All profiles in a group where the name matches the search string that is entered in Search For
By Team	All the profiles in teams where the team name or number matches the search string that is entered in Search For

## About Establishing Security

The security of your Cisco Unified MeetingPlace system includes physical security, software security, and toll-fraud prevention. Your company may already have guidelines for protecting the security of its computer systems.



## Securing the Location

Securing the location of your system prevents unauthorized access to the system technician console port.


**Caution**

Keep the system in an area protected by a lock or a card-key system.

## Securing User Profiles

To prevent unauthorized users from accessing Cisco Unified MeetingPlace over the phone or from a computer, use the security measures described in [Table 2-14](#).

**Table 2-14**      **Methods for Securing User Profiles**

Action	Description
Use password protection	<p>Cisco Unified MeetingPlace requires passwords for access from a phone or computer. User passwords permit access from a computer, and profile passwords permit access over a phone.</p> <p>To ensure effective use of profile passwords, administer the minimum password length and password change parameters in the Configure tab to define password information, including the following:</p> <ul style="list-style-type: none"> <li>• Min profile pwd length (minimum profile password length for phone access)</li> <li>• Change profile pwd (how often users must change their profile passwords)</li> <li>• Min user pwd length (minimum workstation access password length)</li> <li>• Change user pwd (how often users must change their workstation access passwords)</li> <li>• Min meeting pwd length (minimum length for a meeting password)</li> </ul> <p><b>Note</b> We recommend that you require users to change passwords according to your company's policies for similar systems.</p>

Table 2-14 Methods for Securing User Profiles (continued)

Action	Description
Use hacker lockout	<p>Cisco Unified MeetingPlace offers a “hacker lockout” feature, which deactivates any user profile after a number of consecutive unsuccessful login attempts. You define the number of attempts. To do so:</p> <ol style="list-style-type: none"> <li>1. In the MeetingTime Configure tab, select the <b>Usage Parameters</b> topic.</li> <li>2. Enter the maximum number of attempts to access the user profiles.</li> </ol> <p>After users reach the maximum number of retries by phone, the profile is locked. Further attempts to log in result in a “Profile is invalid” message, the caller is transferred to the attendant, and a minor alarm is generated.</p> <p>To unlock a user profile:</p> <ol style="list-style-type: none"> <li>1. In the MeetingPlace System tab, select the <b>View Locked Profiles</b> action.</li> <li>2. Change the User Active? setting in the profile to <b>Yes</b>. (Until you do, this profile cannot be used.) For more information on resetting locked profiles, see the <a href="#">“Problem: User Cannot Log In”</a> section on page 6-20.</li> </ol> <p>Users who exceed the limit of password attempts by computer in MeetingTime are exited from the application. Users can then double-click the MeetingTime icon and try again. (Security is less stringent from the computer than from the phone because outdialing is not an issue.)</p> <p><b>Note</b> This feature can expose the server to a denial of service attack: a hacker simply goes through the list of profiles and locks them all by entering bad passwords, which renders the system unusable until the system administrator unlocks the accounts. Hackers can (and will) avoid the lockout by trying different profile numbers with the same commonly used password rather than the other way around. Consequently, many secure installations do not employ this feature. Cisco recommends that you weigh the costs of possibly making it easier for a hacker to break into an account versus the costs of managing locked accounts and running the risk of critical accounts being locked in an emergency.</p>
Keep the database current	<p>You can also ensure user profile security by maintaining an up-to-date user database. For example, delete or deactivate user profiles of employees who leave the company. For details on removing profiles from the system, see the <a href="#">“About Maintaining the User Database”</a> section on page 5-32.</p>
Use Cisco Unified MeetingPlace SNMP agent	<p>The Cisco Unified MeetingPlace Simple Network Management Protocol (SNMP) agent comes preconfigured with communities labeled MeetingPlace-public and MeetingPlace-private. To prevent unauthorized queries, Cisco recommends changing these community names to names chosen by the customer. For details on changing community names, see the <a href="#">“Setting Up Community Information”</a> section on page D-3.</p> <p>The Cisco Unified MeetingPlace SNMP agent is based on SNMPv1 code, which has security vulnerabilities known to hackers. Cisco recommends blocking the SNMP port using a firewall. If the Cisco Unified MeetingPlace Audio Server is located on the network so that a firewall cannot protect the SNMP port, we recommend disabling SNMP queries. This can be done without disabling trap generation.</p>

## Securing Meetings

All meetings are protected by meeting ID numbers. For each scheduled meeting, you can determine whether the meeting requires both a password and a meeting ID.

If you do not want end users to see listings for meetings to which they have not been invited, the Display Meeting to Everyone? attribute must be set to No when scheduling a meeting. If this attribute is set to Yes, any profile user can view information about this meeting from the Browse Meetings link in Cisco Unified MeetingPlace Web Conferencing and from the MeetingTime interface.

Table 2-15 describes ways to secure meetings.

**Table 2-15**      **Methods for Securing Meetings**

Action	Description
Use meeting passwords	Meeting passwords provide an additional level of security to the meeting. By using the Usage Parameters topic in the Configure tab, you can define the minimum length for a meeting password (Min meeting pwd length).
Restrict meeting attendance	The Who Can Attend attribute allows meeting schedulers to restrict meeting attendance to those users with Cisco Unified MeetingPlace profiles or to profile users who are explicitly invited to meetings. Restricting meeting attendance prevents guest users from joining the meeting.
Secure meetings in session	During a meeting, users can access the in-session meeting features and use the following admittance options to control who can enter the meeting: <ul style="list-style-type: none"> <li>• #21 takes roll call of current participants</li> <li>• #41 locks meeting to prevent additional parties from joining the meeting without permission</li> <li>• #42 admits unannounced participant to meeting</li> <li>• #43 drops last participant who enters the meeting</li> </ul>
Restrict access to meeting records	You can restrict users from recording meetings from the User Profile and User Groups topics in the Configure tab. When scheduling meetings you can determine whether access to recordings of certain meetings are restricted to specific users or require a password.
Restrict use of vanity meeting IDs	When users schedule meetings, by default they can assign <i>vanity</i> (custom or common) meeting IDs, such as 1234. Although vanity meeting IDs are easier for meeting participants to remember and identify, you may want to restrict their use. Doing so adds a level of security and prevents unauthorized users or hackers from easily guessing the ID and gaining access to the meeting. <p>To restrict vanity IDs:</p> <ol style="list-style-type: none"> <li>1. In the Configure tab, select <b>System Parameters</b>.</li> <li>2. For the <b>Allow Vanity Mtg IDs</b> field, choose <b>No</b>. The system assigns a unique, randomly generated ID (which users cannot change) to every meeting scheduled from then on. <p>When users are allowed to assign vanity IDs, you can add a level of security by restricting groups or individual users from assigning vanity IDs to meetings that are scheduled by phone. To do so:</p> </li> <li>3. In the Configure tab, select <b>User Groups or User Profiles</b>.</li> <li>4. For the Can Chg Mtg ID Via Phone field, choose <b>No</b>. User profiles inherit the group setting, but system administrators can change the setting for individual users.</li> </ol> <p><b>Note</b> To protect meeting IDs that can be hacked easily (such as 1234 or ABCD), create zero-port continuous meetings and assign those meeting IDs. Limit those meetings to invitees only, and do not invite other people. (For more information about continuous meetings, see the <a href="#">“About Continuous Meetings”</a> section on page 3-3.)</p>

## Preventing Toll Fraud

Although recent court decisions and Federal Communications Commission (FCC) regulations stipulate that toll fraud is the customer's responsibility and not the responsibility of the equipment vendors, Cisco Unified MeetingPlace provides several ways to prevent unauthorized use. Because Cisco Unified MeetingPlace is a powerful telecommunications system allowing calls in and out, it is important to take measures to prevent unauthorized access to your system, as shown in [Table 2-16](#).

**Table 2-16**      *Methods for Preventing Toll Fraud*

Action	Description
Restrict outdialing privileges	<p>The first level of protection against toll fraud is the user profile, which determines a user's outdial privileges and whether they can schedule meetings that allow guests to attend over the Web.</p> <p>You can restrict outdialing privileges to specific user groups, such as sales and marketing, or to specific user profiles, such as Jones and Smith. In the most extreme case, you can choose to disable impromptu outdialing for all users, virtually eliminating the potential for toll fraud.</p> <p>To ensure that only registered users can outdial from within meetings:</p> <ol style="list-style-type: none"> <li>1. In the Configure tab, select the <b>User Profiles</b> topic.</li> <li>2. For the Can Call Out From Mtgs? attribute, make sure it is set to <i>No</i> in the guest profile.</li> <li>3. Repeat steps 1 and 2 for the <b>User Groups</b> topic.</li> <li>4. To restrict the number of outdials a particular user or guest can make from within each meeting (by pressing #3), set the Max Outdials Per Mtg attribute to a low number.</li> </ol> <p>In addition, if you do not want the system to outdial to guests when they click the <b>Join Voice Conference</b> button from the Web, make sure the Can Allow Guest Outdial in Mtgs attribute is set to <i>No</i> in all user profiles. For more information on this attribute, see the <a href="#">“About User Profiles”</a> section on page 2-14.</p> <p><b>Note</b>    Setting the user profile attribute Can Call Out From Meetings to <i>No</i> does not prevent the user from scheduling a meeting with the Outdial Invitees on First Call attribute set to <i>Yes</i>.</p>
Limit near-term meetings	<p>You can limit the number of near-term meetings (meetings scheduled to occur within six hours of the scheduling time) by setting the near-term limit for the User Groups and User Profiles topics.</p>
Define system-wide restrictions	<p>The next level of security consists of the system outdialing translation tables. The translation tables define which phone numbers the Cisco Unified MeetingPlace system can call. You can configure the system with up to 16 different tables to provide unique capabilities for different user communities on the system. You can also define tables through a PBX.</p> <p>Remember the following information:</p> <ul style="list-style-type: none"> <li>• Be specific about who can and cannot outdial. In the Port Groups and Ports topics in the Configure tab, you can set which ports can handle outgoing calls. You can also set users' outdial privileges in their individual user profiles, or restrict the number of outdials users can make during a meeting.</li> <li>• Define an internal dialing table to restrict specific long distance calls. A Cisco Network Consulting Engineer (NCE) can assist you in setting up a dialing table.</li> <li>• Through a PBX, use blocking tables to block outdial to certain area codes.</li> <li>• Check with your long distance vendor to monitor the use of outgoing lines for unusual outgoing calls.</li> </ul>

**Table 2-16**      *Methods for Preventing Toll Fraud (continued)*

Action	Description
Monitor usage through reports	<p>You can easily review outdialing usage to look for toll fraud patterns. Cisco Unified MeetingPlace provides both a standard outbound dialing report and the capability to export raw data to third party software programs.</p> <p>Use the MeetingTime Outbound Dialing Report, Port Usage Report, Raw Meeting Outdial Information (Users) Report, or Raw System Outdial Report to monitor unusual inbound and outbound activity on a trunk. For descriptions and examples of these reports, see <a href="#">Chapter 4, “Running Reports.”</a></p>

## About Customizing Cisco Unified MeetingPlace Audio Server

While the Audio Server system is completely functional as installed, you can customize the system to suit your special uses and applications. The following sections tell you how to:

- Customize meeting notifications
- Create flex fields
- Choose abbreviated or unabbreviated voice prompts
- Customize the voice prompts that users hear

### Customizing Meeting Notifications

To assist users receiving notifications by e-mail, you can customize your company e-mail messages with information on how to attend meetings on Cisco Unified MeetingPlace and listen to recorded meetings.

#### To Customize Meeting Notifications

- 
- Step 1** In the MeetingTime Configure tab, select the **Company Information** topic, then click **Query**. This topic is located under the Company Specific Information heading in **Views**.
- Step 2** When the values for the various attributes are displayed, scroll down until you see the How to Attend a Meeting and How to Access MeetingNotes attributes.
- Step 3** Click the value area of these fields and enter the message you want to appear in your users' notifications. [Table 2-17](#) show examples of messages to use for the custom notification fields.

**Table 2-17 Meeting Notification Parameters**

Parameter	Examples
How to attend a meeting	“Welcome to <Your company’s name> MeetingPlace conference server. To attend voice conferences on the system, dial the MeetingPlace phone number and follow the voice prompts.”
How to access MeetingNotes	<p>“Users can record meetings, leave voice comments about a meeting, or attach relevant meeting materials. To access this feature, dial the MeetingPlace phone number and select option 3.”</p> <p>If your system uses DID/DDI access for attending meetings and listening to meeting recordings, be sure to provide the appropriate phone access number for each custom notification text field.</p>

## Listing Alternative Cisco Unified MeetingPlace Phone Numbers in Notifications

As a system administrator, you can identify up to three different phone numbers for accessing a Cisco Unified MeetingPlace conference server. For example, specify these phone numbers:

- A toll-free (1-800) number for participants outside of the area
- A local phone number for field staff or local participants
- An extension number for participants to use when calling from within the company

### To Enter Alternative Phone Numbers

- 
- Step 1** Log in to MeetingTime.
- Step 2** In the MeetingTime Configure tab, select the **Telephony Access** topic and click **Query**.
- Step 3** Set the following attributes:
- For the 1st Alternate Ph Number attribute, enter the alternative phone number.
  - For the Label for Notifications attribute, enter a label for the phone number. For example, Toll-Free Number or Extension Number.
- Step 4** If your Cisco Unified MeetingPlace system has a second or third alternative phone number, repeat [Step 2](#) and [Step 3](#), using the 2nd Alternate Ph Number and 3rd Alternative Ph Number attributes.
- Step 5** Click **Save Changes**.
- 

## About Flex Fields

By using flex fields, you can customize profile or meeting fields with your business information. The information specified in flex fields is used for reports.

You can create seven profile and seven meeting flex fields on your system. As the system administrator, you specify the protection level of each field (editable, read-only, or invisible to users). For flex fields 4–7, you can also choose whether users must choose fields values from a list of possible entries (which you create), and whether a flex field requires a value.

Table 2-18 shows examples of profile and meeting flex fields you may want to use for your company.

**Table 2-18 Flex Field Examples**

Profile Flex Fields	Meeting Flex Fields
Cost Center	Conference Room
Billing Exemption	Building Number
Hire Date	Instructor Name
Department Name	Project Name

When you define a flex field, you specify the field title and import title information. The required information for a flex field can be of several different types—text, number, date, or yes/no.

Remember the following information:

- The first seven flex fields are for profile use, and the last seven flex fields are for meeting use.
- Flex fields 4–7 are available in MeetingTime Release 5.1 and later. Earlier versions do not display these fields in the user, group, and meeting records.
- Flex field values are always visible to system administrators in the Configure Profiles and Groups windows.

### To Define Flex Fields

**Step 1** In the Configure tab, select the **Flex Fields** view, then click **Query**.

**Step 2** Assign attributes to the field (see the following table), then click **OK**.

Use Table 2-19 when you assign attributes to a flex field. Your settings display as field attributes and values in the Configure tab.

**Table 2-19 Flex Field Attributes**

Attribute	Description
Active?	Whether the flex field is active. When this attribute is <i>Yes</i> , the flex field is displayed and users can enter a value for it through MeetingTime and Cisco Unified MeetingPlace Web Conferencing.
Title	The name that displays for the flex field in MeetingTime and Cisco Unified MeetingPlace Web Conferencing.
Type	The type of information the flex field contains: Text, Number, Yes/No, or Date.
Import Title	The field title used when importing raw profile report information containing flex field data.

Table 2-19 Flex Field Attributes (continued)

Attribute	Description
Protection Level	<p>The access that end users have to the flex field—invisible, read-only, or editable. Protection levels are useful for flex fields with attributes you do not want users to override (such as billing codes).</p> <p>When this attribute is Invisible, end users cannot see the flex field. When the attribute is Read-only, end users can see, but not edit, the flex field. When the attribute is Editable, end users can see and edit the flex field.</p> <p>Active and visible flex fields are displayed to end users in the scheduling and profile management sections of MeetingTime and Cisco Unified MeetingPlace Web Conferencing.</p>
Uses data from profile?	Whether the default value for the flex field is taken from the user profile.
Use defined choices (for flex fields 4–7 only)	<p>Whether users must choose from a list of predefined values (which you create) to enter in the flex field, or enter an unrestricted value.</p> <p>When this attribute is Yes (the default), users see the list of predefined values in the Schedule and Review tabs. To define values, see the description for the next attribute, User Choice Strings.</p>
User choice strings (for flex fields 4–7 only)	<p>Use to define a list of predefined values when Use Defined Choices is Yes. (When Use Defined Choices is No, no list displays.)</p> <p>To define the values (when When Use Defined Choices is Yes), select User Choice Strings. Then click Add, enter the first value (up to 23 characters) and click OK. Repeat for each value you want in the list. (The combined length of all values cannot exceed 299 characters. Do not include commas in values.) Click OK to save all the values.</p>
Required field? (for flex fields 4–7 only)	<p>Whether the flex field requires a value when users schedule or change a meeting (in the Schedule tab). The default is No. When this attribute is Yes and users try to save a record that includes an empty required field, they see an error message.</p> <p>A flex field in a user profile that inherits the default value from the group profile flex field satisfies the requirement to contain a value.</p>

## About Flex Menus

You can customize the top-level touchtone menu trees that callers use to access their meetings by using Flex Menu applications.

Flex Menu applications provide quick access to do any of the following:

- Join meetings
- Listen to recordings
- Access one or all voice comments
- Access one or all attachments

You can also incorporate standard Cisco Unified MeetingPlace menu trees into your Flex Menu applications, such as the standard attend, schedule, and MeetingNotes branches.

For example, you could define a Flex Menu application to play the following top-level prompts:

- Welcome to Cisco Unified MeetingPlace.



- To attend today's brokerage call, press 1.
- To listen to the recording of yesterday's brokerage call, press 2.
- To review analyst meetings, press 3.
- For other options, press 4.

**Note**

---

The Welcome to Cisco Unified MeetingPlace prompt cannot be changed. If you want to customize this prompt, contact Cisco Unified MeetingPlace Customization Services.

---

Cisco Unified MeetingPlace can support multiple Flex Menu applications in a single system. You assign Flex Menu applications on a port group basis. As such, Cisco Unified MeetingPlace can play different menus to parties depending on the port group that users dial into.

## Accessing Flex Menus

You access Flex Menu features from the System tab in MeetingTime. From this tab, you can do the following:

- Design Flex Menu applications
- Load Flex Menu applications into the phone interface of the Cisco Unified MeetingPlace Audio Server
- Delete Flex Menu applications from the Cisco Unified MeetingPlace Audio Server
- Import Flex Menu applications created elsewhere

## Creating Flex Menus

Creating Flex Menus consists of the following steps:

- Designing a Flex Menu application
- Saving the application
- Completing the application
- Loading the application

### To Design a Flex Menu Application

- 
- Step 1** From the list of Actions in the MeetingTime System tab, choose **Manage Flex Menus**.
- Step 2** In the Attributes list, choose the Flex Menu to use. For a new Flex Menu, choose **New Flex Menu**.
- Step 3** In the Attributes list, choose the Action to perform. For this field, select **Design**.
- Step 4** Click **Execute**.
- 

Flex Menus requires three basic elements:

- Custom Flex Menu prompts
- Programming controls (macros)

- Specifications for past, present, or future meetings that are to be held based on meeting ID or meeting category

#### To Define a Custom Flex Menu Prompt

Custom Flex Menu prompts are voice prompts not normally part of the Cisco Unified MeetingPlace system. In the previous example, the prompt “To attend today’s brokerage call” would be a custom Flex Menu prompt played to the users.

You can create custom flex menu prompts while you are designing Flex Menus.

- 
- Step 1** From the Flex Menu Designer window, click **Prompts**.
- Step 2** In the Prompts window, click **New**.
- Step 3** To name the prompt, click **Edit** and enter the name. The new name appears in the Custom Prompts window.
- Step 4** Repeat [Step 2](#) and [Step 3](#) for all the prompts in your Flex Menu application.
- 

#### To Record a Custom Flex Menu Prompt

- 
- Step 1** By using your phone, dial into Cisco Unified MeetingPlace.
- Step 2** Press **2** to access your profile.
- Step 3** Enter the profile number and profile password for your system manager account.
- Step 4** From the profile main menu, press **9** then **2** to access custom Flex Menu prompts.
- Step 5** Enter the Flex Menu prompt number as shown in the Custom Prompts window in MeetingTime.
- Step 6** Follow the voice prompts to record the prompt.
- 

## Flex Menu Macros

Each Flex Menu application consists of a set of states. Each state consists of an action to perform, parameters specifying what to perform that action on, and “go to” instructions indicating what the next state should be under both normal and error conditions.

[Table 2-20](#) describes which actions or macro types are supported.

**Table 2-20 Macro Types Supported**

Macro Type	Description	Parameters
Play Prompt	Plays custom prompts	Prompt number
Go To Standard Application	Jumps to standard MeetingPlace menus	One of DID meeting, MeetingNotes, Profile Access, Combined Access, or Loop Through Transfer

**Table 2-20 Macro Types Supported (continued)**

Macro Type	Description	Parameters
Option	Plays a menu of up to 9 choices	For each choice, you specify: <ul style="list-style-type: none"> <li>• Touchtone key that selects the option</li> <li>• Prompt to describe this option</li> <li>• State to jump to if this option is selected</li> <li>• Whether option is currently available</li> </ul>
Hang up the call	Hangs up	None
Find meeting	Selects the meeting to attend or review	<ul style="list-style-type: none"> <li>• Choose whether to access current, past, or future meetings</li> <li>• Choose how meetings are defined (by ID or category)</li> <li>• Number of meetings to find</li> <li>• Presentation style of meetings</li> </ul>
Access MeetingNotes	Chooses which objects of selected meeting to review	<ul style="list-style-type: none"> <li>• Meeting recording</li> <li>• All voice comments</li> <li>• All attachments</li> <li>• Specific voice comment</li> <li>• Specific attachment</li> </ul>
Get Profile	Request that user enter valid profile number and password	State to jump to if successful and state to jump to on the following error conditions: <ul style="list-style-type: none"> <li>• No valid ID</li> <li>• Timeout</li> <li>• Too many attempts</li> <li>• Profile in use</li> <li>• User presses *</li> </ul>

**To Use a Flex Menu Macro**

- 
- Step 1** From the Flex Menu Designer window, click **New**. The New Macro screen appears.
- Step 2** Choose the Macro Type you want to use, and click **OK**. The macro appears in the structure panel of the Flex Menu Designer. The Structure panel is divided into columns, which contain parameters.
- Step 3** Click each parameter and fill in the appropriate pop-ups.
- Step 4** Repeat [Step 3](#) for all parameters. You will have to return to those parameters requiring you to enter states that you have not yet programmed, after you have completed those portions of your Flex Menu application.
-

## Finding Meetings

To access meetings to attend or review, you must first find the meetings. You can search for meetings based on their meeting ID or the meeting category.

## Meeting Categories

The Find Meeting macro can find a specific meeting or generate a list of meetings based on the meeting ID or meeting category over a fixed range of time.

In the example, To Review Analyst Meetings, press 3, you would first define a meeting category titled “Analyst Meetings” and assign each relevant meeting to that category.

System managers can define meeting categories in the Configure tab.

Users assign a predefined meeting category to a meeting when they schedule meetings.

## Presentation Styles

Cisco Unified MeetingPlace allows you to choose a single meeting or select from a set of meetings with the same meeting ID or meeting category. When Cisco Unified MeetingPlace generates a menu for the set of meetings, it can use one of several styles to present the list:

- Relative dates (“tomorrow”)
- Dates by name (“Monday”)
- Verbose (default)
- Verbose (without ID)

For example, if daily analyst meetings were held with a “by name” date presentation style, the menu might be:

- To review analyst meetings, press 3.
- For Tuesday’s meeting, press 1.
- For Wednesday’s meeting, press 2.
- For Thursday’s meeting press 3.

## Saving a Flex Menu Application

When you have finished designing a Flex Menu application, do the following procedure to save it.

### To Save a Flex Menu Application

- 
- Step 1** Enter a name for the Flex Menu application in the Name field of the Flex Menu Designer window.
  - Step 2** Enter the description for the Flex Menu application in the Description field.
  - Step 3** Click **Save**.
-

## Completing a Flex Menu Application

When you have saved a Flex Menu application, mark it as Complete in the Flex Menu Designer.

## Loading a Flex Menu Application

After a Flex Menu application has been marked as complete, load it into the Cisco Unified MeetingPlace system.

**Note**

Only those Flex Menu applications marked as complete can be loaded into Cisco Unified MeetingPlace.

---

**To Load a Flex Menu Application in to Cisco Unified MeetingPlace**

---

- Step 1** From the list of Actions in the MeetingTime System tab, choose **Manage Flex Menus**.
  - Step 2** In the Attributes list, choose the Flex Menu to use.
  - Step 3** In the Attributes list, choose the Action to perform. For this field, select **Load**.
  - Step 4** Click **Execute**.
- 

## Using a Flex Menu Application

To use a Flex Menu application, do the following procedure.

**To Use a Flex Menu Application**

---

- Step 1** From the list of Views in the MeetingTime Configure tab, choose **Port Groups**.
  - Step 2** Click the **Query** button to reveal selected values.
  - Step 3** In the Attributes list, choose **Default Access Type**.
  - Step 4** Click in the Values area of this field to select your newly defined Flex Menu Application and click **OK**.
- 

## Importing a Flex Menu Application

There are two reasons to import Flex Menu applications:

- To restore an older exported copy of a Flex Menu application to the same conference server.
- To copy an application exported from another conference server.

**To Import a Flex Menu Application**

---

- Step 1** From the list of Actions in the MeetingTime System tab, choose **Import Flex Menus**.
- Step 2** In the Attributes list, choose the file name of the import file.

- Step 3** In the Attributes list, indicate whether or not you want to create new voice prompt IDs. In general, you should create new voice prompt IDs if you are importing an application created on another conference server. If you are re-importing an application created on the same conference server, you should reuse the old voice prompt IDs.
- Step 4** Click **Execute**.
- 

## Exporting a Flex Menu Application

To use a Flex Menu application on another conference server, or to make a backup of a completed application, export the Flex Menu application to a text file by clicking **Export**.

## Deleting a Flex Menu Application

To delete a Flex Menu application from Cisco Unified MeetingPlace, do the following procedure.

### To Delete a Flex Menu Application

---

- Step 1** From the list of Actions in the MeetingTime System tab, choose **Manage Flex Menus**.
- Step 2** In the Attributes list, choose the Flex Menu to use. This will be the Flex Menu that you will be deleting.
- Step 3** In the Attributes list, choose the Action to perform. For this field, select **Delete**.
- Step 4** Click **Execute**.
- 

## About Customizing Voice Prompts

To customize the voice prompts that users hear, you can do the following:

- Choose abbreviated and unabbreviated voice prompts (see the [“Choosing Abbreviated and Unabbreviated Voice Prompts”](#) section on page 2-38).
- Customize voice prompts (see the [“Customizing Prompts”](#) section on page 2-39).

## Choosing Abbreviated and Unabbreviated Voice Prompts

Users can choose between hearing longer introductory prompts or shorter versions of the prompts while using the system. The prompts they hear depend on their Abbreviated Prompts profile setting. When Abbreviated Prompts is set to Yes, users hear shorter versions of the prompts. (Some standard unabbreviated prompts do not have corresponding abbreviated prompts.)

[Table 2-20](#) shows examples of how Cisco Unified MeetingPlace abbreviates prompts.

**Table 2-21** Voice Prompts

Unabbreviated Prompt	Abbreviated Prompt
“Enter the month for your meeting, followed by the pound key.”	“Enter month then pound.”
“Enter the length of your meeting in minutes, followed by the pound key.”	“Enter length, then pound.”
“Enter the starting time for the meeting in 12-hour format. When finished, press the pound key.”	“Enter starting time, then pound.”
“Enter the number of locations, including your location, followed by the pound key.”	“Enter number of locations, then pound.”
“Your meeting has been scheduled.”	“Meeting scheduled.”

To listen to the abbreviated and unabbreviated prompts, access the voice prompts menu and then choose the option for listening to these prompts (see the [“Accessing the Voice Prompts Menu”](#) section on page 2-39).

## Customizing Prompts

The Cisco Unified MeetingPlace touch-tone phone interface operates by playing a series of voice prompts and requesting touch-tone or spoken response from users. From a touch-tone phone, system administrators can customize all the prompts played. When you customize company identification and voice prompts, you must include the word “MeetingPlace” somewhere in the prompt.

Customize prompts for several reasons, including:

- **Music preferences.** You can change the music that the system plays while users wait for others to attend a conference or for the system to verify scheduling. (You do this by customizing prompts.) You can also replace the music with silence.
- **Change prompts.** You can change the prompts that users hear when they use specific features. For example, a prompt can remind people to dial internal network numbers rather than outside lines when outdialing to internal parties.

## Accessing the Voice Prompts Menu

You customize voice prompts by choosing from the voice prompts menu. As system administrator, you have access to the voice prompts menu from a touch-tone phone. End users, contacts, and attendants do not have access to this menu.

### To Access the Voice Prompts Menu

- 
- Step 1** Dial the Cisco Unified MeetingPlace phone number.
  - Step 2** Enter your profile number and password.  
After the standard functions, you hear the menu option: “For system manager options, press 9.”
  - Step 3** Press **9** for system manager options.
  - Step 4** Press **1** to access the voice prompts menu.

- Step 5** Enter the number for the voice prompt you want to change, then press #.  
For a partial list of voice prompts by number, see the table in the “Recording a New Prompt” section on page 2-40.
- Step 6** Do one of the following:

To	Press
Listen to the unabbreviated prompt	1
Listen to the abbreviated prompt	2
Listen to or record a custom prompt	3
Listen to or record a custom prompt for use with a Flex Menu application	4

## Recording a New Prompt

- Step 1** Access the Voice Prompts menu as described in the “To Access the Voice Prompts Menu” procedure on page 2-39.
- Step 2** Press 3, then press 2.
- Step 3** Record the new prompt, then press #.
- Step 4** Do one of the following:

To	Press
Keep the prompt	1
Record a new prompt	2
Delete the prompt and use the factory standard prompt	3

## Prompts That Can Be Changed

Although you can change any voice prompt in the system, limit the voice prompts you change to those that greet callers or that provide specific telephony access instructions. Changing any prompt related to system features can confuse users.

The following table describes the prompts you can change, including suggested wording. Use Table 2-22 to decide whether to change prompts.

**Table 2-22** Prompts That Can Be Changed

Prompt Number	Delivered Prompt	Suggested Change
155	“Thank you for calling.”	“Thank you for calling <your company name> MeetingPlace system.”



Table 2-22 Prompts That Can Be Changed (continued)

Prompt Number	Delivered Prompt	Suggested Change
303	Scheduling music	Your music, or silence to replace the music. (You must record a minute or more of music or silence.)
304	Meeting music	Your music, or silence to replace the music. (You must record a minute or more of music or silence.)
320	The system prompts you for the date, time, length of meeting, and number of locations in the meeting. The system confirms availability and issues a meeting ID.	Your explanation of scheduling future meetings.
394	“Make a note of the following meeting ID number. If you do not reach your party, you may choose to leave the meeting ID and MeetingPlace phone number with an assistant or in a voice-mail message.”	Your explanation of scheduling immediate meetings.
485	“Enter the phone number to be dialed. When finished, press the pound key.”	Your explanation of how to outdial from a meeting.
486	“The phone number is being dialed. After connecting with the party, you may add them to the meeting by pressing pound, then 1. To disconnect the party and return yourself to the meeting, press pound, then 2.”	Your explanation of how to add outdialed parties to a conference.

Remember the following information:

- You cannot back up custom voice prompts that you record. However, if you need such a backup to be performed, contact Cisco NCE for assistance.
- If you record a new voice prompt, it becomes a custom prompt and the original prompt is not erased. You do not record over the factory standard prompts, but you can revert to factory standard prompts if you decide not to use a custom prompt.

## About Multiserver Meetings

The multiserver meeting feature provides a virtual link between different Cisco Unified MeetingPlace systems so that users on each server can communicate with each other as if they were in the same meeting.



### Note

If both servers also have a Cisco Unified Videoconferencing Multipoint Control Unit (MCU) attached and video participants join the same multiserver meeting from different Cisco Unified Videoconferencing MCU units, the participants from each Cisco Unified Videoconferencing MCU can hear each other through the voice links. However, because there are two separate video conferences being hosted on each Cisco Unified Videoconferencing MCU, the video participants from both conferences cannot see each other.

When users schedule multiserver meetings, they designate one Cisco Unified MeetingPlace server as the primary server responsible for connecting to the other—secondary—servers. MeetingTime client software and Cisco Unified MeetingPlace Web Conferencing each provide an easy-to-use interface for scheduling multiserver meetings.

When a multiserver meeting is set to begin, the primary server places one call to each secondary server over standard phone lines. After the secondary servers receive the call, they add the primary server to their meeting, allowing all users to speak to each other over the server they are connected to.

Multiserver meetings are ideal for:

- Minimizing long-distance calls between major corporate locations. Users in a particular region can connect to their local conference servers, and the conference servers call each other over standard phone lines to form a multiserver meeting. This reduces the number of long distance calls required to connect the users.
- Large conference calls (over 550 participants) that require more than one Cisco Unified MeetingPlace server.

For multiserver meeting system requirements, see the *Installation Planning Guide for Cisco Unified MeetingPlace*, at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html).

## Outdial Behavior

Outdial behavior for multiserver meetings that are scheduled to start at the scheduled start time is determined by the Initiate parameter, which can be set to either “At scheduled start time” or “When 1st person enters.” If the Initiate parameter is set to “When 1st person enters,” the system does not initiate the outdial until the first person joins the meeting, even if the scheduled start time has passed.

In Cisco Unified MeetingPlace Audio Server, the amount of time in which the remote server connection to the other Cisco Unified MeetingPlace servers is established is as follows:

- Four minutes before the scheduled start time of the meeting (if the Early mtg start parameter is more than four minutes)
- Thirty seconds before the scheduled start time of the meeting (if the Early mtg start parameter is four minutes or less)



### Note

If someone attends the meeting early (up to 15 minutes before the scheduled start time), the outdial process starts at that time.

## Configuring Cisco Unified MeetingPlace Servers for Multiserver Meetings

Before users can set up multiserver meetings, the system administrator must do the following:

- On each Cisco Unified MeetingPlace server, provide each user with a user profile
- Create Server Information records on each Cisco Unified MeetingPlace system so that the servers can identify each other when they connect

## Worksheet 2-1 Multiserver Meeting Scheduling Requirements

Table 2-23 shows the requirements for scheduling a multiserver meeting. These requirements are described in detail in the “Configuring Cisco Unified MeetingPlace Servers for Multiserver Meetings” section on page 2-42.

**Table 2-23**      **Worksheet 2-1: Multiserver Meeting Scheduling Requirements**

Multiserver Scheduling Requirements	Done
1. Provide users who will schedule multiserver meetings with profiles on each Cisco Unified MeetingPlace server (see the “ <a href="#">Providing Users with Profiles on the Other Cisco Unified MeetingPlace Servers</a> ” section on page 2-44).	
2. Enable the user profiles of those who are going to schedule meetings with multiserver scheduling privileges (see the “ <a href="#">Providing Users with Profiles on the Other Cisco Unified MeetingPlace Servers</a> ” section on page 2-44).	
3. Create Server Information records on all systems for each Cisco Unified MeetingPlace server (see the “ <a href="#">Creating Server Information Records for Cisco Unified MeetingPlace Servers</a> ” section on page 2-45).	
<p>4. To enable users to schedule multiserver meetings using Cisco Unified MeetingPlace Web Conferencing, make sure that:</p> <ul style="list-style-type: none"> <li>• They are using Microsoft Internet Explorer version 5.5 and later <i>or</i> Netscape version 4.79 and later.</li> <li>• They can access each site as Cisco Unified MeetingPlace Web Conferencing server. If these users can already access each site’s Cisco Unified MeetingPlace web page using their web browser, they can schedule a multiserver meeting.</li> <li>• Cisco Unified MeetingPlace Web Conferencing (release 4.2.5 or higher) is installed and running at each site.</li> </ul> <p>For more information about requirements, see the <i>Administration Guide for Cisco Unified MeetingPlace Web Conferencing</i>, at <a href="http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html">http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html</a>.</p>	
<p>5. To enable users to schedule multiserver meetings by using MeetingTime, make sure that:</p> <ul style="list-style-type: none"> <li>• They can access each Cisco Unified MeetingPlace server through their MeetingTime client software.</li> <li>• They have MeetingTime 5.3 or higher installed on their system.</li> </ul>	

## Worksheet 2-2 Recommendations for Multiserver Meetings

Table 2-24 lists some recommendations to consider when you set up your Cisco Unified MeetingPlace 8106 or 8112 for multiserver meetings. You may need to work with the system administrators of the other Cisco Unified MeetingPlace servers to complete these recommendations.

**Table 2-24**      **Worksheet 2-2: Recommendations for Multiserver Meetings**

Recommendations	Done
1. Make sure that all Cisco Unified MeetingPlace servers are time synchronized by using a Network Time Protocol (NTP) server. This NTP server can be a Cisco Unified MeetingPlace system or an external device. To establish an NTP server, go to the MeetingTime Configure tab, select <b>System Parameters</b> , and enter the IP address of the NTP server.	
2. Make sure all servers are properly named across all Cisco Unified MeetingPlace systems. (For guidelines in naming your system, see the “ <a href="#">Naming Cisco Unified MeetingPlace Servers</a> ” section on page 2-46.)	
3. Record a voice name for the other Cisco Unified MeetingPlace servers (see the “ <a href="#">Recording a Voice Name for Other Cisco Unified MeetingPlace Servers</a> ” section on page 2-47).	

Table 2-24 Worksheet 2-2: Recommendations for Multiserver Meetings (continued)

Recommendations	Done
4. Set the same guard times on all Cisco Unified MeetingPlace servers. (For information on guard times, see the <a href="#">“Managing Port Scheduling with Guard Times”</a> section on page 5-6)	
5. Set the same extend meeting parameters on all Cisco Unified MeetingPlace servers. (For more information, see the <a href="#">“Solving Common Problems of Multiserver Meetings”</a> section on page 2-55)	
6. Record the breakout session warning prompt that plays before participants enter a breakout session (see the <a href="#">“Recording the Breakout Session Warning Prompt”</a> section on page 2-48).	

## Providing Users with Profiles on the Other Cisco Unified MeetingPlace Servers

To schedule a multiserver meeting, a user must have multiserver scheduling privileges and a profile on each Cisco Unified MeetingPlace server that is involved in the meeting. For example, if users need to schedule a multiserver meeting between New York City and London, you must make sure that user has a user profile with multiserver scheduling privileges on the New York City server and the London server.

There are two ways that you can provide users with profiles on other Cisco Unified MeetingPlace servers:

- If they already have a profile on a Cisco Unified MeetingPlace server, have the other servers import this profile into the user database. If users do not already have a profile, create one and then have the other servers import it. For more information on how to import profiles, see the [“Importing User Profile and Group Information”](#) section on page 2-16.
- Have all system administrators create the same “generic” profile on their Cisco Unified MeetingPlace server, and have all schedulers use this profile when setting up a multiserver meeting. This allows all schedulers to log in to each server using the same ID and password. This method, however, can create security and billing issues because each scheduler uses the same profile. For more information on creating user profiles, see the [“About User Profiles”](#) section on page 2-14.

## Allowing Users to Schedule Multiserver Meetings

Before users can schedule multiserver meetings, you must give their user profile multiserver scheduling privileges. You must have system manager privileges to modify a user profile.

### To Give Multiserver Scheduling Privileges to a User Profile

- 
- Step 1** By using MeetingTime, log in to the Cisco Unified MeetingPlace server.
- Step 2** In the MeetingTime Configure tab, select the **User Profiles** topic.
- Step 3** Click the **Find Records** button to access the user profile you want to modify.



**Note** This field is case-sensitive.

---

- Step 4** For the Can Call Other Servers? attribute, choose **Yes**.  
This attribute is under the Outdial Meeting Defaults topic.
- Step 5** For the Time Zone attribute, make sure it is set to the local time zone of the user.

Set the Time Zone parameter in a user profile to the same zone on all Cisco Unified MeetingPlace servers. For example, if the local time zone of the user is America/Los Angeles, their user profile on every server should be set to this time zone no matter where the server is located.

**Step 6** Click **Save Changes**.

## Creating Server Information Records for Cisco Unified MeetingPlace Servers

Before two Cisco Unified MeetingPlace servers can connect, each server must have information about the other server entered into its database. Just as profiles identify Cisco Unified MeetingPlace users, each server must have a Server Information record to identify it to the other servers.

For example, in a multiserver meeting from New York City to London, the New York City server must have in its database a Server Information record for the London server, and vice versa.



### Caution

You must contact the system administrators of the remote Cisco Unified MeetingPlace servers to obtain the correct information about their server. This information is explained in the table following the steps.

### To Create Server Information Records for Cisco Unified MeetingPlace Servers

- Step 1** By using MeetingTime, log in to your local Cisco Unified MeetingPlace Audio Server system.
- Step 2** In the MeetingTime Configure tab, select the **Other MeetingPlace Servers** topic (under the System Configuration view). Then click **New**.
- Step 3** In the fields provided, enter information for the local server. Use the information in [Table 2-25](#).

**Table 2-25** *Other MeetingPlace Servers Fields*

Field	Description
Name	Server name that appears in MeetingTime and Cisco Unified MeetingPlace Web Conferencing when users schedule a multiserver meeting. This name helps users identify the correct server to schedule.
ID number	Meeting participants use this numeric string (consisting of digits 0–9), when they outdial from within a conference to select the server to add to the meeting. We recommend that a server's ID number be the same on each server. Work with the other Cisco Unified MeetingPlace system administrators to determine the ID numbers for all the servers.
Phone number	Phone number of the Cisco Unified MeetingPlace server. This number is used by the system to dial out to the Cisco Unified MeetingPlace server to set up a multiserver meeting. This number is passed through a system translation table and is subject to the rules defined in the translation table.  To check that the correct phone number has been entered, schedule and attend a meeting on your local server and then outdial to this remote server. If the server answers the call, the phone number is correct.
VoIP gateway IP address 1	IP address of the remote server's VoIP gateway. (For more information, see the <a href="#">"About RSNA"</a> section on page 2-66.)
(Optional) VoIP gateway IP address 2	IP address of a second remote server's VoIP gateway, if there is one. (For more information, see the <a href="#">"About RSNA"</a> section on page 2-66.)

**Table 2-25** Other MeetingPlace Servers Fields (continued)

Field	Description
Will accept SNA transfers?	Whether this server accepts single number access transfers. (For more information, see the “About RSNA” section on page 2-66.)
Ethernet address	12-digit (with leading zeros) hex string that represents the Ethernet address of a Cisco Unified MeetingPlace 8100 series server. A Cisco Unified MeetingPlace 8100 series server Ethernet address identifies itself to other Cisco Unified MeetingPlace 8100 series. This Ethernet address must match the Ethernet address that appears in the Server Configuration record (Configure tab) on the server this entry refers to.
Web Publisher location	IP address or the URL of Cisco Unified MeetingPlace Web Conferencing. For Cisco Unified MeetingPlace Web to function correctly, this field must contain the correct URL.
Data conference active?	If the server has the Cisco Unified MeetingPlace Web Conferencing option installed and it is operational, set this field to Yes. If the server does not have this option installed, set the field to No.
Server number	As a standalone server, the Cisco Unified MeetingPlace 8106 or 8112 number is 0.

**Step 4** Click **Save Changes**.

**Step 5** In the fields provided, enter information for the remote server. Use the information in [Table 2-25](#).

**Step 6** Click **Save Changes**.

**Step 7** Using MeetingTime, log in to the remote Cisco Unified MeetingPlace 8100 series that you just created a profile for.

**Step 8** Repeat [Step 2](#) through [Step 5](#) to create a Server Information record of your local Cisco Unified MeetingPlace 8100 series on this remote server. Repeat this procedure until every server contains a Server Information record for every other Cisco Unified MeetingPlace 8100 series server.

## Naming Cisco Unified MeetingPlace Servers

As a system administrator, you can provide descriptive names to the Cisco Unified MeetingPlace servers, which helps users identify which systems to schedule for a multiserver meeting.

As you name servers, remember the following information:

- Make sure to do the following:
  - Name each server with an easily identifiable name
  - Name all servers consistently across all Cisco Unified MeetingPlace systems
- To help users identify a server, include the location of the server in its name. For example, if your organization has one server in New York and another in California, include NY or CA in their names.
- To ensure that all users, no matter which server they are logged into, see the same name for each Cisco Unified MeetingPlace system, you must work with the other Cisco Unified MeetingPlace system administrators to find out the names of their servers.

When you change a server’s name, you must update every Cisco Unified MeetingPlace Audio Server system with the new name. For example, if your company has two Cisco Unified MeetingPlace Audio Server systems and you need to change the name of one, update both servers with the new name.

[Table 2-26](#) shows which records on each server need to be updated.

**Table 2-26** *Records That Must Be Updated on Each Server*

Records to Update on Server 1	Record to Update on Server 2
Server configuration record	Server Information record for Server 1
Server Information record for Server 1	

Do the following procedures, in the order presented:

- [To Enter Information in the Server Configuration Record, page 2-47](#)
- [To Update the Local Server Information Record, page 2-47](#)

#### To Enter Information in the Server Configuration Record

- 
- Step 1** By using MeetingTime, log in to the server you want to rename.
- Step 2** In the Configure tab, select the **Server Configuration** topic, and click **Query**.
- Step 3** Use the < and > buttons to locate the server you want to rename.
- Step 4** For the Server Description attribute, enter a description of the server in the text box that displays, then click **OK**.
- For example, describe a conference server in California as CA-MeetingPlace.
- Step 5** Click **Save Changes**.

#### To Update the Local Server Information Record

- 
- Step 1** By using MeetingTime, log in to the server whose name you changed in the previous section, and select the **Configure** tab.
- Step 2** Select the **Other MeetingPlace Servers** topic, and click **Query**.
- Step 3** Use the < and > buttons to locate the server whose name you just changed.
- Step 4** For the Name attribute, enter the same server description that you entered in [“To Enter Information in the Server Configuration Record” procedure on page 2-47](#).
- Step 5** Click **Save Changes**.
- Step 6** Log in to the other Cisco Unified MeetingPlace servers and update the Server Information record that belongs to the system whose name you changed. Click **Save Changes** after updating each server.
- If the system administrator of another Cisco Unified MeetingPlace system renamed one of their servers, you need to log in to your system and update the Server Information record that belongs to that server.

## Recording a Voice Name for Other Cisco Unified MeetingPlace Servers

When another Cisco Unified MeetingPlace server joins a multiserver meeting, all participants hear the default prompt: “Now attending, another MeetingPlace server.”

To help users better identify the server that is joining the meeting, it is strongly recommended that you change this prompt to include specific information like the server name and location. Make this voice name consistent with the name you gave the server in [“To Enter Information in the Server Configuration Record” procedure on page 2-47](#).

Anyone with system administrator privileges can record a new prompt through their phone.

#### To Record a Voice Name for Another Cisco Unified MeetingPlace Server

---

- Step 1** Dial in to your local Cisco Unified MeetingPlace server.
  - Step 2** Press **2** on your touch-tone phone, and then enter your profile number and password.
  - Step 3** Press **9** to select system manager options.
  - Step 4** Press **3** to select the option to record the name of a remote server.
  - Step 5** Follow the prompts to record a voice name for the other Cisco Unified MeetingPlace server.
- 

## Recording the Breakout Session Warning Prompt

Breakout sessions allow participants connected to the same server to form subgroups by breaking off from the main meeting. In multiserver meetings, this feature does not let participants on different Cisco Unified MeetingPlace servers go into the same breakout session.

Because some users do not know that they cannot meet participants on other servers in the same breakout session, you can record a warning prompt that plays whenever a multiserver meeting participant initiates a breakout session. This warning prompt can tell them about the limitations of this feature.

Note the following points about breakout session prompts:

- All profile users hear the breakout session prompts in their profile language.
- All guests hear the breakout session prompts in the language of the port they are calling on.

#### To Record a Breakout Session Warning Prompt Through a Phone

---

- Step 1** Dial in to your Cisco Unified MeetingPlace 8100 series server.
  - Step 2** Press **2** and then enter your profile number and password.
  - Step 3** Press **9** to access system manager options.
  - Step 4** Press **1** to access the voice prompt menu.
  - Step 5** When asked to enter the number of the prompt you want to change, enter **1309#**.
  - Step 6** Press **3** to access the record option.
  - Step 7** Press **2** to record a custom version of this prompt.
  - Step 8** Record the new breakout session warning prompt followed by the pound (**#**) sign.  
Suggested prompt: “In a multiserver meeting, you cannot go into the same breakout session with a user on another server.”
  - Step 9** Press **1** to accept the new prompt.
-



## Using the Server-to-Server Connection Parameters

When you schedule a multiserver meeting by using MeetingTime, you can determine when you want the primary server to initiate and terminate its connection to the other servers.

The default setting for initiating a connection is for the primary server to connect to the secondary servers at the scheduled start time of the meeting. However, you can also set the primary server to connect to the secondary servers when the first person enters the meeting, which may be before or after the scheduled start time.

Table 2-27 describes the different server-to-server connection parameters and the advantages of each.

**Table 2-27** Server-to-Server Connection Parameters

Setting	Description	Advantage
<b>Initiate</b>		
At scheduled start time	<p>Establishes a connection to the other Cisco Unified MeetingPlace servers:</p> <ul style="list-style-type: none"> <li>• four minutes before the scheduled start time of the meeting (if the early mtg start parameter is more than four minutes)</li> <li>• 30 seconds before the scheduled start time of the meeting (if the early mtg start parameter is four minutes or less)</li> </ul> <p>This is the default setting.</p> <p><b>Note</b> If someone attends the meeting early (up to 15 minutes before the scheduled start time), the outdial process starts at that time.</p>	Guarantees the multiserver connection at the scheduled start time of the meeting.
When the first person enters	Establishes connection to the other servers only when the first participant joins the meeting on the primary server.	If nobody attends a meeting or if participants only attend the meeting on the secondary server, the primary server does not connect to the secondary server, so no long distance phone expenses are incurred.
<b>Terminate</b>		
When meeting ends	Terminates the connection to the secondary servers when the meeting ends, which is a set number of minutes after the last person hangs up. This is the default setting.	Allows users to take a break and leave the meeting for a short period of time without the primary server disconnecting from the secondary servers. Participants must return to the meeting before the Disconnect Empty Port Timer/Early Release Timer ends the meeting.
When last person leaves	Terminates the connection to the secondary servers as soon as the last participant leaves the meeting from either the secondary or primary server.	Saves in long distance phone expenses when the last person leaves the meeting before the scheduled end time.

You can set the server-to-server connection parameters per meeting in the Schedule tab in MeetingTime. You can also use the Scheduling Parameters topic in the Configure tab to change the parameter to a new default value. This new value becomes the default setting when users schedule a new multiserver meeting.

## Monitoring Multiserver Meetings by Using MeetingTime

Use the MeetingTime In Session tab to monitor a multiserver meeting that is taking place. You can view which servers are connected to the multiserver meeting and the participants attending the meeting on the server you are logged into.

To see which participants are attending the same multiserver meeting on other servers, open another MeetingTime window and log in to each of these servers separately. For example, if a meeting is taking place between a New York City server and a London server, use MeetingTime to log in to each server and keep each MeetingTime window open.

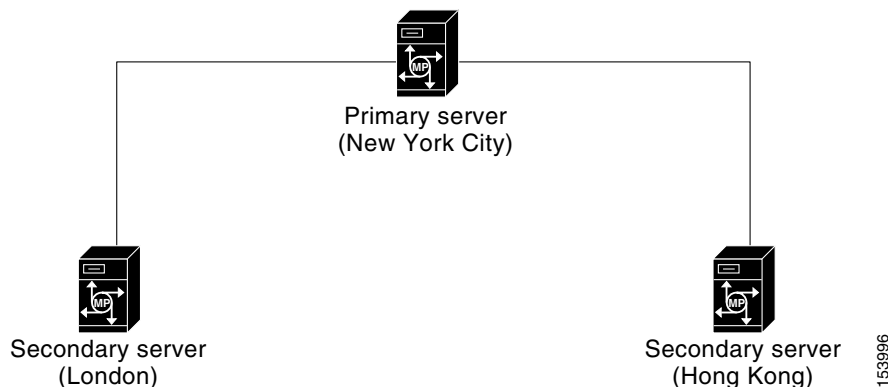
## Scheduling Multiserver Meetings

When setting up a multiserver meeting, you need to schedule individual meetings on each Cisco Unified MeetingPlace server and specify which systems are responsible for connecting all the servers. The server responsible for this connection is the primary server.

At the start of the meeting, the primary server places a call to the secondary servers. The secondary servers then add the primary server to the meeting just as they would any participant who dialed into their system. The primary server communicates information to the secondary servers by using DTMF signaling over the phone connection.

For example, to schedule a meeting between New York City, London, and Hong Kong, set up one meeting on each server. These three separate meetings then connect into one multiserver meeting as soon as the primary server establishes a connection with the other servers. If the New York City server is the primary server, the connections look like [Figure 2-1](#).

**Figure 2-1** Supported Setup for a Multiserver Meeting



Before scheduling a multiserver meeting, we recommend that you write down which servers are involved in the meeting and which server you want as the primary server.

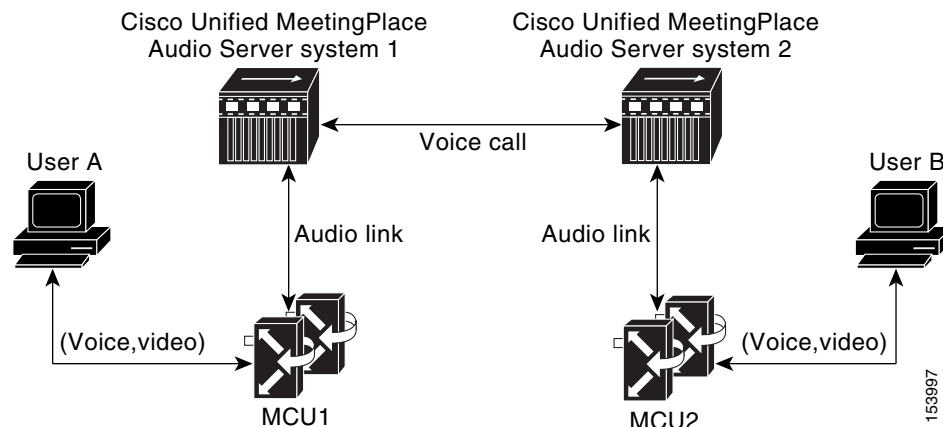
## Scheduling Multiserver Meetings with Video Conferencing

Video participants can join a multiserver meeting and communicate with other participants using other Cisco Unified MeetingPlace 8106 or 8112 servers through the audio (or voice) links. If both servers also have a Cisco Unified Videoconferencing Multipoint Control Unit (MCU) attached and video participants join the same multiserver meeting from different Cisco Unified Videoconferencing MCU units, the participants from each Cisco Unified Videoconferencing MCU can hear each other through the audio links. However, because there are two separate video conferences being hosted on each Cisco Unified Videoconferencing MCU, the video participants from both conferences cannot see each other.

For example, a multiserver meeting is in session between server 1 and server 2. Each server has MCU units. If User A joins the video conference on the MCU1 unit(s) and User B joins the video conference on the MCU2 unit(s), User A and User B can hear each other through audio links. However, they cannot see each other from their video endpoints.

Figure 2-2 illustrates the communication path of the video participants in the multiserver meeting.

**Figure 2-2 Multiserver Meeting with Video Conferencing**



## Inviting Participants and Attaching Documents

Because you schedule more than one Cisco Unified MeetingPlace server, special considerations need to be made when inviting participants and attaching documents.

When inviting participants to a multiserver meeting, each server is responsible for sending out its own notifications. In the previous example, the New York City server sends out notifications for participants that were invited to join the meeting on that server. Although the New York City server is the primary server, it is not responsible for sending out notifications for the Hong Kong and London servers.

When attaching documents to a multiserver meeting, remember to attach the same document to each server involved in the meeting. For example, if you attach a document to the London and New York City servers but forget to attach it to the Hong Kong server, the participants on the Hong Kong server cannot access the attachment.

## Using MeetingTime to Schedule Multiserver Meetings

When scheduling a multiserver meeting using MeetingTime, do not assign more than one primary server to the meeting.

Before you begin, make sure the following are true:

- Your user profile exists on all the Cisco Unified MeetingPlace servers that are involved in the multiserver meeting
- You have multiserver scheduling privileges on each profile

Do the following procedures, in the order presented:

- [To Schedule a Meeting on the Secondary Cisco Unified MeetingPlace Server, page 2-52](#)
- [To Schedule a Meeting on the Primary Server, page 2-52](#)

### To Schedule a Meeting on the Secondary Cisco Unified MeetingPlace Server

- 
- Step 1** In MeetingTime, log in to the secondary server (the one to receive a call from the primary server).
- Step 2** Select the **Schedule** tab, and fill in the meeting details. Add any necessary attachments.  
Make note of the meeting ID, because you will use this same number when you schedule the other servers.
- Step 3** For the # of Calling Sites parameter, be sure to include the primary server in this number.  
For example, if three people from different locations will call into this server, make this number 4.
- Step 4** If you do not want to invite participants to this meeting, click the **Schedule Meeting** button and skip to step 9. To invite participants, choose the Participants option and continue with the next step.
- Step 5** Select a participant who will connect to this secondary server, and click **Add**. Continue selecting and adding all participants who will connect to this server.  
  
For example, if you schedule a New York City to London meeting in which London is the secondary server, add only the participants who will call into the London server. Do not add the participants who will call into the New York City server.
- Step 6** From the drop-down list, choose **Receive Call from a MeetingPlace Server**.  
If you do not see this option, change your user profile to let you schedule multiserver meetings. To change your user profile, see the [“Allowing Users to Schedule Multiserver Meetings”](#) section on page 2-44.
- Step 7** For Server Name, choose the primary server and click **Add**.
- Step 8** When you have added all participants and the primary server to the meeting, click **Schedule Meeting**.
- Step 9** If any other secondary servers need to be scheduled, log in to those servers and repeat [Step 2](#) through [Step 8](#).
- 

### To Schedule a Meeting on the Primary Server

- 
- Step 1** Log in to the Cisco Unified MeetingPlace Audio Server system that will be the primary server.
- Step 2** In the MeetingTime Schedule tab, fill in the meeting details.

Be sure to use the same meeting ID, date, and start time used when scheduling the secondary servers, and add any attachments if necessary.

- Step 3** In the # of Calling Sites parameter, include the number of secondary servers that will be involved in the meeting.
- For example, if three people from different locations will call into this primary server and you have scheduled two secondary servers, make this value 5.
- Step 4** Choose the **Participants** option.
- Step 5** If you want to invite any participants to this primary server, add them to the meeting.
- Step 6** From the drop-down list, choose **Place Call to a MeetingPlace Server**.
- If you do not see this option, change your user profile to let you schedule multiserver meetings. To change your user profile, see the [“Allowing Users to Schedule Multiserver Meetings”](#) section on page 2-44.
- Step 7** For Server Name, choose the name of the secondary server that you scheduled in the [“To Schedule a Meeting on the Secondary Cisco Unified MeetingPlace Server”](#) procedure on page 2-52.
- Step 8** Verify that the meeting ID is the same one you used when scheduling the secondary server, then click **Add**.
- If you scheduled more than one secondary server, be sure to add each one to the meeting.
- Step 9** When you have added all participants and the secondary servers to the meeting, click **Schedule Meeting**.
- 

## Canceling or Changing Details of Multiserver Meetings

To cancel or make changes to a multiserver meeting that has already been scheduled, you can use MeetingTime to reschedule or delete these meetings. However, the changes you make affect only the meeting on the server you are logged into. If you need to make changes that affect the entire multiserver meeting, you must reschedule or delete the meetings on the other Cisco Unified MeetingPlace servers.

### To Cancel or Change Details of a Multiserver Meeting

---

- Step 1** Log in to the Cisco Unified MeetingPlace server that contains the meeting you want to change.
- Step 2** In the MeetingTime Schedule tab, select the meeting you want to change.
- If you do not see the meeting listed, use the **Look for Meeting ID** field to search for the meeting.
- Step 3** Make the changes to the meeting.
- To cancel the entire multiserver meeting, click **Cancel Meeting** and then log in to the other servers to delete the other meetings.
- Step 4** Click **Save Changes**.
- Only the meeting on the server you are logged into is updated. If you have rescheduled the time or date of the meeting, make sure you update the meetings on the other servers as well.
- Step 5** To make the same changes on the other Cisco Unified MeetingPlace servers, repeat [Step 1](#) through [Step 4](#).
-

## Multiserver Meeting Features

The same Cisco Unified MeetingPlace features used in a single server meeting can be used in a multiserver environment. Some of these features, however, do not carry their function across all servers involved in the multiserver meeting.

[Table 2-28](#) describes the features that participants can use when attending a multiserver meeting.

**Table 2-28** Multiserver Meeting Features

Feature	Multiserver Meeting Function
Roll call	Announces the names of the participants connected on the same server. Roll call does not announce the names of participants connected to another Cisco Unified MeetingPlace server.
Record meeting	Records the entire multiserver meeting and stores the recording on the server that requested the recording. As soon as a participant activates the recording feature, a prompt informs all participants that the meeting is being recorded. If participants want the meeting recording to be stored on all servers involved in the meeting, someone from each server must initiate the recording.
Web Conferencing	Allows a document to be shared and collaborated over the entire multiserver meeting as long as there are ports available on the primary server that initiated the web conference. For more information, see the <a href="#">“Using Web Conferencing in Multiserver Meetings” section on page 2-55</a> .
Lock meeting	Allows participants to lock the meeting on the server they are connected to. This feature does not lock the entire multiserver meeting unless one person on each server performs this function.
Meeting message	Announces voice messages to all multiserver meeting participants.
Breakout session	Allows participants connected to the same server to form subgroups by breaking off from the main meeting. This feature does not support participants on different servers to go into the same breakout session.
Muting	Allows a participant to mute their phone line.
View attachments	Allows access to documents, recordings, and URLs if they are attached to the same server the participant is connected to.
Outdial	Allows any participant with outdial privileges to place a call to another person, team, or server and add them to the meeting. For instructions on how to use the outdial feature to add another server to a meeting, see the <a href="#">“Using the Outdial Feature to Add Servers” section on page 2-55</a> .
Announcement prompts	Announces the entry and departure of all meeting participants.
Automatic reconnect operation	When this feature is enabled, a primary server that has lost its connection to a secondary server automatically redials the secondary server to reestablish the meeting. If the connection between two servers becomes lost, users should wait for the connection to be re-established. This feature does not need to be enabled or configured by a system administrator.

## Using the Outdial Feature to Add Servers

If you have outdial privileges, you can use your touch-tone phone to add another Cisco Unified MeetingPlace server to your meeting. To do so, you must know the other server ID number and the meeting ID of the meeting that you want to connect to.

### To Use the Outdial Feature to Add Servers

- 
- Step 1** From within the meeting, press **#39** on your touch-tone phone.
  - Step 2** When prompted, enter the ID number of the server you want to add to the meeting.
  - Step 3** Press **1** to continue.
  - Step 4** When prompted, enter the meeting ID of the meeting that you want to connect to.
  - Step 5** Press **1** to continue.
  - Step 6** Enter the password of the meeting.  
If no password has been assigned, press **#** (the pound sign) only.
  - Step 7** When the servers have successfully connected, the system announces the entry of the server you outdialed.
- 

## Using Web Conferencing in Multiserver Meetings

When a meeting begins, the Cisco Unified MeetingPlace server automatically informs the Web Conferencing server to set up a web conference for the same number of user licenses that were reserved for the system. For example, if a 25-user license meeting were about to start on Cisco Unified MeetingPlace, a 25-user license web conference would also be set up on the Web Conferencing server.

In a multiserver environment, the primary server hosts the web conference. Users on a secondary server are redirected to the Web Conferencing server for the primary server. Cisco Unified MeetingPlace automatically accommodates all web conference participants in the entire multiserver meeting.

For example, if a multiserver meeting is being conducted between New York City and London and a participant on the New York City server initiates a web conference, everyone on the London server who wants to participate in the web conference has their IP connection directed to the New York City server. These users still use their user licenses on the London server for the voice conference, but use user licenses on the New York City server for the web conference.

## Solving Common Problems of Multiserver Meetings

[Table 2-29](#) shows common problems that users may experience when setting up and attending multiserver meetings, and solutions to these problems.

Table 2-29 Troubleshooting Multiserver Meetings

Problem	Solution
When scheduling a multiserver meeting by using Cisco Unified MeetingPlace Web, a user receives an error message that it cannot read the user profile.	This happens because the user probably does not have a user profile on the server they are trying to schedule. To solve this problem, create or import their user profile onto the server they are trying to schedule.
A user wants to schedule a meeting with Cisco Unified MeetingPlace Web Conferencing, but does not see the Schedule Multiserver link.	This happens for one of the following reasons: <ul style="list-style-type: none"> <li>The user does not have multiserver scheduling privileges. To solve this problem, set the Can Schedule Other Servers? parameter in their user profile to Yes.</li> <li>The web browser the user uses is not supported. For browser requirements, see the scheduling requirements table in the <i>Installation Planning Guide for Cisco Unified MeetingPlace</i>.</li> </ul>
A user is trying to schedule a meeting but is unable to use the same meeting ID on each Cisco Unified MeetingPlace server.	This happens if the user is trying to schedule a meeting between two or more networked Cisco Unified MeetingPlace servers, or there is already another meeting scheduled at the same time on the same server with the same meeting ID. To solve this problem, have the user assign a different meeting ID to the meeting.
A user is trying to schedule a meeting by using Cisco Unified MeetingPlace Web Conferencing, but receives an error message that the server cannot be accessed when selecting either a primary or secondary server.	Verify that the server they are trying to access is connected to a Cisco Unified MeetingPlace Web Conferencing server. If it is not connected, users cannot schedule a meeting through their web browser.
A user is in a multiserver meeting and the participants on another server can access an attachment that the user cannot access.	This happens because the person who added the attachment to the other server did not add the attachment to the server the user is connected to.
A user is in a meeting in which the time has been extended, but the other Cisco Unified MeetingPlace server is dropped from the meeting.	This happens if the server ran out of available ports and its extend meeting parameter ran out of time. For all servers to stay connected for the same amount of time, they must each have the same extend meeting parameter. To modify the extend meeting parameter: <ol style="list-style-type: none"> <li>Log in to MeetingTime, and select the <b>Configure</b> tab.</li> <li>Select the <b>Scheduling Parameters</b> topic and click <b>Query</b>.</li> <li>For the Extend Meeting parameter, assign the same value as the other Cisco Unified MeetingPlace servers.</li> <li>Click <b>Save Changes</b>.</li> </ol>
Servers are not connecting for the multiserver meeting.	This happens when a server has the wrong Ethernet address for another server in the meeting. To fix this problem, the system administrators for the Cisco Unified MeetingPlace servers must check the server profiles to see which server has the wrong address.

## About Reservationless Meetings

With the Reservationless Meetings feature, profile users can create impromptu meetings through their touch-tone phones without having to schedule the meetings in advance. Using a unique meeting ID reserved for each user (the user's profile ID), participants can conduct meetings whenever system resources are available and use all available features during the meeting.



Reservationless meetings and standard scheduled meetings can reside on the same Cisco Unified MeetingPlace server. Setting reservationless meetings on or off at the system level determines the prompts that play and how participants attend meetings.

- When reservationless meetings are enabled, users hear the prompts for scheduled and reservationless meetings. Users can attend scheduled and reservationless meetings through a single user interface. When participants attend a regularly scheduled meeting, they are placed directly in the main meeting. When participants attend a reservationless meeting that has not started, they are placed in a waiting room. Scheduled and reservationless meetings use the same pool of conference ports.
- When reservationless meetings are not enabled, users hear the standard prompts for scheduled meetings only. Users may attend only standard scheduled meetings, including immediate meetings. When participants attend a scheduled meeting, they are placed directly in the main meeting (except during lecture-style meetings, when participants are placed initially in the waiting room).
- When reservationless-only meetings are enabled, users start reservationless meetings by using two fewer steps. However, this configuration also prevents profile users from scheduling scheduled meetings through their touch-tone phones. Scheduled meetings can still be scheduled through MeetingTime and Cisco Unified MeetingPlace Web Conferencing.

The Reservationless Meetings feature is enabled using the “mtgmode” CLI command, which must be done only by a Cisco NCE representative. This command is executed once to configure the entire Cisco Unified MeetingPlace system for a particular type of meeting. After the mtgmode command is executed, the system does not need to be restarted for the feature to work.

**Note**

When used with Cisco Unified MeetingPlace Web Conferencing earlier than Release 3.0, Web Conferencing can be enabled after the voice conference has been activated. When used with Release 3.0 or later, reservationless meetings can be started either from Cisco Unified MeetingPlace Web Conferencing or the phone.

## Configuring Reservationless Meetings

When reservationless meetings are enabled, you can configure the use of reservationless meetings in three ways:

- System-wide (all users can or cannot use the feature). See the “[Configuring System-Wide Reservationless Meetings Attributes](#)” section on page 2-58.
- By user group (groups of users may or may not use the feature) See the “[Configuring User Profiles and Groups for Reservationless Meetings](#)” section on page 2-58.
- By user profile (individual users may or may not use the feature). See the “[Configuring User Profiles and Groups for Reservationless Meetings](#)” section on page 2-58.

### Task List for Configuring Reservationless Meetings

1. Enable reservationless meetings on the Cisco Unified MeetingPlace 8106 or 8112 server.

You can enable scheduled meetings, reservationless meetings only, or combined reservationless and scheduled meetings.

2. Restart the Cisco Unified MeetingPlace 8106 or 8112 to activate the feature.
3. Complete the worksheet in the *Installation Planning Guide for Cisco Unified MeetingPlace*, at [http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html).

4. To configure system-wide attributes for reservationless meetings, see the [“Configuring System-Wide Reservationless Meetings Attributes”](#) section on page 2-58.
5. If needed, change the default reservationless meetings parameters (shown in [Worksheet 2-3 Default Values for Reservationless and Scheduled Meetings](#), page 2-63).

**Caution**


---

Because the default settings ensure a smooth conference experience, make changes only when necessary.

---

**Caution**


---

Unlike scheduled meetings, you cannot restrict the number of ports used by a reservationless meeting.

---

## Configuring System-Wide Reservationless Meetings Attributes

When you set system-wide field attributes for reservationless meetings, *all* users can or *no* users can use this feature.

To allow (or prevent) particular users or groups to use reservationless meetings, set the attributes described in the following table. Then see the [“Configuring User Profiles and Groups for Reservationless Meetings”](#) section on page 2-58.

### To Configure System-Wide Reservationless Meeting Attributes

- 
- Step 1** In MeetingTime, select the **System** tab.
  - Step 2** Select the **Reservationless Mtgs** action, and then set the attributes shown in the following table.

Field	Default Value	Description
Enable reservationless	No	Allow or prevent reservationless meetings. This field is read-only.
Owner Initiate with 2 key?	No	When No, meeting owners must enter their profile and password. When Yes, meeting owners start their reservationless meeting by pressing <b>1</b> to attend the meeting and then <b>2</b> to start the meeting (after which they must enter their password).
Allow 3rd party initiate?	Yes	Whether profile users can initiate reservationless meetings before the meeting organizer arrives.
Bill 3rd party initiator?	Yes	Whether the reservationless meeting is billed to the meeting initiator (when a third party initiates the meeting) or the meeting organizer (no matter who initiates the meeting).

- Step 3** Click **Save Changes**.
- 

## Configuring User Profiles and Groups for Reservationless Meetings

For greater flexibility, system administrators may configure individual user profiles and user groups to use the Reservationless Meetings feature.

To enable users and groups to use reservationless meetings, the Enable Reservationless attribute (described in the “[Configuring System-Wide Reservationless Meetings Attributes](#)” section on [page 2-58](#)) must be set to Yes.

### To Configure User Profiles and Groups for Reservationless Meetings

- Step 1** In the MeetingTime Configure tab, select either **User Profiles** or **User Groups**.
- Step 2** Search for the user or group for which you want to set this attribute.
- Step 3** For Attributes, scroll to the **Restrictions** category.
- Step 4** For the Use Reservationless attribute, choose a value, then click **Save Changes**.

The default for user profiles is Group Dflt; the default for user groups is Yes.

[Table 2-30](#) describes the dependencies that apply for various attribute settings.

**Table 2-30** Combinations of Reservationless Meeting Settings

If Enable Reservationless Meeting (System Tab) Is	And Use Reservationless Is	Then
No	Any value	The value in Use Reservationless? is ignored.
Yes	Yes	The profile user or group can use reservationless meetings.
Yes	No	The profile user or group cannot use reservationless meetings.
Yes	<b>Group Dflt</b> (for user profiles)	User profiles use the group setting for the field. <b>Note</b> To allow users to use reservationless meetings, make sure the group setting is <i>Yes</i> .

Remember the following information:

- All users may change their Use Reservationless setting in the Preferences tab. The settings are subject to the same dependencies described in the previous table.
- Users whose profiles are not configured for reservationless meetings do not hear the “To start your meeting” prompt.
- Reservationless meeting IDs are permanently “in use” and not available for others to use when they schedule meetings.

## Configuring Reservationless and Scheduled Meetings

Configuring reservationless and scheduled meetings begins with the “mtgmode” CLI command. For assistance, contact Cisco NCE.

Then, system administrators can configure meetings by setting parameters in MeetingTime. [Table 2-31](#) shows the conditions in which reservationless and scheduled meetings (voice-only interface) can take place.

Table 2-31 Conditions for Reservationless and Scheduled Meetings

Mode	Settings
Combined reservationless and scheduled meetings	<ol style="list-style-type: none"> <li>1. <i>mtgmode -r</i></li> <li>2. MeetingTime Configure tab/User Profiles view/Use Reservationless parameter is <i>Yes</i> or the Group Default is <i>Yes</i></li> <li>3. MeetingTime Configure tab/Port Groups view/Combined Access parameter is <i>Yes</i></li> </ol>
Reservationless (only) meetings	<ol style="list-style-type: none"> <li>1. <i>mtgmode -o</i></li> <li>2. MeetingTime Configure tab/User Profiles view/Use Reservationless parameter is <i>Yes</i>, or <i>Group Default</i> is <i>Yes</i></li> <li>3. MeetingTime Configure tab/Port Groups view/Combined Access parameter is <i>Yes</i></li> </ol>
To Attend (press 1) and Owner Initiate (press 2)	<ol style="list-style-type: none"> <li>1. <i>mtgmode -r</i> or <i>mtgmode -o</i></li> <li>2. Meeting owner's profile setting for the Use Reservationless parameter is <i>Yes</i> (or <i>Group Default</i>)</li> <li>3. MeetingTime System tab/Reservationless Mtgs action/Owner Initiate With 2 Key? parameter is <i>Yes</i></li> <li>4. User's profile says Password Required for Meeting they create</li> </ol>
To Attend (press 1) and 3rd Party Initiate (press 3)	<ol style="list-style-type: none"> <li>1. <i>mtgmode -r</i> or <i>mtgmode -o</i></li> <li>2. Meeting owner's profile setting for the Use Reservationless parameter is <i>Yes</i> (or <i>Group Default</i>)</li> <li>3. MeetingTime System tab/Reservationless Mtgs action/Allow 3rd Party Initiate? is <i>Yes</i></li> <li>4. User's profile setting for Password Required for meetings the user creates is <i>Yes</i></li> </ol>

## Requiring Passwords for Reservationless Meetings

You can ensure that all reservationless meetings are protected by passwords. Requiring a password applies only to participants in voice conferences. This feature does not apply to participants in web and video conferences.

### To Require Passwords for Reservationless Meetings

- Step 1** In the MeetingTime Configure tab, select either **User Groups** or **User Profiles**.
- Step 2** For each user or group that will organize reservationless meetings, select the **Password Required** parameter, and choose **Yes**.
- Step 3** Restart the Cisco Unified MeetingPlace 8106 or 8112 to activate these settings.

The reservationless meeting organizer (or the person who will start the meeting) should communicate the password to all attendees before the meeting begins, so that all attendees can join the meeting without delay. (For example, the meeting organizer can send an e-mail message to all attendees with the meeting phone number, ID, and password.)

For meetings that require meeting passwords, users are asked to enter the password before they are allowed to start or join the meeting.

---

## Starting a Reservationless Meeting

The meeting organizer is responsible for forwarding the meeting ID to all invited participants.

Video participants who are profile users can start a reservationless meeting by signing in to the Cisco Unified MeetingPlace web server and having the server outdial their video terminals.

Phone participants who have a profile can start a reservationless meeting in any of the following ways:

- The Cisco Unified MeetingPlace web server can outdial the reservationless meeting owner.
- When reservationless-only mode is active, the meeting owner presses **2**, hears the “Start your meeting now” prompt, and follows the instructions.
- When reservationless+ scheduled mode or reservationless-only mode is active, the meeting owner can press **1**. The owner then presses **2** to start the meeting. This option requires that the Owner Initiate With 2 Key? parameter (MeetingTime System tab/Reservationless Mtgs action) is set to Yes.
- When reservationless+ scheduled mode or reservationless-only mode is active, any user can press **1**. They then press **3** to start the meeting after optionally creating a password that other participants (including the owner) must use before entering the meeting. This option requires that the Allow 3rd Party Initiate? parameter (MeetingTime System tab/Reservationless Mtgs action) is set to Yes.
- From the Cisco Unified MeetingPlace Web Welcome page, users click the Immediate Meeting button and enter the meeting ID. Any participants in the waiting room are moved into the meeting. (For more information, see the *Administration Guide for Cisco Unified MeetingPlace Web Conferencing*, at [http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html).)

## Attending a Reservationless Meeting

Do the following procedure.

### To Attend a Reservationless Meeting

- 
- Step 1** Users start a meeting by using a method described in the “Starting a Reservationless Meeting” section on page 2-61.
- Step 2** When participants enter the meeting, the Cisco Unified MeetingPlace Audio Server system determines if the meeting has started.
- If the owner has started the meeting, participants can join the meeting.
  - If the owner has not started the meeting (and the Allow 3rd Party Initiate? parameter is No), participants are placed in a waiting room until the owner arrives and starts the meeting. People in the waiting room cannot talk with one another. Video is blocked for video participants.
  - If the owner has not started the meeting (and the Allow 3rd Party Initiate? parameter is Yes), the first participant to join the meeting can start it.
- Step 3** After the meeting has started, participants in the waiting room are moved onto the main floor of the meeting.

If the owner is late or absent, any profile user can activate the meeting by entering their profile number and password, and then bringing the meeting to order.

- Step 4** Use the in-session meeting features. (See the “[About Using Features During Meetings](#)” section on page 3-12.)

## Viewing Reservationless Meeting Data Statistics

To see information about reservationless meetings, you can generate a Raw Meeting Details Information Report and view the following fields:

- The RsvnlessStartID field contains the profile ID of the person who initiated the meeting. This field appears at the end of the report.
- The BillCode field contains the billing code of the meeting originator (the profile user with that meeting ID). However, if the meeting was initiated by a third party and the value of the Bill 3rd Party Initiator field (for Reservationless Mtgs) is Yes, the BillCode field contains the billing code of the user who initiated the meeting.
- A value of Reservationless for the fstartpeopleinwr field tells you which meetings are reservationless meetings.

For more information about Raw Meeting Details Information reports, see the “[Raw Meeting Details Information Data](#)” section on page C-11.

## Recommended Settings for Reservationless Meetings

Use the information in this section for deployment settings for reservationless meetings, settings for combined reservationless and scheduled meetings, and profile number and meeting ID management.

For information about the system requirements for reservationless meetings, see the *Installation Planning Guide for Cisco Unified MeetingPlace*, at

[http://www.cisco.com/en/US/products/sw/5664/ps5669/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/5664/ps5669/prod_installation_guides_list.html).

[Table 2-32](#) shows the recommended deployment settings, which are based on settings for immediate meetings. You can change these settings in MeetingTime, depending on usage.

**Table 2-32 Recommended Deployment Settings for Reservationless Meetings**

Parameter	Recommended Value	Description
<b>Server Configuration</b>		
Floater ports	See <a href="#">Table 2-33</a> and <a href="#">Table 2-34</a> .	Number of ports reserved as floater ports for audio.
Overbook ports		Number of ports reserved to allow for scheduling beyond the number of conference ports readily available on the system.
<b>Scheduling Parameters: Immediate Meetings</b>		
# of ports to schedule	See <a href="#">Table 2-33</a> and <a href="#">Table 2-34</a> .	Default for the number of participants (locations) for an immediate meeting.

**Table 2-32** Recommended Deployment Settings for Reservationless Meetings (continued)

Parameter	Recommended Value	Description
Length of mtg (min)	30	Default length of an immediate meeting (in minutes). Recommended value is 20 or higher. When only one caller is waiting in the waiting room, that caller is disconnected after this immediate meeting length expires.
<b>Scheduling Parameters: Run-time Parameters</b>		
Extend meeting (min)	15	Length of time (in minutes) a meeting is extended if time runs over an if ports are available. Recommend 0 or above. When 0, meetings cannot be extended.

## Worksheet 2-3 Default Values for Reservationless and Scheduled Meetings

Reservationless meetings are assigned predefined parameters to ensure a smooth conference experience. The parameters you set in MeetingTime apply only to standard scheduled meetings. See [Table 2-33](#).

**Table 2-33** Worksheet 2-3: Default Values for Reservationless and Scheduled Meetings

Parameter	Reservationless Meetings Value	Scheduled Meetings Value	Description
<b>User Profiles/User Groups Parameters</b>			
Display mtg to everyone		Yes/No/ Group Default	Whether meetings scheduled by this user display to everyone from MeetingTime and Cisco Unified MeetingPlace Web.
Allow Internet access		Yes/No/ Group Default	Whether meetings allow Internet access.
Display mtg to everyone for reservationless	Yes		Whether reservationless meetings initiated by this user display to everyone from MeetingTime and Cisco Unified MeetingPlace Web.
Allow Internet access for reservationless	Yes		Whether reservationless meetings allow Internet access.
<b>Meeting Preferences</b>			
End of mtg announcement?	No	Yes/No/ Group Default	Whether the system announces the meeting ends in a set number of minutes.
Mtg extension announcements?	No	Yes/No/ Group Default	Whether the system announces the meeting is extended by a set number of minutes.

Table 2-33 Worksheet 2-3: Default Values for Reservationless and Scheduled Meetings (continued)

Parameter	Reservationless Meetings Value	Scheduled Meetings Value	Description
Password required	No	Yes/No/ Group Default	Whether meetings scheduled by this user require a password by default.  You can require all reservationless meetings organized by this user or group to have a password. For more information, see the <a href="#">“Requiring Passwords for Reservationless Meetings”</a> section on page 2-60.  <b>Note</b> Requiring a password applies only to participants in voice conferences. This feature does not apply to participants in web and video conferences
Who can attend?	Anyone	Anyone/ MeetingPlace Users/ Invited Users/ Group Default	Who can attend meetings scheduled by this group.
<b>Sending Notifications</b>			
Enabled for this mtg?	No	Yes/No/ Group Default	Whether this group sends notifications for meetings.
<b>Scheduling Parameters:Meeting Ports</b>			
Default meeting type	All Speaker	All Speaker/ Lecture	Default for meeting type: All Speaker or Lecture.
Meeting start guard time (min)	Does not apply	Numeric—0 to 1440	Number of minutes before scheduled meeting start time that ports are reserved for meeting. Cisco Unified MeetingPlace adds this advance time to requested start time.
Mtg end guard time (min)	0	Numeric—0 to 1440	Number of minutes after scheduled meeting end time that ports remain reserved. The system adds this post meeting time to reserved end time of meeting.
Mtg ID start guard time (min)	Does not apply	Numeric—0 to 1440	Number of minutes before scheduled meeting start time that associated meeting ID or DID/DDI number is reserved.
Mtg ID end guard time (min)	0	Numeric—0 to 1440	Number of minutes after scheduled meeting end time that associated meeting ID or DID/DDI number is reserved.
<b>Run-time Parameters</b>			
Disconnect empty port (min)	0	Numeric—0 to 30	Number of minutes reserved ports are held after everyone hangs up, even when scheduled meeting end time has not arrived.



## Recommended Settings for Combined Reservationless and Scheduled Meetings

Use the values in [Table 2-34](#) to configure a system with both reservationless and scheduled meetings. These values maximize the port utilization and capacity of your system.

For the following table, remember the following information:

- R = percent of traffic used for reservationless meetings
- N = total number of conference ports including capacity assurance (CAP)
- 30 percent can be substituted for standard operating percentage

**Table 2-34** *Recommended Settings for Combined Reservationless and Scheduled Meetings, Audio*

Parameter	Recommended Value
<b>If R &lt; 50 Percent</b>	
Immediate Meetings	3
Overbook ports	$N \times 30$ percent
Floater ports	$N \times 30$ percent
<b>If R <math>\geq</math> 50 Percent</b>	
Immediate Meetings	0
Overbook ports	$N \times 15$ percent
Floater ports	$N \times (R + 25)$ percent

Remember the following information:

- Make sure the total number of scheduling ports available (including overbook ports) is equal to or greater than the largest meeting size you expect to schedule.
- These guidelines are good defaults for a new system. If your system is already configured, however, you may want to keep the existing settings.

## Recommended Settings for Reservationless Meetings Only

Use the values in [Table 2-35](#) to configure a system with reservationless- only meetings. These values maximize the port utilization and capacity of your system.

For the following table, remember the following information:

- R = percent of traffic used for reservationless meetings
- N = total number of conference ports including capacity assurance (CAP)

**Table 2-35** *Recommended Settings for Reservationless-Only Meetings, Audio*

Parameter	Recommended Value
<b>If R = 100 percent</b>	
Immediate Meetings	4
Overbook ports	N

**Table 2-35 Recommended Settings for Reservationless-Only Meetings, Audio (continued)**

Parameter	Recommended Value
Floater ports	N

## Managing Profile Numbers and Meeting IDs for Reservationless Meetings

Because each person's profile number is their reservationless meeting ID, profile numbers cannot match existing meeting IDs when reservationless meetings is turned on.

- If you try to create a profile number that matches an existing meeting ID, the system tells you of the conflict. To correct the problem, change the existing meeting ID or select another profile number for the user.
- End users cannot schedule meetings with a meeting ID that matches another profile number.

When you migrate a system from standard scheduled meetings to combined scheduled and reservationless meetings, any scheduled meetings using a profile number as the meeting ID remain as scheduled meetings after the switchover.

## Identifying Profile and Meeting ID Conflicts in Reservationless Meetings

Meeting conflicts can occur if you are converting your system from scheduled meeting mode to scheduled + reservationless mode (or reservationless-only mode), for example. These conflicts occur if future scheduled meetings have meeting ID numbers equal to the profile numbers of any reservationless users.

A utility, `mtgconflicts`, is available to help you identify profile ID and meeting ID conflicts. If a conflict is found, you see a list of conflicting meetings. To resolve the conflict, either keep the scheduled meetings or change the meeting IDs.

A Cisco NCE representative can assist you by running the `mtgconflicts` utility to check for these conflicts.

## About RSNA

Reservationless Single Number Access (RSNA) allows multiple Cisco Unified MeetingPlace Audio Servers to appear as one server to the user community. All users who host (as a profile user) or attend (as a profile user or as a guest) a reservationless meeting can access the meeting by dialing the phone number of the server that is local to that user, regardless of which server is hosting the meeting. Users are then redirected to the server that is hosting the meeting.

You can also configure extended RSNA prefixes, indicating specific Audio Server/codec support combinations. With extended prefixes, you can control the codec that is used in redirecting calls from one server to another.

If you are setting up RSNA for the first time, see the following sections:

- [RSNA Requirements, page 2-67](#)
- [About Extended RSNA Prefixes, page 2-68](#)
- [Setting Up RSNA for the First Time, page 2-70](#)
- [Troubleshooting RSNA, page 2-75](#)

If you are adding extended prefixes to an existing RSNA configuration, see the following sections:

- [Extended RSNA Prefix Requirements, page 2-67](#)
- [About Extended RSNA Prefixes, page 2-68](#)
- [Adding Extended Prefixes to an Existing RSNA Configuration, page 2-74](#)
- [Troubleshooting RSNA, page 2-75](#)

## RSNA Requirements

- RSNA requires that all voice communication with the Cisco Unified MeetingPlace server uses VoIP and SIP. Any PSTN or H.323 end points must go through a SIP integration to communicate with the system. This implementation depends on the use of the SIP “REFER method” call transfer mechanism, as specified in RFC 3515. All participating SIP end points, including a Cisco Unified MeetingPlace H.323/SIP Gateway server, any SIP integrations that communicate with Cisco Unified MeetingPlace, and any phones or other terminals that communicate directly with the system by using SIP must support the SIP REFER method.

A SIP phone that does not support the REFER method does not transfer correctly and cannot attend meetings that require a transfer. In this situation, users are asked to dial the phone number of the hosting server, as if they entered an unrecognized meeting ID.

- System administrators must ensure the following:
  - All participating Cisco Unified MeetingPlace servers have synchronized user databases
  - All user profiles for active users are present on all systems
- Use Cisco Unified MeetingPlace Directory Services to synchronize user databases across multiple Cisco Unified MeetingPlace systems. The following fields in each user profile on all servers must be set identically:
  - User ID
  - Scheduling Home Server

This configuration assumes that profile numbers are assigned across the system (for example, profile ID 1234 on servers A and B both refer to the same person). This configuration also assumes that either server can authenticate the user for both servers.

  - Passwords must be synchronized. If the password is not the same across the system, the user is provisionally authenticated (and must reenter the password for access as a profile user after exiting the meeting). Also, if users want to rerecord their name on a remote server, they need to know their password on that server.
- If you are using extended RSNA prefixes, all requirements for extended prefixes must be met. See the following “[Extended RSNA Prefix Requirements](#)” section.

## Extended RSNA Prefix Requirements

- The following Cisco Unified MeetingPlace component versions:
  - Audio Server 5.4(1.4) or later
  - MeetingTime 5.4(1.1) or later
  - H.323/SIP Gateway 5.3(1.5) or later

- Voice gateways involved in the RSNA transfer must support transcoding and be running IOS 12.4.9T or a later release.
- All requirements for the RSNA feature. See the preceding “RSNA Requirements” section.

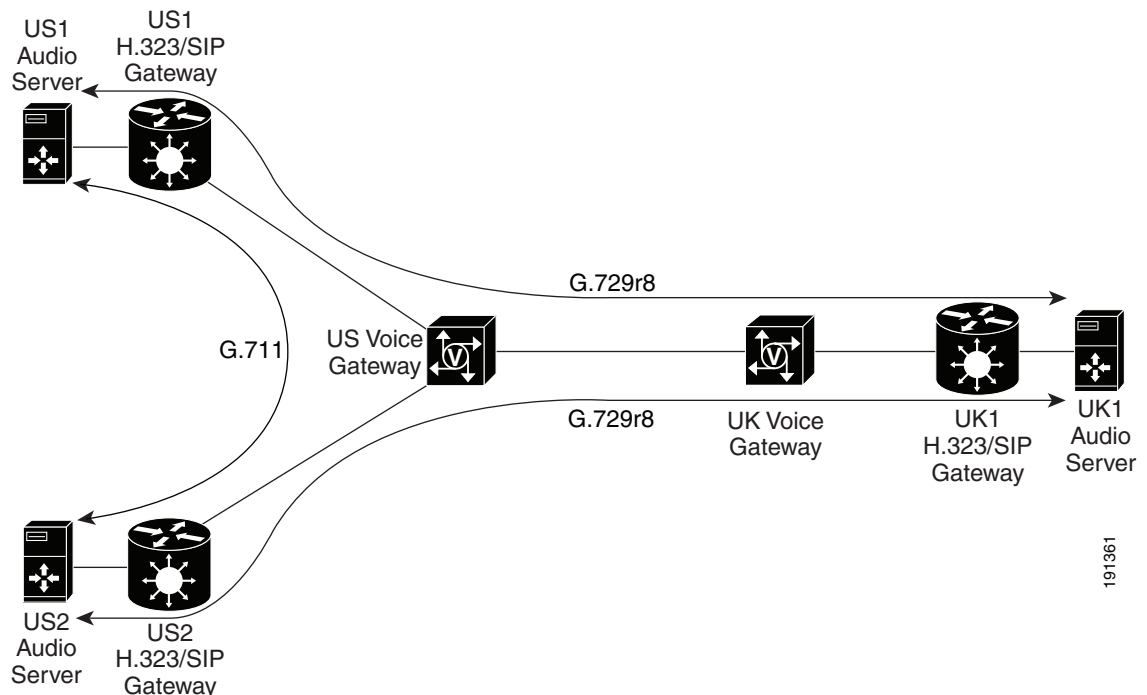
## About Extended RSNA Prefixes

In some circumstances, you may want to be able to control the type of codec that is used when performing RSNA transfers between particular servers. Extended RSNA prefixes allow you to specify the codec that is used during the call transfer by using a codec configuration prefix value in the dial peers on each voice gateway. In MeetingTime, you configure a server record on each Cisco Unified MeetingPlace Audio Server for every other server that will participate in RSNA transfers. In the server record, you specify a value for the Extended RSNA Codec, and MeetingTime returns an extended prefix value. You use the extended prefix value as the destination pattern when configuring the dial peers for transferring calls to that server. In each dial peer, you also specify which codec to use on the transferred calls.

## Extended RSNA Prefix Configuration Example

The example in Figure 2-3 shows a topology with two Cisco Unified MeetingPlace Audio Servers in the United States and one in the United Kingdom. In this scenario, calls that are transferred between the U.S. servers (US1 and US2) should use the G.711 codec, and calls that are transferred between the U.S. servers and the UK server (or vice versa) should use the G.729r8 codec.

**Figure 2-3** RSNA Transfer Paths Utilizing Different Codecs



On the Audio Servers in this example, configuring an Extended RSNA Codec in MeetingTime for every other server results in the extended prefix values shown in Table 2-36.

**Table 2-36** Extended Prefix Values for Other Servers on US1

Server	Extended Prefix
US1	0101
US2	0201
UK1	0301

Note that the actual codec used when transferring calls depends on the dial-peer configuration on the gateway, not on the value of the Extended RSNA Codec field. Any codec (other than None) can be chosen for the Extended RSNA Codec field in order to generate the extended prefix; however, the codec you choose for a given server should be consistent across all of the Audio Servers in order to generate the same extended prefix for that server (for example, use G.711uLaw when configuring the Other Servers record for US1 on both US2 and UK1).

Given these prefix values, the U.S. voice gateway would be configured with dial peers such as the following to match the extended prefixes:

```
dial-peer voice 210 voip
  description rsna_refer_to_us1
  destination-pattern 0101
  session protocol sipv2
  session target ipv4:10.10.10.1
  dtmf-relay rtp-nte
  codec g711ulaw
  no vad
!
dial-peer voice 220 voip
  description rsna_refer_to_us2
  destination-pattern 0201
  session protocol sipv2
  session target ipv4:10.10.10.2
  dtmf-relay rtp-nte
  codec g711ulaw
  no vad
!
dial-peer voice 230 voip
  description rsna_refer_to_UK1
  destination-pattern 0301
  session protocol sipv2
  session target ipv4:10.10.10.3
  dtmf-relay rtp-nte
  codec g729r8
  no vad
!
```

The outgoing dial peers on the UK voice gateway will look something like this:

```
dial-peer voice 210 voip
  description rsna_refer_to_us1
  destination-pattern 0101
  session protocol sipv2
  session target ipv4:10.10.10.1
  dtmf-relay rtp-nte
  codec g729r8
  no vad
!
dial-peer voice 220 voip
  description rsna_refer_to_us2
  destination-pattern 0201
```

```

session protocol sipv2
session target ipv4:10.10.10.2
dtmf-relay rtp-nte
codec g729r8
no vad
!

```

## Setting Up RSNA for the First Time



### Note

If the system is already configured to use RSNA and you are adding extended prefixes, see the “[Adding Extended Prefixes to an Existing RSNA Configuration](#)” section on page 2-74 instead.

Setting up RSNA involves configuring settings on the Cisco Unified MeetingPlace Audio Servers to enable RSNA, and adding dial peers to the Cisco voice gateways in your network to handle RSNA transfers.

See the following sections:

- [Configuring the Audio Servers for RSNA Transfers](#), page 2-70
- [Configuring a Cisco Voice Gateway for RSNA Transfers](#), page 2-72

You can also configure a complementary “reservationless WebConnect” service for Cisco Unified MeetingPlace Web Conferencing. For more information, see the *Administration Guide for Cisco Unified MeetingPlace Web Conferencing*, at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html).

However, because WebConnect and RSNA work independently, you must ensure that each is configured correctly to be synchronized.

## Configuring the Audio Servers for RSNA Transfers

Do the three procedures in this section in the order presented to enable single number access on the Cisco Unified MeetingPlace Audio Servers.

- In the “[To Create Other Cisco Unified MeetingPlace Servers Records](#)” procedure, you create an Other MeetingPlace Servers record for each remote server that will participate in RSNA.
- In the “[To Enable the System for RSNA](#)” procedure, you turn on the RSNA transfer mechanism by enabling the system for RSNA.
- In the “[To Configure Users and Groups for RSNA](#)” procedure, you enable remote users to use the RSNA feature by setting attributes in the MeetingTime Configure tab. Each user is assigned to a specific server identified by the Scheduling Home Server value in the user profile. This value is used to look up an Other MeetingPlace Servers record.

### To Create Other Cisco Unified MeetingPlace Servers Records



#### Caution

To avoid a loopback condition, do not create an Other MeetingPlace Servers record with an ID Number that matches the Scheduling Home Server setting.

**Step 1** In the MeetingTime Configure tab, select the **Other MeetingPlace Servers** view.

**Step 2** Create a new record with the following values:

Attribute	Do This
Name	Enter the name of the remote server.
ID number	Enter a number between 101 and 32767. This number must match the value of the Scheduling Home Server attribute (set in the profile for users for that server).  <b>Note</b> Setting this field to 0 (zero) prevents this record from being used. This field must contain a value greater than 100. For example, 102 and 121 are valid values; however, 007 is invalid.
Phone number	Access phone number for the remote server (used to play a prompt if a transfer fails).
Ethernet address	Enter the Ethernet address of the remote server (the same address used to generate license keys on that server).
VoIP gateway IP address 1	Enter the IP address of the remote server VoIP gateway.
(Optional) VoIP gateway IP address 2	Enter the IP address of a second remote server VoIP gateway, if there is one.  <b>Note</b> When configuring one VoIP gateway, enter the IP address of the gateway for VoIP Gateway IP Address 1, and leave VoIP Gateway IP Address 2 blank. When configuring two VoIP gateways, enter different IP addresses for VoIP Gateway IP Address 1 and VoIP Gateway IP Address 2. Do not enter a value for VoIP Gateway IP Address 2 if VoIP Gateway IP Address 1 is blank or set to 0.0.0.0.
Will accept SNA transfers?	Choose <b>Yes</b> .
Extended RSNA Codec	Choose a codec in order to generate an Extended RSNA Prefix value for the remote server. If you do not want to use the Extended RSNA Prefix feature, choose <b>None</b> .  After you choose the codec and save your changes, MeetingTime displays a value in the Extended Prefix field. You will use this value when configuring dial peers for the RSNA transfer on the voice gateway.  <b>Note</b> The actual codec used when transferring calls depends on the dial-peer configuration on the gateway, not on the value of the Extended RSNA Codec field. Any codec (other than None) can be chosen for the Extended RSNA Codec field in order to generate the extended prefix; however, the codec you choose for this server record should be consistent with the value you choose for the remote server in MeetingTime on other Audio Servers in order to generate the same extended prefix on each Audio Server.

**Step 3** Repeat [Step 1](#) and [Step 2](#) for each participating server to create Other MeetingPlace Servers records for all other servers.

**Step 4** Click **Save Changes**.

Make sure that all ID Number values and Scheduling Home Server values are identical across participating servers.

**To Enable the System for RSNA**

**Note** *For Cisco Unified MeetingPlace 8112 Only:* Setting the RSNA Enabled attribute to No on a Cisco Unified MeetingPlace 8112 applies only to the server that is transferring a call (not receiving a call).

- Step 1** In the MeetingTime Configure tab, select the **Usage Parameters** view.
- Step 2** Scroll to the **SNA Settings** attributes. For the RSNA Enabled attribute, choose **Yes**.
- Step 3** Click **Save Changes**.

**To Configure Users and Groups for RSNA**

- Step 1** In the MeetingTime Configure tab, select the **User Profile** or **User Group** view.
- Step 2** For the Scheduling Home Server attribute (in the Identification attributes category), enter a number between 101 and 32767 that matches the ID Number value set in [Step 2](#) in the “[To Create Other Cisco Unified MeetingPlace Servers Records](#)” procedure on page 2-70.
- This value must be the same as the ID Number value and must not be 0 (zero). The range should start at 101, and not 1. For example, 1 to 32767 should instead be 101 to 32767.



**Caution** Confirm that the records on the home server are configured correctly. If they are incorrect, the call will not be transferred and the reservationless meeting will be held on the local server of the user.

- Step 3** Confirm that the Use Reservationless attribute (in the Restrictions attributes category) is set to either **Yes** or **Group Dflt(Yes)**.
- Step 4** Click **Save Changes**.
- Step 5** Confirm that the following attributes are set correctly:

Attribute	Value
RSNA Enabled (in the Configure tab, Usage Parameters view)	Yes For more information, see the “ <a href="#">To Enable the System for RSNA</a> ” procedure on page 2-72.
Will Accept SNA Transfers (in the Configure tab, Other MeetingPlace Servers view)	Yes For more information, see the “ <a href="#">To Create Other Cisco Unified MeetingPlace Servers Records</a> ” procedure on page 2-70.

**Configuring a Cisco Voice Gateway for RSNA Transfers**

In this section, you add dial peers to the Cisco voice gateways in your network to handle RSNA transfers.



### To Configure a Cisco Voice Gateway for RSNA Transfers

- Step 1** Telnet into the router, and enter the requested login information.
- Step 2** Enter **show running-config**.  
The current configuration of the Cisco voice gateway displays.
- Step 3** To ensure that the router sends calls from any endpoint to a particular Cisco Unified MeetingPlace H.323/SIP Gateway, enter the following configuration information.

Enter	Notes
dial-peer voice <i>[number]</i> voip	Required. <i>[number]</i> is a numeric tag that differs depending on how you have set up your voice network.
description <i>[text]</i>	Optional. <i>[text]</i> is a description of this configuration; for example, <i>Send call to US1 IPGW</i> .
destination-pattern <i>[0000]</i>	<i>[0000]</i> is the destination pattern (dialed number) in your dial plan.
session protocol sipv2	Required.
session target ipv4: <i>[000.00.0000]</i>	<i>[000.00.0000]</i> is the IP address of the Cisco Unified MeetingPlace H.323/SIP Gateway server to which calls will be sent.
dtmf-relay rtp-nte	Required. Allows DTMF relay using NTE RTP packets. DTMF tones are encoded in the NTE format and transported in the same RTP channel as the voice.
req-qos <i>[type]</i>	Optional. <i>[type]</i> is the type of requested Quality of Service (QOS); for example, <i>controlled-load</i> .
codec <i>[codec]</i>	<i>[codec]</i> is the voice-compression (codec) type; for example, <i>g711ulaw</i> .
no vad	Optional but recommended. Disables voice-activity detection.

- Step 4** To set up a dial peer to handle the SIP REFER request, enter the following configuration information:

Enter	Notes
dial-peer voice <i>[number]</i> voip	Required. <i>[number]</i> is a numeric tag that differs depending on how you have set up your voice network.
description <i>[text]</i>	Optional. <i>[text]</i> is a description of this configuration; for example, <i>SIP REFER to US1</i> .
application session	Required for IOS releases prior to 12.3.
destination-pattern <i>[0000]</i>	If you are using the Extended RSNA Prefix feature, <i>[0000]</i> must match the Extended Prefix string displayed in MeetingTime on the originating Cisco Unified MeetingPlace Audio Server, as shown in the “Other MeetingPlace Servers” configuration for the server being transferred to.  If you are not using the Extended RSNA Prefix feature, <i>[0000]</i> must match the RSNA Prefix configured on the Cisco Unified MeetingPlace H.323/SIP Gateway server.
session protocol sipv2	Required

Enter	Notes
session target ipv4:[000.00.0000]	000.00.0000 is the IP address of the Cisco Unified MeetingPlace H.323/SIP Gateway server to transfer calls to.
dtmf-relay rtp-nte	Required. Allows DTMF relay using NTE RTP packets. DTMF tones are encoded in the NTE format and transported in the same RTP channel as the voice.
req-qos [type]	Optional. [type] is the type of requested Quality of Service (QOS); for example, <i>controlled-load</i> .
codec [codec]	[codec] is the voice-compression (codec) type; for example, <i>g711ulaw</i> .
no vad	Optional but recommended. Disables voice-activity detection.

**Step 5** Enter **exit**, then enter **exit** again.

**Step 6** Enter **write memory** to apply the configuration settings.

## Adding Extended Prefixes to an Existing RSNA Configuration



### Note

The instructions in this section assume the system is already set up to use RSNA. If it is not, see the [“Setting Up RSNA for the First Time”](#) section on page 2-70 instead. The instructions there include options for using extended prefixes.

Do the two procedures in this section in the order listed to use extended prefixes.

In the following procedure, on each Audio Server that participates in RSNA transfers, you configure the Extended RSNA Codec in MeetingTime for all other participating servers.

### To Configure the Extended RSNA Codec

- 
- Step 1** In the MeetingTime Configure tab, select **Other MeetingPlace Servers**.
  - Step 2** Click **Query**.
  - Step 3** Click the forward arrow to select a server that will participate in RSNA transfers.
  - Step 4** For the Extended RSNA Codec field, select a codec to be used when calls are transferred to this server.
  - Step 5** Click **Save Changes**.
  - Step 6** Note the value returned in the Extended Prefix field. You will use this value when configuring a dial peer on the voice gateway.
  - Step 7** Repeat [Step 3](#) through [Step 6](#) for all remaining Audio Servers that participate in RSNA transfers.
  - Step 8** Repeat [Step 1](#) through [Step 7](#) on each remaining Audio Server that participates in RSNA transfers.
- 

In the following procedure, for each extended prefix generated in the preceding procedure, you configure the Cisco voice gateways with dial peers to transfer calls using the proper codec.

### To Configure the Voice Gateway with a Dial Peer for the Extended RSNA Prefix

- Step 1** Telnet into the router, and enter the requested login information.
- Step 2** Enter **show running-config**.  
The current configuration of the Cisco voice gateway displays.
- Step 3** To set up a dial peer to handle the SIP REFER request, enter the following configuration information:

Enter	Notes
dial-peer voice <i>[number]</i> voip	Required. <i>[number]</i> is a numeric tag that differs depending on how you have set up your voice network.
description <i>[text]</i>	Optional. <i>[text]</i> is a description of this configuration; for example, <i>SIP REFER to US1</i> .
destination-pattern <i>[0000]</i>	<i>[0000]</i> must match the extended prefix string displayed in MeetingTime in <a href="#">Step 6</a> of the “ <a href="#">To Configure the Extended RSNA Codec</a> ” procedure on page 2-74.
session protocol sipv2	Required.
session target ipv4: <i>[000.00.0000]</i>	<i>000.00.0000</i> is the IP address of the Cisco Unified MeetingPlace H.323/SIP Gateway server to transfer calls to.
dtmf-relay rtp-nte	Required. Allows DTMF relay using NTE RTP packets. DTMF tones are encoded in the NTE format and transported in the same RTP channel as the voice.
req-qos <i>[type]</i>	Optional. <i>[type]</i> is the type of requested Quality of Service (QOS); for example, controlled-load.
codec <i>[codec]</i>	<i>[codec]</i> is the voice-compression (codec) type; for example, g711ulaw.
no vad	Optional but recommended. Disables voice activity detection.

- Step 4** Repeat [Step 3](#) for each unique extended prefix string.
- Step 5** Enter **exit**, then enter **exit** again.
- Step 6** Enter **write memory** to apply the configuration settings.

## Troubleshooting RSNA

See the following sections:

- [Resolving Recorded User Name Problems, page 2-75](#)
- [Viewing Alarm Codes for RSNA, page 2-76](#)

### Resolving Recorded User Name Problems

A user may have a different recorded name on each server. The first time that logged-in users attend a meeting hosted on each remote server, they are asked to record their name.

If users do not like their user name on some server, have them note the meeting with the undesirable recording, and tell their system administrator. The system administrator should then find that meeting, determine which server is the problem, and give users the phone number to call to access that server. Users can then enter their profile on that server and rerecord the user name.

## Viewing Alarm Codes for RSNA

Table 2-37 describes minor alarms that may be generated by the RSNA feature. These descriptions may help system administrators to troubleshoot problems.

**Table 2-37** RSNA Alarm Codes

Alarm	Description
0x30130 (196912) "RSNA transfer loop? UserID=%d MtgOwner=%d"	(Minor alarm) RSNA transfer loop. Indicates an inter-server configuration conflict or user database synchronization problem.
0x30134 (196916) "RSNA userunknown, user=%08x%08x%08x%08x"	(Minor alarm) User identified in an RSNA transfer is unknown. Indicates a user database inter-server synchronization problem.
0x30137 (196919) "RSNA: Password mismatch, user=%08x%08x%08x%08x"	(Minor alarm) Password provided in the transfer information block does not match the local user's password. Indicates an inter-server database synchronization problem.
0x30138 (196920) "RSNA: Info block verification failed, ex=%#x"	(Minor alarm) Corrupted information block received from the transferring server. Indicates the information was corrupted in transmission, a software version mismatch, clock skew, or an attempt at forgery. Look up the secondary exception code (ex=) for more specifics.

## Scheduling Reservationless Meetings with Web Conferencing

When reservationless meetings are used with Cisco Unified MeetingPlace Web Conferencing by using releases earlier than Release 3.0, web conferencing can be enabled after the voice conference has been activated. When used with Release 3.0 or later, reservationless meetings can be started either from the Web or the phone.

Exceptions to this behavior are with immediate meetings or scheduled meetings that begin now. If a meeting ID is not selected and a user clicks the Immediate Meeting button in the Cisco Unified MeetingPlace Web Conferencing home page (or schedules a meeting with a start time of now or earlier), the system creates a reservationless meeting with the user's profile number. On the second try, the user receives an error message because a reservationless meeting already exists. This also happens when scheduling from Cisco Unified MeetingPlace for Outlook and MeetingTime.

When reservationless meeting participants join the web conference, all participants—including those in the waiting room—may share. However, users in the waiting room cannot use the in-session features.

## System Rules

As you work with reservationless meetings, remember the following system rules:

- The default parameters for reservationless meetings are the parameters set for immediate meetings. For example, if the default meeting length for immediate meetings is 30 minutes, reservationless meetings wait 30 minutes for initiation before ending. If the meeting has not started within 30 minutes of the first participant entering the waiting room, or prompts all participants: "The meeting organizer has not arrived. Please try again later."

- The web conferencing component of a reservationless meeting ends when the voice conference ends.
- After users log into the system, they remain logged in. If they exit to the top menu, they do not have to enter their profile and password again. If they join another meeting, they join with their recorded profile name.
- Profile users may end any reservationless meeting they join by pressing **#812**. Profile users may also end scheduled meetings.
- Users can leave a meeting and return to the main menu by pressing **#9**. This command works when reservationless meetings is turned on or off.
- The Reservationless Meeting feature is available for U.S. English, U.K. English, French (Canada), French (France), Japanese, German, Portuguese (Brazil), and Spanish (Americas) languages.

## About Cisco Unified MeetingPlace Language System Option

The Cisco Unified MeetingPlace Language System Option offers support for up to four languages simultaneously. Users can hear prompts in an available configured languages. When no language has been selected, the system defaults to U.S. English.

Each system contains only the prompts for the languages installed and configured.

Languages can be selected at the meeting, user profile, and port group level. These language selections determine the language that Cisco Unified MeetingPlace uses at any time. For example, prompts played to an entire meeting are played in the meeting language, while prompts played to individuals are played in the language specified by the user's profile or the language selected while in the system.

## Enabling the Cisco Unified MeetingPlace Language Option Key

An option key is an alphanumeric string, similar to a serial number, that needs to be entered into the Cisco Unified MeetingPlace database to activate a system option.

### To Enable the Cisco Unified MeetingPlace Language Option Key

- 
- Step 1** Locate the option key on the license document.
  - Step 2** In the MeetingTime Configure tab, for Views, select the **System Options** topic, and click **Query**.
  - Step 3** Click the **>** button to locate the option for Languages.
  - Step 4** For the Number of Licenses attribute, enter the number of languages for your Cisco Unified MeetingPlace system.  
  
The number of licenses must match the number of languages that correspond to your Cisco Unified MeetingPlace language option key.
  - Step 5** For the Option Key attribute, enter the option key number.
  - Step 6** Click **Save Changes**.
-

## Choosing Languages

This section describes the prompts a user hears when more than one language is installed and configured. A hierarchy determines which language the system uses. When a language is selected at one of the following levels, users hear prompts in the selected language.

1. Meeting
2. Profile
3. Port group
4. System default (always U.S. English)

Language selections at a lower level override language selections at a higher level.

## Multilingual System Rules

The following is a list of guidelines to keep in mind when you configure Cisco Unified MeetingPlace for additional languages:

- If the Port Group parameter is not configured for a language, Cisco Unified MeetingPlace plays the system default language (U.S. English).
- After guest users select a language, they hear prompts in this language until they enter the meeting.
- The profile language of a user plays after the user logs into the system.
- After a user enters a meeting, individual prompts are played in the profile language of the user, if the user has logged into the system or in the language that the user selected while in the system.
- The meeting language plays after the user enters the meeting.
- The meeting language defaults to the profile language of the scheduler, unless another language is specified through MeetingTime.
- Pressing the star key (\*) returns you to the previous menu.
- For multiple languages, the language selection order is determined by the order in which language CD-ROMs have been loaded.

For multiple language systems with ports configured to a language, prompts continue in the port language until users enter the meeting. For an example, see the tables in the [“Setting Meeting Language Prompts”](#) section on page 2-78.

## Setting Meeting Language Prompts

The tables in the following sections show the prompts and language for various language configurations.

Remember the following information:

- To accommodate guest users, each installed language is played at the “Welcome to MeetingPlace” menu. This allows a guest who does not understand the system default or port configured language to navigate the system.
- During a meeting, prompts played to all participants are played with the meeting language setting. For example: “By request of <user>, this meeting is being recorded.”
- After entering a meeting ID, prompts played to individuals use the language you selected when you started the phone call or when you logged into your profile. Examples of such personal prompts: “Muted” and “There are five people in the meeting.”

- To hear “Welcome to MeetingPlace” in one of the configured languages, port groups must be configured in the individual language.
- Prompts used when outdialing to a meeting participant are determined by the individual language setting in the guest profile.
- For multilingual systems, the order in which prompts are played is determined by the order in which the language CDs have been loaded.

## One-Language System

Table 2-38 shows the standard voice prompts for a one-language system.

**Table 2-38** *One-Language System Prompts*

Prompt	Language
“Welcome to MeetingPlace.”	U.S. English
“To attend a meeting, press 1.”	U.S. English
“To access your profile, press 2.”	U.S. English
“To review MeetingNotes, press 3.”	U.S. English
“To hear MeetingPlace overview, press 9.”	U.S. English
“To reach assistance, press 0.”	U.S. English

## Four-Language System, Port Not Configured

Table 2-39 shows the voice prompts for a four-language system, with the port not configured (assuming that users press 5 to select Japanese when prompted).

**Table 2-39** *Four-Language System Prompts*

Prompt	Language
“Welcome to MeetingPlace.”	U.S. English
“To select English, press 1.”	U.S. English
“To select English, press 4.”	U.K. English
“To select Japanese, press 5.”	Japanese
“To select French, press 6.”	Canadian French
“To attend a meeting, press 1.”	Japanese
“To access your profile, press 2.”	Japanese
“To access MeetingNotes, press 3.”	Japanese
“To hear MeetingPlace overview, press 9.”	Japanese
“To reach assistance, press 0.”	Japanese

## Two-Language System, Port Configured for Japanese

Table 2-40 shows the voice prompts for a two-language system, with the port configured for Japanese.

**Table 2-40 Two-Language System Prompts**

<b>Prompt</b>	<b>Language</b>
“Welcome to MeetingPlace.”	Japanese
“To attend a meeting, press 1.”	Japanese
“To access your profile, press 2.”	Japanese
“To access MeetingNotes, press 3.”	Japanese
“To select English, press 4.”	U.S. English
“To hear a MeetingPlace overview, press 9.”	Japanese
“To reach assistance, press 0.”	Japanese